WEB APPLICATION ATTACK VECTORS

2026

FIND.
UNDERSTAND.
EXPLOIT.
DEFEND.

REAL-WORLD EXAMPLES

TECHNIQUES THAT MATTER

DEFENSIVE INSIGHTS

STEVE T.

Web Application Attack Vectors 2026

An Advanced Guide for Security Professionals and Developers (Updated Edition)

Steve T.

This book is available at
https://leanpub.com/webapplicationattackvectors2026

This version was published on 2026-06-19

Contents

Web Application Attack Vectors 2026 . . . . . **1**
About this Book 1

Table of Contents **3**
Foreword 4
Preface 5
Who This Book Is For 5
Prerequisites 5
Ethical Considerations and Legal Disclaimer 5
How This Book Is Structured 5
Chapter 1: Beyond the Basics - Revisiting the Foundations with an Advanced Lens 6
1.1 Advanced Reconnaissance and Information Gathering 6
1.1.1 OSINT for Web Targets (Subdomain Enumeration, Tech Stack Fingerprinting, Dev/Secret Leakage) 6
1.1.2 Active Probing Techniques (Advanced Port Scanning, Service Versioning, WAF Detection/Fingerprinting) 6
1.1.3 JavaScript Source Code Analysis (Endpoint Discovery, Logic Flaws, Secret Exposure) 6
1.1.4 API Discovery and Mapping (Swagger/OpenAPI, GraphQL Introspection, Traffic Analysis) 6
1.2 Understanding Modern Web Architectures 7
1.2.1 Single Page Applications (SPAs) and Client-Side Routing 7
1.2.2 Microservices and API Gateways 7
1.2.3 Serverless Functions (FaaS) 7
1.2.4 Content Delivery Networks (CDNs) and Edge Computing 7
1.3 Advanced Proxy Usage and Configuration (Burp Suite/OWASP ZAP) 7
1.3.1 Custom Scripting (Macros, Extenders, Python/Ruby Integration) 8
1.3.2 Advanced Scoping and Target Definition 8
1.3.3 Collaboration Features and Project Management 8

Chapter 2: Deep Dive into Injection Vulnerabilities 9
2.1 SQL Injection: Advanced Exploitation 9
2.1.1 Second-Order SQL Injection 9
Definition and Concept: 9
Mechanism Breakdown: 9
Example Scenario: User Profile Update and Display 9
Detection Challenges: 9
Exploitation Techniques: 9
Mitigation: 10
2.1.2 Advanced Blind SQLi Techniques (Time-Based, Error-Based, Boolean-Based Optimization) 11
Boolean-Based Blind SQLi: Optimization Strategies 11
Time-Based Blind SQLi: Handling Instability and Optimizing 11
Error-Based Blind SQLi: Leveraging Conditional Errors 11
Combining Techniques and Tooling: 11
Mitigation Reminder: 11
2.1.3 Out-of-Band (OOB) SQL Injection 12
Prerequisites: 12
Mechanism: 12
Techniques by Database System: 12
Data Exfiltration Formatting: 12
Challenges and Considerations: 12
Tooling: 12
Mitigation: 12
2.1.4 Exploiting Specific Database Features 14
PostgreSQL Specific Features: 14
Microsoft SQL Server (MSSQL) Specific Features: 14
Oracle Specific Features: 14
MySQL/MariaDB Specific Features: 14
Mitigation: 14
2.1.5 WAF Bypass Techniques for SQLi 15
Common WAF Detection Mechanisms for SQLi: 15
Bypass Techniques: 15
Methodology and Tooling: 15
Conclusion on WAF Bypass: 15
2.2 NoSQL Injection 16
Key Differences from SQL Injection: 16
2.2.1 Identifying NoSQL Databases 16

