



Bug Bounty Walkthrough

How I did my first bug bounty in Twitter

CHETHINE LIYANARACHCHI

Table of Contents

1. Acknowledgement	4
2. Assessment Objectives	5
3. Introduction	6
4. Overview of the Twitter	6
5. In-scope domains	6
6. Out-of-scope domains	7
7. Risk Level Information	9
8. Vulnerability Overview	10
9. Information Gathering	11
1) Subdomain Enumeration	
• Sublist3r	17
• Recon -ng	28
• Crt.sh	31
2) Find Open Ports and Running Devices on The Network	
• Nmap	32
3) Public Device Enumeration	
• Shodan.io	40
4) Check the Status of Firewall Protection in Target Domains	
• Wafw00f	42
10. Vulnerability Scanning Tool	
• Nikto	48
• Netsparker	51
• OWASP ZAP	52
• Burp Suite Professional	53
11. Vulnerability Scanning	
• Target Domain: https://twitter.com	55
• Target Domain: https://vine.co	65
• Target Domain: https://periscope.tv	75
• Target Domain: https://pscp.tv	79

• Target Domain: https://gnip.com	84
• Target Domain: https://mopub.com	88
12. Overview Of the Vulnerabilities	92
13. Conclusion	93
14. Reference	94

Acknowledgement

The lecturer in charge of the Web Security module, Dr. Lakmal Rupasinghe, and Ms. Chethana Liyanapathirana, who guided us through the process of completing this assignment, are to be thanked. They gave us with valuable counsel and were there for us at difficult times. The encouragement and assistance they provided us were extremely beneficial in ensuring the successful completion of the project.

In addition, I would like to express my gratitude to Ms. Chathu Udagedara and Ms. Menaka Moonamaldeniya, who assisted us in completing this task effectively by providing us with practical knowledge.

Second, I'd like to express my gratitude to my parents and friends, who were invaluable in assisting me in completing my work in the allotted time.

Assessment Objectives

This assignment was completed for the Web Security module in the second year, second semester of the second year. I was given the task of conducting a security evaluation of the website <http://twitter.com>. The primary goal of this assignment is to identify potential security vulnerabilities in the target domain that could result in a breach of security, and to categorize those vulnerabilities according to the level of risk they pose.

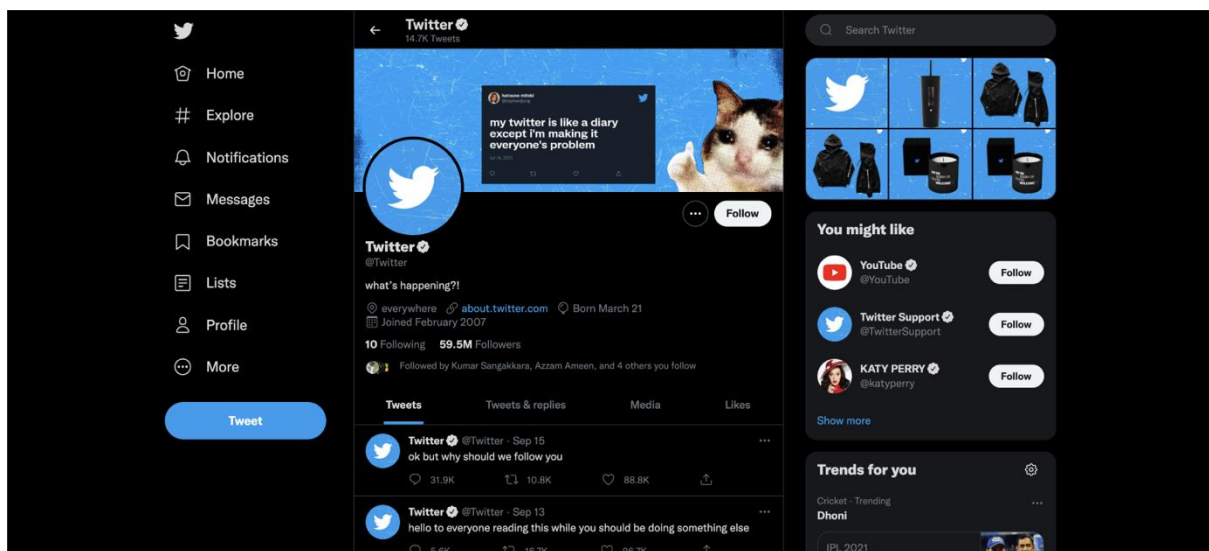
Introduction

In my hunt for bug bounty programs on Hacker One, I came across a bug bounty program for the social media platform Twitter. I have selected this as my assignment in second year second semester web security module.

hackerone Link: <https://hackerone.com/twitter?type=team>

Overview of the Twitter.

Twitter is one of the most widely used social media platforms, and it is mostly used for microblogging and short messages. In 2006, Jack Dorsey, Noah Glass, Biz Stone, and Evan Williams founded the social networking site Twitter. Mr. Jack Dorsey serves as the company's chief executive officer at the moment.










The primary goal of this project is to detect vulnerabilities in the Twitter platform and identify the relevant risks to those vulnerabilities. The auditing scope will be limited for domains that are published by twitter in hackerone.




In scope domains

- 1) *.twitter.com
- 2) *.vine.co
- 3) *.periscope.tv
- 4) *.pscp.tv
- 5) *.twimg.com
- 6) gnip.com
- 7) mopub.com
- 8) niche.co

9) snappytv.com

10) twitterflightschool.com

Domain	*.twitter.com	 Critical
Domain	*.vine.co	 Critical
Domain	*.periscope.tv	 Critical
Domain	*.pscp.tv	 Critical
Domain	*.twimg.com	 Critical
Domain	gnip.com	 Critical
Domain	mopub.com	 Critical

Domain	niche.co	 Critical
Domain	snappytv.com	 Critical
Domain	twitterflightschool.com	 Medium

Out Of Scope Domains

1) Status.twitter.com

Out Of Scope Vulnerabilities

- Physical attacks on a user's device
- Physical attacks on Twitter's property or data centers
- Forms with missing CSRF tokens (we require evidence of actual CSRF vulnerability)
- Password and account recovery policies, such as expiration of reset links or password complexity
- Invalid or missing SPF (Sender Policy Framework) data

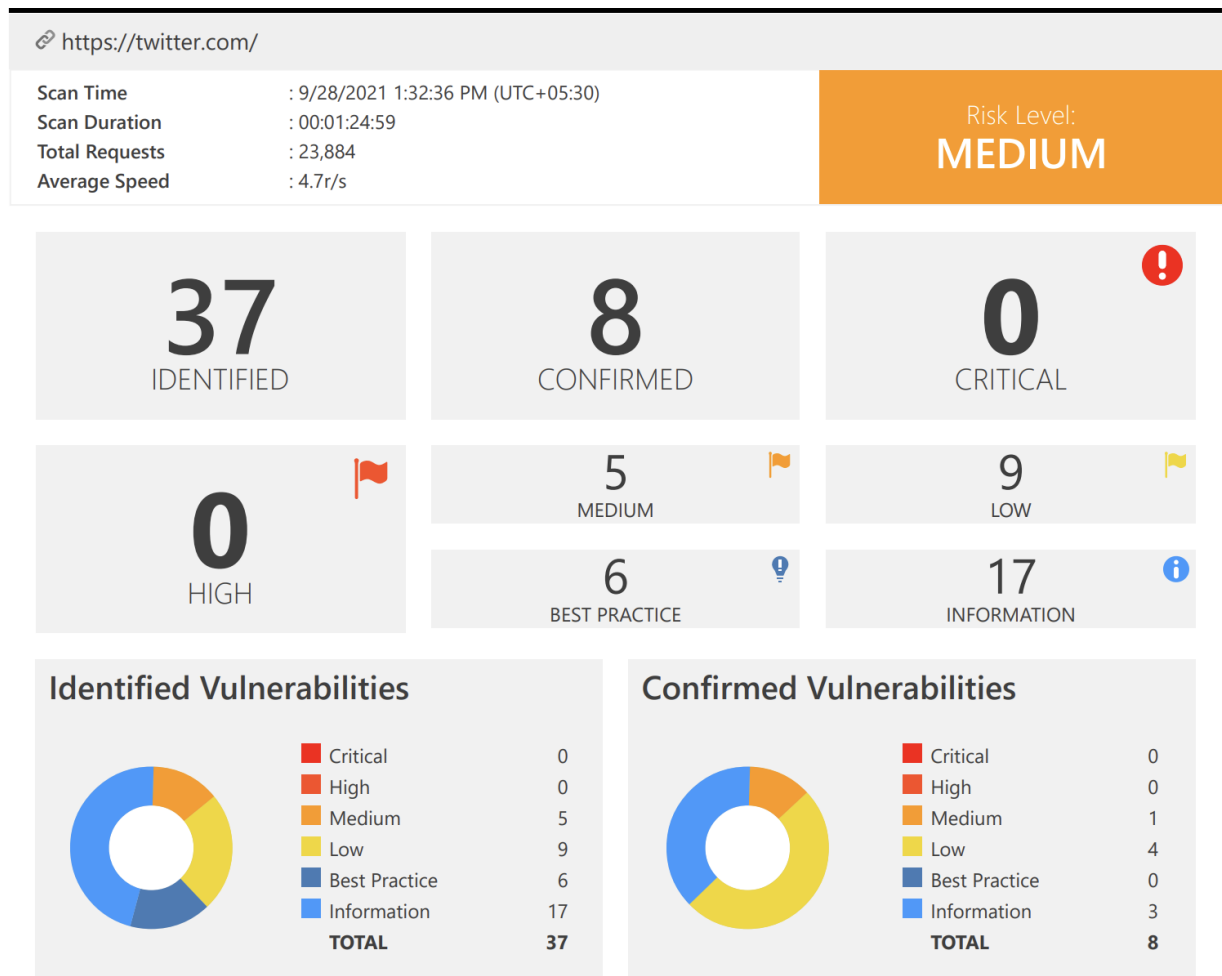
- Content spoofing / text injection
- Issues with applications or protocols outside of Twitter's control
- Spam reports
- Bypassing URL malware detection
- Issues with no clearly recognized security impact, such as clickjacking on a static website, missing security headers, or detailed error messages
- Social engineering of Twitter employees or contractors
- Network or application layer issues that cause a Denial of Service (DoS) to Twitter's servers.
- Broken URLs from Twitter blog posts, press releases, or support articles that lead to unclaimed Twitter Handles or a site where the controlled contents cannot be downloaded to the victim's disk.
- Issues with unlocking client-side capabilities in Twitter programs that have been changed, rooted, or jailbroken.

Risk Level Information

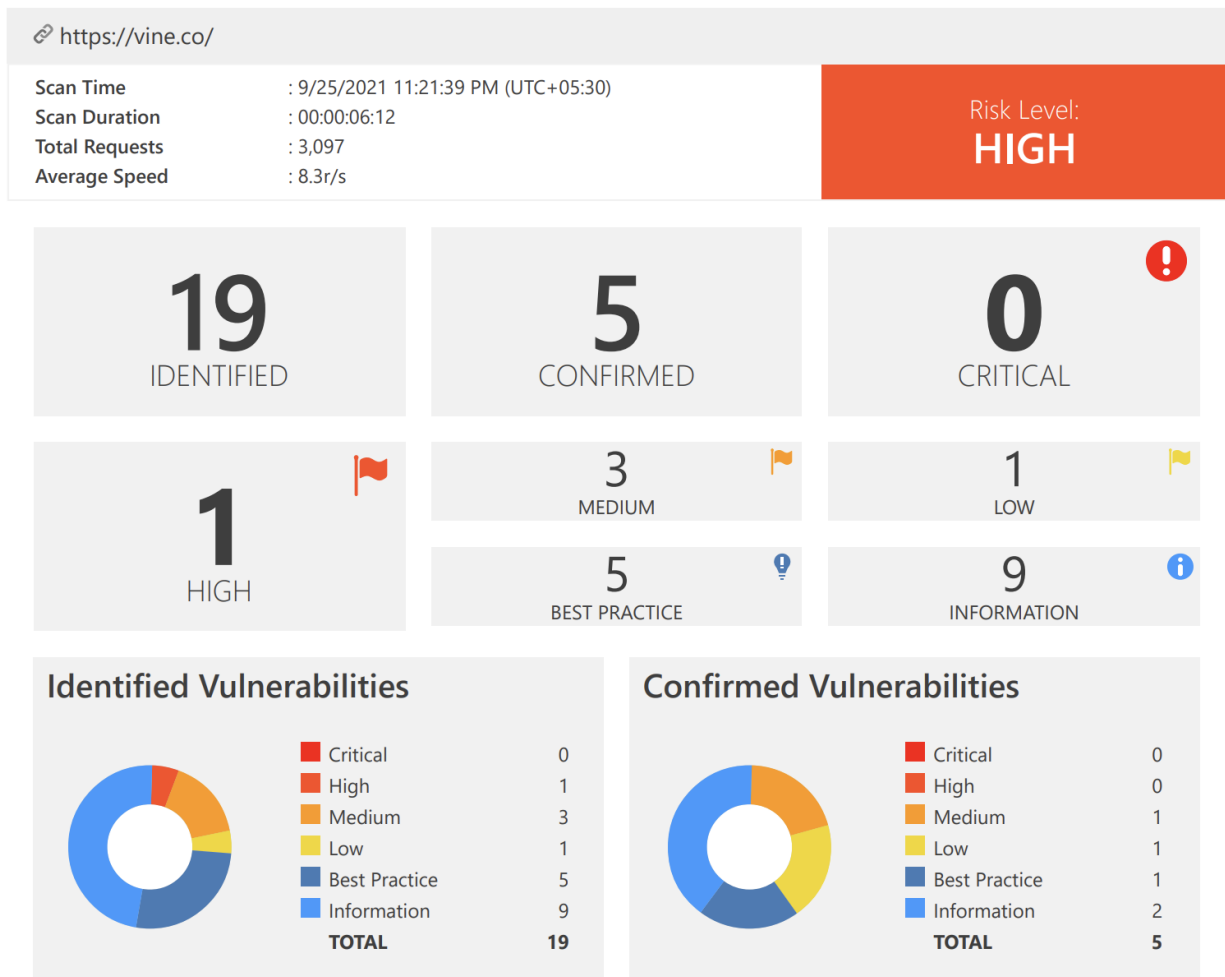
High	This indicates that the highest level of risk is associated with a specific vulnerability. When a vulnerability is classified as high-risk, there is a high likelihood that an attacker will attempt to exploit it. The attacker's actions may result in the modification or destruction of data from the web application.
Medium	This indicates that a specific vulnerability is associated with a medium risk level. By taking advantage of these types of vulnerabilities, an attacker can obtain access to sensitive information at a low level.
Low	This indicates that a given vulnerability is associated with a low risk level. If an attacker succeeds in exploiting a low-level vulnerability, the resulting impact on the web application will be minimal. The attacker may be able to obtain some insight into the web application.
Informative	The risk level associated with these types of vulnerabilities is quite low.

Vulnerability Overview

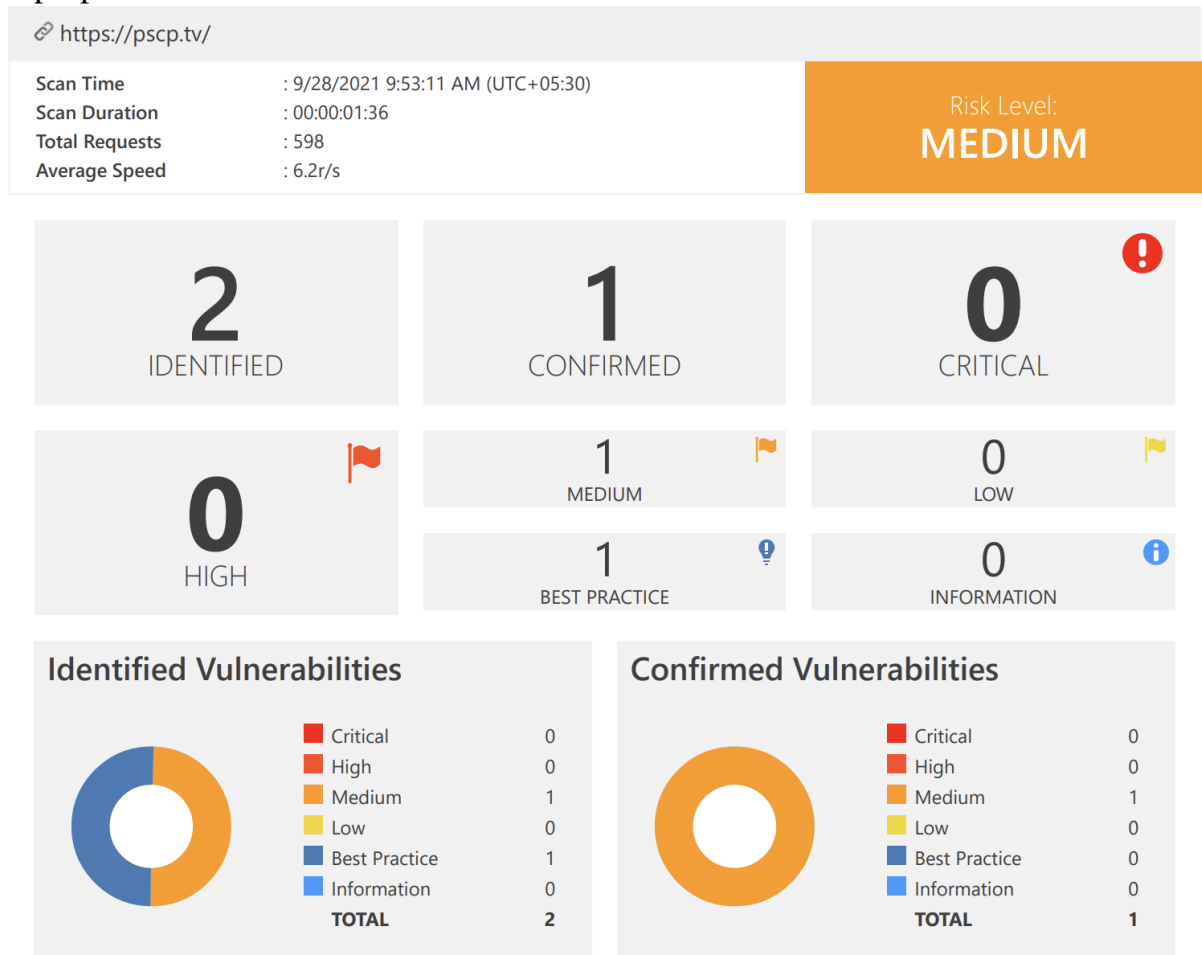
1. *.twitter.com



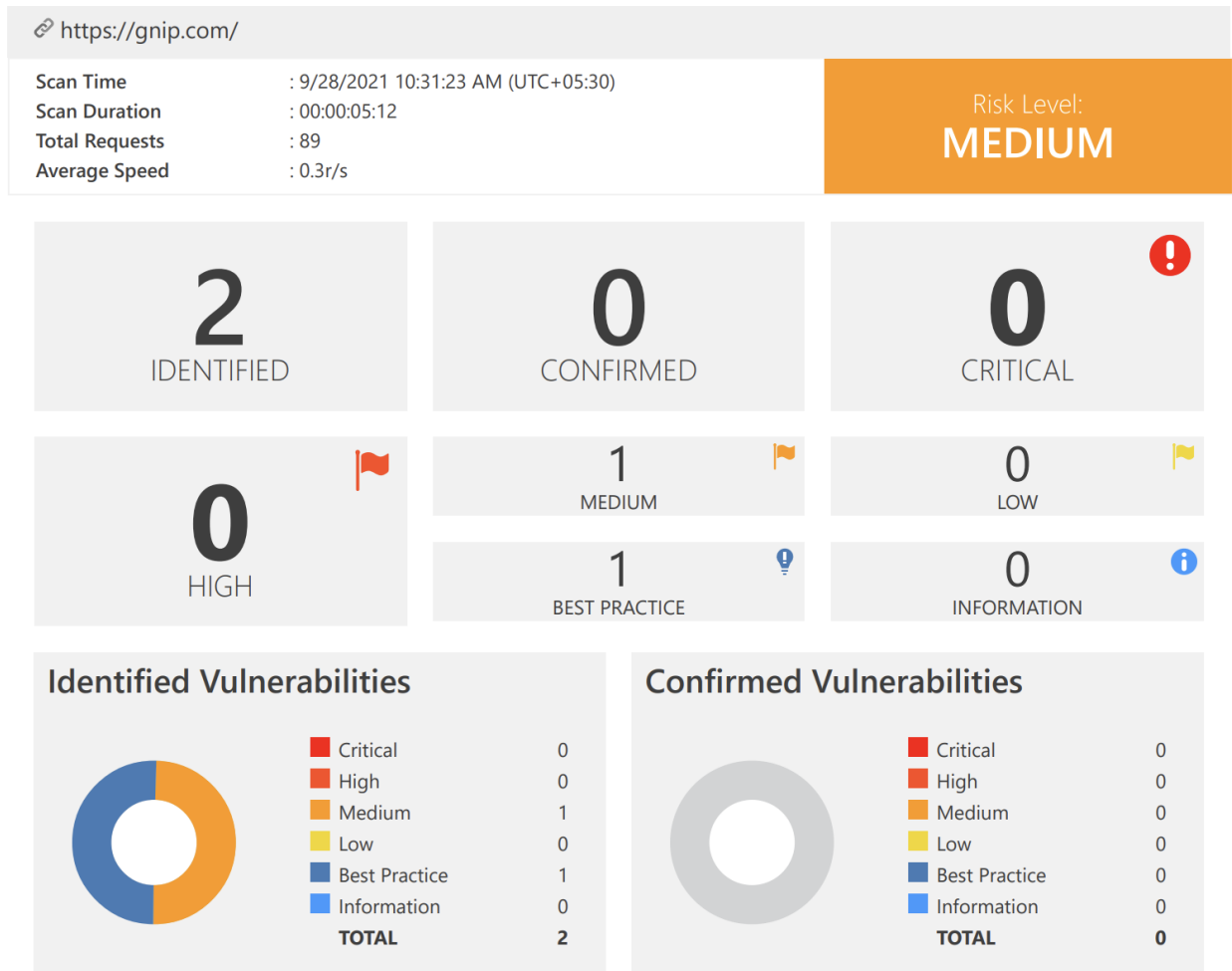
2. *.vine.co



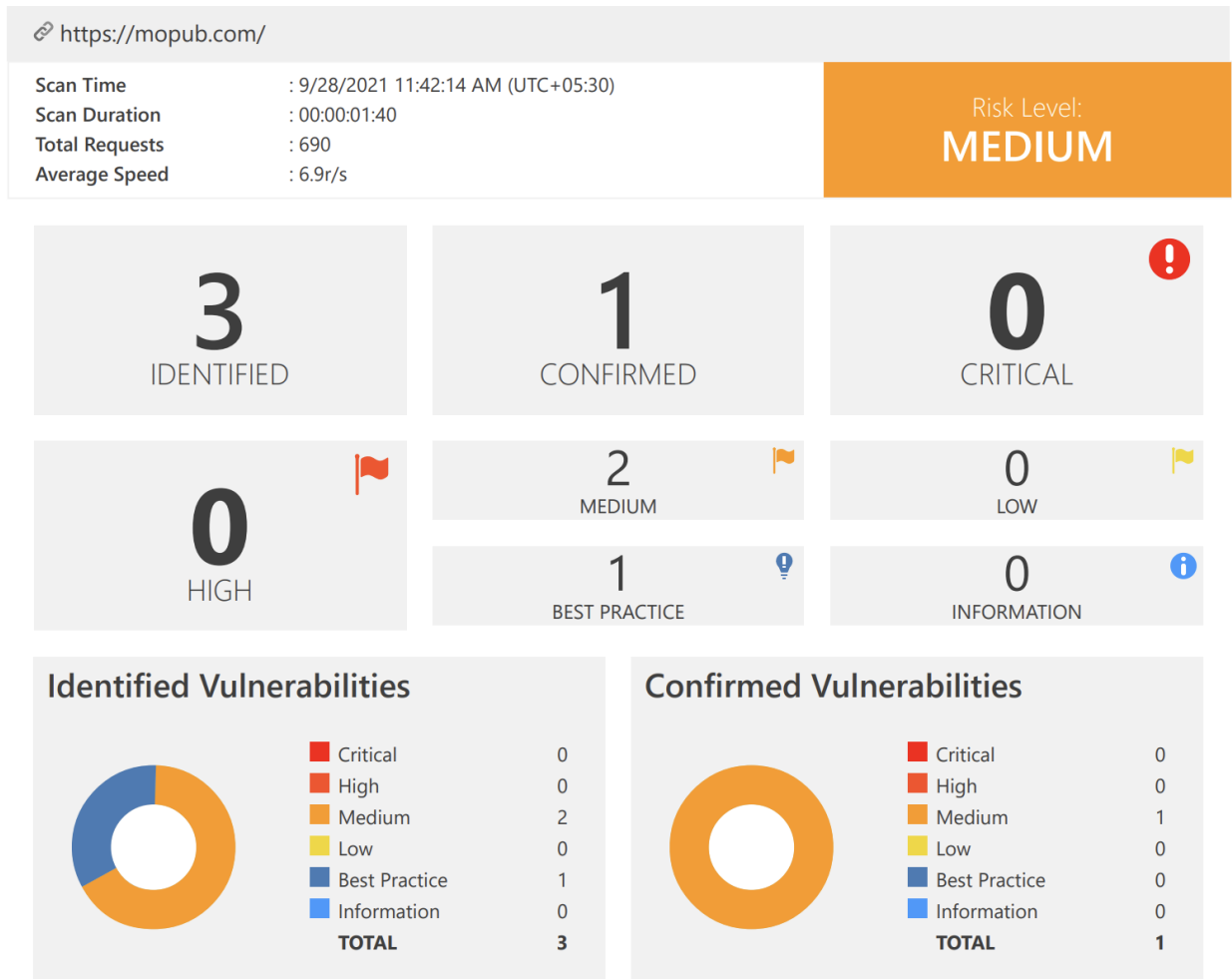
3. *.pscp.tv



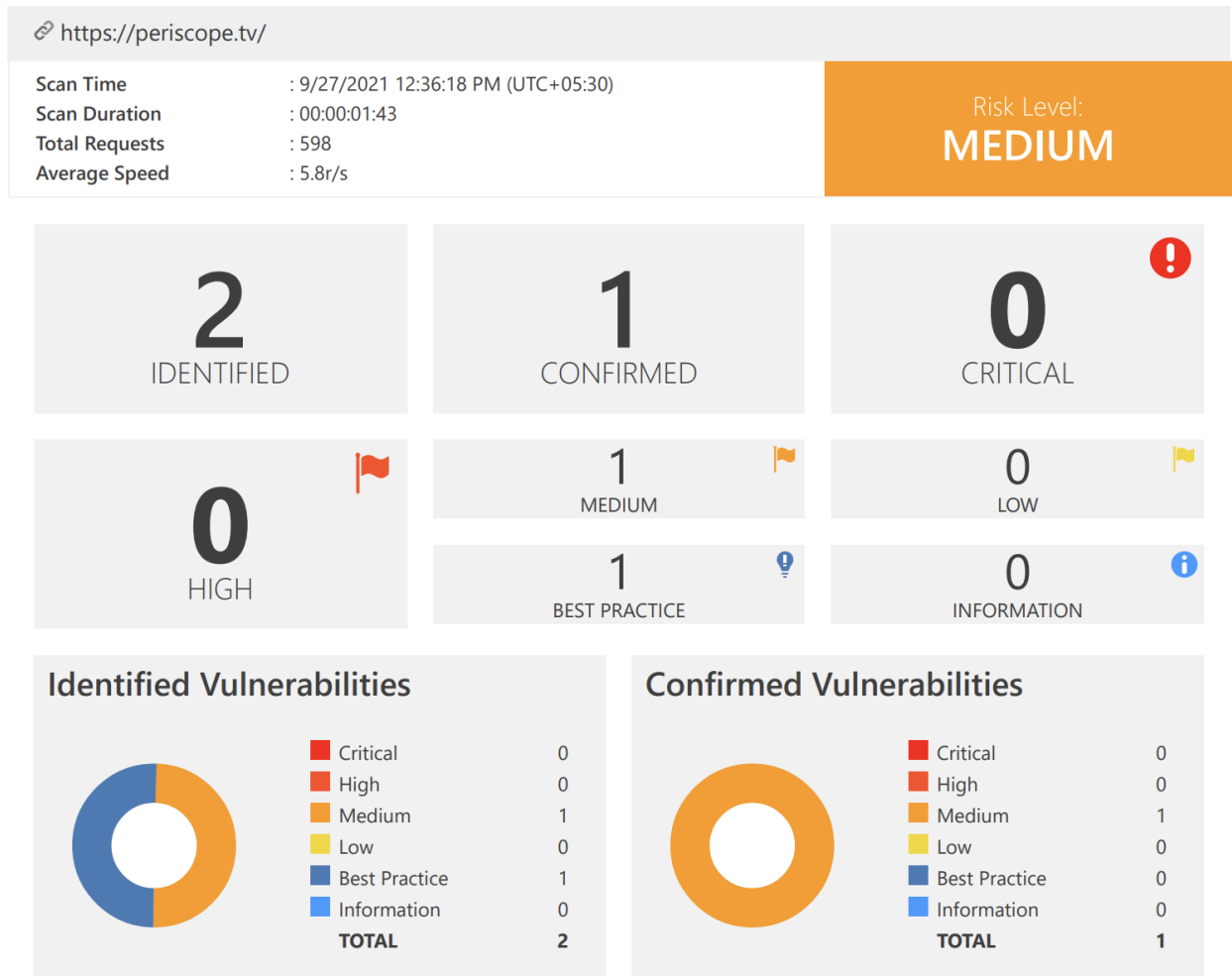
4. gnip.com



5. mopub.com



6. periscope.tv



Information Gathering

Information gathering is one of the most important stage in bug bounty process. Pen testers are gathered all the publicly available information about the website. This Information gathering process is also known as reconnaissance phrase. Hacker one and all other bug bounty platforms publish all the in-scope domains and out scope domains. Pen testers mainly focused about in-scope websites and tend to collect as much as possible information about the relevant company. Information gathering can be done in two ways.

1. Passive: This refers to collect publicly available information and other data without contacting the target web site or application
2. Active: This refers to collect information by contacting target web application or website.

For this assignment, I will use passive information gathering technique.

Subdomain Enumeration

Subdomain Enumeration is the process of finding valid and resolvable subdomains for one or more domains. For subdomain enumeration process I have used several tools.

1. Sublist3r
2. Recon-ng
3. Crt.sh

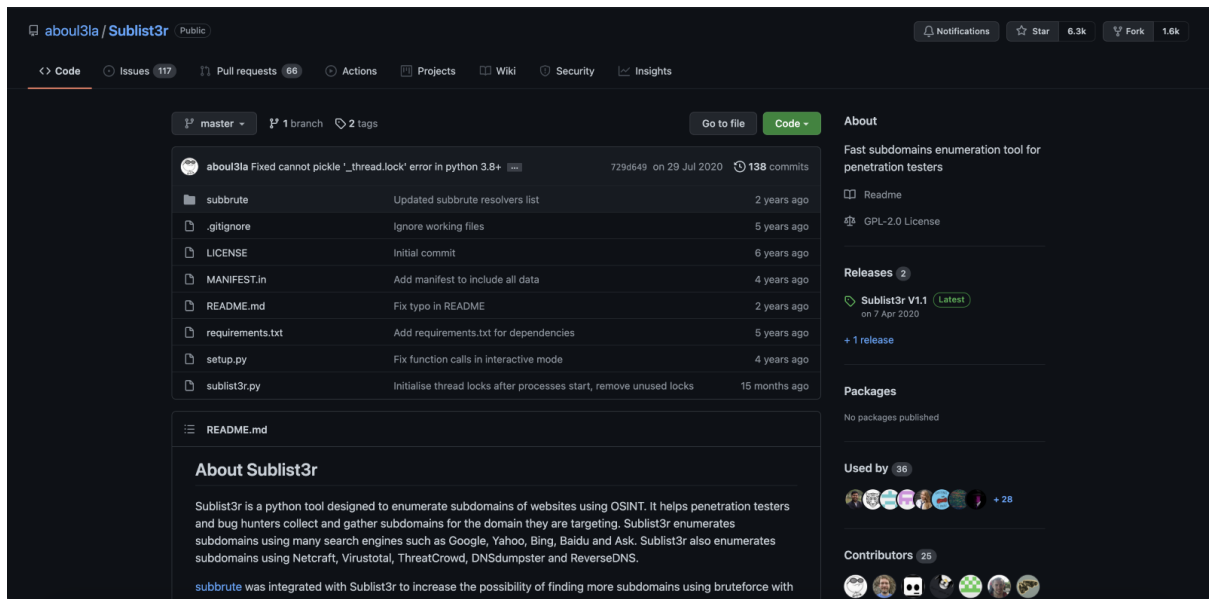
Sublist3r

This tool is created using python and most of the pen testers and bug bounty hunter use to collect subdomain for the domain they are targeting.

First, I have installed sublist3r to my virtual machine.

To install this, I have visited to below GitHub page and then I have cloned it to my machine.

GitHub Link: <https://github.com/aboul31a/Sublist3r>



```
[x]-[chethine@chethine-vmwarevirtualplatform]-[~]
$git clone https://www.github.com/about3la/Sublist3r.git
```

Then after cloning process, Next, I installed pip to my virtual machine.

```
[chethine@chethine-vmwarevirtualplatform]-[~/Sublist3r]
$sudo pip install -r requirements.txt
```

As mentioned before sublist3r is python tool. In that case, install python to the machine as well.

```
[chethine@chethine-vmwarevirtualplatform]-[~/Sublist3r]
$sudo apt-get install -y python3-pip
```

Then I have entered python sublist3r.py -h to view the help options.

```
[x]-[chethine@chethine-vmwarevirtualplatform]-[~/Sublist3r]
$python sublist3r.py -h
```

After that, to check this tool I have entered python sublist3r.py -d gmail.com to get subdomain of entered domain.

```
[chethine@chethine-vmwarevirtualplatform]~[/Sublist3r]  
$python sublist3r.py -d gmail.com  
  
      _--_      _--_      _--_      _--_      _--_  
    / ____| |__ | |__ | |__ | |__ | |__ | |__ | |__ |  
   \___ \| | | | | | | | | | | | | | | | | | | | | |  
      ___) | | | | | | | | | | | | | | | | | | | | |  
     [____/ \__,_| |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
```

Coded By Ahmed Aboul-Ela - @aboul3la

```
[~] Enumerating subdomains now for gmail.com  
[~] Searching now in Baidu..  
[~] Searching now in Yahoo..  
[~] Searching now in Google..  
[~] Searching now in Bing..  
[~] Searching now in Ask..  
[~] Searching now in Netcraft..  
[~] Searching now in DNSdumpster..  
[~] Searching now in Virustotal..  
[~] Searching now in ThreatCrowd..  
[~] Searching now in SSL Certificates..  
[~] Searching now in PassiveDNS..
```

Using Sublist3r to find subdomains of twitter.com

```
[*]-[chuti subhost-vulnerable-platform]-[~/Sublist3r]
[*]$python sublist3r.py -d twitter.com

          SUBDOMAINS
          SUBDOMAINS

# Coded By Ahmed About-Ela - @aboul3la

[*] Enumerating subdomains now for twitter.com
[*] Searching now in Baldu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[*] Error: Virustotal probably now is blocking our requests
[*] Total Unique Subdomains Found: 961

http---twitter.com
ww1.1.http---twitter.com
ww1.10.http---twitter.com
ww1.10.http---twitter.com
ww1.11.http---twitter.com
ww1.11.http---twitter.com
ww1.12.http---twitter.com
ww1.14.http---twitter.com
ww1.15.http---twitter.com
ww1.16.http---twitter.com
ww1.17.http---twitter.com
ww1.18.http---twitter.com
ww1.19.http---twitter.com
ww1.2009.http---twitter.com
ww1.2010.http---twitter.com
ww1.2011.http---twitter.com
ww1.2013.http---twitter.com
ww1.2014.http---twitter.com
ww1.2016.http---twitter.com
ww1.2017.http---twitter.com
ww1.2019.http---twitter.com
```

Total of 961 unique subdomains has been found.

```

api-41-0-0-41-6-7.twitter.com
api-41-1-1-41-0-0.twitter.com
api-41-1-1-41-4-2.twitter.com
api-41-4-1-41-5-1.twitter.com
api-41-4-2-41-0-0.twitter.com
api-41-4-2-41-5-2.twitter.com
api-41-4-2-41-6-5.twitter.com
api-41-4-2-41-6-6.twitter.com
api-41-4-2-41-6-7.twitter.com
api-41-4-3-41-4-2.twitter.com
api-41-4-3-41-5-2.twitter.com
api-41-4-3-41-6-3.twitter.com
api-41-4-3-41-6-5.twitter.com
api-41-4-3-41-6-6.twitter.com
api-41-5-1-41-5-2.twitter.com
api-41-5-1-41-6-4.twitter.com
api-41-5-1-41-6-5.twitter.com
api-41-5-1-41-6-7.twitter.com
api-41-5-2-41-0-0.twitter.com
api-41-5-2-41-6-1.twitter.com
api-41-5-2-41-6-2.twitter.com
api-41-5-2-41-6-7.twitter.com
api-41-6-0-41-0-0.twitter.com
api-41-6-0-41-4-1.twitter.com
api-41-6-0-41-4-3.twitter.com
api-41-6-0-41-6-4.twitter.com
api-41-6-0-41-6-5.twitter.com
api-42-0-0.twitter.com
api-43-0-0.twitter.com
api-44-0-0.twitter.com
api-45-0-0.twitter.com
api-46-0-0.twitter.com
api-47-0-0.twitter.com
api-stream.twitter.com
api-backup.twitter.com
api2.twitter.com
api3-backup.twitter.com
api4.twitter.com
apiwiki.twitter.com
apple.twitter.com
arsenal.twitter.com
arthouse.twitter.com
de-clx.ase.twitter.com
askobama.twitter.com
assets9.twitter.com

```

```

marketing-staging.twitter.com
measure1.twitter.com
measure2.twitter.com
measure3.twitter.com
media.twitter.com
media-staging.twitter.com
mla-api.twitter.com
audubon.mla1.twitter.com
puppetserver.mla1.twitter.com
puppetserver3.mla1.twitter.com
audubon.mli1.twitter.com
alb.twitter.com
mafighting.twitter.com
mobile.twitter.com
www.mobile.twitter.com
mobile-staging1.twitter.com
mobile-staging2.twitter.com
mobile-staging3.twitter.com
mobile-staging4.twitter.com
mobile-staging5.twitter.com
mobilefeedback.twitter.com
monsterstrike.twitter.com
ap-internal.twitter.com
ms1.twitter.com
ms2.twitter.com
ms3.twitter.com
ms4.twitter.com
ms5.twitter.com
music.twitter.com
music-partner.twitter.com
mx1.twitter.com
mx2.twitter.com
mx3.twitter.com
mx4.twitter.com
nabc.twitter.com
nationalgeographic.twitter.com
neptune.twitter.com
atl-vpn1-eu.net.twitter.com
atl-vpn2-eu.net.twitter.com
nauth-lab-aui.net.twitter.com
smf1-mal-eu1.net.twitter.com
smf1-mal-eu2.net.twitter.com
saic-vpn1-eu.net.twitter.com
saic-vpn2-eu.net.twitter.com
vpn-lab-aui.net.twitter.com
netnod-lx-ge-a-gth-1500.twitter.com

```

Using Sublist3r to find subdomains of vine.co

```

[chen@kali-vmware:~/toolsplatform]$ cd ~/Sublist3r
$ python sublist3r.py -d vine.co

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for vine.co
[-] Searching now in Baldu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in Threatcrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 37
shop.thevine.co
www.shop.thevine.co
www.vine.co
admin.vine.co
archive.vine.co
atla.vine.co
blog.vine.co
brand.vine.co
www.brand.vine.co
cdn.vine.co
mtc.cdn.vine.co
mtc-0.cdn.vine.co
v.cdn.vine.co
wildcard.cdn.vine.co
dev-svc.vine.co
devel.vine.co
engineering.vine.co
get.vine.co
grape.vine.co
help.vine.co
ar-help.vine.co

```

```

wildcard.cdn.vine.co
dev-svc.vine.co
level.vine.co
engineering.vine.co
get.vine.co
grape.vine.co
help.vine.co
ar.help.vine.co
es.help.vine.co
fr.help.vine.co
ja.help.vine.co
pt.help.vine.co
tk.help.vine.co
meda.vine.co
media.vine.co
music.vine.co
now.vine.co
platform.vine.co
prd.vine.co
ops02.prd.vine.co
svc.vine.co
pypicloud.svc.vine.co
videobeta.vine.co
www.videobeta.vine.co

```

Using Sublist3r to find subdomains of periscope.tv

```

[chethi@chethi-vmwarevirtualplatform] ~/Sublist3r
$ python sublist3r.py -d periscope.tv

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for periscope.tv
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSDumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 180
www.periscope.tv
admin.periscope.tv
api.periscope.tv
assets.periscope.tv
canary-api.periscope.tv
canary-channels.periscope.tv
canary-guest.periscope.tv
canary-notification-service.periscope.tv
canary-payman.periscope.tv
canary-text-classification.periscope.tv
canary-transcode-proxy-us-east-1.periscope.tv
canary-transcode-us-east-1.periscope.tv
canary-video-us-east-1.periscope.tv
canary-web.periscope.tv
channels.periscope.tv
chatman-ap-northeast-1.periscope.tv
chatman-ap-southeast-2.periscope.tv
chatman-ap-central-1.periscope.tv
chatman-eu-west-1.periscope.tv
chatman-replay-us-east-1.periscope.tv
chatman-replay-us-west-1.periscope.tv
chatman-replay-us-west-2.periscope.tv

```

```

chatman-sa-east-1.periscope.tv
chatman-us-east-1.periscope.tv
chatman-us-west-1.periscope.tv
chatman-us-west-2.periscope.tv
dev-admin.periscope.tv
dev-ap-northeast-1.periscope.tv
dev-ap-southeast-1.periscope.tv
dev-ap-southeast-2.periscope.tv
dev-api.periscope.tv
dev-audit-trail.periscope.tv
dev-channels.periscope.tv
dev-chatman-ancillary-eu-west-1.periscope.tv
dev-chatman-replay-eu-west-1.periscope.tv
dev-chatman-replay-us-west-2.periscope.tv
dev-email.periscope.tv
dev-embed.periscope.tv
dev-eu-west-1.periscope.tv
dev-m.periscope.tv
dev-masks.periscope.tv
dev-notification-service.periscope.tv
dev-payman.periscope.tv
dev-profile.periscope.tv
dev-public-api.periscope.tv
dev-public-api-assets.periscope.tv
dev-replay.periscope.tv
dev-signer.periscope.tv
dev-signer-eu-west-1.periscope.tv
dev-signer-us-west-2.periscope.tv
dev-text-classification.periscope.tv
dev-tn.periscope.tv
dev-transcode-eu-west-1.periscope.tv
dev-transcode-proxy-eu-west-1.periscope.tv
dev-transcode-proxy-us-west-2.periscope.tv
dev-transcode-us-west-2.periscope.tv
dev-us-east-1.periscope.tv
dev-video-eu-west-1.periscope.tv
dev-video-us-west-2.periscope.tv
dev-vidman-eu-west-1.periscope.tv
dev-web.periscope.tv
dev-web-eu-west-1.periscope.tv
dev-www.periscope.tv
email.periscope.tv
email-service.periscope.tv
embed.periscope.tv
guest.periscope.tv
help.periscope.tv
hls.periscope.tv
lex-us-west-2.periscope.tv

```



```

prerflight-web.periscope.tv
prod-ap-northeast-1.periscope.tv
prod-ap-southeast-2.periscope.tv
prod-assets.periscope.tv
prod-chatman-ancillary-ap-northeast-1.periscope.tv
prod-chatman-ancillary-ap-southeast-1.periscope.tv
prod-chatman-ancillary-eu-central-1.periscope.tv
prod-chatman-ancillary-eu-west-1.periscope.tv
prod-chatman-ancillary-us-east-1.periscope.tv
prod-chatman-ancillary-us-west-1.periscope.tv
prod-chatman-ancillary-us-west-2.periscope.tv
prod-eu-central-1.periscope.tv
prod-masks.periscope.tv
prod-profile.periscope.tv
prod-public-api-assets.periscope.tv
prod-replay-ap-northeast-1-public.periscope.tv
prod-replay-ap-southeast-2-public.periscope.tv
prod-replay-eu-central-1-public.periscope.tv
prod-replay-eu-west-1-public.periscope.tv
prod-replay-us-east-1-public.periscope.tv
prod-replay-us-west-2-public.periscope.tv
prod-sa-east-1.periscope.tv
prod-text-classification.periscope.tv
prod-transcode-ap-northeast-2.periscope.tv
prod-transcode-ap-south-1.periscope.tv
prod-transcode-ap-southeast-1.periscope.tv
prod-transcode-ap-southeast-2.periscope.tv
prod-transcode-eu-central-1.periscope.tv
prod-transcode-eu-west-1.periscope.tv
prod-transcode-eu-west-3.periscope.tv
prod-transcode-proxy-ap-northeast-1.periscope.tv
prod-transcode-proxy-ap-south-1.periscope.tv
prod-transcode-proxy-ap-southeast-1.periscope.tv
prod-transcode-proxy-eu-west-3.periscope.tv
prod-transcode-proxy-us-east-1.periscope.tv
prod-transcode-sa-east-1.periscope.tv
prod-transcode-us-east-1.periscope.tv
prod-transcode-us-west-1.periscope.tv
prod-transcode-us-west-2.periscope.tv
prod-us-east-1.periscope.tv
prod-us-west-1.periscope.tv
prod-us-west-2.periscope.tv
prod-video-ap-northeast-1.periscope.tv
prod-video-ap-northeast-2.periscope.tv
prod-video-ap-south-1.periscope.tv
prod-video-ap-southeast-1.periscope.tv
prod-video-ap-southeast-2.periscope.tv
prod-video-eu-central-1.periscope.tv

```

```

signer-ap-northeast-2.periscope.tv
signer-ap-south-1.periscope.tv
signer-ap-southeast-2.periscope.tv
signer-eu-central-1.periscope.tv
signer-eu-west-1.periscope.tv
signer-sa-east-1.periscope.tv
signer-us-west-2.periscope.tv
text-classification.periscope.tv
tn.periscope.tv
vault.periscope.tv
video.periscope.tv
prod-ec-ap-northeast-1.video.periscope.tv
prod-ec-ap-southeast-1.video.periscope.tv
prod-ec-eu-central-1.video.periscope.tv
prod-ec-us-east-1.video.periscope.tv
prod-ec-us-west-1.video.periscope.tv
prod-fastly-ap-northeast-1.video.periscope.tv
prod-fastly-ap-northeast-2.video.periscope.tv
prod-fastly-ap-south-1.video.periscope.tv
prod-fastly-ap-southeast-1.video.periscope.tv
prod-fastly-ap-southeast-2.video.periscope.tv
prod-fastly-eu-central-1.video.periscope.tv
prod-fastly-eu-west-1.video.periscope.tv
prod-fastly-eu-west-3.video.periscope.tv
prod-fastly-sa-east-1.video.periscope.tv
prod-fastly-us-east-1.video.periscope.tv
prod-fastly-us-west-1.video.periscope.tv
prod-fastly-us-west-2.video.periscope.tv
vidman-ap-northeast-1.periscope.tv
vidman-ap-northeast-2.periscope.tv
vidman-ap-southeast-1.periscope.tv
vidman-ap-southeast-2.periscope.tv
vidman-eu-central-1.periscope.tv
vidman-eu-west-1.periscope.tv
vidman-sa-east-1.periscope.tv
vidman-us-east-1.periscope.tv
vidman-us-west-2.periscope.tv
web.periscope.tv
web-ap-northeast-2.periscope.tv
web-ap-south-1.periscope.tv
web-ap-southeast-1.periscope.tv
web-ap-southeast-2.periscope.tv
web-eu-west-1.periscope.tv
web-sa-east-1.periscope.tv
web-us-east-1.periscope.tv
web-us-west-1.periscope.tv
web-us-west-2.periscope.tv

```

Using Sublist3r to find subdomains of pscp.tv

```

[cheth@chethl-virtualplatform]~$[Sublist3r]
$ python sublist3r.py -d pscp.tv

Sublist3r
1000.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for pscp.tv
[-] Searching now in Botdoo..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 239
www.pscp.tv
a.pscp.tv
api.pscp.tv
api-ws.pscp.tv
assets.pscp.tv
eu.pscp.tv
audit-trail.pscp.tv
b.pscp.tv
br.pscp.tv
ca.pscp.tv
canary-channels.pscp.tv
canary-chatman-ancillary-us-west-2.pscp.tv
canary-exp-video-us-east-1.pscp.tv
canary-fleets-us-west-1.pscp.tv
canary-fleets-us-west-2.pscp.tv
canary-guest.pscp.tv
canary-proxy.pscp.tv
canary-safety.pscp.tv
canary-text-classification.pscp.tv
canary-transcode-proxy-us-east-1.pscp.tv
canary-transcode-us-east-1.pscp.tv

```


```
canary-guest.pscp.tv
canary-proxsee.pscp.tv
canary-safety.pscp.tv
canary-text-classification.pscp.tv
canary-transcode-proxy-us-east-1.pscp.tv
canary-transcode-us-east-1.pscp.tv
canary-video-us-east-1.pscp.tv
canary-web.pscp.tv
channel-thumbnails-dev.pscp.tv
channel-thumbnails-live.pscp.tv
channels.pscp.tv
chatman-replay-ap-northeast-1.pscp.tv
chatman-replay-eu-central-1.pscp.tv
chatman-replay-us-east-1.pscp.tv
chatman-replay-us-west-2.pscp.tv
d.pscp.tv
dch.pscp.tv
de.pscp.tv
dev-api.pscp.tv
dev-apt-ws.pscp.tv
dev-assets.pscp.tv
dev-audit-trail.pscp.tv
dev-channels-thumbnails.pscp.tv
dev-chatman-ancillary-us-west-2.pscp.tv
dev-chatman-replay-eu-west-1.pscp.tv
dev-chatman-replay-us-west-2.pscp.tv
dev-email.pscp.tv
dev-embed.pscp.tv
dev-exp-video-eu-west-1.pscp.tv
dev-exp-video-us-west-2.pscp.tv
dev-fleets.pscp.tv
dev-fleets-us-west-2.pscp.tv
dev-guest.pscp.tv
dev-hlspull.pscp.tv
dev-lex-us-east-1.pscp.tv
dev-masks.pscp.tv
dev-proxsee.pscp.tv
dev-public-apt-assets.pscp.tv
dev-safety.pscp.tv
dev-signer.pscp.tv
dev-signer-eu-west-1.pscp.tv
dev-text-classification.pscp.tv
dev-thumbnail.pscp.tv
dev-transcode-us-west-2.pscp.tv
dev-turn.pscp.tv
dev-video-eu-west-1.pscp.tv
dev-video-us-west-2.pscp.tv
dev-vidman-eu-west-1.pscp.tv
```

```
hls.pscp.tv
hlspull.pscp.tv
ie.pscp.tv
jp.pscp.tv
kr.pscp.tv
lex-us-west-2.pscp.tv
metrics.pscp.tv
notification-service.pscp.tv
or.pscp.tv
other.pscp.tv
payman.pscp.tv
preflight-web.pscp.tv
prod-assets.pscp.tv
prod-channels-thumbnails.pscp.tv
prod-chatman-ancillary-ap-northeast-1.pscp.tv
prod-chatman-ancillary-eu-central-1.pscp.tv
prod-chatman-ancillary-us-east-1.pscp.tv
prod-chatman-ancillary-us-west-2.pscp.tv
prod-exp-video-ap-northeast-1.pscp.tv
prod-exp-video-ap-southeast-2.pscp.tv
prod-exp-video-eu-central-1.pscp.tv
prod-exp-video-eu-west-1.pscp.tv
prod-exp-video-sa-east-1.pscp.tv
prod-exp-video-us-east-1.pscp.tv
prod-masks.pscp.tv
prod-playback-ap-northeast-1.pscp.tv
prod-playback-ap-southeast-2.pscp.tv
prod-playback-eu-central-1.pscp.tv
prod-playback-eu-west-1.pscp.tv
prod-playback-sa-east-1.pscp.tv
prod-playback-us-east-1.pscp.tv
prod-playback-us-west-1.pscp.tv
prod-playback-us-west-2.pscp.tv
prod-profile.pscp.tv
prod-public-apt-assets.pscp.tv
prod-text-classification.pscp.tv
prod-thumbnail.pscp.tv
prod-thumbnail-small.pscp.tv
prod-transcode-ap-northeast-2.pscp.tv
prod-transcode-ap-south-1.pscp.tv
prod-transcode-ap-southeast-1.pscp.tv
prod-transcode-ap-southeast-2.pscp.tv
prod-transcode-eu-central-1.pscp.tv
prod-transcode-eu-west-1.pscp.tv
prod-transcode-eu-west-3.pscp.tv
prod-transcode-proxy-ap-south-1.pscp.tv
prod-transcode-proxy-ap-southeast-2.pscp.tv
prod-transcode-proxy-eu-central-1.pscp.tv
```

```
prod-cloudfront-tn-ap-southeast-1-replay.video.pscp.tv
prod-cloudfront-tn-eu-southeast-1-replay.video.pscp.tv
prod-cloudfront-tn-eu-central-1-live.video.pscp.tv
prod-cloudfront-tn-eu-central-1-replay.video.pscp.tv
prod-cloudfront-tn-eu-west-1-live.video.pscp.tv
prod-cloudfront-tn-eu-west-1-replay.video.pscp.tv
prod-cloudfront-tn-eu-west-3-live.video.pscp.tv
prod-cloudfront-tn-eu-west-3-replay.video.pscp.tv
prod-cloudfront-tn-sa-east-1-live.video.pscp.tv
prod-cloudfront-tn-sa-east-1-replay.video.pscp.tv
prod-cloudfront-tn-us-east-1-live.video.pscp.tv
prod-cloudfront-tn-us-east-1-replay.video.pscp.tv
prod-cloudfront-tn-us-west-1-live.video.pscp.tv
prod-cloudfront-tn-us-west-1-replay.video.pscp.tv
prod-cloudfront-tn-us-west-2-live.video.pscp.tv
prod-cloudfront-tn-us-west-2-replay.video.pscp.tv
prod-ec-ap-northeast-1.video.pscp.tv
prod-ec-ap-northeast-2.video.pscp.tv
prod-ec-ap-south-1.video.pscp.tv
prod-ec-ap-southeast-1.video.pscp.tv
prod-ec-ap-southeast-2.video.pscp.tv
prod-ec-eu-central-1.video.pscp.tv
prod-ec-eu-west-1.video.pscp.tv
prod-ec-eu-west-3.video.pscp.tv
prod-ec-sa-east-1.video.pscp.tv
prod-ec-us-east-1.video.pscp.tv
prod-ec-us-west-1.video.pscp.tv
prod-ec-us-west-2.video.pscp.tv
prod-fastly-ap-northeast-1.video.pscp.tv
prod-fastly-ap-northeast-2.video.pscp.tv
prod-fastly-ap-south-1.video.pscp.tv
prod-fastly-ap-southeast-1.video.pscp.tv
prod-fastly-ap-southeast-2.video.pscp.tv
prod-fastly-eu-central-1.video.pscp.tv
prod-fastly-eu-west-1.video.pscp.tv
prod-fastly-eu-west-3.video.pscp.tv
prod-fastly-sa-east-1.video.pscp.tv
prod-fastly-us-east-1.video.pscp.tv
prod-fastly-us-west-1.video.pscp.tv
prod-fastly-us-west-2.video.pscp.tv
vidman-ap-northeast-1.pscp.tv
vidman-ap-northeast-2.pscp.tv
vidman-ap-southeast-1.pscp.tv
vidman-ap-southeast-2.pscp.tv
vidman-eu-central-1.pscp.tv
vidman-eu-west-1.pscp.tv
vidman-eu-west-3.pscp.tv
vidman-sa-east-1.pscp.tv
```

Using Sublist3r to find subdomains of twimg.com

```
[~]# cd [~/chethl-mmware/virtualplatform/] && ./Sublist3r.py  
$python Sublist3r.py -d twtng.com
```



```
Info:com

# Coded By Ahmed Aboul-Ela - @aboull3la

[-] Enumerating subdomains now for twtng.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now In Bing..
[-] Searching now In Ask..
[-] Searching now In Ncraft..
[-] Searching now In DNSDumpster..
[-] Searching now In Virustotal..
[-] Searching now In ThreatCrowd..
[-] Searching now In SSL Certificates..
[-] Searching now In PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[+] Total Unique Subdomains Found: 256
www.twtng.com
twtng.com
P.twtng.com
a0.twtng.com
a1.twtng.com
a2.twtng.com
a3.twtng.com
a4.twtng.com
a5.twtng.com
abs.twtng.com
abs-0.twtng.com
abs-ak.twtng.com
abs-ec.twtng.com
abs-ft.twtng.com
abs-gc.twtng.com
abs-o.twtng.com
abs-o-ak.twtng.com
abs-o-ec.twtng.com
abs-o-ft.twtng.com
abs-t-1.twtng.com
abs-t-2.twtng.com
```

g0.twimg.com
g0.twimg.com
g5-staging.twimg.com
gs.twimg.com
gs.twimg.com
gu.twimg.com
hca.twimg.com
httpspbs.twimg.com
i.twimg.com
image-proxy-origin.twimg.com
lpv6.twimg.com
jp.twimg.com
l.twimg.com
l.twimg.com
ec.e-lv.twimg.com
p-ca-e-lv.e-lv.twimg.com
p-va-e-lv.e-lv.twimg.com
p-va-e-lv.e-lv.twimg.com
ft.e-lv.twimg.com
p-ca-ft.e-lv.e-lv.twimg.com
p-du-ft.e-lv.e-lv.twimg.com
p-fr-ft.e-lv.e-lv.twimg.com
p-fr-ft.e-lv.e-lv.twimg.com
p-sg-ft.e-lv.e-lv.twimg.com
p-syd-ft.e-lv.e-lv.twimg.com
p-tyo-1.ft.e-lv.e-lv.twimg.com
p-tyo-ft.e-lv.e-lv.twimg.com
t-ca-e-lv.e-lv.twimg.com
ll.e-lv.twimg.com
p-du-1.e-lv.e-lv.twimg.com
p-du-1.e-lv.e-lv.twimg.com
p-du-1.e-lv.e-lv.twimg.com
p-sg-1.e-lv.e-lv.twimg.com
p-va-1.e-lv.e-lv.twimg.com
t-ca-1.e-lv.e-lv.twimg.com
lv.twimg.com
us-east-2-ca-e-lv.e-lv.twimg.com
med1.lv.twimg.com
hlsv1e-akc.med1.m.lv.twimg.com
hlsv1e-akcq2.med1.m.lv.twimg.com
hlsv1e-akcqs.med1.m.lv.twimg.com
hlsv1e-akcqs.med1.m.lv.twimg.com
hlsv1e-akcsqs.med1.m.lv.twimg.com
hlsv1e-13c.med1.m.lv.twimg.com
hlsv1e-13c1.med1.m.lv.twimg.com
hlsv1e-13c2.med1.m.lv.twimg.com
hlsv1e-13c3.med1.m.lv.twimg.com
hlsv1e-13c4.med1.m.lv.twimg.com

ma2.twing.com
ma3.twing.com
med1.twing.com
mobile-staging.twing.com
mobile-staging2.twing.com
mobile-stagings.twing.com
mobile-staging.twing.com
mobile1.twing.com
mobile2-1.twing.com
mobile3.twing.com
mobile4.twing.com
o.twing.com
o-0.twing.com
o-0k.twing.com
o-0c.twing.com
o-0r.twing.com
o-1a.twing.com
o-2ero.twing.com
oem.twing.com
oem-o.twing.com
o-0.twing.com
o-dev.twing.com
psb.twing.com
psb-0.twing.com
psb-ak.twing.com
psb-bb.twing.com
psb-c.twing.com
psb-ft.twing.com
psb-gc.twing.com
psb-h1.twing.com
psb-h1-c.twing.com
psb-h2.twing.com
psb-h2-c.twing.com
psb-o.twing.com
psb-o-ak.twing.com
psb-o-c.twing.com
psb-o-ft.twing.com
psb-1.twing.com
psb-2.twing.com
psb-2-3.twing.com
psb-4.twing.com
psb-5.twing.com
psb-a.twing.com
psb-v6.twing.com
psb-zero.twing.com
net-conn-test.twing.com
pr.twing.com


```

syndication.twimg.com
syndication.twimg.com
edm.syndication.twimg.com
eb.syndication.twimg.com
httpscdn.syndication.twimg.com
syndication-o.twimg.com
callfeather.twimg.com
tast.twimg.com
ton.twimg.com
ton-0.twimg.com
ton-ak.twimg.com
ton-ec.twimg.com
ton-ft.twimg.com
ton-o.twimg.com
ton-o-ak.twimg.com
ton-o-ec.twimg.com
ton-o-ft.twimg.com
ton-ta.twimg.com
ton-zero.twimg.com
ttc.twimg.com
tweet.twimg.com
twitter.twimg.com
v.twimg.com
video.twimg.com
edge-cname.video.twimg.com
video-0.twimg.com
video-ak.twimg.com
video-eb.twimg.com
video-ec.twimg.com
video-ec.twimg.com
video-gc.twimg.com
video-h2.twimg.com
video-o.twimg.com
video-o-ak.twimg.com
video-o-ec.twimg.com
video-o-ft.twimg.com
video-staging.twimg.com
video-t-1.twimg.com
video-t-2.twimg.com
video-t-3.twimg.com
video-t-4.twimg.com
video-t-5.twimg.com
video-zero.twimg.com
vttc.twimg.com
widgets.twimg.com
wilcard.twimg.com
wildcard.twimg.com
wildcard-eb.twimg.com
vndication.twimg.com

```

Using Sublist3r to find subdomains of gnip.com

```

[cheeth@cheethi-vmwarevirtualplatform]~/Sublist3r
$ python sublist3r.py -d gnip.com

Sublist3r
# Coded By Ahmed Aboul-El* @aboul3la

[-] Enumerating subdomains now for gnip.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Metacraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 105

www.gnip.com
account-api.gnip.com
adobe-sic-2.gnip.com
amihan.gnip.com
api.gnip.com
avatar.gnip.com
bastion.gnip.com
camp.bastion.gnip.com
csi.bastion.gnip.com
gnip-api.bastion.gnip.com
hqe.bastion.gnip.com
mynewsdesk.bastion.gnip.com
ooo.bastion.gnip.com
beyondthearc.gnip.com
blog.gnip.com
blog-origin.gnip.com
brandwatch.gnip.com
brent.gnip.com
chrpify.gnip.com
client-vpn.gnip.com
www.client-vpn.gnip.com
cog.gnip.com