2.2.2 Syntax Differences and Attack Vectors 16
Example Scenario (MongoDB Focus): 16
Attack Vector 1: Bypassing Authentication via Operator Injection . . . 16
Attack Vector 2: Injecting via URL Parameters (if applicable) 16
2.2.3 Exploiting Operator Injection (`$where`, `$regex`, `$ne`, etc.) 17
2.2.4 Server-Side JavaScript Injection via NoSQL 17
Mitigation Strategies: 17
2.3 Server-Side Template Injection (SSTI) 18
Core Concept: 18
Example Scenario (Python/Flask/Jinja2): 18
2.3.1 Identifying Templating Engines 18
2.3.2 Context Escapes and Sandbox Bypasses 18
2.3.3 Crafting Payloads for RCE 18
Payload Example (Common Jinja2 RCE): 18
2.3.4 Exploiting Blind SSTI 18
Mitigation: 19
2.4 XML External Entity (XXE) Injection 20
XML Fundamentals: DTDs and Entities 20
The Vulnerability: 20
2.4.1 Classic XXE for File Disclosure 20
Common File Paths to Target: 20
2.4.2 XXE for Server-Side Request Forgery (SSRF) 20
2.4.3 Out-of-Band XXE (OOB-XXE) 20
2.4.4 Billion Laughs Attack (XML Bomb / DoS) 20
2.4.5 Exploiting Blind XXE (Error-Based) 21
2.4.6 Content-Type and Parser Specific Exploitation 21
Mitigation (Crucial): 21
2.5 OS Command Injection: Advanced Contexts 22
Recap of Basic Command Injection: 22
Advanced Contexts and Injection Points: 22
2.5.1 Bypassing Filters (Whitespace, Blacklisted Characters, Globbing) 22
2.5.2 Blind OS Command Injection 22
2.5.3 Exploiting Context-Specific Injection Points (ImageMagick, FFmpeg, etc.) 22
Mitigation: 22
2.6 React2Shell and React Server Component Deserialization 24
2.7 Blind Deserialization and Mitigation Bypass (Expanded) 26
Chapter 3: Authentication and Authorization Bypass Techniques . . . 27

3.1 JSON Web Token (JWT) Attacks 27
JWT Structure: 27
3.1.1 Signature Attacks (`alg=none`, Key Confusion, Null Signature) . . . 27
3.1.2 Weak Secret Brute-Forcing 28
Mechanism: 28
Tools for Brute-Forcing: 28
Factors Affecting Success: 28
Impact: 28
Mitigation: 28
3.1.3 Header Parameter Injection (`kid`, `jku`, `x5u`) 29
The Vulnerability: 29
`jku` (JWK Set URL) Attack: 29
`x5u` (X.509 URL) Attack: 29
`kid` (Key ID) Path Traversal / SQL Injection Attack: 29
General Best Practices: 29
3.1.4 Replay Attacks and Timing Issues 30
Replay Attacks: 30
Timing Issues (`exp`, `nbf`, `iat`): 30
Mitigation Strategies for Replay and Timing Issues: 30
3.2 SAML Attacks 31
SAML Flow Overview (SP-Initiated SSO): 31
SAML Structure (XML): 31
3.2.1 Signature Wrapping (XML Signature Wrapping - XSW) 31
3.2.2 Assertion Manipulation (Modifying Attributes, Validity Period) . . 31
3.2.3 Cross-Site Scripting (XSS) via SAML Responses 31
3.3 OAuth 2.0 and OpenID Connect Flaws 32
Key Actors in OAuth 2.0 / OIDC: 32
OAuth 2.0 Grant Types (Flows): 32
3.3.1 Implicit Grant Flow Issues 32
3.3.2 Redirect URI Validation Bypass 32
3.3.3 State Parameter Fixation/Hijacking 32
3.3.4 Scope Misconfiguration and Privilege Escalation 32
3.3.5 Client Secret Leakage and Consequences 32
3.4 Multi-Factor Authentication (MFA) Bypass Strategies 34
3.4.1 Exploiting Weak Recovery Mechanisms 34
3.4.2 Rate Limiting and Brute-Force on OTPs 34
3.4.3 Bypassing MFA During Initial Login Flow 34
3.4.4 Session Token Reuse After MFA 34

3.4.5 Social Engineering and Factor Compromise 34
3.5 Complex Access Control Vulnerabilities 35
3.5.1 Horizontal and Vertical Privilege Escalation via Parameter Manipulation 35
3.5.2 Exploiting State Machines and Workflow Logic Flaws 35
3.5.3 HTTP Method Tampering for Authz Bypass 35
3.5.4 Insecure Direct Object References (IDOR) in Complex Systems (GUIDs, Hashed IDs) 35
Overall Mitigation Strategy for Access Control: 35
3.6 OAuth 2.1 Implementation Pitfalls 36
3.7 OAuth Implementation Best Practices Summary 38
Chapter 4: Exploiting Complex Client-Side Vulnerabilities 39
4.1 Advanced Cross-Site Scripting (XSS) 39
4.1.1 DOM-Based XSS Deep Dive (Sources, Sinks, Taint Tracking) 39
4.1.2 Mutation XSS (mXSS) 40
The Problem: Sanitization vs. Browser Parsing Quirks 40
Example Scenario (Conceptual): 40
Key Characteristics of mXSS: 40
Discovering mXSS: 40
Impact: 40
Mitigation: 40
4.1.3 XSS in Uncommon Contexts (SVG, MathML, Service Workers, WebSockets) 41
1. XSS within SVG (Scalable Vector Graphics) 41
2. XSS within MathML (Mathematical Markup Language) 41
3. XSS via Service Workers 41
4. XSS via WebSockets 41
General Principle: 41
4.1.4 Bypassing Content Security Policy (CSP) 42
Understanding CSP Directives: 42
Common Source Values: 42
CSP Bypass Techniques: 42
Developing Secure CSPs: 42
4.1.5 Exploiting PostMessage Vulnerabilities 43
How `postMessage` Works: 43
Vulnerabilities in `postMessage` Implementation: 43
Finding `postMessage` Vulnerabilities: 43
4.1.6 Universal XSS (UXSS) and Browser-Level Flaws (Conceptual) . . . 44

Key Differences from Standard XSS: . . . 44
Root Causes and Conceptual Examples: . . . 44
Impact: . . . 44
Mitigation and Responsibility: . . . 44
Conclusion on UXSS: . . . 44
4.2 JavaScript Prototype Pollution . . . 45
Understanding Prototypes in JavaScript: . . . 45
The Vulnerability: . . . 45
4.2.1 Identifying Vulnerable Code Patterns . . . 45
4.2.2 Client-Side Exploitation . . . 45
Finding Gadgets: . . . 45
4.2.3 Server-Side Exploitation (Context) . . . 45
Mitigation: . . . 45
4.3 DOM Clobbering . . . 47
The Mechanism: Named Access on `window` and `document` . . . 47
The Vulnerability: . . . 47
Example Scenario: . . . 47
Key Clobbering Patterns and Targets: . . . 47
4.3.1 Overwriting Global Variables and Functions . . . 47
4.3.2 Bypassing Security Checks (DOMPurify, etc.) . . . 47
4.3.3 Chaining with Other Vulnerabilities . . . 48
Mitigation: . . . 48
4.4 Advanced Cross-Site Request Forgery (CSRF) . . . 49
Classic CSRF Recap: . . . 49
4.4.1 CSRF against JSON Endpoints . . . 49
4.4.2 Bypassing Referer Checks and Origin Headers . . . 49
4.4.3 Login/Logout CSRF Attacks . . . 49
4.4.4 Exploiting CSRF in APIs without Standard Browser Protections . . . 49
General CSRF Best Practices: . . . 49
4.5 Clickjacking and UI Redressing: Advanced Techniques . . . 50
Classic Clickjacking Recap: . . . 50
4.5.1 Bypassing Frame-Busting Scripts . . . 50
4.5.2 Drag-and-Drop Attacks . . . 50
4.5.3 Exploiting Nested Contexts and Partial Overlays . . . 50
4.5.4 Content Security Policy `frame-ancestors` Bypass (Misconfigurations) . . . 50
Mitigation: . . . 50
Conclusion on Clickjacking: . . . 51

Chapter 5: Server-Side Request Forgery (SSRF) - In Depth 52
5.1 Identifying SSRF Vulnerabilities 52
5.1.1 Explicit SSRF (URL Parameters) 52
5.1.2 Blind SSRF (No Direct Response) 52
5.1.3 SSRF via Uncommon Protocols (`gopher://`, `dict://`, `file://`) . 52
SSRF via Data Formats and Headers: 52
5.2 Exploitation Techniques 53
5.2.1 Internal Network Scanning and Port Enumeration 53
5.2.2 Interacting with Internal Services 53
5.2.3 Reading Local Files (`file://` wrapper) 53
5.2.4 Cloud Instance Metadata Abuse 53
5.2.5 Chaining SSRF with Other Vulnerabilities 53
5.3 Bypassing SSRF Filters 54
Common Filtering Strategies: 54
Bypass Techniques: 54
Testing Bypass Techniques: 54
Mitigation (Building Robust Filters): 54
Chapter 6: Deserialization Vulnerabilities 55
6.1 Understanding Serialization and Deserialization 55
6.1.1 Common Formats 55
6.1.2 The Concept of Gadget Chains 55
6.2 Java Deserialization Attacks 56
6.2.1 Identifying Vulnerable Libraries (e.g., Apache Commons Collections) 56
Identifying Vulnerable Applications: 56
6.2.2 Using Tools like `ysoserial` 56
6.2.3 Exploiting Custom Serializable Objects 56
6.2.4 Targeting RMI, JMX, JMS Endpoints 56
Mitigation Strategies for Java Deserialization: 56
6.3 PHP Deserialization (Object Injection) 57
6.3.1 Identifying `unserialize()` Usage 57
PHP Serialized Format Recap: 57
6.3.2 Finding POP (Property Oriented Programming) Gadgets 57
6.3.3 Exploiting Phar Deserialization (`phar://` wrapper) 57
Mitigation for General PHP Deserialization: 57
6.4 Python Deserialization (Pickle) 58
6.4.1 The `pickle` Module Dangers 58
Python Pickle Format (Conceptual): 58
Identifying Vulnerable Code: 58