```

```

flye.gnip.com
garantl.gnip.com
gnip-api.gnip.com
gnip-api-staging.gnip.com
gnip-api.gnip.com
gnip-stream.gnip.com
historical.gnip.com
hootsuite.gnip.com
hqe.gnip.com
jhuapl.gnip.com
jim.gnip.com
john.gnip.com
johnstest.gnip.com
kantarmedia.gnip.com
kreger.gnip.com
lp.gnip.com
m2g.gnip.com
mail.gnip.com
naven.gnip.com
nedallia.gnip.com
nedallia.gnip.com
mutualind.gnip.com
mynewsdesk.gnip.com
netbase.gnip.com
newsclip.gnip.com
nordstrom.gnip.com
nuvi.gnip.com
nuvi2.gnip.com
nuvi3.gnip.com
nuvi4.gnip.com
cheferator1.ops.gnip.com
admit1-cl2-den-vw-ops.gnip.com
cloud1-cl2-den-vw-ops.gnip.com
nagios-cl2-den-vw-ops.gnip.com
nagios1-cl2-den-vw-ops.gnip.com
pablo.gnip.com
pinl.gnip.com
prectise.gnip.com
account-api-prod.gnip.com
api-prod.gnip.com
cache-child1a.prod.gnip.com
grapherator1-cl2-den-vw-prod.gnip.com
nagios-cl2-den-vw-prod.gnip.com
www.nagios-cl2-den-vw-prod.gnip.com
nagios1-cl2-den-vw-prod.gnip.com
console.prod.gnip.com
historical.prod.gnip.com
nagios.prod.gnip.com

```

Using Sublist3r to find subdomains of mopub.com

```
[chethi@chethi-vmwarevirtualplatform]~/Sublist3r
$ python sublist3r.py -d mopub.com

Sublist3r
# Coded By Ahmed About-Elia - @aboul3la

[-] Enumerating subdomains now for mopub.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 95
www.mopub.com
ab.mopub.com
www.ab.mopub.com
adpreview.mopub.com
ads.mopub.com
testing-ads.mopub.com
v3.ads.mopub.com
internal.v3.ads.mopub.com
ads-staging.mopub.com
adserver.mopub.com
admin.adserver.mopub.com
adstats-staging.mopub.com
analytics.mopub.com
android-native-ads.mopub.com
api-staging.mopub.com
app.mopub.com
app2.mopub.com
cb.mopub.com
cdn-cms.mopub.com
cdn1.mopub.com
cdn2.mopub.com
```

```
data-tracer.mopub.com
demand.mopub.com
developers.mopub.com
engineering.mopub.com
fonts.mopub.com
frontend-staging.mopub.com
frontend-staging-preview.mopub.com
help.mopub.com
hummingbird.mopub.com
images.mopub.com
marketplace-admin-staging.mopub.com
marketplace-staging.mopub.com
media.mopub.com
memonitor.mopub.com
voxel.read.mongostats.mopub.com
voxel.write.mongostats.mopub.com
mopub-dfp.mopub.com
mpx.mopub.com
admin.mpx.mopub.com
voxel.read.admin.mpx.mopub.com
voxel.write.admin.mpx.mopub.com
cpp.tmp.mpx.mopub.com
cpp-test.tmp.mpx.mopub.com
internal.mpx.mopub.com
voxel.mpx.mopub.com
mpx-dashboard.mopub.com
ns-d01.mopub.com
ns-d02.mopub.com
ns-d03.mopub.com
ns-d04.mopub.com
ns-r01.mopub.com
ns-r02.mopub.com
ns-r03.mopub.com
ns-r04.mopub.com
public.billing.master.postgres.mopub.com
public.fe.master.postgres.mopub.com
public.mpxidder.master.postgres.mopub.com
preflight.mopub.com
a.r10.mopub.com
b.r10.mopub.com
c.r10.mopub.com
d.r10.mopub.com
reporting.mopub.com
s.mopub.com
s2.mopub.com
s2s-test.mopub.com
secure-ads.mopub.com
sentry.mopub.com
```

Using Sublist3r to find subdomains of niche.co

```
[chethi@chethi-vmwarevirtualplatform]~/Sublist3r
$ python sublist3r.py -d niche.co

Sublist3r
# Coded By Ahmed About-Elia - @aboul3la

[-] Enumerating subdomains now for niche.co
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 9
www.niche.co
aws.niche.co
blog.niche.co
docs.niche.co
docs-ops.niche.co
search3.niche.co
web16.niche.co
web17.niche.co
web18.niche.co
```

Using Sublist3r to find subdomains of snappytv.com

```
cheth@cheth-virtualplatform:~/Sublist3r
$ python sublist3r.py -d snappytv.com

Sublist3r
Data:com
# Coded By Ahmed About-Ela - @aboul3la

[-] Enumerating subdomains now for snappytv.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 206
www.snappytv.com
api.snappytv.com
api.snappytv.com
archive.snappytv.com
a.aws.snappytv.com
193.autocap182.a.aws.snappytv.com
279.autocap182.a.aws.snappytv.com
328.autocap182.a.aws.snappytv.com
363.autocap182.a.aws.snappytv.com
599.autocap182.a.aws.snappytv.com
751.autocap182.a.aws.snappytv.com
765.autocap182.a.aws.snappytv.com
845.autocap182.a.aws.snappytv.com
881.autocap182.a.aws.snappytv.com
972.autocap182.a.aws.snappytv.com
987.autocap192.a.aws.snappytv.com
229.autocap234.a.aws.snappytv.com
661.autocap234.a.aws.snappytv.com
847.autocap246.a.aws.snappytv.com
112.autocap263.a.aws.snappytv.com
292.autocap272.a.aws.snappytv.com
841.autocap290.a.aws.snappytv.com
```

```
880.autocap328.a.aws.snappytv.com
982.autocap328.a.aws.snappytv.com
967.autocap328.a.aws.snappytv.com
888.autocap340.a.aws.snappytv.com
autocap380.a.aws.snappytv.com
270.autocap380.a.aws.snappytv.com
173.autocap426.a.aws.snappytv.com
248.autocap426.a.aws.snappytv.com
331.autocap426.a.aws.snappytv.com
149.autocap453.a.aws.snappytv.com
295.autocap453.a.aws.snappytv.com
423.autocap453.a.aws.snappytv.com
autocap513.a.aws.snappytv.com
884.autocap565.a.aws.snappytv.com
121.autocap598.a.aws.snappytv.com
493.autocap620.a.aws.snappytv.com
1080.autocap630.a.aws.snappytv.com
153.autocap646.a.aws.snappytv.com
149.autocap662.a.aws.snappytv.com
34.autocap662.a.aws.snappytv.com
411.autocap662.a.aws.snappytv.com
569.autocap662.a.aws.snappytv.com
753.autocap662.a.aws.snappytv.com
844.autocap678.a.aws.snappytv.com
854.autocap746.a.aws.snappytv.com
496.autocap751.a.aws.snappytv.com
871.autocap751.a.aws.snappytv.com
472.autocap758.a.aws.snappytv.com
776.autocap758.a.aws.snappytv.com
887.autocap758.a.aws.snappytv.com
268.autocap790.a.aws.snappytv.com
775.autocap820.a.aws.snappytv.com
9.autocap845.a.aws.snappytv.com
149.autocap845.a.aws.snappytv.com
187.autocap845.a.aws.snappytv.com
245.autocap845.a.aws.snappytv.com
325.autocap845.a.aws.snappytv.com
331.autocap845.a.aws.snappytv.com
368.autocap845.a.aws.snappytv.com
4.autocap845.a.aws.snappytv.com
480.autocap845.a.aws.snappytv.com
550.autocap845.a.aws.snappytv.com
612.autocap845.a.aws.snappytv.com
622.autocap845.a.aws.snappytv.com
631.autocap845.a.aws.snappytv.com
655.autocap845.a.aws.snappytv.com
728.autocap845.a.aws.snappytv.com
739.autocap845.a.aws.snappytv.com
```

```
149.autocap845.a.aws.snappytv.com
187.autocap845.a.aws.snappytv.com
245.autocap845.a.aws.snappytv.com
325.autocap845.a.aws.snappytv.com
331.autocap845.a.aws.snappytv.com
368.autocap845.a.aws.snappytv.com
4.autocap845.a.aws.snappytv.com
480.autocap845.a.aws.snappytv.com
550.autocap845.a.aws.snappytv.com
612.autocap845.a.aws.snappytv.com
622.autocap845.a.aws.snappytv.com
631.autocap845.a.aws.snappytv.com
655.autocap845.a.aws.snappytv.com
728.autocap845.a.aws.snappytv.com
739.autocap845.a.aws.snappytv.com
846.autocap845.a.aws.snappytv.com
859.autocap845.a.aws.snappytv.com
920.autocap845.a.aws.snappytv.com
387.autocap863.a.aws.snappytv.com
338.autocap863.a.aws.snappytv.com
827.autocap869.a.aws.snappytv.com
139.autocap843.a.aws.snappytv.com
463.autocap952.a.aws.snappytv.com
510.autocap952.a.aws.snappytv.com
670.autocap952.a.aws.snappytv.com
787.autocap952.a.aws.snappytv.com
846.autocap952.a.aws.snappytv.com
m1011.aws.snappytv.com
m1082.aws.snappytv.com
blog.snappytv.com
dashboard.snappytv.com
mbed.snappytv.com
flash.snappytv.com
frame.snappytv.com
partner-android.git.snappytv.com
flurry.git.snappytv.com
sc-connect-www.git.snappytv.com
web.git.snappytv.com
logging.snappytv.com
logstash.snappytv.com
magnun.snappytv.com
media.snappytv.com
beta.media.snappytv.com
stage.media.snappytv.com
prod.mediahd.snappytv.com
aws.snappytv.com
node.snappytv.com
origin.snappytv.com
```

```

mailserver.p.snappytv.com
afbe2.p.snappytv.com
ma.p.snappytv.com
inet.nat.p.snappytv.com
new.p.snappytv.com
nge@web.p.snappytv.com
n3.p.snappytv.com
old4.p.snappytv.com
extranet.portal.p.snappytv.com
us.west.2.prod.p.snappytv.com
origin.r5flytvrqva8y.p.snappytv.com
nge@web.rdc.p.snappytv.com
s.p.snappytv.com
smokemarkets2.p.snappytv.com
pa.d.students05.p.snappytv.com
syakyou.p.snappytv.com
test2.p.snappytv.com
upe.p.snappytv.com
gsmm.ws.p.snappytv.com
puppet.snappytv.com
ral.snappytv.com
relay.snappytv.com
smokeping.snappytv.com
aplice.snappytv.com
stage.snappytv.com
api.stage.snappytv.com
static.snappytv.com
stats.snappytv.com
statsbeta.snappytv.com
statastage.snappytv.com
testing.snappytv.com
cmu.testing.snappytv.com
al.contact.testing.snappytv.com
ewea.testing.snappytv.com
hdpadmin.testing.snappytv.com
horagal.testing.snappytv.com
label.testing.snappytv.com
multimedia.testing.snappytv.com
mye-supportcentre.testing.snappytv.com
skype.token.testing.snappytv.com
aws.in.testing.snappytv.com
tune.in.snappytv.com
fas01.usw1.snappytv.com
fas01.usw1.snappytv.com
apt02.usw2.snappytv.com
181.archive01.usw2.snappytv.com
780.archive02.usw2.snappytv.com
150.archive03.usw2.snappytv.com

```

Using Sublist3r to find subdomains of twitterflightschool.com

```

[cheth@cheth-virtualplatform]~/Sublist3r
$python sublist3r.py -d twitterflightschool.com

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for twitterflightschool.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in Threatcrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 11
www.twitterflightschool.com
dev.twitterflightschool.com
havas.twitterflightschool.com
ipg.twitterflightschool.com
learning-locker.twitterflightschool.com
microsoft.twitterflightschool.com
moodle.twitterflightschool.com
origin.twitterflightschool.com
publicis.twitterflightschool.com
static.twitterflightschool.com
stg.twitterflightschool.com

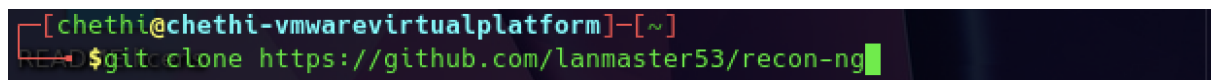
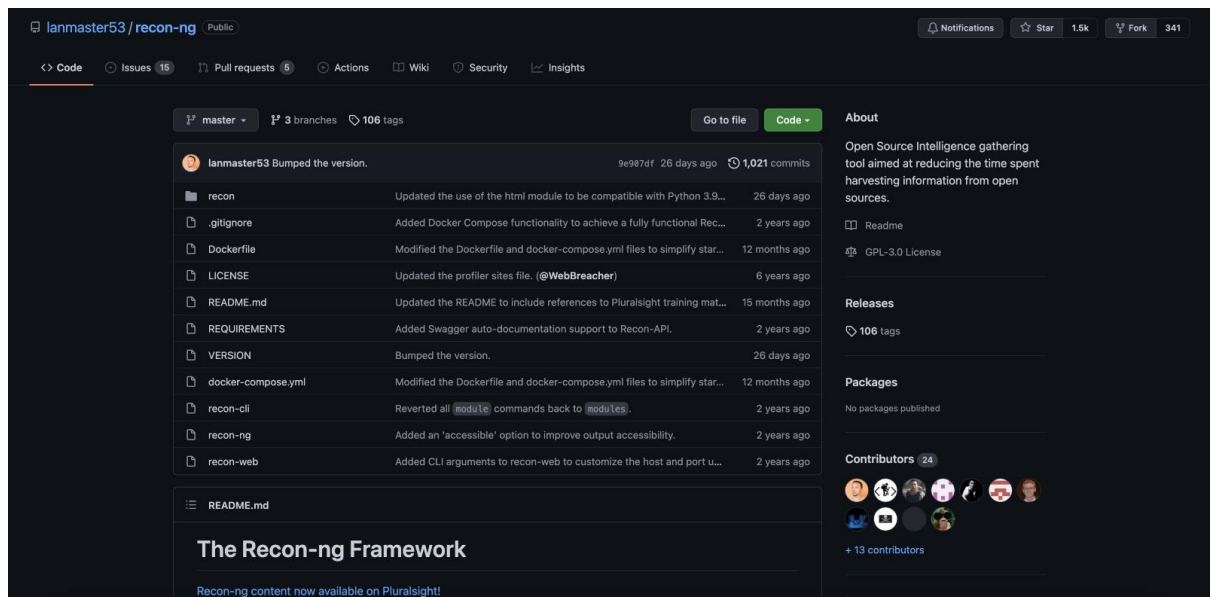
```


Recon-ng

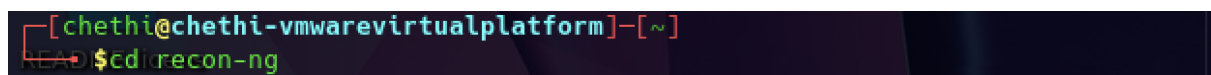
Recon-ng is also a python-based tool. This tool is one of the widely used tool because it provides a powerful environment and also its interface is similar to the Metasploit as well.

Like the sublist3r this tool is can clone from GitHub to your machine.

GitHub link: <https://github.com/lanmaster53/recon-ng>



Then I have open the recon-ng directory.



After that, I have installed pip by using pip install -r REQUIREMENTS command



Then installation will complete and can open by giving recon-ng command

[illegible]

```
[recon-ng][default] > help

Commands (type [help?] <topic>):

back      Exits the current context
dashboard Displays a summary of activity
db         Interfaces with the workspace's database
exit      Exits the framework
help      Displays this menu
index     Creates a module index (dev only)
keys      Manages third party resource credentials
marketplace Interfaces with the module marketplace
modules   Interfaces with installed modules
options   Manages the current context options
python    Starts a Python Debugger session (dev only)
script    Records and executes command scripts
shell     Executes shell commands
show      Shows various framework items
snapshots Manages workspace snapshots
spool     Spools output to a file
workspaces Manages workspaces

[recon-ng][default] > dashboard
  This workspace has no record of activity.
[recon-ng][default] > dashboard
  This workspace has no record of activity.
[recon-ng][default] > marketplace search 'gmail.com'...
  Searching module index for 'gmail.com'...
[!] No modules found.
Searches marketplace modules

Usage: marketplace search <regex>

[recon-ng][default] > marketplace search google
  Searching module index for 'google'...

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| recon/domains-hosts/google_site_web | 1.0 | not installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
```

```
[recon-ng][default] > metasploit install recon/domains-hosts/google_site_web
Module installed: recon/domains-hosts/google_site_web
Reloading modules...
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > info

Name: Google Hostname Enumerator
Author: Tim Ternes (@lanmaster53)
Version: 1.0

Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.

Options:


| Name   | Current Value | Required | Description                              |
|--------|---------------|----------|------------------------------------------|
| SOURCE | default       | yes      | source of input (see 'info' for details) |



Source Options:


|             |                                                              |
|-------------|--------------------------------------------------------------|
| default     | SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL |
| -string-    | string representing a single input                           |
| -path-      | path to a file containing a list of inputs                   |
| query <sql> | database query returning one column of inputs                |


```

Then I used recon-ng tool to find subdomains in twitter.com. Before that step we have set twitter.com as the host in recon-ng.

```
[recon-ng][default][google_site_web] > options unset source
SOURCE => None:help.twitter.com
[recon-ng][default][google_site_web] > info
[recon-ng]
Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Project: staging.twitter.com
Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
the results.
Options:
Name      Current Value Required Description
-----
SOURCE    twitter.com  yes      source of input (see 'info' for details)
Source Options:
default: SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<strings> twitter string representing a single input
<path> twitter path to a file containing a list of inputs
<query> <sql> database query returning one column of inputs
```

```
[recon-ng][default][google_site_web] > options set SOURCE twitter.com
SOURCE => twitter.com
[recon-ng][default][google_site_web] > info
[recon-ng]
Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Project: staging.twitter.com
Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
the results.
Options:
Name      Current Value Required Description
-----
SOURCE    twitter.com  yes      source of input (see 'info' for details)
Source Options:
default: SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<strings> twitter string representing a single input
<path> twitter path to a file containing a list of inputs
<query> <sql> database query returning one column of inputs
```

After setting up the domain, give run command to proceed forward.

```
[recon-ng][default][google_site_web] > run
[recon-ng]
Country: None
Host: tweetdeck.twitter.com
Ip Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
-----
Country: None
Host: help.twitter.com
Ip Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
-----
Country: None
Host: blog.twitter.com
Ip Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
-----
Country: None
Host: mobile.twitter.com
Ip Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
-----
```

This tool is a web interface known as certificate transparency log. Anyone can find certificates of any domain with a pattern. In that case I have searched using term of “twitter.com” to find sub domains.

31

Find Open Ports and Running Devices on The Target Network

Nmap

Nmap is used to find hosts and services on a particular computer network by sending packets and analysing the responses. This tool is free, and it is created by Gordon Lyon in 1997.

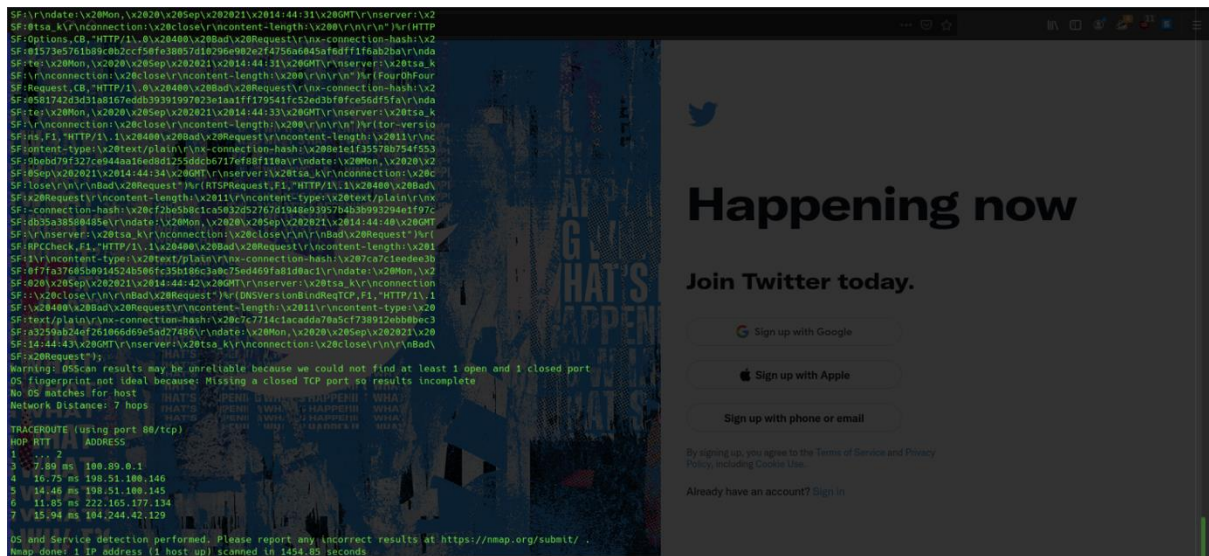
Before using this tool, first we must install it to our machine. For that enter sudo apt-get Nmap on the terminal and then give password. Normally it takes two minutes for the installation process.

```
[chethi@chethi-vmwarevirtualplatform ~]$ sudo apt-get install nmap
[sudo] password for chethi:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  nmap-common
Suggested packages:
  ncat ndiff zenmap
The following packages will be upgraded:
  nmap nmap-common
2 upgraded, 0 newly installed, 0 to remove and 586 not upgraded.
Need to get 5,973 kB of archives.
After this operation, 392 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 https://mirror.bx.sg/parrot rolling/main amd64 nmap amd64 7.92+dfsg1-1 [1,988 kB]
Get:2 https://apac-mirror.parrot.sh/mirrors/parrot rolling/main amd64 nmap-common all 7.92+dfsg1-1 [4,064 kB]
Fetched 5,973 kB in 3s (2,487 KB/s)
Reading changelogs... Done
(Reading database ... 489211 files and directories currently installed.)
Preparing to unpack .../nmap_7.92+dfsg1-1_amd64.deb ...
Unpacking nmap (7.92+dfsg1-1) over (7.91+dfsg1-1kali1) ...
Preparing to unpack .../nmap-common_7.92+dfsg1-1_all.deb ...
Unpacking nmap-common (7.92+dfsg1-1) over (7.91+dfsg1-1kali1) ...
Setting up nmap-common (7.92+dfsg1-1) ...
Setting up nmap (7.92+dfsg1-1) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for mailcap (3.69) ...
Scanning application launchers.
Removing duplicate launchers or broken launchers.
Launchers are updated.
```

Then to check is it install correctly or not, type nmap and observe the output.

```
[chethi@chethi-vmwarevirtualplatform ~]$ nmap
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] (target specification)
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PPH: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/connect()/ACK/window/fin/scan
  -sU: UDP Scan
  -sN/sP/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p21; -p1-65535; -p U53,111,137,T:21-25,89,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  --sc: equivalent to --script=default
```

After Completing installation process, I have entered command to Nmap to find open ports and running devices on twitter.com which is target URL.



[Click here](#) to view the results of Nmap scan.

Finding open ports and running devices on vine.co

```

# nmap -sS -A -p- -T4 -oN vine.txt vine.co
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 15:23 +0530
Nmap scan report for vine.co (52.37.214.157)
Host is up (0.43s latency).
Other addresses for vine.co (not scanned): 52.89.87.282
DNS record for 52.37.214.157: ec2-52-37-214-157.us-west-2.compute.amazonaws.com
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: Couldn't establish connection on port 25
443/tcp   open  ssl/http     Apache/2.4.18 (Ubuntu)
|_http_title: 400 The plain HTTP request was sent to HTTPS port
|_ssl_cert: Subject: commonName=vine.co
|_Subject Alternative Names: DNS:vine.co, DNS:platform.vine.co, DNS:www.vine.co
|_Not valid before: 2021-06-06T00:00:00
|_Not valid after: 2022-07-05T23:59:59
|_ssl_date: TLS randomness does not represent time
|_http_frame_info: Problem with XML parsing of /evox/about
Fingerprints:
|_GetRequest:
|_HTTP/1.1 200 OK
|_Date: Mon, 11 Oct 2021 10:45:09 GMT
|_Content-Type: text/html; charset=utf-8
|_Content-Length: 6871
|_Connection: close
|_Cache-Control: max-age=600
|_X-Content-Type-Options: nosniff
|_X-Frame-Options: SAMEORIGIN
|_Strict-Transport-Security: max-age=631138519
|_Content-Security-Policy: default-src https; data: vine; img-src 'self' data: https://vine.co https://vines.s3.amazonaws.com https://archive.vine.co https://*.twimg.com https://*.cdn.vine.co https://media.vineapp.com https://*.co https://analytics.twitter.com https://ssl.google-analytics.com https://stats.g.doubleclick.net https://twemoji.maxcdn.com https://twitter.github.io/script-src 'self' 'unsafe-inline' 'unsafe-eval' https://vine.co https://*.twitter.com https://vines.s3.amazonaws.com https://archive.vine.co https://*.cdn.vine.co https://platform.vine.co https://stats.g.doubleclick.net https://ssl.google-analytics.com
|_HTTPOptions:
|_HTTP/1.1 200 OK
|_Date: Mon, 11 Oct 2021 10:45:10 GMT
|_Content-Type: text/html; charset=utf-8
|_Content-Length: 0
|_Connection: close
|_Allow: HEAD, OPTIONS, GET
|_Cache-Control: max-age=3600
|_X-Content-Type-Options: nosniff
|_X-Frame-Options: SAMEORIGIN
|_Strict-Transport-Security: max-age=631138519

```

```

X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=631138519
Content-Security-Policy: default-src https; data: vine; img-src 'self' data: https://vine.co https://vines.s3.amazonaws.com https://archive.vine.co https://*.twimg.com https://*.cdn.vine.co https://media.vineapp.com https://*.co https://analytics.twitter.com https://ssl.google-analytics.com https://stats.g.doubleclick.net https://twemoji.maxcdn.com https://twitter.github.io/script-src 'self' 'unsafe-inline' 'unsafe-eval' https://vine.co https://*.twitter.com https://vines.s3.amazonaws.com https://archive.vine.co https://*.cdn.vine.co https://platform.vine.co https://stats.g.doubleclick.net https://ssl.google-analytics.com
h2
|_http/1.1
|_allow:
|_h2
|_http/1.1
Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF:Port 443:TCPv6:92.54.51.32-70b01611a11e11e6141855P:65.54-pe-line-qn
SF:uRv(GetRequest:2165,"HTTP/1.1,x2020bVx200KvRvndate:v20Mon,v2011x200
SF:ictv202021x2018:45:09xv200HTvRvContent-Type:v20text/html;x20charset
SF:uiff-BvRvContent-Length:v206091vRvConnection:v20closevRvCache-Cont
SF:rolv20max-age=600vRvX-Content-Type-Options:v20nosniffvRvX-Frame-Op
SF:tions:v20SAMEORIGINvRvStrict-Transport-Security:v20max-age=631138519
SF:vRvContent-Security-Policy:v20default-srcv20https:v20data:v20vine:
SF:img-srcv20'self'v20data:v20https://vine.co,v20https://vines.s3.a
SF:amazonaws.com,v20https://archive.vine.co,v20https://*.twimg.com,v20
SF:https://*.cdn.vine.co,v20https://media.vineapp.com,v20https://t
SF:co,v20https://analytics.twitter.com,v20https://ssl.google-analytics
SF:v.com,v20https://stats.g.doubleclick.net,v20https://twemoji.maxcdn
SF:com,v20https://twitter.github.io/script-srcv20'self'v20'unsafe-in
SF:line'v20'unsafe-eval'v20https://vine.co,v20https://*.twitter.com\
SF:co,v20https://vines.s3.amazonaws.com,v20https://archive.vine.co,v20ht
SF:tps://*.cdn.vine.co,v20https://platform.vine.co,v20https://stats
SF:g.doubleclick.net,v20https://ssl.google-analytics.com'vRvHTTPOptions
SF:ns:727,"HTTP/1.1,x2020bVx200KvRvndate:v20Mon,v2011x200Cv202021x2
SF:018:45:10xv200HTvRvContent-Type:v20text/html;x20charset=utf-8vRvCon
SF:nt-Length:v200vRvConnection:v20closevRvAllow:v20HEAD,v20OPTIONS
SF:v20GETvRvCache-Control:v20max-age=3600vRvX-Content-Type-Options:v
SF:20nosniffvRvX-Frame-Options:v20SAMEORIGINvRvStrict-Transport-Securit
SF:y:v20max-age=631138519vRvContent-Security-Policy:v20default-srcv20h
SF:tps:v20data:v20vine:img-srcv20'self'v20data:v20https://vine.co
SF:v20https://vines.s3.amazonaws.com,v20https://archive.vine.co,v20ht
SF:tps://*.cdn.vine.co,v20https://*.twimg.com,v20https://media.vin
SF:eapp.com,v20https://t.co,v20https://analytics.twitter.com,v20https://
SF:ssl.google-analytics.com,v20https://stats.g.doubleclick.net,v20ht
SF:tps://twemoji.maxcdn.com,v20https://twitter.github.io/script-src'
SF:x20'self'v20'unsafe-inline'v20'unsafe-eval'v20https://vine.co,v20ht
SF:tps://*.twitter.com,v20https://vines.s3.amazonaws.com,v20https://
SF:archive.vine.co,v20https://*.cdn.vine.co,v20https://platform.vin
SF:e.co,v20https://stats.g.doubleclick.net,v20https://
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

```



```

Network Distance: 7 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 ... 2
3 6.38 ms 100.89.0.1
4 12.94 ms 108.51.100.146
5 11.45 ms 198.51.100.145
6 12.94 ms 222.165.177.134
7 12.67 ms ec2-52-37-214-157.us-west-2.compute.amazonaws.com (52.37.214.157)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3227.81 seconds

```

Finding open ports and running devices on pscp.tv

```

[~]-[root@cheetah-virtualplatform ~]# nmap -sS -A -p- -iL pscp.txt pscp.tv
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 15:23 +0530
Nmap scan report for pscp.tv (13.232.33.228)
Host is up (6.048s latency).
Other addresses for pscp.tv (not scanned): 13.233.203.245
DNS record for 13.232.33.228: ec2-13-232-33-228.ap-south-1.compute.amazonaws.com
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
|_smtp-command: Couldn't establish connection on port 25
88/tcp    open  http
|_fingerprint-strings:
|_FourOhFourRequest:
|_HTTP/1.1 301 Moved Permanently
|_Content-Type: text/plain; charset=utf-8
|_Date: Mon, 11 Oct 2021 10:44:31 GMT
|_Location: https://172.27.7.174/nice%20ports%2C/Tri%6Eity.txt%2ebak
|_Referer-Policy: origin
|_Strict-Transport-Security: max-age=10886400000; includeSubDomains; preload
|_Vary: Accept, Accept-Encoding
|_X-Frame-Options: ALLOW-FROM https://twitter.com/
|_X-Periscope-Web-Version: 3
|_X-RateLimit-Limit: 3000
|_X-RateLimit-Remaining: 2999
|_Content-Length: 90
|_Connection: Close
|_Moved Permanently. Redirecting to https://172.27.7.174/nice%20ports%2C/Tri%6Eity.txt%2ebak
|_GetRequest:
|_HTTP/1.1 301 Moved Permanently
|_Content-Type: text/plain; charset=utf-8
|_Date: Mon, 11 Oct 2021 10:44:29 GMT
|_Location: https://172.27.7.174/
|_Referer-Policy: origin
|_Strict-Transport-Security: max-age=10886400000; includeSubDomains; preload
|_Vary: Accept, Accept-Encoding
|_X-Frame-Options: ALLOW-FROM https://twitter.com/
|_X-Periscope-Web-Version: 3
|_X-RateLimit-Limit: 3000
|_X-RateLimit-Remaining: 2999
|_Content-Length: 95
|_Connection: Close
|_Moved Permanently. Redirecting to https://172.27.7.174/
|_HTTPOptions:
|_HTTP/1.1 403 Forbidden