6.4.2 Crafting Malicious Pickle Payloads (`__reduce__`) 58
Mitigation (Crucial): 58
6.5 .NET Deserialization 59
6.5.1 Targeting `BinaryFormatter`, `LosFormatter`, `JSON.NET`, `XmlSerializer` 59
6.5.2 Using Tools like `ysoserial.net` 59
Mitigation Strategies for .NET Deserialization: 59
6.6 Blind Deserialization and Mitigation Bypass 60
Blind Deserialization Exploitation: 60
Mitigation Bypass Techniques: 60
Conclusion on Blind Exploitation and Bypasses: 60
Chapter 7: Attacking APIs and Microservices 61
7.1 REST API Security Testing 61
7.1.1 Authentication/Authorization Flaws (API Keys, JWT, OAuth) 61
7.1.2 Rate Limiting and Resource Exhaustion 61
7.1.3 Mass Assignment Vulnerabilities 61
7.1.4 Injection Vulnerabilities in API Parameters 61
7.1.5 SSRF via API Endpoints 61
7.2 GraphQL Security Testing 62
GraphQL Fundamentals: 62
7.2.1 Introspection Query Abuse 62
7.2.2 Denial of Service via Deeply Nested/Complex Queries 62
7.2.3 Authorization Bypass in Resolvers 62
7.2.4 Batching Attack Amplification 62
7.2.5 Injection within GraphQL Arguments 62
7.3 Attacking gRPC and Protocol Buffers 63
gRPC Fundamentals: 63
7.3.1 Service Discovery and Method Enumeration 63
7.3.2 Manipulating Protobuf Payloads 63
7.3.3 Authentication and Authorization Issues 63
7.3.4 Exploiting Server Reflection 63
7.3.5 Denial of Service 63
7.3.6 Traditional Injection (via Protobuf Data) 63
Mitigation Strategies Specific to gRPC: 64
7.4 API Gateway and Service Mesh Security Issues 65
7.4.1 Misconfigurations in Routing and Authentication (API Gateways / Ingress) 65
7.4.2 Bypassing Security Policies at the Gateway 65

7.4.3 Service Mesh Security Issues (e.g., Istio, Linkerd) 65
Testing and Mitigation Strategies: 65
Chapter 8: Exploiting Business Logic Flaws 66
8.1 Identifying Logic Flaws 66
8.1.1 Understanding Application Workflows 66
8.1.2 Threat Modeling Business Processes 66
8.1.3 Looking for Assumptions and Edge Cases 66
8.2 Common Patterns 66
8.2.1 Parameter Tampering for Unauthorized Actions 66
8.2.2 Exploiting Weak Validation Logic 66
8.2.3 Circumventing Multi-Step Processes 67
8.2.4 Price Manipulation and Discount Abuse (Revisited) 67
8.2.5 Feature Abuse 67
Mitigation for Business Logic Flaws: 67
8.3 Race Conditions 68
8.3.1 Identifying Potential Race Conditions (TOCTOU - Time-of-Check to Time-of-Use) 68
8.3.2 Exploitation Techniques 68
8.3.3 Tools and Techniques for Triggering Race Conditions 68
Mitigation Strategies: 68
Chapter 9: Web Cache Poisoning and Deception 69
9.1 Understanding Web Caching Mechanisms 69
9.2 Cache Poisoning Techniques 69
9.2.1 Exploiting Unkeyed Inputs (Headers, Cookies) 69
9.2.2 HTTP Request Smuggling for Cache Poisoning 69
9.2.3 Chaining with XSS or Open Redirects 69
Mitigation for Cache Poisoning: 69
9.3 Cache Deception Attacks 69
Mitigation for Cache Deception: 70
9.4 Edge Side Includes (ESI) Injection 70
9.4.1 Identifying ESI Usage: 70
9.4.2 Exploiting ESI for SSRF and XSS: 70
Chapter 10: HTTP Request Smuggling 71
10.1 Understanding Ambiguous Requests (CL.TE, TE.CL, TE.TE) 71
10.1.1 CL.TE: Front-End uses `Content-Length`, Back-End uses `Transfer-Encoding` 71
10.1.2 TE.CL: Front-End uses `Transfer-Encoding`, Back-End uses `Content-Length` 71

10.1.3 TE.TE: Front-End and Back-End both use `Transfer-Encoding`, but one can be Downgraded/Obfuscated 71
10.2 Identifying Request Smuggling Vulnerabilities 71
10.3 Exploitation Techniques 72
10.3.1 Bypassing Front-End Security Controls 72
10.3.2 Session Hijacking / Request Hijacking 72
10.3.3 Web Cache Poisoning via Request Smuggling 72
10.3.4 Cross-Site Scripting (XSS) via Smuggled Requests 72
Mitigation: 72
10.4 HTTP/3 QUIC Request Smuggling and TOCTOU (QUIC-er Races) 73
10.5 HTTP/3 Impact on Traditional Attack Vectors 74
Chapter 11: Cloud-Native Application Security 75
11.1 Serverless (FaaS) Security Issues 75
11.2 Container Security (Docker, Kubernetes) 75
11.3 Cloud Storage Misconfigurations (S3, Azure Blob, GCS) 75
11.4 Infrastructure as Code (IaC) Security Review 75
Chapter 12: Advanced Evasion Techniques 76
12.1 Bypassing Web Application Firewalls (WAFs) 76
12.2 Bypassing Client-Side Controls 76
12.3 Rate Limit Bypass Techniques 76
Conclusion on Evasion: 76
12.4 WAFFLED: Parsing Discrepancy-Based WAF Bypass 77
12.5 AI-Powered WAF Bypass Optimization 79
Chapter 13: Exploit Chaining and Post-Exploitation 80
13.1 The Art of Chaining Vulnerabilities 80
13.2 Web-Based Post-Exploitation 80
Conclusion: 80
Chapter 14: Reporting, Remediation, and Future Trends 81
14.1 Writing High-Quality Technical Reports 81
14.2 Advanced Remediation Strategies 81
14.3 Emerging Threats and Future Trends 81
Concluding Thoughts: 81
Appendix A: Tooling Quick Reference 82
Appendix B: Useful Payloads and Cheat Sheets 83

Web Application Attack Vectors 2026

An Advanced Guide for Security Professionals and Developers (Updated Edition)

About this Book

This book provides a deep, technical exploration of advanced web application attack vectors relevant to modern architectures. It moves significantly beyond introductory concepts, covering sophisticated techniques for injection exploitation, authentication bypasses, client-side attacks, SSRF, deserialization flaws, API security testing, business logic exploitation, cache poisoning, HTTP request smuggling, cloud-native vulnerabilities, evasion techniques, exploit chaining, and emerging trends.

This 2026 updated edition adds substantial new content covering:

- **React2Shell (CVE-2025-55182):** A critical RCE in React Server Components with active exploitation by state-sponsored threat actors
- **WAFFLED:** Parsing discrepancy-based WAF bypass techniques discovered via black-box fuzzing research
- **HTTP/3 QUIC Security:** New TOCTOU race condition attacks (QUIC-er Races, Single Datagram Attacks) and QUIC-LEAK vulnerability
- **OAuth 2.1 Pitfalls:** Device code phishing (Storm-2372), consent phishing, cross-app attacks, domain resurrection, DPoP misuse
- **AI/ML-Powered Web Attacks:** Prompt injection, AI-driven reconnaissance, deepfake social engineering, LLMjacking, MCP server attacks
- **WebAssembly Security:** WASM memory safety, WASM-to-JS binding exploitation, side-channel attacks
- **IoT Web API Security:** MQTT/CoAP vulnerabilities, DDoS amplification, physical security implications
- **Software Supply Chain Attacks:** npm/PyPI package injection, Hugging Face model poisoning

Written for intermediate to advanced security professionals, this guide equips penetration testers, application security engineers, and developers with the knowledge and practical techniques needed to understand, identify, and defend against the evolving threats targeting today's web applications.