```

```

[~]-[root@cheetah-virtualplatform ~]# nmap -sS -A -p- -iL pscp.txt pscp.tv
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 15:23 +0530
Nmap scan report for pscp.tv (13.232.33.228)
Host is up (6.048s latency).
Other addresses for pscp.tv (not scanned): 13.233.203.245
DNS record for 13.232.33.228: ec2-13-232-33-228.ap-south-1.compute.amazonaws.com
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
|_smtp-command: Couldn't establish connection on port 25
88/tcp    open  http
|_fingerprint-strings:
|_FourOhFourRequest:
|_HTTP/1.1 301 Moved Permanently
|_Content-Type: text/plain; charset=utf-8
|_Date: Mon, 11 Oct 2021 10:44:31 GMT
|_Location: https://172.27.7.174/nice%20ports%2C/Tri%6Eity.txt%2ebak
|_Referer-Policy: origin
|_Strict-Transport-Security: max-age=10886400000; includeSubDomains; preload
|_Vary: Accept, Accept-Encoding
|_X-Frame-Options: ALLOW-FROM https://twitter.com/
|_X-Periscope-Web-Version: 3
|_X-RateLimit-Limit: 3000
|_X-RateLimit-Remaining: 2999
|_Content-Length: 90
|_Connection: Close
|_Moved Permanently. Redirecting to https://172.27.7.174/nice%20ports%2C/Tri%6Eity.txt%2ebak
|_GetRequest:
|_HTTP/1.1 301 Moved Permanently
|_Content-Type: text/plain; charset=utf-8
|_Date: Mon, 11 Oct 2021 10:44:29 GMT
|_Location: https://172.27.7.174/
|_Referer-Policy: origin
|_Strict-Transport-Security: max-age=10886400000; includeSubDomains; preload
|_Vary: Accept, Accept-Encoding
|_X-Frame-Options: ALLOW-FROM https://twitter.com/
|_X-Periscope-Web-Version: 3
|_X-RateLimit-Limit: 3000
|_X-RateLimit-Remaining: 2999
|_Content-Length: 95
|_Connection: Close
|_Moved Permanently. Redirecting to https://172.27.7.174/
|_HTTPOptions:
|_HTTP/1.1 403 Forbidden
|_RTSPRequest, X11Probe:
|_HTTP/1.1 400 BAD_REQUEST
|_Content-Length: 0
|_Connection: Close
|_http-title: Did not follow redirect to https://pscp.tv/
|_443/tcp open  ssl/https
|_http-title: Did not follow redirect to https://www.pscp.tv/
|_ssl-cert: Subject: commonName=*.pscp.tv
|_Subject Alternative Name: DNS:*.pscp.tv, DNS:pscp.tv
|_Not valid before: 2021-07-01T00:00:00
|_Not valid after: 2022-07-30T23:59:59
|_fingerprint-strings:
|_FourOhFourRequest:
|_HTTP/1.1 302 Found
|_Content-Type: text/plain; charset=utf-8
|_Date: Mon, 11 Oct 2021 10:44:30 GMT
|_Location: https://www.172.27.7.174/nice%20ports%2C/Tri%6Eity.txt%2ebak
|_Referer-Policy: origin
|_Strict-Transport-Security: max-age=10886400000; includeSubDomains; preload
|_Vary: Accept, Accept-Encoding
|_X-Content-Type-Options: nosniff
|_X-Download-Options: noopen
|_X-Frame-Options: ALLOW-FROM https://twitter.com/
|_X-Periscope-Web-Version: 3
|_X-RateLimit-Limit: 3000
|_X-RateLimit-Remaining: 2999
|_X-XSS-Protection: 1; mode=block
|_Content-Length: 62
|_Connection: Close
|_Found. Redirecting to https://www.172.27.7.174/nice%20ports%2C/Tri%6Eity.txt%2ebak
|_GetRequest, HTTPOptions:
|_HTTP/1.1 302 Found
|_Content-Type: text/plain; charset=utf-8

```

[illegible]

```
[*]-[root@cheetah-vmwarevirtualplatform]~[/home/cheetah]
#nmap -sS -A -p -T4 -oN gnip.txt gnip.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 15:23 +0530
Nmap scan report for gnip.com (13.225.0.4)
Host is up (0.021s latency).
Other addresses for gnip.com (not scanned): 13.225.0.19 13.225.0.129 13.225.0.111
rDNS record for 13.225.0.4: server-13-225-0-4.sln52.r.cloudfront.net
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, DNSVersionBInndReqTCP, FourOrFourRequest, GenericLines, GetRequest, HTTPOptions, JavaRMI, Kerberos, LANDesk-RC, LDAPBInndReq, LDAPSearchReq, LPDString, NCP, NotesRPC, RPCCheck, RSPR
|_   equest, STPOptions, SMBProgleg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, afp, ms-sql-s, oracle-tns:
|_   500 Syntax error, command unrecognized
|_   -tcp-commands: Couldnt establish connection on port 25
|_   80/tcp open  http      Amazon CloudFront httpd
|_   -http-title: Did not follow redirect to https://developer.twitter.com/en/enterprise
|_   443/tcp open  ssl/http  Amazon CloudFront httpd
|_   ssl-err: Subject name mismatch: gnip.com/organizationName=Twitter, Inc./stateOrProvinceName=California/countryName=US
|_   Suggest Alternative Name: DNS1: gnip.com, DNS2:gnip.com
|_   Not valid before: 2021-07-15T00:00:00
|_   Not valid after: 2022-07-14T23:59:59
|_   -http-title: Did not follow redirect to https://developer.twitter.com/en/enterprise
|_   -service: Subject name mismatch: retfing data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SFPort25-TCPv7.92v1-7d0-1b11f1me6164511b-x86_64-pc-linux-gnuvfr(Ge
SF:erCLines,28,"500x205syntaxx20error,x20commandx20unrecognizedvrn")%
SF:r(GetRequest,28,"500x205syntaxx20error,x20commandx20unrecognizedvrn
SF:r(HttpOptions,28,"500x205syntaxx20error,x20commandx20unrecognized
SF:rVrn")%r(TPOptions,28,"500x205syntaxx20error,x20commandx20unrecog
SF:izedvrn")%r(RPCCheck,28,"500x205syntaxx20error,x20commandx20unrecog
SF:nizedvrn")%r(DNSVersionBInndReqTCP,28,"500x205syntaxx20error,x20comma
SF:ndx20unrecognizedvrn")%r(DNSStatusRequestTCP,28,"500x205syntaxx20err
SF:r,x20commandx20unrecognizedvrn")%r(SSLSessionReq,28,"500x205syntaxx
SF:20commandx20unrecognizedvrn")%r(TerminalServerCookie,28,"5
SF:00x205syntaxx20error,x20commandx20unrecognizedvrn")%r(TLSSessionReq
SF:28,"500x205syntaxx20error,x20commandx20unrecognizedvrn")%r(Kerbero
SF:s,28,"500x205syntaxx20error,x20commandx20unrecognizedvrn")%r(SMBPro
SF:gleg,28,"500x205syntaxx20error,x20commandx20unrecognizedvrn")%r(X11
SF:Probe,28,"500x205syntaxx20error,x20commandx20unrecognizedvrn")%r(Fo
SF:urOrFourRequest,28,"500x205syntaxx20error,x20commandx20unrecognized
SF:rVrn")%r(LPDString,28,"500x205syntaxx20error,x20commandx20unrecognize
SF:dVrn")%r(LDAPSearchReq,28,"500x205syntaxx20error,x20commandx20unrec
SF:ognizedvrn")%r(LDAPBInndReq,28,"500x205syntaxx20error,x20commandx20
SF:unrecognizedvrn")%r(STPOptions,28,"500x205syntaxx20error,x20commandx
SF:20unrecognizedvrn")%r(LANDesk-RC,28,"500x205syntaxx20error,x20commen
```



```

SF:0command\x20unrecognized\r\n")\r\n(SSLSessionReq,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(TerminalServerCookie,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(TLSsessionReqSF:1,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(Kerberos,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(SMBProSF:0gleg,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(X11SF:0Probe,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(FoSF:0ur0hFourRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(LPDString,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(LDAPSearchReq,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(LDAPBindReq,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(SIPoptions,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(LANDesk-KC,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(TerminalServer,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(NCP,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(NotesRPC,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(JavaRMI,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(WMSRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(oracle-tns,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(as-sql-s,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")\r\n(ftp,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone[WAP/webcam/printer/game console
Running: Astra embedded, Apple embedded, GoPro embedded, Konica Minolta embedded, Ouya embedded
OS CPE: cpe:/h:astra67311 cpe:/h:appleairport.express cpe:/h:gooprother03 cpe:/h:konicaminolta.bizhub.250
OS details: Astra 67311 VoIP phone or Apple AirPort Express WAP, GoPro HERO3 camera, Konica Minolta bizhub 250 printer, OUYA game console
Network Distance: 11 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 ... 10
11 14.40 ms server-13-225-0-4.sns2.r.cloudfront.net (13.225.0.4)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3046.48 seconds

```

Finding open ports and running devices on mopub.com

```

[+]--[root@chethi-virtualplatform]~/home/chethi
#nmap -sS -A -p- -T4 -oN mopub.txt mopub.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 15:23 +0530
Nmap scan report for mopub.com (192.48.236.12)
Host is up (0.018s latency).
Other addresses for mopub.com (not scanned): 192.48.236.11 192.48.236.9 192.48.236.10
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  tcpwrapped
|_smtp-comands: Couldn't establish connection on port 25
80/tcp    open  http      tsa_b
|_http-server-header: tsa_b
|_fingerprint-strings:
|_DNSVersionIndReqTCP:
|_HTTP/1.1 400 Bad Request
|_content-length: 11
|_content-type: text/plain
|_x-connection-hash: 3c3dfa45acc9b01ebdea67d979e9913f4cf52426d01c86b0065744ba167826be
|_date: Mon, 11 Oct 2021 10:44:57 GMT
|_server: tsa_b
|_connection: close
|_Request
|_Four0hFourRequest:
|_HTTP/1.0 400 Bad Request
|_x-connection-hash: aa18bae729d1567e538a346cf2962dc612c760b708acce15b214475eaf74ca
|_date: Mon, 11 Oct 2021 10:44:49 GMT
|_server: tsa_b
|_connection: close
|_content-length: 0
|_GetRequest:
|_HTTP/1.0 400 Bad Request
|_x-connection-hash: 466622ec70ac10f2d01c2ba142df27b0b3825cc7edffea8947470360227012f
|_date: Mon, 11 Oct 2021 10:44:43 GMT
|_server: tsa_b
|_connection: close
|_content-length: 0
|_HTTPOptions:
|_HTTP/1.0 400 Bad Request
|_x-connection-hash: 291b178c6cb8990af9f333e5799540e0d214e3e2c40df24c5cf301c7961e2b0
|_date: Mon, 11 Oct 2021 10:44:44 GMT
|_server: tsa_b
|_connection: close
|_content-length: 0
|_RPCCheck:
|_HTTP/1.1 400 Bad Request
|_content-length: 11

```

```

|_HTTP/1.1 400 Bad Request
|_content-length: 11
|_content-type: text/plain
|_x-connection-hash: 55f1dd6dd233f1b050c095faa92207349c5b380304435ac753d1544aa67b1cd
|_date: Mon, 11 Oct 2021 10:44:55 GMT
|_server: tsa_b
|_connection: close
|_Request
|_RTSPRequest:
|_HTTP/1.1 400 Bad Request
|_content-length: 11
|_content-type: text/plain
|_x-connection-hash: e6c5ced4042a5d3930715773ed019ee6ce5917b77c0ae711378598b4efe8dd25
|_date: Mon, 11 Oct 2021 10:44:46 GMT
|_server: tsa_b
|_connection: close
|_Request
|_X11Probe:
|_HTTP/1.1 400 Bad Request
|_content-length: 11
|_content-type: text/plain
|_x-connection-hash: aa8c7fa2ec01eb1e44cf90879486448f04dcee678038e12ea1421df682d1de95
|_date: Mon, 11 Oct 2021 10:44:47 GMT
|_server: tsa_b
|_connection: close
|_Request
|_http-title: Did not follow redirect to https://www.mopub.com/
|_403/tcp open  ssl/https tsa_b
|_tls-alpn:
|_h2
|_http/1.1
|_http-title: Did not follow redirect to https://www.mopub.com/
|_ssl-date: TLS randomness does not represent time
|_fingerprint-strings:
|_DNSVersionIndReqTCP:
|_HTTP/1.1 400 Bad Request
|_content-length: 11
|_content-type: text/plain
|_x-connection-hash: 7a55cc230f33a566f754c0b05171bb3d18b5e2f90582aa26a811d4b38b249e2c
|_date: Mon, 11 Oct 2021 10:45:11 GMT
|_server: tsa_b
|_connection: close
|_Request
|_Four0hFourRequest:
|_HTTP/1.0 400 Bad Request
|_x-connection-hash: 40d7367b7bee34b957f69f0210bf1907de4278667f62fb7f02b0d50c1a13d0

```

[illegible]

```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3253.71 seconds
```

```
[root@chealth-virtualplatform ~]# nmap -sS -sV -iL ip.txt -oN nmap.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 15:23 +0530
Failed to resolve "snappytv.com".
WARNING: No targets were specified, so 0 hosts scanned. (0.00s/1s)
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.93 seconds (0.00s/1s)
```

```
[~] [root@chaitin-virtualplatform: ~]# nmap -v
```

```
Nmap scan report for twitterflightschool.com
Host: 35.155.103.137
OS: Linux 3.10 (Ubuntu 12.04 LTS)
Nmap scan report for twitterflightschool.com (not scanned): 54.212.7.6
DNS record for 35.155.103.137: ec2-35-155-103-137.us-west-2.compute.amazonaws.com
Not shown: 65531 filtered tcp ports (no-response)
```

```
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  HTTPS
|_ ssh-hostkey: 1022:9c:1d:2e:1f:1a:26:15:b6:62:a3:27:2e:47:2e (ED25519)
|_ 2048 17:21:60:3f:6f:5c:82:b4:4c:c7:8b:b4:c0:7:63:97:9f (RSA)
|_ 256 e3:40:d0:e4:75:bd:08:62:13:7b:00:dd:2d:4a:1a:63:6c (ECDSA)
|_ 256 b0:d3:b4:b7:73:f1:a2:26:15:b6:62:a3:27:2e:47:2e (ED25519)
|_ tcp_open: tcpwrapped
|_ smtp_commands: Couldn't establish connection on port 25
80/tcp    open  Apache httpd 2.4.6 ((CentOS)) OpenSSL/1.0.2k-fips
|_ http-title: Did not follow redirect to https://twitterflightschool.com/
|_ http-server-header: Apache/2.4.6 ((CentOS)) OpenSSL/1.0.2k-fips
443/tcp   open  ssl/http
|_ http-title: Did not follow redirect to https://www.twitterflightschool.com/
|_ http-server-header: Apache/2.4.6 ((CentOS)) OpenSSL/1.0.2k-fips
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=twitterflightschool.org/organizationName=Twitter, Inc./stateOrProvinceName=California/countryName=US
|_ Subject Alternative Name: DNS:twitterflightschool.com, DNS:www.twitterflightschool.com, DNS:puplicis.twitterflightschool.com, DNS:tppg.twitterflightschool.com
|_ Not valid before: 2021-08-04T00:00:00
|_ Not valid after: 2022-08-03T23:59:59
Warning: OS detection may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 7 hops
```

```
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 ... 2
3 12.72 ms 100.89.0.1
4 16.33 ms 100.51.100.146
5 14.91 ms 100.51.100.145
6 13.00 ms 222.165.177.134
7 12.88 ms ec2-35-155-103-137.us-west-2.compute.amazonaws.com (35.155.103.137)
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 3297.48 seconds

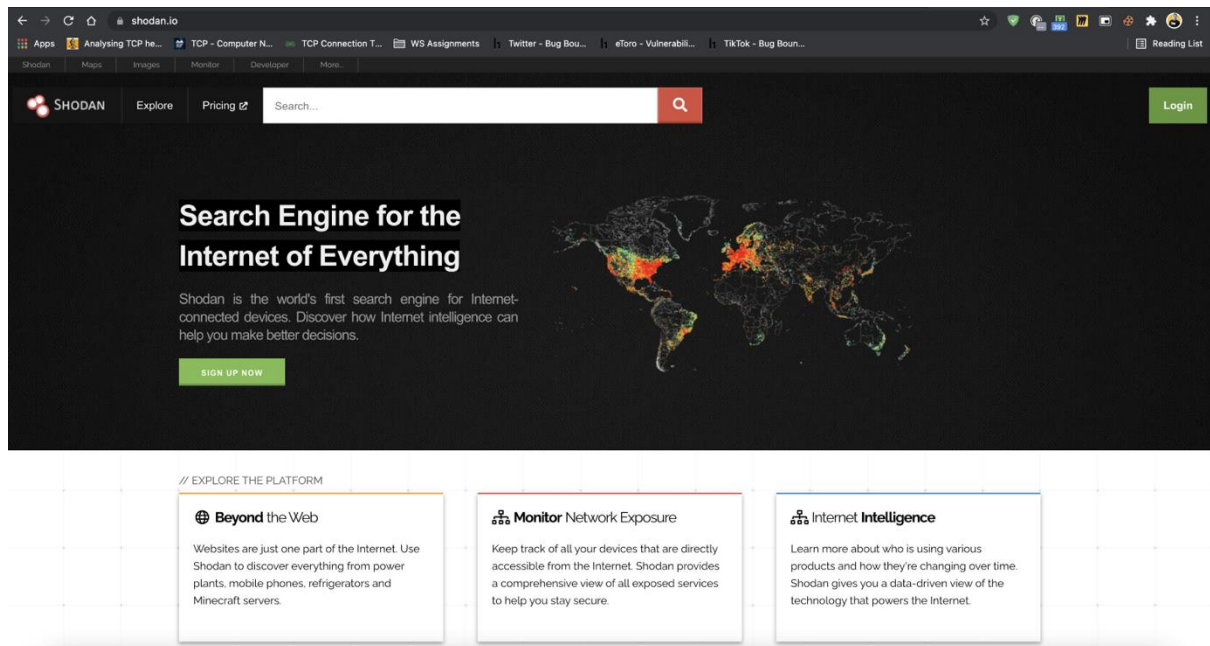
```
[root@chethi-vmwarevirtualplatform]~# nmap -sS -A -p - -T4 -oN twimg.txt twimg.com
Starting Nmap 7.92 (https://nmap.org) at 2021-10-11 15:23 +0530
Nmap scan report for twimg.com
Host: twimg.com [104.24.192.100]
OS: Linux 3.10 (Ubuntu)
Nmap done: 0 IP addresses (0 hosts up) scanned in 3.77 seconds
```


Public Device Enumeration

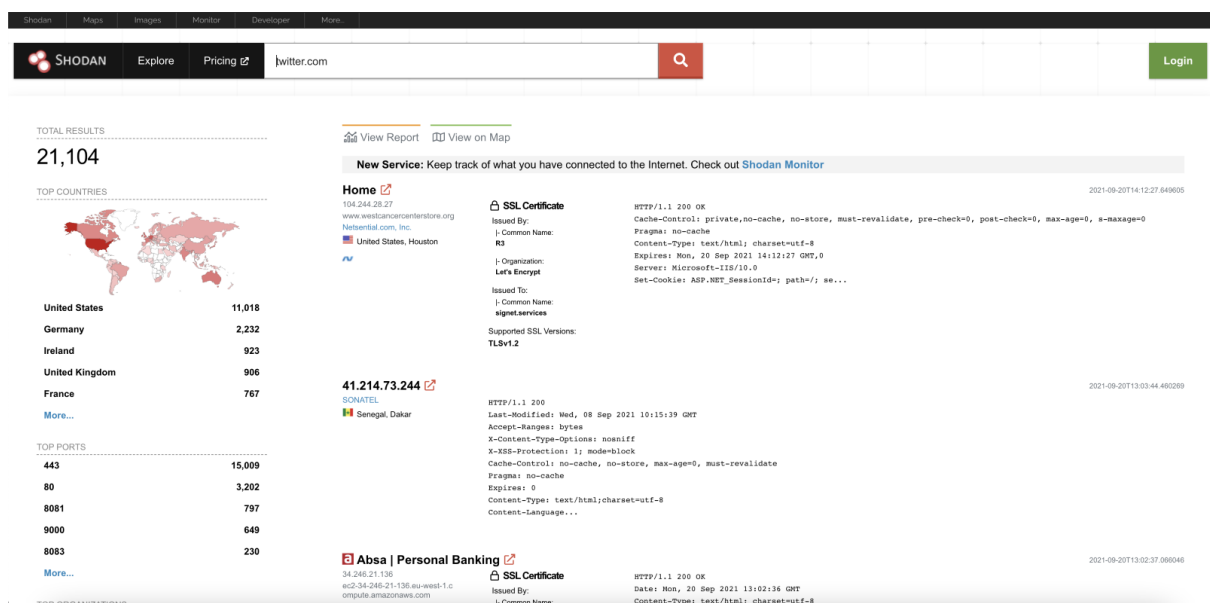
Shodan.io

Shodan.io is one of the most popular search engines used to find devices which are connected over the internet. The main difference between Shodan and google is, Google used to find webpages and Shodan tries to find devices which are connected over a public IP address.

Website Link: <https://www.shodan.io/>



We use shodan.io to collect details about web server and other relevant information about the target.



Shodan
Maps
Images
Monitor
Developer
More...

SHODAN
Explore
Pricing
Search...

104.244.28.27
Regular View
Raw Data
History

Houston

Login

© OpenMapTiles Satellite | © MapTiler | © OpenStreetMap contributors

// LAST UPDATE: 2021-09-20

General Information

Hostnames
www.westcancercenterstore.org

Domains
WESTCANCERCENTERSTORE.ORG

Country
United States

City
Houston

Organization
Netsential.com, Inc.

ISP
YHC Corporation

ASN
AS3900

Open Ports

80
443

// 80 / TCP

-70537096 | 2021-09-14T19:08:01.627626

Microsoft IIS httpd 10.0

HTTP/1.1 301 Moved Permanently
Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0, max-age=0, s-maxage=0
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Expires: 0
Location: https://104.244.28.27/
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Date: Tue, 14 Sep 2021 19:08:00 GMT
Content-Length: 145

// 443 / TCP

-684054404 | 2021-09-20T14:12:27.649605

Web Technologies

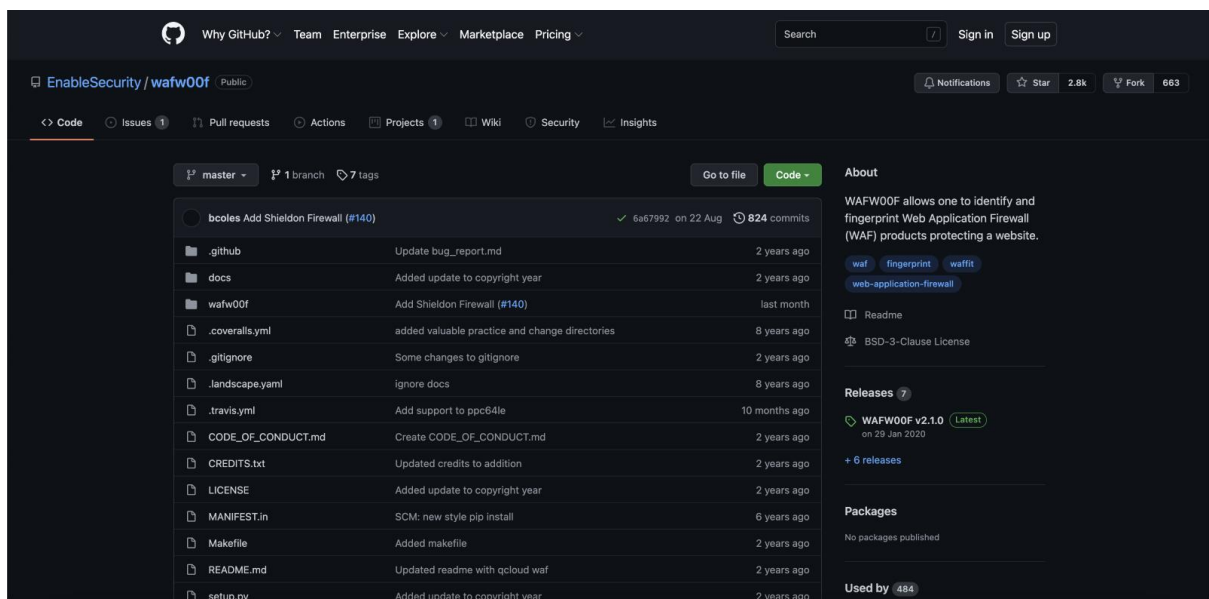
Check The Status of Firewall Protection In Target Domains

For this check-up I used wafw00f tool.

Wafw00f

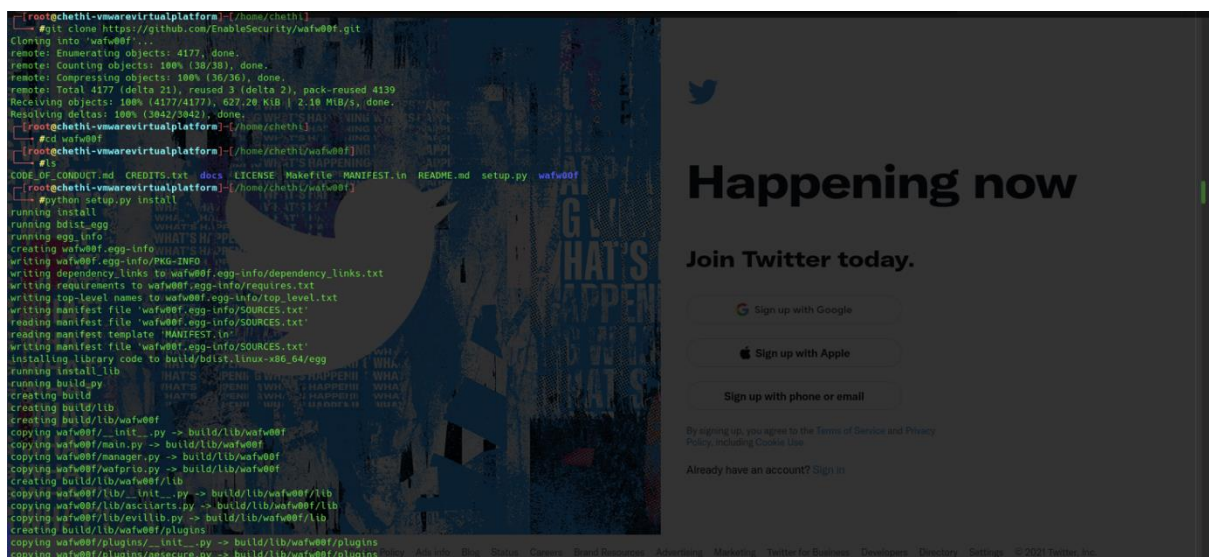
Wafw00f is one of the widely used web application firewall detection tool. Wafw00f is a python tool, and it finds firewalls of web applications by analysing the responses. First, I installed that tool to my machine. To do that I have cloned wafw00f from GitHub.

GitHub Link: <https://github.com/EnableSecurity/wafw00f>



The screenshot shows the GitHub repository page for 'wafw00f' by 'EnableSecurity'. The repository is public and has 2.8k stars and 663 forks. The file list on the left includes: .github, docs, wafw00f, .coveralls.yml, .gitignore, .landscape.yml, .travis.yml, CODE_OF_CONDUCT.md, CREDITS.txt, LICENSE, MANIFEST.in, Makefile, README.md, and setup.py. The right sidebar shows the repository's description, a README link, BSD-3-Clause license, releases (WAFW00F v2.1.0), and packages (no packages published).

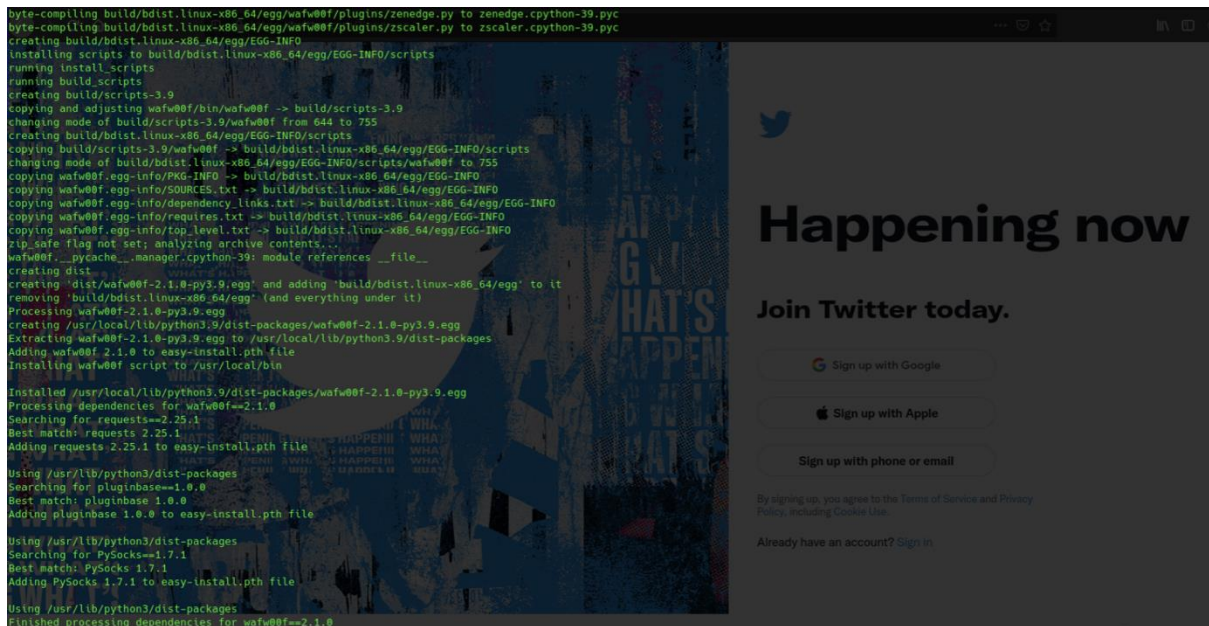
Then I have followed below steps to complete the installation process.



The screenshot shows a terminal window with the following commands and output:

```
[root@chethi-vmwarevirtualplatform] ~/home/chethi
# git clone https://github.com/EnableSecurity/wafw00f.git
Cloning into 'wafw00f'...
remote: Enumerating objects: 4177, done.
remote: Counting objects: 100% (38/38), done.
remote: Compressing objects: 100% (36/36), done.
remote: Total 4177 (delta 21), reused 3 (delta 2), pack-reused 4139
Receiving objects: 100% (4177/4177), 627.20 KiB | 2.10 MiB/s, done.
Resolving deltas: 100% (3942/3942), done.
# cd wafw00f
# python setup.py install
running install
running egg_info
creating wafw00f.egg-info
writing wafw00f.egg-info/PKG-INFO
writing dependency links to wafw00f.egg-info/dependency_links.txt
writing requirements to wafw00f.egg-info/requirements.txt
writing top-level names to wafw00f.egg-info/top_level.txt
writing manifest file 'wafw00f.egg-info/SOURCES.txt'
reading manifest file 'wafw00f.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
writing manifest file 'wafw00f.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
running install_lib
creating build
creating build/lib
creating build/lib/wafw00f
copying wafw00f/_init_.py -> build/lib/wafw00f
copying wafw00f/main.py -> build/lib/wafw00f
copying wafw00f/manager.py -> build/lib/wafw00f
copying wafw00f/wafw00f.py -> build/lib/wafw00f
creating build/lib/wafw00f/lib
copying wafw00f/lib/_init_.py -> build/lib/wafw00f/lib
copying wafw00f/lib/asciart.py -> build/lib/wafw00f/lib
copying wafw00f/lib/evil.py -> build/lib/wafw00f/lib
creating build/lib/wafw00f/plugins
copying wafw00f/plugins/_init_.py -> build/lib/wafw00f/plugins
copying wafw00f/plugins/secure.py -> build/lib/wafw00f/plugins
```

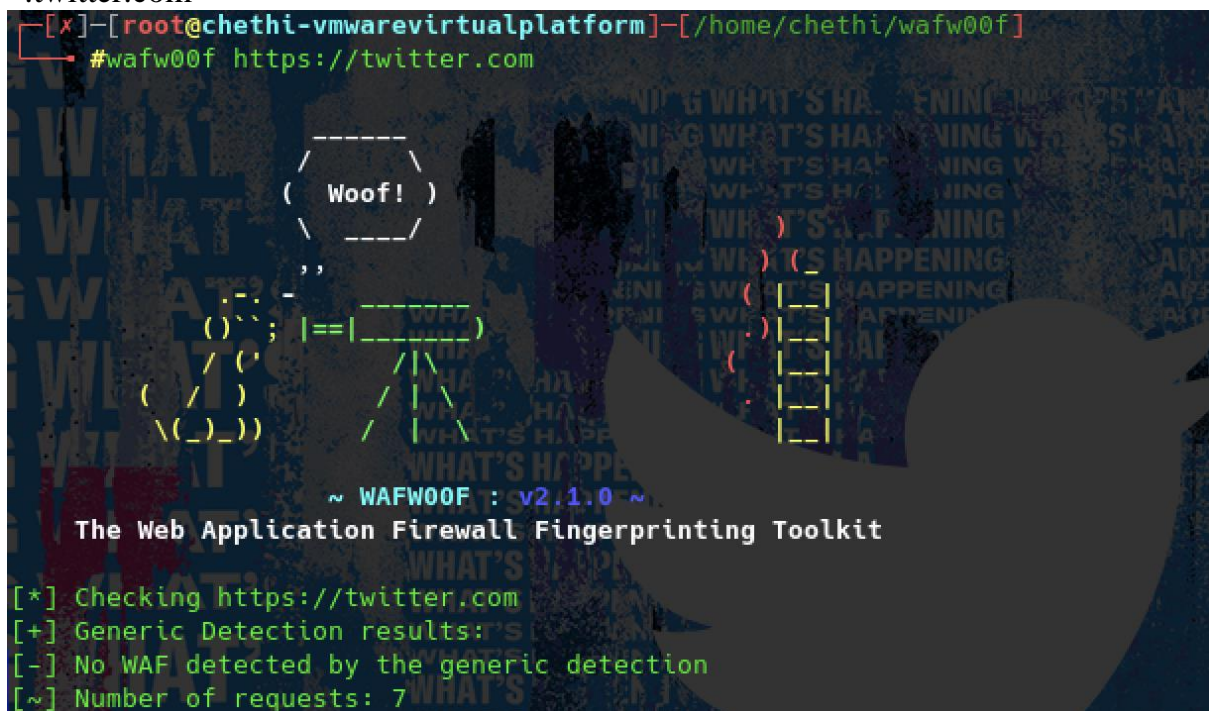
Overlaid on the terminal is a Twitter sign-up overlay with the text 'Happening now', 'Join Twitter today.', and options to sign up with Google, Apple, or phone/email. It also includes a link to sign in if the user already has an account.



After completing the installation process. I have entered my in-scope domains to check the status of firewall detection.

Results of wafw00f

*.twitter.com




```
[root@chethi-vmwarevirtualplatform]--[ /home/chethi/wafw00f ]
```

```
#wafw00f https://vine.co
```

```
( WOOF! )
```

```
' , _ _ _ _  
| |   // --  
/' " -//  
/*====*/  
/_/ \_/  
|| \_/ \  
\\ \_  
\_/\_\_
```

```
404 Hack Not Found  
  
X X X X X  
X X X X X    405 Not Allowed  
X X X X X  
  
X X X X X    403 Forbidden  
X X X X X  
  
502 Bad Gateway      500 Internal Error  
X X X X X  
X X X X X
```

```
~ WAFW00F : v2.1.0 ~
```

```
The Web Application Firewall Fingerprinting Toolkit
```

```
[*] Checking https://vine.co  
[+] Generic Detection results:  
[-] No WAF detected by the generic detection  
[~] Number of requests: 7
```

```
[root@chethi-vmwarevirtualplatform]--[/home/chethi/wafw00f]
#wafw00f https://periscope.tv

-----
( Woof! )
\ _____ )
, , _____ ) ( _
) ; |==| _____ ) ( |__|
/ ( ' / \ \ _____ ( |__|
( / ) / | \ \ _____ . |__|
\ ( ) ) / | \ \ _____ |__|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://periscope.tv
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```


gnip.com

```
[root@chethi-vmwarevirtualplatform]--[ /home/chethi/wafw00f]
#wafw00f https://gnip.com

      /-----\
      (   Woof!   )
      \-----/
      ',
      .-. -
      ( )'; |==|-----)
      / ( '      /|\
      ( / )      / | \
      \(_)_ )    /  | \

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://gnip.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

*. pscp.tv

```
[root@chethi-vmwarevirtualplatform]--[ /home/chethi/wafw00f]
#wafw00f https://pscp.tv

      /-----\
      (   Woof!   )
      \-----/
      ',
      .-. -
      ( )'; |==|-----)
      / ( '      /|\
      ( / )      / | \
      \(_)_ )    /  | \

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://pscp.tv
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

mopub.com

```
[root@chethi-vmwarevirtualplatform]~[~/home/chethi/wafw00f]
#wafw00f https://mopub.coms
( Woof! )
404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://mopub.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

*.twimg.com

This domain output error.

```
[root@chethi-vmwarevirtualplatform]~[~/home/chethi/wafw00f]
#wafw00f https://twimg.com
( Woof! )
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] checking https://twimg.com
ERROR:wafw00f:Something went wrong HTTPSPool(host='twimg.com', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f7414cb5ade>: failed to establish a new connection: [Errno -5] No address associated with hostname'))
ERROR:wafw00f:Site twimg.com appears to be down
```

*.niche.co

This domain output error.

```
[chethi@chethi-vmwarevirtualplatform]~[~/wafw00f]
#wafw00f https://niche.co
( Woof! )
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] checking https://niche.co
ERROR:wafw00f:Something went wrong HTTPSPool(host='niche.co', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f16fb34225b>: failed to establish a new connection: [Errno -3] Temporary failure in name resolution'))
ERROR:wafw00f:Site niche.co appears to be down
```

This domain output error.

*twitterflightschool.com

47

Vulnerability Scanning Tool

Nikto

Nikto is a web scanner which is used to scan web servers. This tool is free and open source. Mainly nikto scans for dangerous files, outdated versions and versions specific problems. However, nikto is not a stealthy web scanning tool because it tests the webserver in the quickest way possible.

To check the in-scope domains I have used `nikto -h <domain>` command structure and to save the results I have modified the command like `nikto -h <domain> -o <name.txt>`. I provided the links to view the output text files in each domain.

Results of Nikto

*.twitter.com

```
[chethi@chethi-vmwarevirtualplatform ~]$ sudo nikto -h https://twitter.com
- Nikto v2.1.6 [chethi@chethi-vmwarevirtualplatform ~]$
-----
+ Target IP: 194.244.42.129
+ Target Hostname: twitter.com
+ Target Port: 443 [chethi@chethi-vmwarevirtualplatform ~]$
-----
+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Twitter, Inc./CN=twitter.com
+ Ciphers: TLS_AES_256_GCM_SHA384
+ Issuer: /C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
+ Start Time: 2021-09-21 10:22:47 (GMT+5:30)
-----
+ Server: tsb.k
+ Cookie personalization_id created without the httponly flag
+ Cookie guest_id created without the httponly flag
+ Retrieved x-poweredby header: Express
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'x-connection-hash' found, with contents: 2f1ccdf4fb2290a61eb1b5105e8afaae47c65d35704e33163215fb02c9d76e9
+ Uncommon header 'cross-origin-embedder-policy' found, with contents: unsafe-none
+ Uncommon header 'expiry' found, with contents: Tue, 21 Mar 1991 05:00:00 GMT
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin-allow-popups
+ The site uses SSL and Expect-CT header is not present.
+ Uncommon header 'x-transaction-id' found, with contents: 71aidd2d729b8159
+ Uncommon header 'perf' found, with contents: 0
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/?escaped_fragment=/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?lang=/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/hashtag/%3c%/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search?q=%23/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/realtime/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/users/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/%3c%/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?ref=src/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?src=/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?followers/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?following/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/account/deactivated/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/settings/deactivated/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?escaped_fragment=/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?lang=/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/hashtag/%3c%/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search?q=%23/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/realtime/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/users/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
```

[Click here to view the output of *.twitter.com](#)

*. vine.co

```
(chethi@chethi-vmwarevirtualplatform)~$  
$nikto -h https://vine.co -o niktovine.txt  
-----  
Nikto v2.1.6  
-----  
+ Target IP: 52.89.87.202  
+ Target Hostname: vine.co [1/1]  
+ Target Port: 443  
-----  
+ SSL Info: Subject: /CN=vine.co  
Ciphers: ECDHE-RSA-AES128-GCM-SHA256  
Issuer: /C=US/O=Amazon/OU=Server CA 18/CN=Amazon  
+ Message: Multiple IP addresses found: 52.89.87.202, 34.216.243.30 [18 CAs]  
+ Start Time: 2021-09-21 11:22:47 (GMT-5)  
-----  
+ Server: No banner retrieved  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The site uses SSL and Expect-CT header is not present.  
+ All CGI directories 'found', use '-C none' to test none  
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html  
+ Server banner has changed from '' to 'awselb/2.0' which may suggest a NAF, load balancer or proxy is in place.  
+ Allowed HTTP Methods: HEAD, OPTIONS, GET  
+ /cgi/cgi/cart32.exe: request cart32.exe/cart32clientlist: 1001 85-00-88 GMT  
+ /webcgi/cart32.exe: request cart32.exe/cart32clientlist: content: Same-origin-allow-pseudo  
+ /cgi-914/cart32.exe: request cart32.exe/cart32clientlist  
+ /cgi-915/cart32.exe: request cart32.exe/cart32clientlist /salm0202/000159  
+ /bin/cart32.exe: request cart32.exe/cart32clientlist  
+ /cgi/cart32.exe: request cart32.exe/cart32clientlist: all possible dirs  
+ /webcgi/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-bin/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /aws-bin/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-sys/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-local/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /h/bin/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgibin/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgis/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /scripts/cart32.exe: request cart32.exe/cart32clientlist: redirect HTTP code (200)  
+ /cgi-win/cart32.exe: request cart32.exe/cart32clientlist: redirect HTTP code (200)  
+ /cgi-bin/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-exe/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-home/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-perl/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-bin/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-bin/sdb/cart32.exe: request cart32.exe/cart32clientlist: redirect HTTP code (200)  
+ /cgi-mid/cart32.exe: request cart32.exe/cart32clientlist: forbidden or redirect HTTP code (200)  
+ /cgi-cgi/classified.cgi: Check Phrack 55 for info by RFP: forbidden or redirect HTTP code (200)  
+ /webcgi/classified.cgi: Check Phrack 55 for info by RFP: forbidden or redirect HTTP code (200)  
+ /cgi-914/classified.cgi: Check Phrack 55 for info by RFP: forbidden or redirect HTTP code (200)  
-----  
+ 1 host(s) tested
```

[Click here to view the output of *. vine.co](#)

*. periscope.tv

```
(chethi@chethi-vmwarevirtualplatform)~$  
$nikto -h https://periscope.tv -o niktoperiscope.txt  
-----  
Nikto v2.1.6  
-----  
+ Target IP: 54.169.149.15  
+ Target Hostname: periscope.tv  
+ Target Port: 443  
-----  
+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Twitter, Inc./CN=*.periscope.tv  
Ciphers: ECDHE-RSA-AES128-GCM-SHA256  
Issuer: /C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1  
+ Message: Multiple IP addresses found: 54.169.149.15, 13.251.195.231  
+ Start Time: 2021-09-21 11:30:08 (GMT-5)  
-----  
+ Server: No banner retrieved  
+ X-Frame-Options header is set to allow framing from https://twitter.com/. This does not have full cross-browser support (only in IE and Firefox) and may lead to the header being ignored.  
+ Uncommon header 'x-ratelimit-remaining' found, with contents: 2999  
+ Uncommon header 'x-ratelimit-limit' found, with contents: 3000  
+ Uncommon header 'x-periscope-web-version' found, with contents: 3  
+ The site uses SSL and Expect-CT header is not present. It may suggest a NAF, load balancer or proxy is in place.  
+ Root page / redirects to: https://www.periscope.tv/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to / over HTTP/1.0. The value is "172.17.7.86".  
+ Server is using a wildcard certificate: *.periscope.tv  
+ /.well-known/assetlinks.json: Google Asset Links Specification file may contain server info, per RFC-5785. See https://github.com/google/digitalassetlinks/blob/master/well-known/details.md  
+ 7790 requests: 0 error(s) and 8 item(s) reported on remote host  
+ End Time: 2021-09-21 12:04:34 (GMT-5) (2866 seconds)  
-----  
+ 1 host(s) tested
```

[Click here to view the output of *. periscope.tv](#)

*. pscp.tv

```
(chethi@chethi-vmwarevirtualplatform)~$  
$nikto -h https://pscp.tv -o niktopsctp.txt  
-----  
Nikto v2.1.6  
-----  
+ Target IP: 13.234.236.39  
+ Target Hostname: pscp.tv  
+ Target Port: 443  
-----  
+ SSL Info: Subject: /CN=*.pscp.tv  
Ciphers: ECDHE-RSA-AES128-GCM-SHA256  
Issuer: /C=US/O=Amazon/OU=Server CA 18/CN=Amazon SHA256 2020 CA1  
+ Message: Multiple IP addresses found: 13.234.236.39, 15.206.128.225  
+ Start Time: 2021-09-21 11:31:29 (GMT-5)  
-----  
+ Server: No banner retrieved  
+ X-Frame-Options header is set to allow framing from https://twitter.com/. This does not have full cross-browser support (only in IE and Firefox) and may lead to the header being ignored.  
+ Uncommon header 'x-periscope-web-version' found, with contents: 3  
+ Uncommon header 'x-ratelimit-limit' found, with contents: 3000  
+ Uncommon header 'x-ratelimit-remaining' found, with contents: 2999  
+ The site uses SSL and Expect-CT header is not present.  
+ Root page / redirects to: https://www.pscp.tv/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to / over HTTP/1.0. The value is "172.27.17.47".  
+ Server is using a wildcard certificate: *.pscp.tv  
+ /.well-known/assetlinks.json: Google Asset Links Specification file may contain server info, per RFC-5785. See https://github.com/google/digitalassetlinks/blob/master/well-known/details.md  
+ 7788 requests: 0 error(s) and 8 item(s) reported on remote host  
+ End Time: 2021-09-21 12:11:05 (GMT-5) (2376 seconds)  
-----  
+ 1 host(s) tested
```

[Click here to view the output of *. pscp.tv](#)

*.twimg.com

```
[chethi@chethi-vmwarevirtualplatform]~$  
$nikto -h https://twimg.com -o niktotwimg.txt  
- Nikto v2.1.6  
-----  
+ ERROR: Invalid IP: 13.234.236.39
```

[Click here](#) to view the output of *.twimg.com

gnip.com

```
[chethi@chethi-vmwarevirtualplatform]~$  
$nikto -h https://gnip.com -o niktognip.txt  
- Nikto v2.1.6  
-----  
+ Target IP: 52.84.228.47  
+ Target Hostname: gnip.com  
+ Target Port: 443  
+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Twitter, Inc./CN=*.gnip.com  
+ Message: Header: Multiple IP addresses found: 52.84.228.47, 52.84.228.58, 52.84.228.73, 52.84.228.20  
+ Start Time: 2021-09-21 11:36:16 (GMT-5)  
+ Servers: AmazonS3  
+ Retrieved via header: 1:1 3227fbd0d40d1d78aad88753ced298.cloudfront.net (CloudFront)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.  
+ Uncommon header 'x-amz-cf-pop' found, with contents: SIN2-C1  
+ Uncommon header 'x-amz-cf-id' found, with contents: VzB_v9942f30z3Ga0tJJq2jQem-1NWw90sms3cr73TU-bbu0P2SueA==  
+ Uncommon header 'x-cache' found, with contents: Hit from cloudfront  
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.  
+ The site uses SSL and Expect-CT header is not present.  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Root page / redirects to: https://developer.twitter.com/en/enterprise  
+ Uncommon header 'x-edge-origin-shield-skipped' found, with contents: 0  
+ No CGI Directories found (use '-c all' to force check all possible dirs)  
+ Server banner has changed from 'AmazonS3' to 'CloudFront' which may suggest a WAF, load balancer or proxy is in place  
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:140BF10B:SSL routines:ssl3_get_record:wrong version number at /var/lib/nikto/plugins/LW2.pm line 5157.  
+ Scan terminated: 20 error(s) and 10 item(s) reported on remote host  
+ End Time: 2021-09-21 11:39:23 (GMT-5) (167 seconds)  
+ 1 host(s) tested
```

[Click here](#) to view the output of gnip.com

mopub.com

```
[chethi@chethi-vmwarevirtualplatform]~$  
$nikto -h https://mopub.com -o niktomopub.txt  
- Nikto v2.1.6  
-----  
+ Target IP: 192.48.236.12  
+ Target Hostname: mopub.com  
+ Target Port: 443  
+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Twitter, Inc./CN=*.mopub.com  
+ Message: Header: Multiple IP addresses found: 192.48.236.12, 192.48.236.11, 192.48.236.10, 192.48.236.9  
+ Start Time: 2021-09-21 11:37:37 (GMT-5)  
+ Servers: tso.B  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ Uncommon header 'x-connection-hash' found, with contents: 72431ac8b58c5ef356cd067a03676423c88f2e93d807cc6c83466fa412241dcd  
+ The site uses SSL and Expect-CT header is not present.  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Root page / redirects to: https://www.mopub.com/  
+ No CGI Directories found (use '-c all' to force check all possible dirs)  
+ Server is using a wildcard certificate: *.mopub.com  
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: Invalid argument  
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host  
+ End Time: 2021-09-21 11:48:19 (GMT-5) (642 seconds)  
+ 1 host(s) tested
```

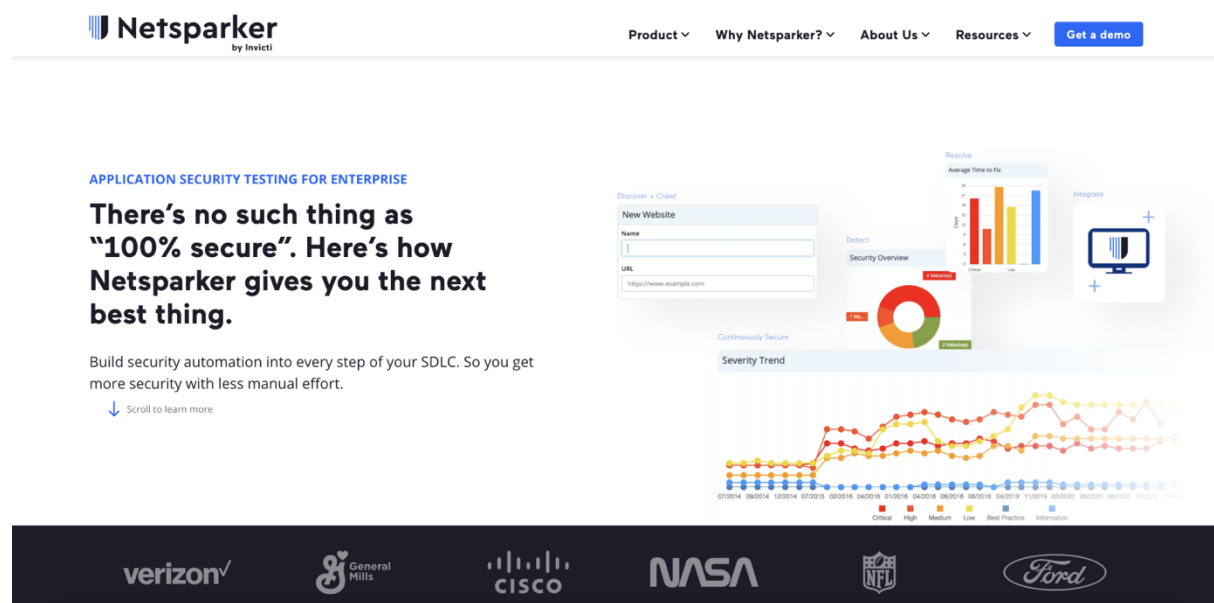
[Click here](#) to view the output of mopub.com

Netsparker

Netsparker is one of the widely used vulnerability identification tool among pen testers and bug bounty hunters. Netsparker is web application security solution which is used to identify vulnerabilities automatically. It is first released to the market in the 2009. Ferruh Mavituna is the founder and current CEO of the Netsparker.

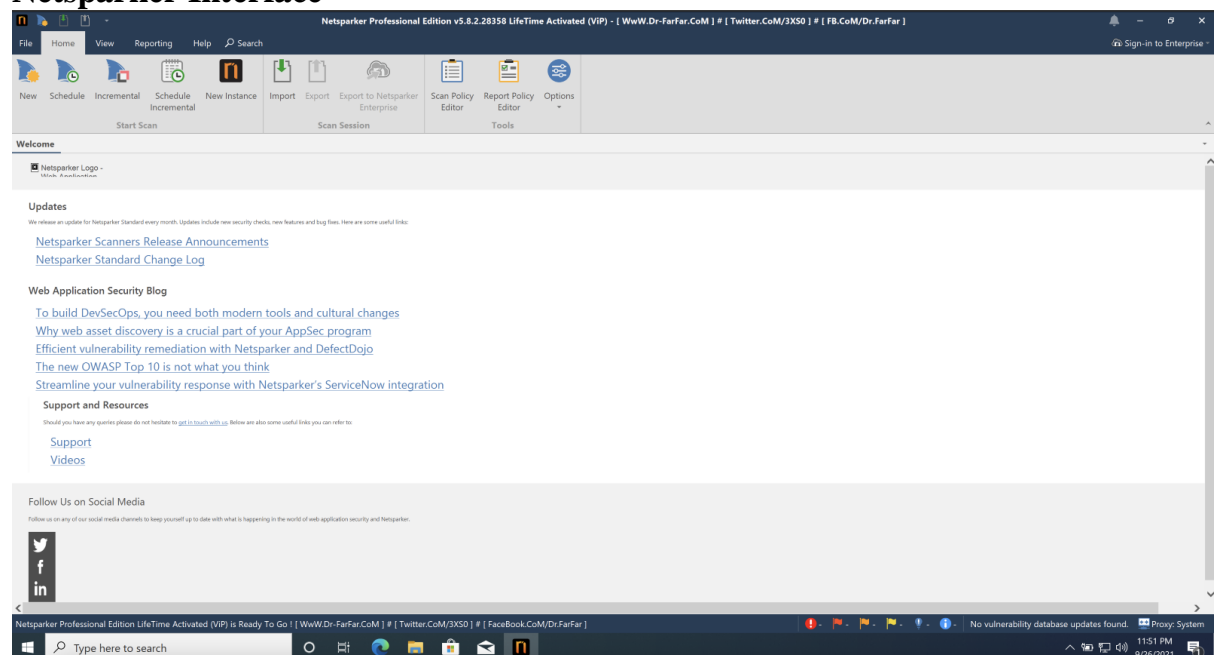
This tool is very popular because we do not want have access to source code, do not need to install an agent or specialized software. Netsparker is available as desktop software and it available as multi-user cloud-based service.

Link: <https://www.netsparker.com/product/>



The image shows the Netsparker website landing page. At the top, there is a navigation bar with the Netsparker logo (by invicti) on the left and links for Product, Why Netsparker?, About Us, Resources, and a Get a demo button on the right. The main content area features a large heading: "APPLICATION SECURITY TESTING FOR ENTERPRISE" followed by the text "There's no such thing as '100% secure'. Here's how Netsparker gives you the next best thing." Below this, it says "Build security automation into every step of your SDLC. So you get more security with less manual effort." and a "Scroll to learn more" link. To the right, there are several charts and graphs: a "Discover + Crawl" section with a "New Website" form, a "Detect" section with a "Security Overview" donut chart, a "Resolve" section with a bar chart titled "Average Time to Fix", and a "Severity Trend" line graph. At the bottom, there is a dark banner with logos for Verizon, General Mills, Cisco, NASA, NFL, and Ford.

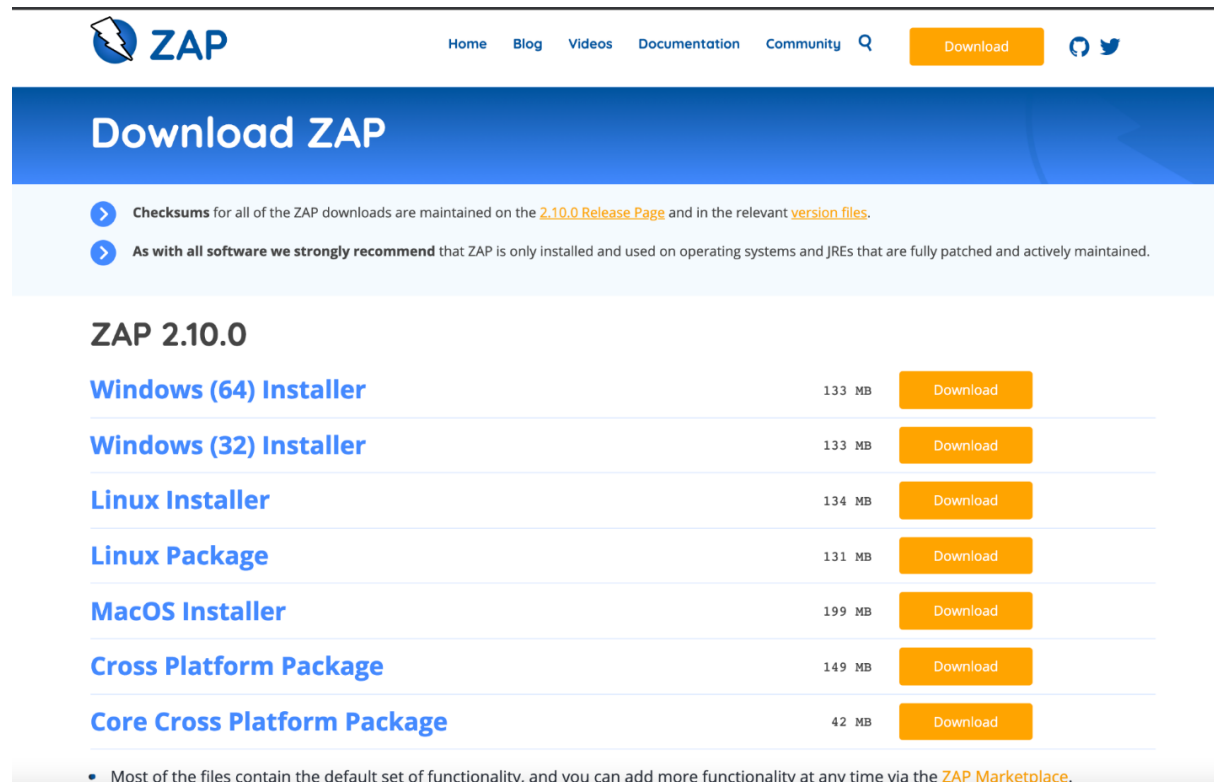
Netsparker Interface



The image shows the Netsparker Professional Edition v5.8.2.28358 interface. The top bar displays the version and activation status: "Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (VIP) - [WwW.Dr.FarFar.CoM] # [Twitter.CoM/3XS0] # [FB.CoM/Dr.FarFar]". Below this is a menu bar with File, Home, View, Reporting, Help, and Search. The main toolbar contains icons for New, Schedule, Incremental, New Instance, Import, Export, Export to Netsparker Enterprise, Scan Policy Editor, Report Policy Editor, and Options. The main content area is titled "Welcome" and contains sections for Updates, Web Application Security Blog, and Support and Resources. The bottom status bar shows "Netsparker Professional Edition LifeTime Activated (VIP) is Ready To Go [WwW.Dr.FarFar.CoM] # [Twitter.CoM/3XS0] # [Facebook.CoM/Dr.FarFar]" and a system tray with a clock showing 11:51 PM on 9/26/2021.

OWASP ZAP

Like Netsparker, OWASP ZAO is also one of widely used web app scanner. You can download OWASP ZAP by going to [this link](#). Then you can choose the correct download file according to your operating system.



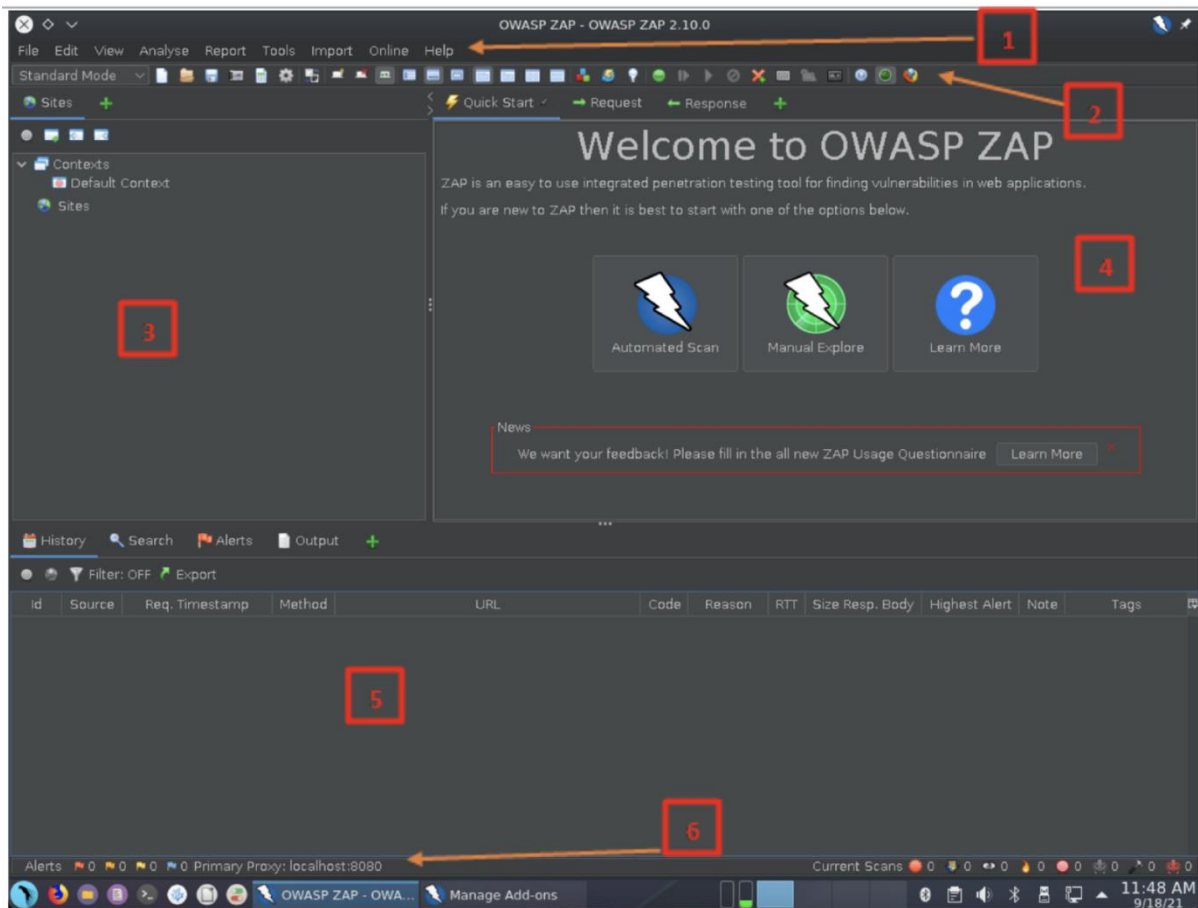
The screenshot shows the OWASP ZAP download page. At the top, there is a navigation bar with links for Home, Blog, Videos, Documentation, and Community, along with a search icon and a 'Download' button. Below the navigation bar is a large blue banner with the text 'Download ZAP'. Underneath the banner, there are two informational points: 'Checksums for all of the ZAP downloads are maintained on the 2.10.0 Release Page and in the relevant version files.' and 'As with all software we strongly recommend that ZAP is only installed and used on operating systems and JREs that are fully patched and actively maintained.' Below this, the section 'ZAP 2.10.0' is displayed. It contains a table of download links for various operating systems and packages, each with a 'Download' button and the file size in MB.

Operating System / Package	File Size (MB)	Download Button
Windows (64) Installer	133 MB	Download
Windows (32) Installer	133 MB	Download
Linux Installer	134 MB	Download
Linux Package	131 MB	Download
MacOS Installer	199 MB	Download
Cross Platform Package	149 MB	Download
Core Cross Platform Package	42 MB	Download

• Most of the files contain the default set of functionality, and you can add more functionality at any time via the [ZAP Marketplace](#).

First, let's look at what OWASP ZAP is. OWASP ZAP is an open-source web application security scanner. The main goal of Zap is to allow easy penetration testing to find the vulnerabilities in web applications. It is one of the most widely used web app scanners in the world. Both beginners and pentester experts use OWASP ZAP.

After installing OWASP ZAP to the Parrot OS, we can open it, and its interface will look like this.



1. Menu bar - This bar is used to access automated and manual tools.
2. Toolbar - This provides easy access to commonly used access.
3. Tree Window - Displays the Sites tree and the Scripts tree.
4. Workspace window - Show requests, responses, and scripts and allow editing of them.
5. Information Window - Show all the information of automated and manual tools.
6. Footer - Show summary of the alerts.

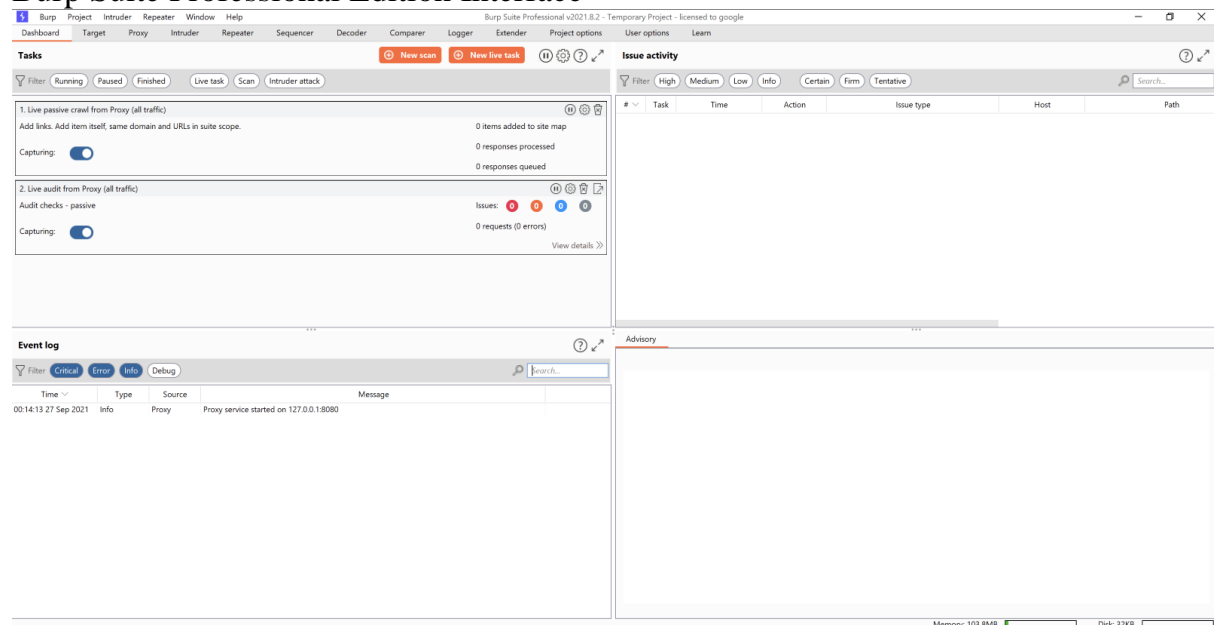
Burp Suite Professional

As we discussed before Burp Suite is another set of tools which used for penetration testing of web apps. PortSwigger has developed this tool. Mainly burp suite has three editions and they are community edition, professional edition, enterprise edition. Community edition is available free and we have to pay subscription fee for professional and enterprise editions.

Link: <https://portswigger.net/burp>



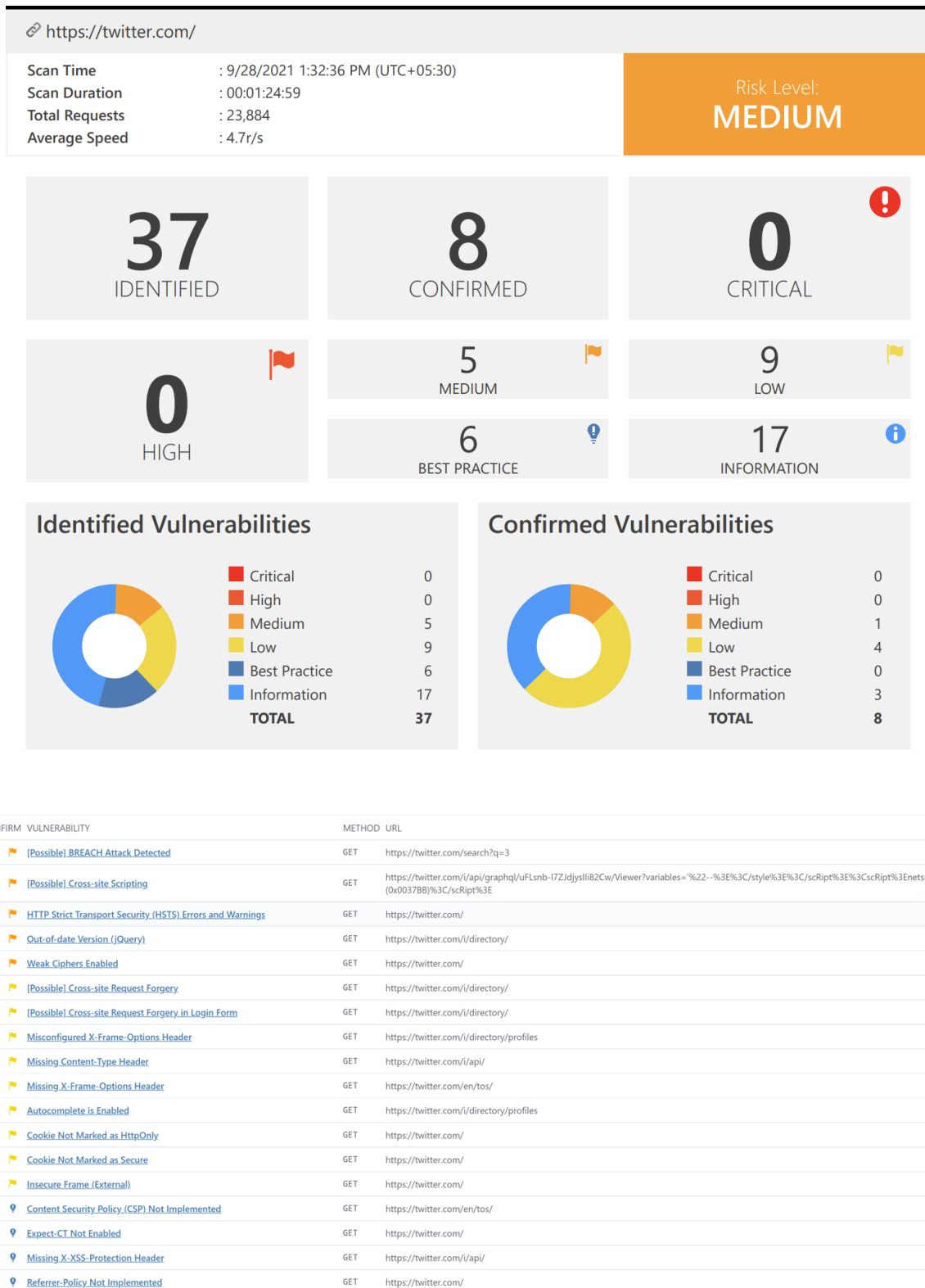
Burp Suite Professional Edition Interface



Vulnerability Scanning

To the vulnerability scanning purpose I have used Netsparker professional version.

Vulnerability Summary



🔍	🔗	Referrer-Policy Not Implemented	GET	https://twitter.com/	0
🔍	🔗	SameSite Cookie Not Implemented	GET	https://twitter.com/i/js_inst?c_name=ui_metrics	0
🔍	🔗	Subresource Integrity (SRI) Not Implemented	GET	https://twitter.com/	5
🔍	🔗	[Possible] Internal Path Disclosure (Windows)	GET	https://twitter.com/c/5.js	9
🔍	🔗	[Possible] Login Page Identified	GET	https://twitter.com/i/directory/profiles	6
🔍	🔗	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://twitter.com/	17
🔍	🔗	Apple's App-Site Association (AASA) Detected	GET	https://twitter.com/.well-known/apple-app-site-association	
🔍	🔗	Content Security Policy (CSP) Nonce Without Matching Script Block	GET	https://twitter.com/en/tos	
🔍	🔗	Crossdomain.xml Detected	GET	https://twitter.com/crossdomain.xml	
🔍	🔗	data: Used in a Content Security Policy (CSP) Directive	GET	https://twitter.com/	
🔍	🔗	Disabled X-XSS-Protection Header	GET	https://twitter.com/	
🔍	🔗	ExpressJS Identified	GET	https://twitter.com/	
🔍	🔗	No Script Block Detected with the Hash Value Declared in Content Security Policy (CSP)	GET	https://twitter.com/en/tos	
🔍	🔗	Nonce Usage Detected in Content Security Policy (CSP) Directive	GET	https://twitter.com/	
🔍	🔗	OpenSearch.xml Detected	GET	https://twitter.com/opensearch.xml	
🔍	🔗	Weak Nonce Detected in Content Security Policy (CSP) Declaration	GET	https://twitter.com/	
🔍	🔗	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://twitter.com/	
🔍	🔗	Autocomplete Enabled (Password Field)	GET	https://twitter.com/i/directory/profiles	
🔍	🔗	Forbidden Resource	GET	https://twitter.com/i/api/	



1.Weak Ciphers Enabled

- Severity: MEDIUM
- Method: GET

Impact

- In some cases, attackers may decode SSL traffic that is transmitted between your server and your visitors.

Vulnerability Details

- While using encrypted communication, Netsparker discovered that weak ciphers were being utilized (SSL).

- When it comes to protecting secure communication with your visitors, you should only allow powerful ciphers on your web server to be used.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take

For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH:AESGCM:EDH:AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- Click Start, click Run, type regedt32 or type regedit, and then click OK.
- In Registry Editor, locate the following registry key: HKEYLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
- Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

2. [Possible] BREACH Attack Detected

- Severity: MEDIUM
- Method: GET

Impact

- In spite of the fact that you are utilizing an SSL/TLS protected connection, an attacker can still monitor the victim's encrypted traffic and cause the victim's computer to submit HTTP requests to the compromised web server by using invisible frames. Using these procedures, an attacker might steal information from the website and use it to carry out the following actions:
 1. Inject partial plaintext they have uncovered into a victim's requests
 2. Measure the size of encrypted traffic

Request

```
1 GET /search?q=3 HTTP/1.1
2 Host: twitter.com
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 Cookie: guest_id=v1%3A163281615778514028; personalization_id="v1_NzNn+YtIZpV1SL1A04rXLg="; gt=1442761652445712387; ct0=e0626f5c0a21dd79a61c77f13676bc12; att=1-GDMKZZOviJHdy3tcof9aMl
8 Referer: https://twitter.com/opensearch.xml
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
10 X-Scanner: Netsparker
```


Response

```
1 HTTP/1.1 200 OK
2 cache-control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
3 expiry: Tue, 31 Mar 1981 05:00:00 GMT
4 transfer-encoding: chunked
5 pragma: no-cache
6 server: tsa_k
7 x-content-type-options: nosniff
8 x-xss-protection: 0
9 cross-origin-embedder-policy: unsafe-none
10 strict-transport-security: max-age=631138519
11 x-frame-options: DENY
12 x-connection-hash: 14eb4d0a380b52fc4420005d9220c024c7e7bf2c9729f6b17d244d72fcbf77a5
13 x-powered-by: Express
14 last-modified: Tue, 28 Sep 2021 08:12:05 GMT
15 content-type: text/html; charset=utf-8
16 cross-origin-opener-policy: same-origin-allow-popups
17 content-security-policy: connect-src 'self' blob: https://*.giphy.com https://*.pscp.tv https://*.video.pscp.tv https://*.twimg.com https://api.twitter.com https://api-stream.twitter.com
18 date: Tue, 28 Sep 2021 08:12:05 GMT
19 content-encoding:
20
21 <!DOCTYPE html>
22 <html dir="ltr" lang="en">
23 <meta charset="utf-8" />
24 <meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0,viewport-fit=cover" /><link rel="preconnect" href="//abs.twimg.com" /><link rel="dns-
25 <meta property="og:site_name" content="Twitter" /><meta name="google-site-verification" content="acY00cR5z6puMzLn6hLDZ1lnNHXPt570Istz1vnCV0" /><meta name="facebook-domain-verify
26 <meta name="apple-mobile-web-app-title" content="Twitter" />
27 <meta name="apple-mobile-web-app-status-bar-style" content="white" />
28
29 <meta name="apple-mobile-web-app-title" content="Twitter" />
30 <meta name="apple-mobile-web-app-status-bar-style" content="white" />
31 <meta name="theme-color" content="#ffffff" />
32 <meta http-equiv="origin-trial" content="Apin4chgTX+4eFXKD+ErQlKRB/VtZ/dvnLf9Y9Nen15r1xJcf81alryTHYQiuU1z9Q49MqGXqya1SmqWzHJqQAAABneyJvcmlnaW410iJodHRwczovL3R3aXR0ZXIuY290tojQ0MyIs:
33 html{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%;-webkit-tap-highlight-color:rgba(0,0,0,0);}
34 body{margin:0;}
35 button::-moz-focus-inner,input::-moz-focus-inner{border:0;padding:0;}
36 input::-webkit-inner-spin-button,input::-webkit-outer-spin-button,input::-webkit-search-cancel-button,input::-webkit-search-decoration,input::-webkit-search-results-button,input::-we
37 [stylesheet-group="0.1"]{}
38 :focus:not([data-focus-visible-polyfill]){outline: none;}
39 [stylesheet-group="1"]{}
40 .css-1dbjc4n{-ms-flex-align:stretch;-ms-flex-direction:column;-ms-flex-negative:0;-ms-flex-preferred-size:auto;-webkit-align-items:stretch;-webkit-box-align:stretch;-webkit-box-dire
41 .css-90loas{border:0 solid black;box-sizing:border-box;color:rgba(0,0,0,1.00);display:inline;font:14px -apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,Helvetica,Arial,sans-serif;
42 .css-16my406{color:inherit;font:inherit;white-space:inherit;}
43 [stylesheet-group="2.2"]{}
44 .r-13awgt0{-ms-flex:1 1 0%;-webkit-flex:1;flex:1;}
45 .r-4qtap9{display:inline-block;}
46 .r-ywje1{margin-bottom:auto;margin-left:auto;margin-right:auto;margin-top:auto;}
47 .r-hvic4{display:none;}
48 .r-1adg3ll{display:block;}
49 [stylesheet-group="2.2"]{}
50 .r-12vffkv{*{pointer-events:auto;}
51 .r-12vffkv{pointer-events:none!important;}
52 .r-14lw9ot{background-color:rgba(255,255,255,1.00);}
53 .r-1p0dtai{bottom:0px;}
54 .r-1d2f490{left:0px;}
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

Solutions to take

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue

an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.

4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

3. [Possible] Cross-site Scripting

- Severity: MEDIUM
- Method: GET

Impact

- Many various attacks can be carried out with the use of XSS, including but not limited to the following:
 1. Interfering with a user's current active session.
 2. Changing the look of the page within the victim's browser.
 3. Mounting a successful phishing attack.
 4. Intercepting data and performing man-in-the-middle attacks.

Request

```
1 GET /i/api/graphql/uFlnb-172jdjys1I182Cw/Viewer?variables=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00378B)%3C/scRipt%3E HTTP/1.1
2 Host: twitter.com
3 Accept: */*
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 authorization: Bearer AAAAAAAAAAAAAAAAAANRIlgAAAAAnNwIzUejRC0uH5E6I8xnZz4puTs%3D1Zv7ttfk8LF81IUq16cHjlTVju4FA33AGWjCpTnA
7 Cache-Control: no-cache
8 Content-Type: application/json
9 Cookie: guest_id=v1%3A163281615778514028; personalization_id="v1_NzNn+YtIZpY1SL1A04rXLg=="; gt=1442761652445712387; ct0=e0626f5c0a21dd79a61c77f136760c12; att=1-GDMKZZOv1JHdy3tcor9aMkm2x
10 Referer: https://twitter.com/
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
12 x-guest-token: 1442761652445712387
13 X-Scanner: Netsparker
14 x-twitter-active-user: yes
15 x-twitter-client-language: en
16
```

Response

```
1 HTTP/1.1 400 Bad Request
2 server: tsa_k
3 content-length: 323
4 strict-transport-security: max-age=631138519
5 x-connection-hash: 1750695See948137772b3ebd4c37150ae009ac578fcc4a8e43f7487dd701e80
6 content-type: application/json; charset=utf-8
7 content-encoding:
8 date: Tue, 28 Sep 2021 08:47:41 GMT
9 cache-control: no-cache, no-store, max-age=0
10
11 {"errors":[{"message":"'Unexpected character ('' (code 39)): expected a valid value (JSON String, Number, Array, Object or token 'null', 'true' or 'false')\n at [Source: (String)]\""}]}
```

Solutions to take

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include [OWASP Reform](#) and [Microsoft Anti-Cross-site Scripting](#) libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

4. HTTP Strict Transport Security (HSTS) Errors and Warnings

- Severity: MEDIUM
- Method: GET

Impact

The HSTS Warning and Error messages may provide an opportunity for attackers to circumvent HSTS, allowing them to view and modify your interactions with the website.

Request

```
1 GET / HTTP/1.1
2 Host: twitter.com
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
8 X-Scanner: Netsparker
9
```

Response

```
1 HTTP/1.1 200 OK
2 cache-control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
3 set-cookie: personalization_id="v1_mPuHUBoJH66JrTxypWMBNQ="; Max-Age=63072000; Expires=Thu, 28 Sep 2023 08:03:13 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None
4 set-cookie: guest_id=v13A163281619298614327; Max-Age=63072000; Expires=Thu, 28 Sep 2023 08:03:13 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None
5 expiry: Tue, 31 Mar 1981 05:00:00 GMT
6 transfer-encoding: chunked
7 pragma: no-cache
8 server: tsa_k
9 x-content-type-options: nosniff
10 x-xss-protection: 0
11 cross-origin-embedder-policy: unsafe-none
12 strict-transport-security: max-age=631138519
13 x-frame-options: DENY
14 x-connection-hash: bb74a16db8a4e667f3e1d101e60acf4873c8784175bfc4b1f4043b69316c100d
15 x-powered-by: Express
16 last-modified: Tue, 28 Sep 2021 08:03:13 GMT
17 content-type: text/html; charset=utf-8
18 cross-origin-opener-policy: same-origin-allow-popups
19 content-security-policy: connect-src 'self' blob: https://*.giphy.com https://*.pscp.tv https://*.video.pscp.tv https://*.twimg.com https://api.twitter.com https://api-stream.twitter.com
20 date: Tue, 28 Sep 2021 08:03:13 GMT
21 content-encoding:
22
23 <!DOCTYPE html>
24 <html dir="ltr" lang="en">
25 <meta charset="utf-8" />
```

```

28 <meta name="apple-mobile-web-app-title" content="Twitter" />
29 <meta name="apple-mobile-web-app-status-bar-style" content="white" />
30 <meta name="theme-color" content="#ffffff" />
31 <meta http-equiv="origin-trial" content="AplR4chqTX+4eFxDK+ErQlKR8/VtZ/dvnlfd9Y9Nen15r1xJcf81alryTHYQiuUlz9Q49MqGXqyA15mqWzHqQwAAABneyJvcmlnaW41OjJodHRwczovL3R3aXR0ZXIuY29tOjQ0MyIsIn
html<-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%;-webkit-tap-highlight-color:rgba(0,0,0,0);}
32 body{margin:0;}
33 button::-moz-focus-inner,input::-moz-focus-inner{border:0;padding:0;}
34 input::-webkit-inner-spin-button,input::-webkit-outer-spin-button,input::-webkit-search-cancel-button,input::-webkit-search-decoration,input::-webkit-search-results-button,input::-wet
35 [stylesheet-group="0.1"]{}
36 :focus:not([data-focus-visible-polyfill]){outline: none;}
37 [stylesheet-group="1"]{}
38 .css-1dbjc4n{-ms-flex-align:stretch;-ms-flex-direction:column;-ms-flex-negative:0;-ms-flex-preferred-size:auto;-webkit-align-items:stretch;-webkit-box-align:stretch;-webkit-box-direct
39 .css-90l0ao{border:0 solid black;box-sizing:border-box;color:rgba(0,0,0,1.00);display:inline;font:14px -apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,Helvetica,Arial,sans-serif;ma
40 .css-16my406{color:inherit;font:inherit;white-space:inherit;}
41 [stylesheet-group="2"]{}
42 .r-13wgt0{-ms-flex:1 1 0%;-webkit-flex:1;flex:1;}
43 .r-4atop9{display:inline-block;}
44 .r-ywje5l{margin-bottom:auto;margin-left:auto;margin-right:auto;margin-top:auto;}
45 .r-hvic4v{display:none;}
46 .r-1adg3ll{display:block;}
47 [stylesheet-group="2.2"]{}
48 .r-12vffkv*{pointer-events:auto;}
49 .r-12vffkv{pointer-events:none!important;}
50 .r-14lw9ot{background-color:rgba(255,255,255,1.00);}
51 .r-1p0dtai{bottom:0px;}

```

```

58 .r-1xvlist{height:1.25em;}
59 .r-dnmrz{max-width:100%;}
60 .r-bnwqim{position:relative;}
61 .r-1plcui{vertical-align:text-bottom;}
62 .r-1rvibr{-moz-user-select:none;-ms-user-select:none;-webkit-user-select:none;user-select:none;}
63 .r-13gxp9{color:rgba(29,161,242,1.00);}
64 .r-wy61x{height:72px;}
65 .r-u8s1d{position:absolute;}
66 .r-1blnp2b{width:72px;}
67 .r-1yxxob0{top:60%;}
68 .r-1b2b6em{line-height:2em;}
69 .r-q4m81j{text-align:center;}</style><body style="background-color: #FFFFFF;">
70 <noscript>
71 <style>
72 body {
73   -ms-overflow-style: scrollbar;
74   overflow-y: scroll;
75   overscroll-behavior-y: none;
76 }
77
78 .errorContainer {
79   background-color: #FFF;
80   color: #0F1419;
81   max-width: 600px;
82   margin: 0 auto;
83   padding: 10%;

```

I

```

91
92 .errorButton a {
93   background: #1DA1F2;
94   border-radius: 2.5em;
95   color: white;
96   padding: 1em 2em;
97   text-decoration: none;
98 }
99
100 .errorButton a:hover,
101 .errorButton a:focus {
102   background: rgb(26, 145, 218);
103 }
104
105 .errorFooter {
106   color: #657786;
107   font-size: 80%;
108   line-height: 1.5;
109   padding: 1em 0;
110 }
111
112 .errorFooter a,
113 .errorFooter a:visited {
114   color: #657786;
115   text-decoration: none;
116   padding-right: 1em;

```

I

```

152 }
153 </style><div aria-label="Loading-" class="css-1dbjc4n r-14lw9ot r-1p0dtai r-1d2f490 r-1xcajam r-zchlnt r-ipmSaf" id="placeholder"><svg viewBox="0 0 24 24" aria-hidden="true" class="r-
154 //# sourceMappingURL=https://ton.local.twitter.com/responsive-web-internal/sourcemaps/client-web-legacy/runtime.208e6aa5.js.map</script><script type="text/javascript" charset="utf-8"
155 if (!window._SCRIPTS_LOADED_['main']) {
156   document.getElementById('ScriptLoadFailure').style.display = 'block';
157   var criticalScripts = ["polyfills","vendors-main","i18n","main"];
158   for (var i = 0; i < criticalScripts.length; i++) {
159     var criticalScript = criticalScripts[i];
160     if (!window._SCRIPTS_LOADED_[criticalScript]) {
161       document.getElementsByName("failedScript")[0].value = criticalScript;
162       break;
163     }
164   }
165 }
166 })()</script><script nonce="YTczMDh1MDQ0tN2Y5Yy00Mm1xLTk2YzktYzZmNTBkZjNjZGRj">document.cookie = decodeURIComponent("gt=1442761800097796099; Max-Age=10800; Domain=.twitter.com; Path=/

```

Solutions to take

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

- In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
 - The max-age must be at least 31536000 seconds (1 year)
 - The includeSubDomains directive must be specified
 - The preload directive must be specified
 - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

5. Out-of-date Version (jQuery)

- Severity: MEDIUM
- Method: GET

Impact

Due to the fact that this is an old version of the software, it may be susceptible to attacks.

Request

```

1 GET /i/directory/ HTTP/1.1
2 Host: twitter.com
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 Cookie: guest_id=v1%3A163281615778517028; personalization_id="v1_NzNn+YtIZpY1SL1A04rXLg="; gt=1442761652445712387; ct0=e0626f5c0a21dd79a61c77f13676bc12; _ga=GA1.2.2016665518.1632816164
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
9 X-Scanner: Netsparker
10
```

Response

```

1 HTTP/1.1 200 OK
2 cache-control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
3 set-cookie: fm=0; Max-Age=0; Expires=Tue, 28 Sep 2021 08:03:33 GMT; Path=/; Domain=twitter.com; Secure; HTTPOnly
4 set-cookie: twitter_sess=Bah7C5IKZmwhc2hJQzomQWw0aW9uQ29udHJvbGxlcjo6Rmxc2g6OKZsYXNo%250A5GfZaHsABjoKQHVzZWR7ADoHaWQ1J3VyxMDQ5YzY3M3NmEwNDUuWmM2NWNmZjEwX250AMTV1MGVjY2ZkOg9jcmVhdGVkX2
5 strict-transport-security: max-age=631138519
6 server: tsa_k
7 x-twitter-response-tags: BouncerCompliant
8 x-content-type-options: nosniff
9 x-xss-protection: 0
10 x-transaction: fcd97a91680ad102
11 expires: Tue, 31 Mar 1981 05:00:00 GMT
12 x-frame-options: DENY
13 content-security-policy: script-src https://ssl.google-analytics.com https://twitter.com 'unsafe-eval' https://*.twimg.com https://api.twitter.com 'nonce-EWdk/LQ4KcYe20Eo4igGIQ==' ht
14 content-length: 87990
15 x-connection-hash: 8029281e4be231476a8c51bac63eaa2895d3f129af7d2c95182991ca10e3b42
16 last-modified: Tue, 28 Sep 2021 08:03:33 GMT
17 content-type: text/html; charset=utf-8
18 x-ua-compatible: IE=edge, chrome=1
19 status: 200 OK
20 pragma: no-cache
21 date: Tue, 28 Sep 2021 08:03:33 GMT
22 content-encoding:
23
24 <!DOCTYPE html>
25 <html lang="en" data-scribe-reduced-action-queue="true">

34 <meta charset="utf-8">
35 <script nonce="EWdk/LQ4KcYe20Eo4igGIQ==">
36   !function(){window.initErrorstack=[];window.onerror=function(r,i,n,o,t){r.indexOf("Script error.")>-1||window.initErrorstack.push({errorMsg:r,url:i,1
37   }
38   }
39
40
41 <script id="bouncer_terminate_iframe" nonce="EWdk/LQ4KcYe20Eo4igGIQ==">
42   if (window.top != window) {
43     window.top.postMessage({bouncer: true, 'event': 'complete'}, '*');
44   }
45 </script>
46 <script id="swift_action_queue" nonce="EWdk/LQ4KcYe20Eo4igGIQ==">
47   !function(){function e(e){if(e){if(e=window.event),!e)return!1;if(e.timestamp=(new Date).getTime(),!e.target&&e.srcElement&&(e.target=e.srcElement),document.documentElement.getAttr
48   }
49 <script id="composition_state" nonce="EWdk/LQ4KcYe20Eo4igGIQ==">
50   !function(){function t(t){t.target.setAttribute("data-in-composition",true)}function n(t){t.target.removeAttribute("data-in-composition")}document.addEventListener&&(document.a
51 </script>
52
53 <link rel="stylesheet" href="https://abs.twimg.com/a/1631636492/css/t1/twitter_core.bundle.css" class="coreCSSBundles">
54 <link rel="stylesheet" class="moreCSSBundles" href="https://abs.twimg.com/a/1631636492/css/t1/twitter_more_1.bundle.css">
55 <link rel="stylesheet" class="moreCSSBundles" href="https://abs.twimg.com/a/1631636492/css/t1/twitter_more_2.bundle.css">
56
57 <link rel="dns-prefetch" href="https://pbs.twimg.com">
58 <link rel="dns-prefetch" href="https://t.co">
```



```

58 <link rel="dns-prefetch" href="https://t.co">
59 <link rel="preload" href="https://abs.twimg.com/k/en/init.en.40304fb5ce7a3d755fd2.js" as="script">
60 <link rel="preload" href="https://abs.twimg.com/k/en/0.common.en.9d80b91c33318d17dde1.js" as="script">
61
62 <title>Twitter / Profiles Directory / a - Azzzzzzzreen</title>
63 <meta name="robots" content="NOODP">
64 <meta name="description" content="Find friends and people you&#39;re interested in on the Twitter Profiles Directory, featuring profiles from a to Azzzzzzzreen">
65
66
67 <meta name="msapplication-TileImage" content="//abs.twimg.com/favicons/win8-tile-144.png"/>
68 <meta name="msapplication-TileColor" content="#00aced"/>
69
70
71
72
73 <meta name="facebook-domain-verification" content="moho2ug7zs57jjijyvwrd8wb5a08h" />
74
75
76
77 <link rel="mask-icon" sizes="any" href="https://abs.twimg.com/a/1631636492/icons/favicon.svg" color="#1da1f2">
78
79 <link rel="shortcut icon" href="//abs.twimg.com/favicons/favicon.ico" type="image/x-icon">
80 <link rel="apple-touch-icon" href="https://abs.twimg.com/icons/apple-touch-icon-192x192.png" sizes="192x192">
81
82 <link rel="manifest" href="/manifest.json">
83

```

```

286 <li><a href="?lang=de" data-lang-code="de" title="German" class="js-language-link js-tooltip" rel="noopener">Deutsch</a></li>
287 <li><a href="?lang=en-gb" data-lang-code="en-gb" title="British English" class="js-language-link js-tooltip" rel="noopener">English UK</a></li>
288 <li><a href="?lang=es" data-lang-code="es" title="Spanish" class="js-language-link js-tooltip" rel="noopener">Español</a></li>
289 <li><a href="?lang=fil" data-lang-code="fil" title="Filipino" class="js-language-link js-tooltip" rel="noopener">Filipino</a></li>
290 <li><a href="?lang=fr" data-lang-code="fr" title="French" class="js-language-link js-tooltip" rel="noopener">Français</a></li>
291 <li><a href="?lang=hr" data-lang-code="hr" title="Croatian" class="js-language-link js-tooltip" rel="noopener">Hrvatski</a></li>
292 <li><a href="?lang=it" data-lang-code="it" title="Italian" class="js-language-link js-tooltip" rel="noopener">Italiano</a></li>
293 <li><a href="?lang=hu" data-lang-code="hu" title="Hungarian" class="js-language-link js-tooltip" rel="noopener">Magyar</a></li>
294 <li><a href="?lang=nl" data-lang-code="nl" title="Dutch" class="js-language-link js-tooltip" rel="noopener">Nederlands</a></li>
295 <li><a href="?lang=no" data-lang-code="no" title="Norwegian" class="js-language-link js-tooltip" rel="noopener">Norsk</a></li>
296 <li><a href="?lang=pl" data-lang-code="pl" title="Polish" class="js-language-link js-tooltip" rel="noopener">Polski</a></li>
297 <li><a href="?lang=pt" data-lang-code="pt" title="Portuguese" class="js-language-link js-tooltip" rel="noopener">Português</a></li>
298 <li><a href="?lang=ro" data-lang-code="ro" title="Romanian" class="js-language-link js-tooltip" rel="noopener">Română</a></li>
299 <li><a href="?lang=sk" data-lang-code="sk" title="Slovak" class="js-language-link js-tooltip" rel="noopener">Slovenčina</a></li>
300 <li><a href="?lang=fi" data-lang-code="fi" title="Finnish" class="js-language-link js-tooltip" rel="noopener">Suomi</a></li>
301 <li><a href="?lang=sv" data-lang-code="sv" title="Swedish" class="js-language-link js-tooltip" rel="noopener">Svenska</a></li>
302 <li><a href="?lang=vi" data-lang-code="vi" title="Vietnamese" class="js-language-link js-tooltip" rel="noopener">Tiếng Việt</a></li>
303 <li><a href="?lang=tr" data-lang-code="tr" title="Turkish" class="js-language-link js-tooltip" rel="noopener">Türkçe</a></li>
304 <li><a href="?lang=el" data-lang-code="el" title="Greek" class="js-language-link js-tooltip" rel="noopener">Ελληνικά</a></li>
305 <li><a href="?lang=bg" data-lang-code="bg" title="Bulgarian" class="js-language-link js-tooltip" rel="noopener">Български език</a></li>
306 <li><a href="?lang=ru" data-lang-code="ru" title="Russian" class="js-language-link js-tooltip" rel="noopener">Русский</a></li>
307 <li><a href="?lang=sr" data-lang-code="sr" title="Serbian" class="js-language-link js-tooltip" rel="noopener">Српски</a></li>
308 <li><a href="?lang=uk" data-lang-code="uk" title="Ukrainian" class="js-language-link js-tooltip" rel="noopener">Українська мова</a></li>
309 <li><a href="?lang=he" data-lang-code="he" title="Hebrew" class="js-language-link js-tooltip" rel="noopener">עברית</a></li>
310 <li><a href="?lang=ar" data-lang-code="ar" title="Arabic" class="js-language-link js-tooltip" rel="noopener">العربية</a></li>
311 <li><a href="?lang=fa" data-lang-code="fa" title="Persian" class="js-language-link js-tooltip" rel="noopener">فارسی</a></li>

```

```

</div>
</div>
</div>
<div class="hidden" id="hidden-content">
<iframe aria-hidden="true" class="tweet-post-iframe" name="tweet-post-iframe"></iframe>
<iframe aria-hidden="true" class="dm-post-iframe" name="dm-post-iframe"></iframe>
</div>
<input type="hidden" id="init-data" class="json-data" value="{&quot;keyboardShortcuts&quot;:[{&quot;name&quot;:&quot;Actions&quot;,&quot;description&quot;:&quot;Shortcuts for c
<br>
<input type="hidden" class="swift-boot-module" value="app/pages/directory/directory">
<input type="hidden" id="swift-module-path" value="https://abs.twimg.com/k/swift/en">
<br>
<script src="https://abs.twimg.com/k/en/init.en.40304fb5ce7a3d755fd2.js" async></script>
</body>
</html>
<br>
<span class="Icon Icon--reply UIWalkthrough-icon"></span>
Join the conversation
</h3>
<p class="UIWalkthrough-message">
Add your thoughts about any Tweet with a Reply. Find a topic you're passionate about, and jump right in.
</p>
</div>
<br>
<div class="UIWalkthrough-step UIWalkthrough-step--trends">
<h3 class="UIWalkthrough-title">
<span class="Icon Icon--discover UIWalkthrough-icon"></span>
Learn the latest
</h3>
<p class="UIWalkthrough-message">
Get instant insight into what people are talking about now.
</p>
</div>
<br>
<div class="UIWalkthrough-step UIWalkthrough-step--wtf">
<h3 class="UIWalkthrough-title">
<span class="Icon Icon--follow UIWalkthrough-icon"></span>
Get more of what you love
</h3>
<p class="UIWalkthrough-message">

```


Known Vulnerabilities in this version

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing `<script>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

External References

- [CVE-2020-11023](#)

I

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

External References

- [CVE-2020-11022](#)

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of `Object.prototype` pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native `Object.prototype`.

Affected Versions

1.0 to 3.3.1

External References

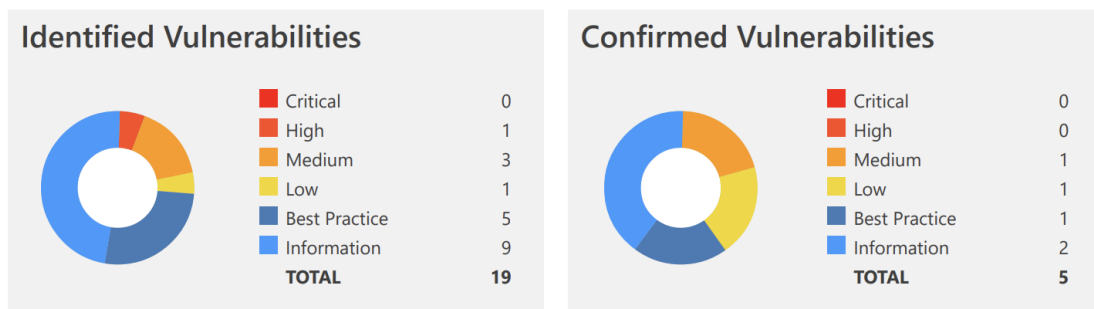
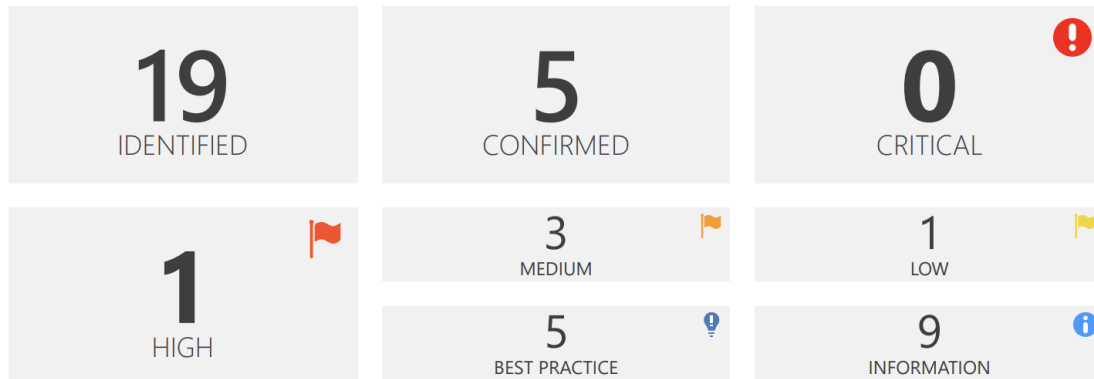
- [CVE-2019-11358](#)

To the vulnerability scanning purpose I have used Netsparker professional version.

Vulnerability Summary

https://vine.co/

Scan Time	: 9/25/2021 11:21:39 PM (UTC+05:30)	Risk Level: HIGH
Scan Duration	: 00:00:06:12	
Total Requests	: 3,097	
Average Speed	: 8.3r/s	



CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Moment.js)	GET	https://vine.co/	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://vine.co/	
	Out-of-date Version (jQuery)	GET	https://vine.co/	
	Weak Ciphers Enabled	GET	https://vine.co/	
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://vine.co/	
	Expect-CT Not Enabled	GET	https://vine.co/	
	Missing X-XSS-Protection Header	GET	https://vine.co/	
	Referrer-Policy Not Implemented	GET	https://vine.co/	
	Subresource Integrity (SRI) Not Implemented	GET	https://vine.co/	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://vine.co/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://vine.co/	
	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://vine.co/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://vine.co/	
	default-src Used in Content Security Policy (CSP)	GET	https://vine.co/	
	Email Address Disclosure	GET	https://vine.co/privacy	
	OpenSearch.xml Detected	GET	https://vine.co/opensearch.xml	
	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://vine.co/	
	OPTIONS Method Enabled	OPTIONS	https://vine.co/	
	Robots.txt Detected	GET	https://vine.co/robots.txt	

Target Domain: <https://vine.co/>

Dear Vine Community - thank you for all the inspiration, laughs, and loops. We have now placed Vine in an archived state. For more information, [click here](#).



[Help](#) [Terms](#) [Privacy](#) [Attribution](#) Did it for the Vine. © 2018 Twitter, Inc.

1. Out-of-date Version (Moment.js)

- Severity: HIGH
- Method: GET

Impact

- Because of the out-of-date version, this vulnerability can be exploited to launch a variety of attacks.

Known Vulnerabilities

Moment.js Regular Expression Denial of Service (ReDoS) Vulnerability

Affected versions of the package are vulnerable to Regular Expression Denial of Service (ReDoS) attacks for any locale that has separate format and standalone options and format input can be controlled by the user. An attacker can provide a specially crafted input to the format function, which nearly matches the pattern being matched. This will cause the regular expression matching to take a long time, all the while occupying the event loop and preventing it from processing other requests and making the server unavailable (a Denial of Service attack).

<https://nynk.io/vuln/moment20161019>

Affected Versions

0.3.0 to 2.15.1

External References

-

Moment.js Uncontrolled Resource Consumption Vulnerability

The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than [CVE-2016-4055](#).

Affected Versions

0.3.0 to 2.19.2

External References

[CVE-2017-18214](#)

Request

```
1 GET / HTTP/1.1
2 Host: vine.co
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
8 X-Scanner: Netsparker
9
10
```

Response

```
1 HTTP/1.1 200 OK
2 X-Content-Type-Options: nosniff
3 Connection: keep-alive
4 Content-Security-Policy: default-src https: data: vine;;img-src 'self' data: https://vine.co https://vines.s3.amazonaws.com https://archive.vine.co https://*.twimg.com https://*.cdn.vine
5 Content-Length: 6718
6 X-Frame-Options: SAMEORIGIN
7 Strict-Transport-Security: max-age=631138519
8 Content-Type: text/html; charset=utf-8
9 Date: Sat, 25 Sep 2021 17:56:25 GMT
10 Cache-Control: max-age=600
11
12 <!DOCTYPE html>
13 <html lang="en"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1,minimum-scale=1,maximum
14 .body {
15     background-color: white;
16     min-height: 100vh;
17 }
18 .banner {
19     background: #7870cc;
20     color: white;
21     font-size: 18px;
22     font-weight: 300;
23     line-height: 1.5;
24     margin-bottom: 20px;
25     padding: 30px 20px;
26     text-align: center;
27 }
28
29 .banner a {
30     color: white;
31     text-decoration: underline;
32 }
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54 .content > * {
55     margin-bottom: 25px;
56 }
57
58 .footer {
59     bottom: 0;
60     display: -webkit-box;
61     display: -ms-flexbox;
62     display: flex;
63     position: fixed;
64     width: 100%;
65 }
66
67 .footer li {
68     color: rgba(238, 128, 92, 0.75);
69     font-size: 18px;
70 }
71
72 .footer li a {
73     color: rgba(238, 128, 92, 0.75);
74     text-decoration: none;
75 }
76
77 .footer li a:hover {
78     text-decoration: underline;
79 }
80
81 </style><base href="/"><meta name="vine-ember/config/environment" content="%78%22modulePrefix%22%3A%22vine-ember%22%2C%22environment%22%3A%22production%22%2C%22baseURL%22%3A%22/%22%2C%22
window.APP_CONFIG.ASSETS_CDN_PREFIX = 'https://v.cdn.vine.co/w/a001567d-assets/';</script></body></html>
```

2. Weak Ciphers Enabled

- Severity: MEDIUM
- Method: GET

Impact

- In some cases, attackers may decode SSL traffic that is transmitted between your server and your visitors.

Vulnerability Details

- While using encrypted communication, Netsparker discovered that weak ciphers were being utilized (SSL).
- When it comes to protecting secure communication with your visitors, you should only allow powerful ciphers on your web server to be used.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take

For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
- In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
- Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```


3.HTTP Strict Transport Security (HSTS) Errors and Warnings

- Severity: MEDIUM
- Method: GET

Impact

The HSTS Warning and Error messages may provide an opportunity for attackers to circumvent HSTS, allowing them to view and modify your interactions with the website.

Request

```
1 GET / HTTP/1.1
2 Host: vine.co
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
8 X-Scanner: Netsparker
9
10
```

Response

```
1 HTTP/1.1 200 OK
2 X-Content-Type-Options: nosniff
3 Connection: keep-alive
4 Content-Security-Policy: default-src https: data: vine;img-src 'self' data: https://vine.co https://vines.s3.amazonaws.com https://archive.vine.co https://*.twimg.com https://*.cdn.vine.co https://media.vineapp.com h
5 Content-Length: 6718
6 X-Frame-Options: SAMEORIGIN
7 Strict-Transport-Security: max-age=631138519
8 Content-Type: text/html; charset=utf-8
9 Date: Sat, 25 Sep 2021 17:56:40 GMT
10 Cache-Control: max-age=600
11
12 <!DOCTYPE html>
13 <html lang="en"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1,minimum-scale=1,maximum-scale=1"><link rel="search" hr
14
15 .body {
16     background-color: white;
17     min-height: 100vh;
18 }
19 .banner {
20     background: #7870cc;
21     color: white;
22     font-size: 18px;
23     font-weight: 300;
24     line-height: 1.5;
25     margin-bottom: 20px;
26     padding: 30px 20px;
27     text-align: center;
28 }
29 .banner a {
30     color: white;
31     text-decoration: underline;
32 }
33
34
35 .content {
36     -webkit-box-align: center;
37     -ms-flex-align: center;
38     align-items: center;
39     display: -webkit-box;
40     display: -ms-flexbox;
41     display: flex;
42     -webkit-box-orient: vertical;
43     -webkit-box-direction: normal;
44     -ms-flex-direction: column;
45     flex-direction: column;
46     font-size: 72px;
47     height: 50vh;
48     -webkit-box-pack: center;
49     -ms-flex-pack: center;
50     justify-content: center;
51     margin-top: 50px;
52 }
53
54 .content > * {
55     margin-bottom: 25px;
56 }
57
58 .footer {
59     bottom: 0;
60     display: -webkit-box;
61     display: -ms-flexbox;
62     display: flex;
63     position: fixed;
64     width: 100%;
65 }
```

```

57
58 .footer {
59     bottom: 0;
60     display: -webkit-box;
61     display: -ms-flexbox;
62     display: flex;
63     position: fixed;
64     width: 100%;
65 }
66
67 .footer li {
68     color: rgba(238, 128, 92, 0.75);
69     font-size: 18px;
70 }
71
72 .footer li a {
73     color: rgba(238, 128, 92, 0.75);
74     text-decoration: none;
75 }
76
77 .footer li a:hover {
78     text-decoration: underline;
79 }
80 </style><base href="/"><meta name="vine-ember/config/environment" content="k78k2modulePrefixk22k3A8k2vine-emberk22k2environmentk22k3A8k22productionk22k2baseURLk22k3A8k22locationTypek22k3A8k22auto%k22k2

```

Solutions to take

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

Serve a valid certificate

If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists

Serve an HSTS header on the base domain for HTTPS requests:

The `max-age` must be at least 31536000 seconds (1 year)

The `includeSubDomains` directive must be specified

The `preload` directive must be specified

If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

4.Out-of-date Version (jQuery)

- Severity: MEDIUM
- Method: GET

Impact

Due to the fact that this is an old version of the software, it may be subject to exploitation.

Vulnerabilities

According to Netsparker, the target web site is utilizing jQuery, and it has been determined that it is out of date.

Request

```

1 GET / HTTP/1.1
2 Host: vine.co
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
8 X-Scanner: Netsparker
9
10

```

Response

```
1 HTTP/1.1 200 OK
2 X-Content-Type-Options: nosniff
3 Connection: keep-alive
4 Content-Security-Policy: default-src https: data: vine;;img-src 'self' data: https://vine.co https://vines.s3.amazonaws.com https://archive.vine.co https://*.twimg.com https://*.cdn.vine.co https://media.vineapp.com https://media.vineapp.com
5 Content-Length: 6718
6 X-Frame-Options: SAMEORIGIN
7 Strict-Transport-Security: max-age=631138519
8 Content-Type: text/html; charset=utf-8
9 Date: Sat, 25 Sep 2021 17:56:25 GMT
10 Cache-Control: max-age=600
11
12 <!DOCTYPE html>
13 <html lang="en"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1,minimum-scale=1,maximum-scale=1"><link rel="search" href="https://vine.co/sitemap.xml">
14 <body>
15 <div>
16 <div>
17 <div>
18 <div>
19 <div>
20 <div>
21 <div>
22 <div>
23 <div>
24 <div>
25 <div>
26 <div>
27 <div>
28 <div>
29 <div>
30 <div>
31 <div>
32 <div>
33 <div>
34 <div>
35 <div>
36 <div>
37 <div>
38 <div>
39 <div>
40 <div>
41 <div>
42 <div>
43 <div>
44 <div>
45 <div>
46 <div>
47 <div>
48 <div>
49 <div>
50 <div>
51 <div>
52 <div>
53 <div>
54 <div>
55 <div>
56 <div>
57 <div>
58 <div>
59 <div>
60 <div>
61 <div>
62 <div>
63 <div>
64 <div>
65 <div>
66 <div>
67 <div>
68 <div>
69 <div>
70 <div>
71 <div>
72 <div>
73 <div>
74 <div>
75 <div>
76 <div>
77 <div>
78 <div>
79 <div>
80 <div>
81 <div>
```

Known Vulnerabilities in this Version

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the `dataType` option, causing `text/javascript` responses to be executed.

Affected Versions

1.8.0 to 2.2.4

External References

[CVE-2015-9251](#)

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

External References

[CVE-2020-11023](#)

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

External References

[CVE-2020-11022](#)

jQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of `Object.prototype` pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native `Object.prototype`.

Affected Versions

1.0 to 3.3.1

External References

[CVE-2019-11358](#)

5. Insecure Transportation Security Protocol Supported (TLS 1.0)

- Severity: LOW
- Method: GET

Impact

In order to see the encryption communication between your website and its visitors, attackers can undertake man-in-the-middle attacks on your website.

Vulnerability

- Netsparker has determined that your web server is capable of supporting the insecure transportation security protocol (TLS 1.0).
- There are various problems with TLS 1.0. In order to exploit vulnerabilities such as BEAST (Browser Exploit Against SSL/TLS), an attacker might cause connection failures and prompt the use of TLS 1.0 to trigger the use of the protocol.
- Since June 30, 2018, websites that use TLS 1.0 are declared non-compliant by the PCI Security Standards Council.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

For Nginx, locate any use of the directive ssl_protocols in the nginx.conf file and remove TLSv1.

```
ssl_protocols TLSv1.2;
```

For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

Click on Start and then Run, type regedt32 or regedit, and then click OK.
In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

Locate a key named Server or create if it doesn't exist.

Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".

For lighttpd, put the following lines in your configuration file:

```
ssl.use-ssl-v2 = "disable"  
ssl.use-ssl-v3 = "disable"  
ssl.openssl-ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up  
ssl.ec-curve = "secp384r1"
```


6. Insecure Transportation Security Protocol Supported (TLS 1.1)

- Severity: HIGH
- Method: GET

Impact

Due to the deprecation of web browsers, your website will be inaccessible to visitors.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the nginx.conf file and remove TLSv1.1.

24 / 66

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
 1. Click on Start and then Run, type regedt32 or regedit, and then click OK.
 2. In Registry Editor, locate the following registry key or create if it does not exist:

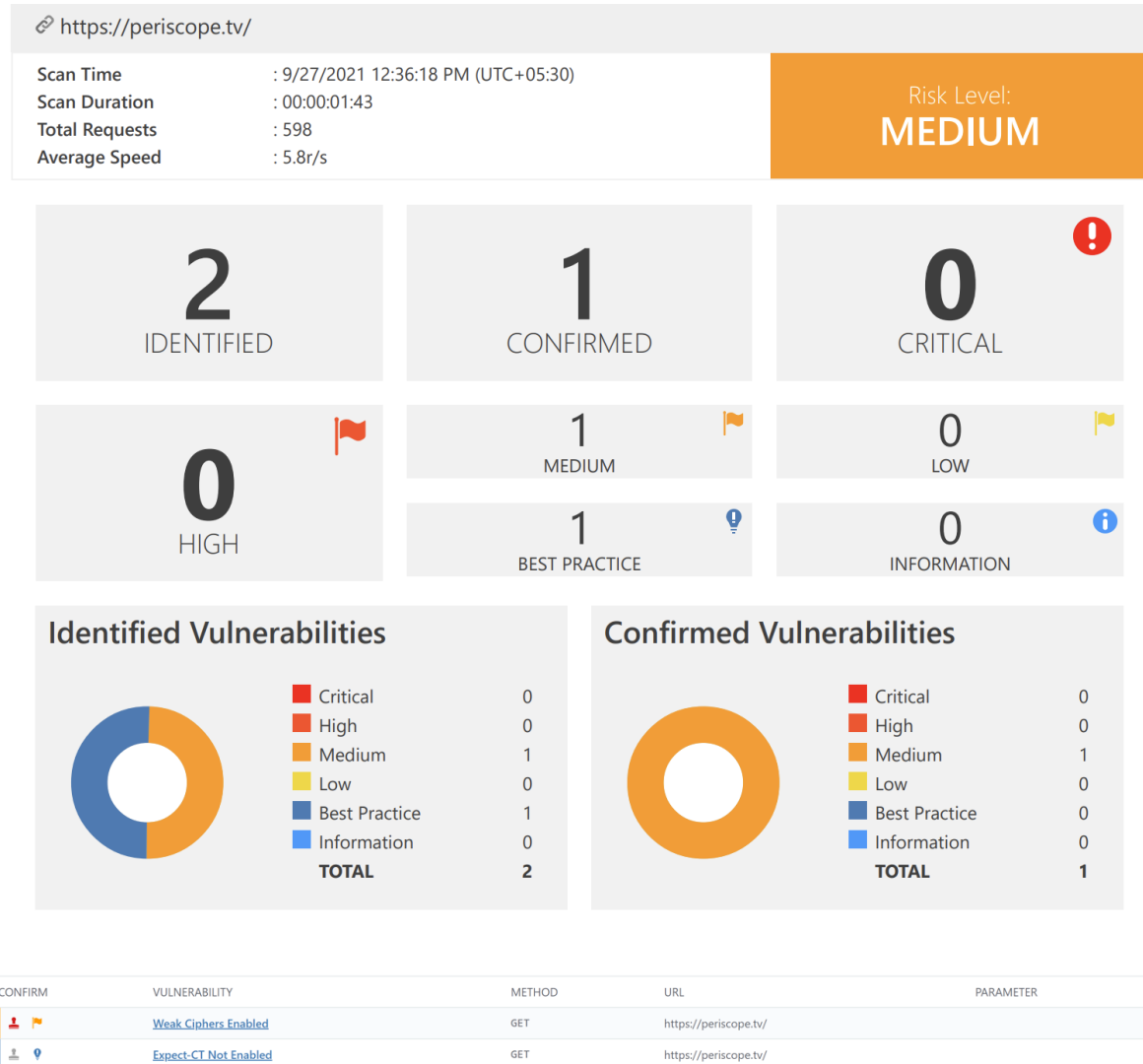
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

3. Locate a key named Server or create if it doesn't exist.
 4. Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"  
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up  
ssl.ec-curve = "secp384r1"
```

To the vulnerability scanning purpose of below domain, I have used Netsparker professional version and Burp Suite professional version.

Vulnerability Summary



Target Domain: <https://www.periscope.tv/>



Periscope is saying goodbye 👋

Periscope is grateful to you for going LIVE together and being part of this community. Past public broadcasts will continue to be available on Periscope web. [Learn more](#)
Keep the conversation going on Twitter.

[Go to Twitter](#)



1. Weak Ciphers Enabled

- Severity: LOW
- Method: GET

Impact

- In some cases, attackers may decode SSL traffic that is transmitted between your server and your visitors.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
- b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
- c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

2. Strict Transport Security Not Enforced

- Severity: LOW
- Method: GET

Impact

Users connecting to the application using unencrypted connections are not prevented by the application. An attacker with access to a legitimate user's network traffic might circumvent the application's SSL/TLS encryption and use it as a platform for assaults on its users. This attack is carried out by rewriting HTTPS links to HTTP, ensuring that if a user clicks on a link to the site from an HTTP website, their browser will never attempt to use an encrypted connection. This operation is automated with the `sslstrip` utility.

An attacker must be in a position to intercept and manipulate the victim's network communication in order to exploit this vulnerability. When a client talks with the server across an insecure connection, such as public Wi-Fi or a corporate or home network that is shared with a compromised machine, this scenario occurs.

Switched networks and other common defences are insufficient to prevent this. This attack might also be carried out by an attacker in the user's ISP or the application's hosting infrastructure. It's worth noting that a sophisticated opponent might target any connection made across the Internet's basic infrastructure.

Request

```
1 GET /ios-attribution/ HTTP/1.1
2 Host: www.periscope.tv
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/92.0.4515.159 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
-
```

Response

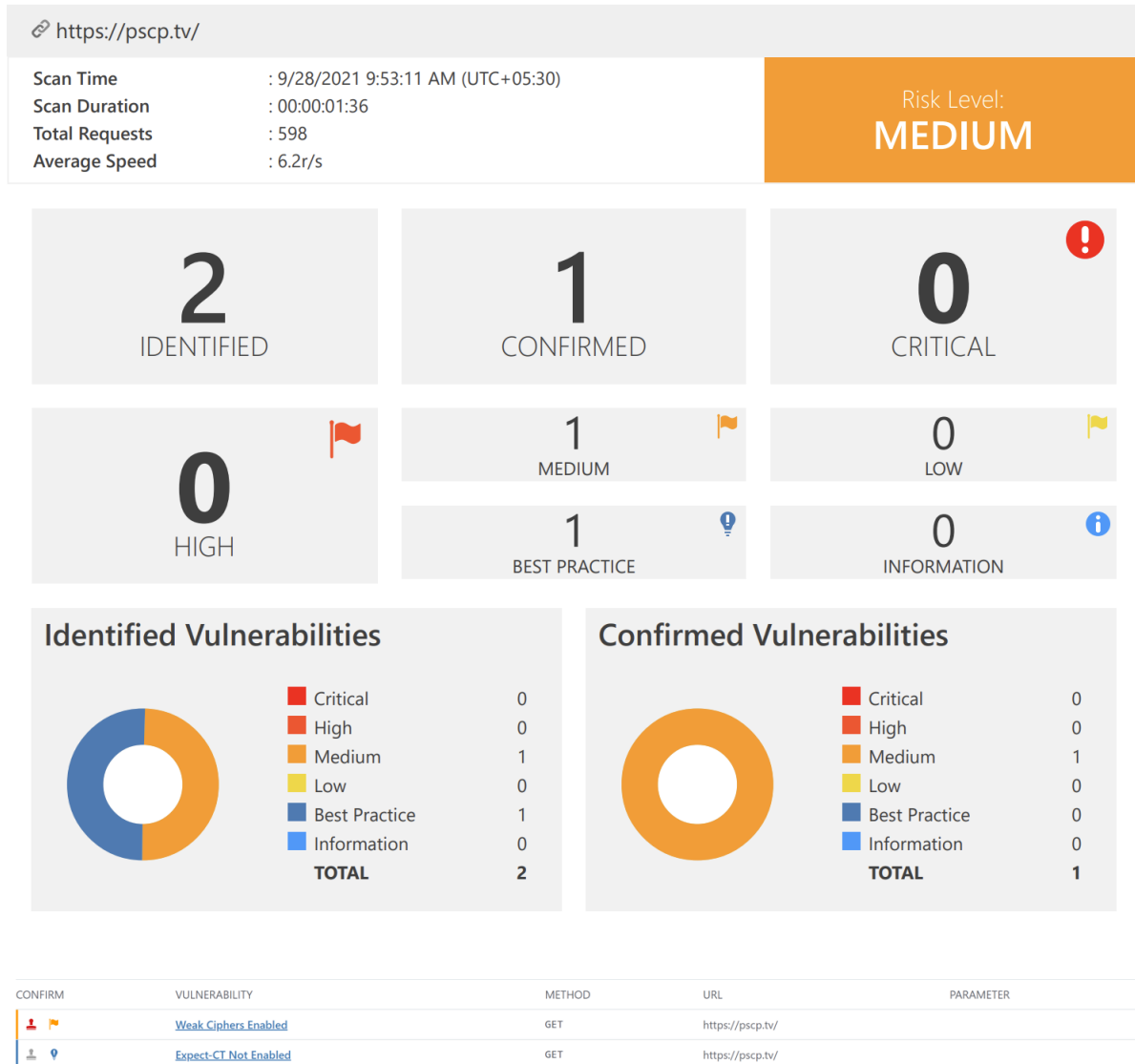
```
1 HTTP/1.1 400 Bad Request
2 Cache-Control: no-store
3 Content-Security-Policy: media-src 'self' data: blob: https://*.pscp.tv/ https://*.periscope.tv/ https://*.global.ssl.fastly.net https://*.twimg.com https://
  ault-src 'self' blob: https://*.global.ssl.fastly.net https://*.pscp.tv/ https://*.periscope.tv/; object-src 'self' https://*.pscp.tv/ https://*.periscope.tv/
  -src 'self' blob: https://*.pscp.tv/ https://*.periscope.tv/ https://twitter.com https://periscope-all.firebaseio.com/ https://*.google.com/recaptcha/ https:
  .google.com/ https://*.google.com/recaptcha/ https://*.gstatic.com/recaptcha/ https://appleid.cdn-apple.com 'unsafe-eval' 'nonce-ldfal39fadc74841be52b9ed46612
  ss-global.bitmovin.com https://www.googleapis.com/ https://securetoken.googleapis.com https://s3.us-west-2.amazonaws.com/periscope-user-data-reports-prod/ htt
4 Content-Type: text/html; charset=utf-8
5 Date: Mon, 27 Sep 2021 07:13:15 GMT
6 Referrer-Policy: origin
7 Set-Cookie: pscp-csrf-9102dfal-d6b3-47f6-8fb7-79a7102f732e; Max-Age=2592000; Domain=.periscope.tv; Path=/; Expires=Wed, 27 Oct 2021 07:13:13 GMT; HttpOnly; S
8 Strict-Transport-Security: max-age=10886400000; includeSubDomains; preload
9 Vary: Accept-Language, Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-Download-Options: noopen
12 X-Frame-Options: ALLOW-FROM https://twitter.com/
13 X-Periscope-Web-Version: 3
14 X-RateLimit-Limit: 3000
15 X-RateLimit-Remaining: 2998
16 X-XSS-Protection: 1; mode=block
17 Connection: Close
18 Content-Length: 15425
19
20 <!doctype html>
21 <html>
  <head>
    <title data-react-helmet="true">
      400
    </title>
    <meta data-react-helmet="true" name="robots" content="noindex, nofollow"/>
    <meta charset="utf-8"/>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no"/>
    <meta name="referrer" content="always"/>
    <meta name="twitter:widgets:csp" content="on"/>
    <meta id="bitmovin" content="https://assets.pscp.tv/resources/bitmovin-7.8.18"/>
    <link rel="shortcut icon" href="https://assets.pscp.tv/images/favicon.ico"/>
    <link rel="stylesheet" href="https://assets.pscp.tv/css/styleSheet.2a699898d2605bd7fd9241e2a549f68f.css"/>
    <style type="text/css" data-styled-components="ivAUyz cfWLEm jSjNk hqIxtk bgBCYq ccdTfJ dHiwq latUan" data-styled-components-is-local="true">
      /* sc-component-id: sc-keyframes-ivAUyz */
      @-webkit-keyframes ivAUyz {
        0% {

```

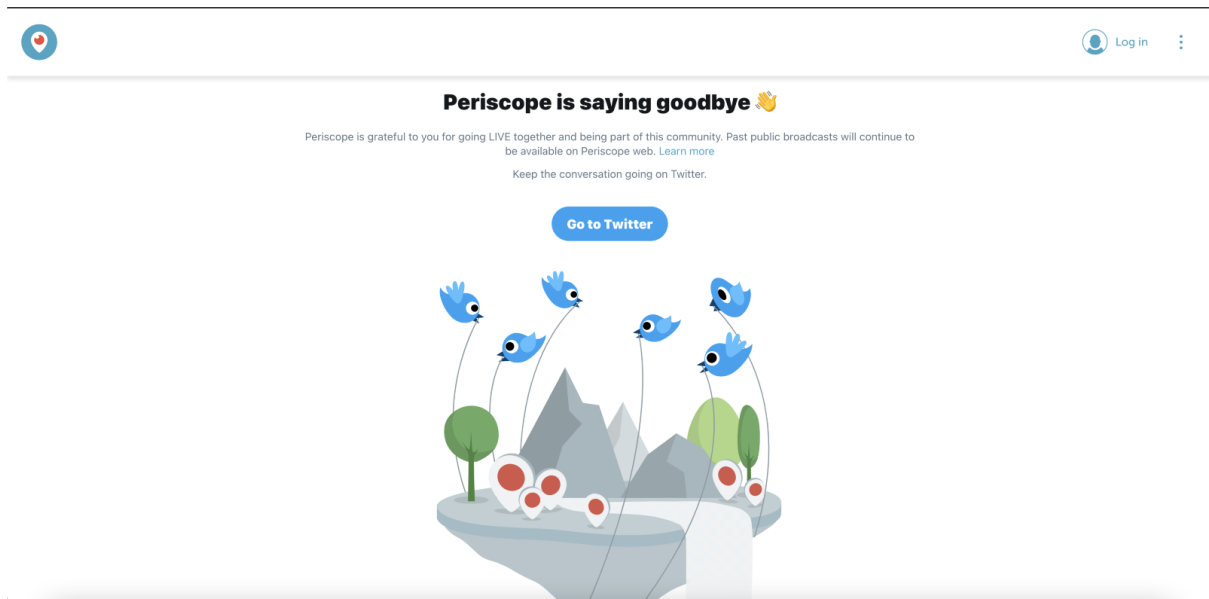
Part this issue has is: **Strict-Transport-Security: max-age=10886400000; includeSubDomains;**

To the vulnerability scanning purpose of below domain, I have used Netsparker professional version and Burp Suite professional version.

Vulnerability Summary



Target Domain: <https://www.pscp.tv/>



1. Weak Ciphers Enabled

- Severity: LOW
- Method: GET

During secure communication, weak ciphers are permitted to be used (SSL).

Impact

- In some cases, attackers may decode SSL traffic that is transmitted between your server and your visitors.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take:

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- a. Click Start, click Run, type regedt32 or type regedit, and then click OK.
- b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
- c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

1. Strict Transport Security Not Enforced

- Severity: LOW
- Method: GET

Impact

Users are able to connect to the program via unencrypted connections because the application does not detect this. Using network traffic modification, an attacker might bypass the application's usage of SSL/TLS encryption, allowing them to utilize the application as a platform for attacks on the application's users. It is possible to carry out this attack by rewriting HTTPS links to appear as HTTP, so that when a targeted victim clicks on a link to the site from an HTTP website, their browser does not attempt to use an encrypted connection. SslStrip is an automated tool that streamlines this operation.

For an attacker to be successful in exploiting this vulnerability, they must be in a position to intercept and manipulate the victim's network communication. In most cases, this scenario occurs when a client talks with a server across an insecure connection, such as a public Wi-Fi hotspot or a workplace or home network that is shared with a malicious computer. Common defenses, such as switched networks, are insufficient to keep this from happening. This attack might also be carried out by an attacker who is located within the user's Internet service provider or within the application's hosting infrastructure. Important to keep in mind: a highly sophisticated opponent might possibly target any connection made across the Internet's fundamental infrastructure.

```
1 GET /privacy.html/ HTTP/1.1
2 Host: www.pscp.tv
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
  Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

```

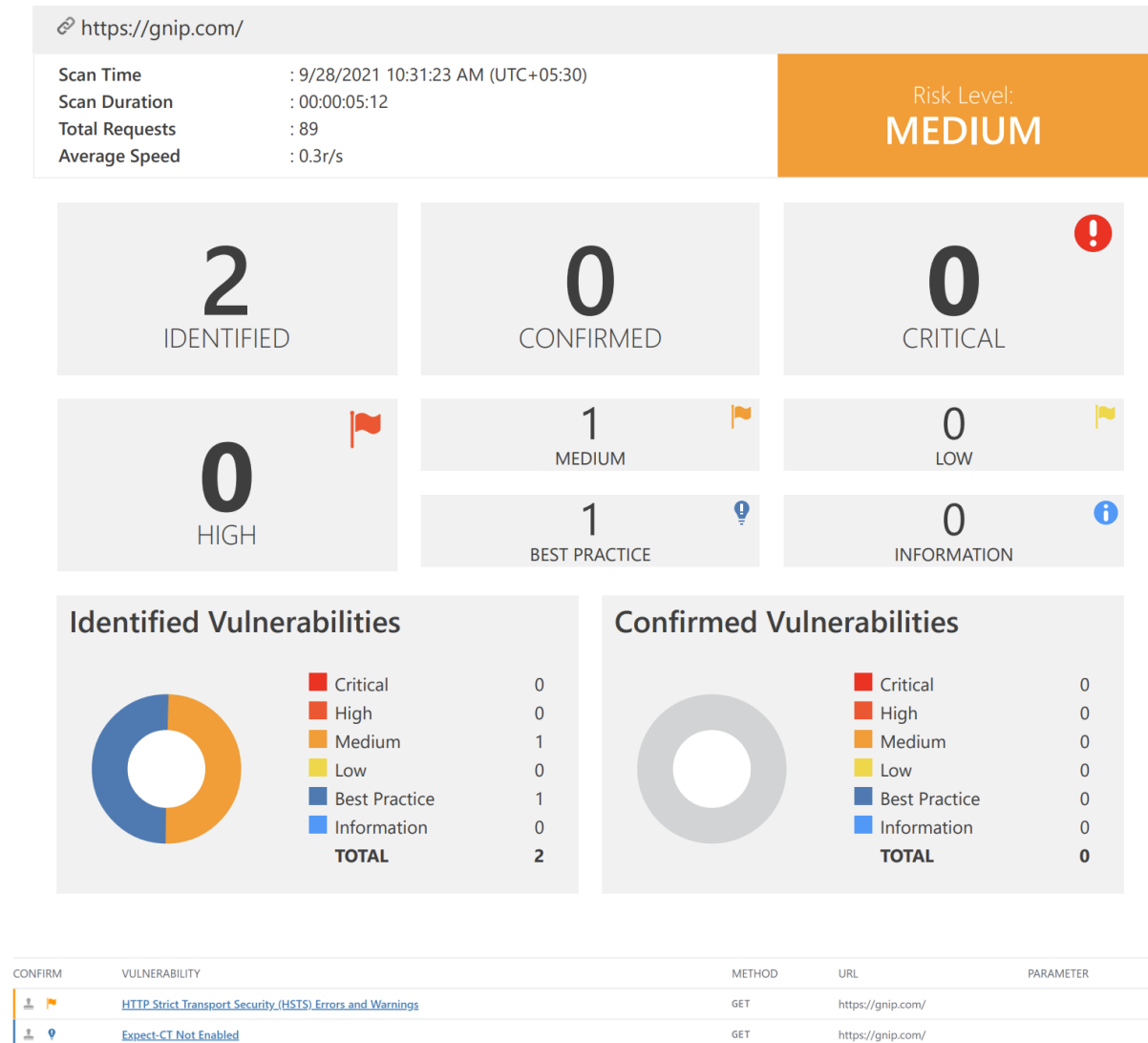
HTTP/1.1 400 Bad Request
2 Cache-Control: no-store
3 Content-Security-Policy: media-src 'self' data; blob: https://*.pscp.tv/ https://*.periscope.tv/ https://*.global.ssl.fastly.net https://*.twimg.com https://
  ault-src 'self' blob: https://*.global.ssl.fastly.net https://*.pscp.tv/ https://*.periscope.tv/; object-src 'self' https://*.pscp.tv/ https://*.periscope.tv/
  -src 'self' blob: https://*.pscp.tv/ https://*.periscope.tv/ https://twitter.com https://periscope-all.firebaseio.com/ https://*.google.com/recaptcha/ https:
  .google.com/ https://*.google.com/recaptcha/ https://*.gstatic.com/recaptcha/ https://appleid.cdn-apple.com 'unsafe-eval' 'nonce-cacc772f86394bef8059b2c592bab
  ss-global.bitmovin.com https://www.googleapis.com/ https://securetoken.googleapis.com https://s3.us-west-2.amazonaws.com/periscope-user-data-reports-prod/ htt
4 Content-Type: text/html; charset=utf-8
5 Date: Tue, 28 Sep 2021 04:40:20 GMT
6 Referer-Policy: origin
7 Set-Cookie: pscp-csrf=8bacbc90-6251-49e8-a922-8db518b4f2b0; Max-Age=2592000; Domain=.pscp.tv; Path=/; Expires=Thu, 28 Oct 2021 04:40:19 GMT; HttpOnly; Secure
8 Strict-Transport-Security: max-age=10886400000; includeSubDomains; preload
9 Vary: Accept-Language, Accept-Encoding
10 X-Content-Type-Options: noSNIff
11 X-Download-Options: noopen
12 X-Frame-Options: ALLOW-FROM https://twitter.com/
13 X-Periscope-Web-Version: 3
14 X-RateLimit-Limit: 3000
15 X-RateLimit-Remaining: 2998
16 X-XSS-Protection: 1; mode=block
17 Content-Length: 15411
18 Connection: Close

20 <!doctype html>
21 <html>
    <head>
      <title data-react-helmet="true">
        400
      </title>
      <meta data-react-helmet="true" name="robots" content="noindex, nofollow"/>
      <meta charSet="utf-8"/>
      <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no"/>
      <meta name="referrer" content="always"/>
      <meta name="twitter:widgets:csp" content="on"/>
      <meta id="bitmovin" content="https://assets.pscp.tv/resources/bitmovin-7.8.18"/>
      <link rel="shortcut icon" href="https://assets.pscp.tv/images/favicon.ico"/>
      <link rel="stylesheet" href="https://assets.pscp.tv/css/stylesheet.2a699898d2605bd7fd9241e2a549f68f.css"/>
      <style type="text/css" data-styled-components="ivAUyz cFWLEm jSzjNk hqIXtk bGyCq codTfJ dHIwKq latUan" data-styled-components-is-local="true">
        /* sc-component-id: sc-keyframes-ivAUyz */
        @-webkit-keyframes ivAUyz{
          0%{
            opacity:0;
            -webkit-transform:translateX(-60px);
            -ms-transform:translateX(-60px);
            transform:translateX(-60px);
          }
          65%{
            opacity:.6;
          }
          90%{
            -webkit-transform:translateX(-24px);
            -ms-transform:translateX(-24px);
            transform:translateX(-24px);
            opacity:.6;
          }
          100%{
            -webkit-transform:translateX(-25px);
            -ms-transform:translateX(-25px);
            transform:translateX(-25px);

```


To the vulnerability scanning purpose of below domain, I have used Netsparker professional version.

Vulnerability Summary



Target Domain: <https://www.gnip.com>



Help us build a better experience for you! Take the 2-minute Twitter Developer survey.

Twitter API for Enterprise

Unleash the power of Twitter data

Twitter's enterprise API platform delivers real-time and historical social data to power your business at scale.

Apply for enterprise access

1. HTTP Strict Transport Security (HSTS) Errors and Warnings

- Severity: MEDIUM
- Method: GET

Impact

The HSTS Warning and Error messages may provide an opportunity for attackers to circumvent HSTS, allowing them to view and modify your interactions with the website.

Request

```
1 GET / HTTP/1.1
2 Host: developer.twitter.com
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
8 X-Scanner: Netsparker
9
10
```

Response

```
1 HTTP/1.1 200 OK
2 set-cookie: personalization_id="v1_GiiHRX/E9hzGMDTX6aevA=="; Max-Age=63072000; Expires=Thu, 28 Sep 2023 05:01:33 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None
3 set-cookie: guest_id=v1K3A163280529301430661; Max-Age=63072000; Expires=Thu, 28 Sep 2023 05:01:33 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None
4 set-cookie: ct0s55f03b1b2a634cee0fd9eca732d6763b; Max-Age=21600; Expires=Tue, 28 Sep 2021 11:01:33 GMT; Path=/; Domain=.twitter.com; Secure
5 set-cookie: cms-csp-nonce=1c94ef556971c24cdd28f97bafed37f; Max-Age=15; Expires=Tue, 28 Sep 2021 05:01:48 GMT; Path=/; Secure
6 server: tsa_k
7 transfer-encoding: chunked
8 expires: Tue, 28 Sep 2021 05:01:33 GMT
9 x-connection-hash: da6761b99ff7f9339ef864928b8fffc0cb42f316f62701c83a99f0f256512655
10 x-xss-protection: 0
11 content-security-policy: default-src 'self'; connect-src 'self' https://*.twimg.com https://*.twitter.com https://api.meetup.com https://s1259914507.t.eloqua.com https://api.compan
12 age: 355043
13 x-frame-options: SAMEORIGIN
14 accept-ranges: bytes
15 strict-transport-security: max-age=631138519
16 content-type: text/html
17 content-encoding:
18 date: Tue, 28 Sep 2021 05:01:33 GMT
19 vary: Cookie,X-Twitter-Internal,X-Twitter-IP-Tags
20 cache-control: max-age=0
21
22 <!DOCTYPE html>
23 <html lang="en" dir="ltr" prefix="og: http://ogp.me/ns#" data-behavior="118n" data-environment="prod" data-server-mode="publish" data-dc="s" class=" twtr-type--chirp">
24   <head>
25     <meta charset="utf-8"/>
26
27   <meta name="viewport" content="width=device-width, initial-scale=1"/>
```

```

28 <title>Twitter Enterprise APIs | Twitter Developer Platform </title>
29 <meta name="description" content="Twitter's enterprise API platform delivers real-time and historical social data to power your business at scale. Apply for enterprise access to Twit
30
31 <link rel="canonical" href="https://developer.twitter.com/en/products/twitter-api/enterprise"/>
32 <meta property="og:url" content="https://developer.twitter.com/en/products/twitter-api/enterprise"/>
33
34
35
36
37
38
39 <meta property="og:type" content="article"/>
40 <meta property="og:title" content="Twitter Enterprise APIs"/>
41 <meta property="og:description" content="Twitter's enterprise API platform delivers real-time and historical social data to power your business at scale. Apply for enterprise access
42 <meta property="og:image" content="https://cdn.cms-twigitalassets.com/content/dam/developer-twitter/redesign-2021-images/og-social-card/devwebsite_card_tn.jpg.twimg.768.jpg"/>
43 <meta name="keywords"/>
44
45
46 <meta name="twitter:card" content="summary_large_image"/>
47
48
49
50
51
52 <meta name="twitter:widgets:new-embed-design" content="on"/>
53 <meta name="twitter:widgets:csp" content="on"/>
54
55
56
57 <link href="https://abs.twimg.com/favicons/favicon.ico" rel="shortcut icon" type="image/x-icon"/>
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72 <script type="application/json" id="analytics-settings">{&quot;google&quot;:{&quot;accounts&quot;:[],&quot;options&quot;:{&quot;displayAdvertisingFeatures&quot;:false}},&quot;scribe
73
74
75
76
77
78
79
80 <link rel="preload" href="https://fonts.twitter.com/chirp/chirp-bold-italic-web.woff2" as="font" type="font/woff2" crossorigin/>
81 <link rel="preload" href="https://fonts.twitter.com/chirp/chirp-bold-web.woff2" as="font" type="font/woff2" crossorigin/>
82 <link rel="preload" href="https://fonts.twitter.com/chirp/chirp-display-extended-black-web.woff2" as="font" type="font/woff2" crossorigin/>
83 <link rel="preload" href="https://fonts.twitter.com/chirp/chirp-regular-web.woff2" as="font" type="font/woff2" crossorigin/>
84 <link rel="preload" href="https://fonts.twitter.com/chirp/chirp-regular-italic-web.woff2" as="font" type="font/woff2" crossorigin/>
85 <link rel="preload" href="https://fonts.twitter.com/chirp/chirp-extended-bold-web.woff2" as="font" type="font/woff2" crossorigin/>
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999

```

Solutions to take

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
 - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
 - The max-age must be at least 31536000 seconds (1 year)
 - The includeSubDomains directive must be specified
 - The preload directive must be specified

4 / 10

- If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

2. Weak Ciphers Enabled

- Severity: LOW
- Method: GET

Impact

- In some cases, attackers may decode SSL traffic that is transmitted between your server and your visitors.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take

Configure your web server to respond with Expect-CT header.

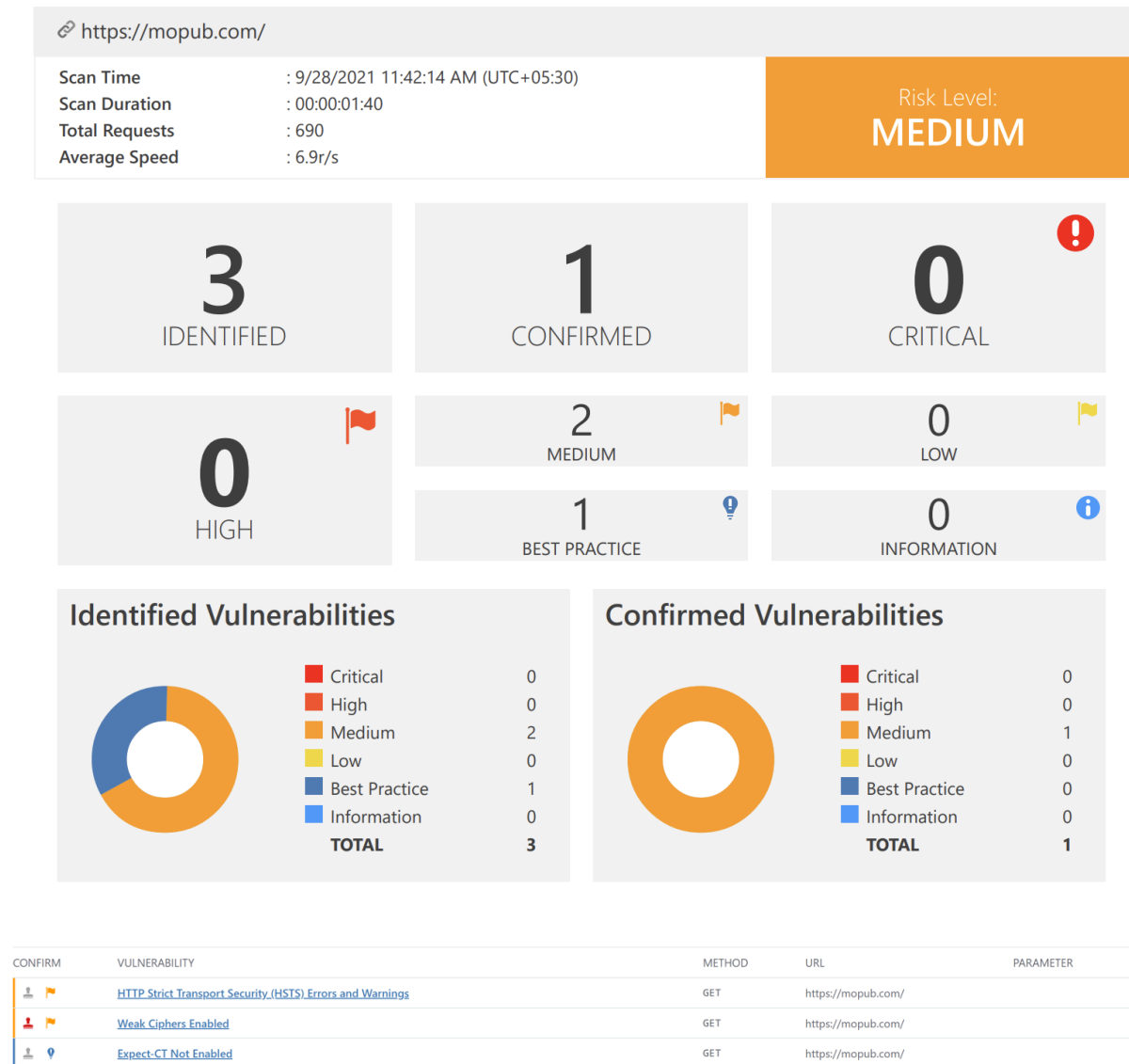
```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT **enforce** mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

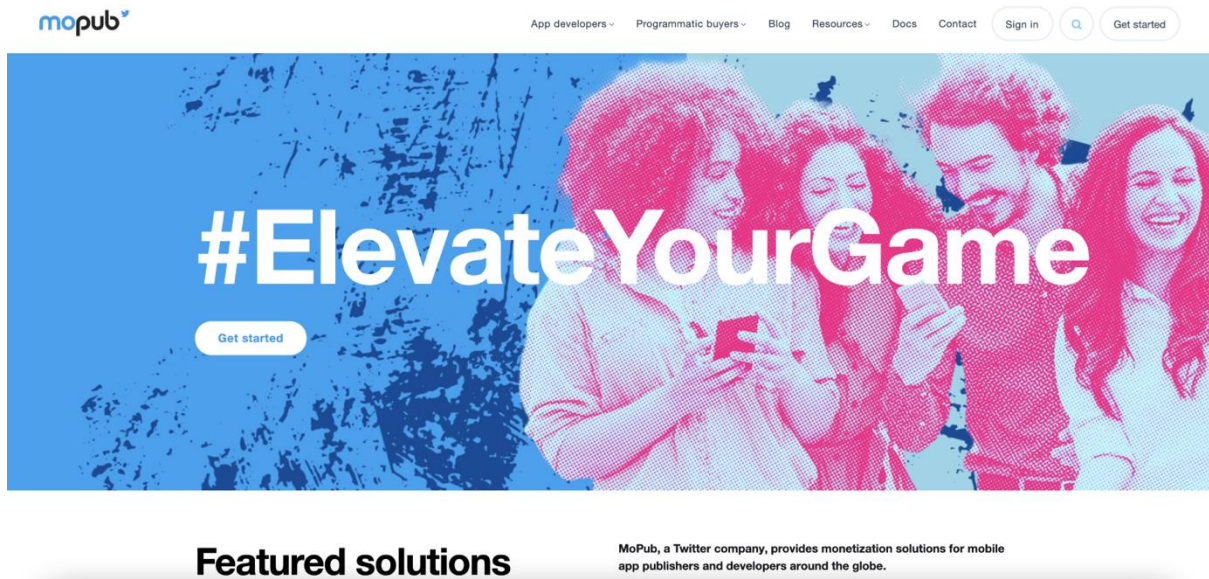
```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

To the vulnerability scanning purpose of below domain, I have used Netsparker professional version.

Vulnerability Summary



Target Domain: <https://www.mopub.com>



1. HTTP Strict Transport Security (HSTS) Errors and Warnings

- Severity: MEDIUM
- Method: GET

Impact

The HSTS Warning and Error messages may provide an opportunity for attackers to circumvent HSTS, allowing them to view and modify your interactions with the website.

Request

```
1 GET / HTTP/1.1
2 Host: www.mopub.com
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-us,en;q=0.5
6 Cache-Control: no-cache
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
8 X-Scanner: Netsparker
^
```

Response

```
1 HTTP/1.1 200 OK
2 set-cookie: cms-csp-nonce=266ffe54428a9741907cbbf43e62e7c; Max-Age=15; Expires=Tue, 28 Sep 2021 06:12:39 GMT; Path=/; Secure
3 server: tsa_a
4 transfer-encoding: chunked
5 expires: Tue, 28 Sep 2021 06:12:34 GMT
6 x-connection-hash: 75e5079e536db5bd9c6eece368614bf78ede03b4bedd3bbd338ae8dd7fd552c
7 x-xss-protection: 0
8 content-security-policy: default-src 'self'; connect-src 'self' https://s1259914507.t.eloqua.com https://www.google-analytics.com https://syndication.twitter.com https://api.company
9 age: 6747
10 x-frame-options: SAMEORIGIN
11 accept-ranges: bytes
12 strict-transport-security: max-age=631138519
13 content-type: text/html
14 content-encoding:
15 date: Tue, 28 Sep 2021 06:12:24 GMT
16 vary: X-Twitter-Internal,X-Twitter-IP-Tags
17 cache-control: max-age=0
18
19 <!DOCTYPE html>
20 <html lang="en" dir="ltr" prefix="og: http://ogp.me/ns#" data-behavior="118n" data-environment="prod" data-server-mode="publish" data-dc="s">
21   <head>
22     <meta charset="utf-8"/>
23
24     <meta name="viewport" content="width=device-width, initial-scale=1"/>
25
26     <title>In-app monetization for app publishers | MoPub</title>
27     <meta name="description" content="MoPub, a Twitter company, provides monetization solutions for mobile app publishers and developers around the globe. See how we help maximize your a
```

```

36 <meta property="og:type" content="article"/>
37 <meta property="og:title" content="In-app monetization for app publishers | MoPub"/>
38 <meta property="og:description" content="MoPub, a Twitter company, provides monetization solutions for mobile app publishers and developers around the globe. See how we help maximize
39 <meta property="og:image" content="https://www.mopub.com/content/dam/mopub-aem-twitter/resource-pdf/en/homepage/mopub-web-tweetcard-r1.jpg.twimg.768.jpg"/>
40 <meta name="keywords"/>
41
42
43 <meta name="twitter:card" content="summary_large_image"/>
44 <meta name="twitter:site" content="mopub"/>
45

```

Solutions to take

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
 - If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
 - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
 - Serve an HSTS header on the base domain for HTTPS requests:
 - The max-age must be at least 31536000 seconds (1 year)
 - The includeSubDomains directive must be specified
 - The preload directive must be specified
- 4 / 10
- If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

2. Weak Ciphers Enabled

- Severity: MEDIUM
- Method: GET

During secure communication, weak ciphers are permitted to be used (SSL)

Impact

- In some cases, attackers may decode SSL traffic that is transmitted between your server and your visitors.

Request

[NETSPARKER] SSL Connection

Response

[NETSPARKER] SSL Connection

Solutions to take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- a. Click Start, click Run, type regedt32 or type regedit, and then click OK.
- b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
- c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

Overview of Vulnerabilities

Vulnerability	Risk Level
twitter.com	
Weak Ciphers Enabled	Medium
[Possible] BREACH Attack Detected	Medium
[Possible] Cross-site Scripting	Medium
HTTP Strict Transport Security (HSTS) Errors and Warnings	Medium
Out-of-date Version (jQuery)	Medium
vine.co	
Out-of-date Version (Moment.js)	High
Weak Ciphers Enabled	Medium
HTTP Strict Transport Security (HSTS) Errors and Warnings	Medium
Out-of-date Version (jQuery)	Medium
Insecure Transport Security Protocol Supported (TLS 1.0)	Low
Insecure Transport Security Protocol Supported (TLS 1.0)	High
periscope.tv	
Weak Ciphers Enabled	Low
Strict Transport Security Not Enforced	Low
pscp.tv	
Weak Ciphers Enabled	Low
Strict Transport Security Not Enforced	Low
gnip.com	
HTTP Strict Transport Security (HSTS) Errors and Warnings	Medium
Weak Ciphers Enabled	Low
mopub.com	
HTTP Strict Transport Security (HSTS) Errors and Warnings	Medium
Weak Ciphers Enabled	Medium

Conclusion

This study has emphasized the vulnerabilities of the www.twitter.com domain and made recommendations for its protection. All of the vulnerabilities that have been identified are classified according to their risk level, which includes high, medium, low, and informational. Aside from that, I've included detailed descriptions of the tools I've used and the installation process I went through to complete this work.

A comprehensive security strategy was developed and implemented to ensure that the web application is protected from cyber-attacks. I've uncovered two high-risk vulnerabilities that need to be addressed. Aside from that, the majority of the vulnerabilities are of low to medium severity.

Reference

<https://github.com/aboul3la/Sublist3r>

<https://github.com/nmap/nmap>

<https://github.com/lanmaster53/recon-ng>

<https://github.com/EnableSecurity/wafw00f>

<https://www.youtube.com/watch?v=EoaDgUgS6QA>

<https://www.youtube.com/watch?v=IWbmP0Z-yQg>