Table of Contents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Foreword

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Preface

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Who This Book Is For

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Prerequisites

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Ethical Considerations and Legal Disclaimer

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

How This Book Is Structured

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 1: Beyond the Basics - Revisiting the Foundations with an Advanced Lens

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.1 Advanced Reconnaissance and Information Gathering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.1.1 OSINT for Web Targets (Subdomain Enumeration, Tech Stack Fingerprinting, Dev/Secret Leakage)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.1.2 Active Probing Techniques (Advanced Port Scanning, Service Versioning, WAF Detection/Fingerprinting)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.1.3 JavaScript Source Code Analysis (Endpoint Discovery, Logic Flaws, Secret Exposure)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.1.4 API Discovery and Mapping (Swagger/OpenAPI, GraphQL Introspection, Traffic Analysis)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.2 Understanding Modern Web Architectures

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.2.1 Single Page Applications (SPAs) and Client-Side Routing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.2.2 Microservices and API Gateways

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.2.3 Serverless Functions (FaaS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.2.4 Content Delivery Networks (CDNs) and Edge Computing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.3 Advanced Proxy Usage and Configuration (Burp Suite/OWASP ZAP)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.3.1 Custom Scripting (Macros, Extenders, Python/Ruby Integration)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.3.2 Advanced Scoping and Target Definition

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1.3.3 Collaboration Features and Project Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 2: Deep Dive into Injection Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.1 SQL Injection: Advanced Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.1.1 Second-Order SQL Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Definition and Concept:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mechanism Breakdown:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Example Scenario: User Profile Update and Display

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Detection Challenges:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Exploitation Techniques:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.1.2 Advanced Blind SQLi Techniques (Time-Based, Error-Based, Boolean-Based Optimization)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Boolean-Based Blind SQLi: Optimization Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Time-Based Blind SQLi: Handling Instability and Optimizing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Error-Based Blind SQLi: Leveraging Conditional Errors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Combining Techniques and Tooling:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Reminder:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.1.3 Out-of-Band (OOB) SQL Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Prerequisites:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mechanism:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Techniques by Database System:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Data Exfiltration Formatting:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Challenges and Considerations:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Tooling:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.1.4 Exploiting Specific Database Features

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

PostgreSQL Specific Features:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Microsoft SQL Server (MSSQL) Specific Features:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Oracle Specific Features:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

MySQL/MariaDB Specific Features:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.1.5 WAF Bypass Techniques for SQLi

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Common WAF Detection Mechanisms for SQLi:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Bypass Techniques:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Methodology and Tooling:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Conclusion on WAF Bypass:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.2 NoSQL Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Key Differences from SQL Injection:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.2.1 Identifying NoSQL Databases

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.2.2 Syntax Differences and Attack Vectors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Example Scenario (MongoDB Focus):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Attack Vector 1: Bypassing Authentication via Operator Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Attack Vector 2: Injecting via URL Parameters (if applicable)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.2.3 Exploiting Operator Injection (`$where`, `$regex`, `$ne`, etc.)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.2.4 Server-Side JavaScript Injection via NoSQL

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Strategies:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.3 Server-Side Template Injection (SSTI)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Core Concept:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Example Scenario (Python/Flask/Jinja2):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.3.1 Identifying Templating Engines

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.3.2 Context Escapes and Sandbox Bypasses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.3.3 Crafting Payloads for RCE

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Payload Example (Common Jinja2 RCE):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.3.4 Exploiting Blind SSTI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.4 XML External Entity (XXE) Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

XML Fundamentals: DTDs and Entities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

The Vulnerability:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.4.1 Classic XXE for File Disclosure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Common File Paths to Target:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.4.2 XXE for Server-Side Request Forgery (SSRF)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.4.3 Out-of-Band XXE (OOB-XXE)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.4.4 Billion Laughs Attack (XML Bomb / DoS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.4.5 Exploiting Blind XXE (Error-Based)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.4.6 Content-Type and Parser Specific Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation (Crucial):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.5 OS Command Injection: Advanced Contexts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Recap of Basic Command Injection:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Advanced Contexts and Injection Points:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.5.1 Bypassing Filters (Whitespace, Blacklisted Characters, Globbing)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.5.2 Blind OS Command Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.5.3 Exploiting Context-Specific Injection Points (ImageMagick, FFmpeg, etc.)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6 React2Shell and React Server Component Deserialization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6.1 Overview of CVE-2025-55182 (CVSS 10.0)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6.2 The React Flight Protocol and RSC Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6.3 Exploit Chain Mechanics (Prototype Traversal, Thenable Execution, Blob Resolution)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6.4 In-the-Wild Exploitation: Threat Actor Activity (Earth Lamia, Jackpot Panda)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6.5 Detection Indicators (next-action, rsc-action-id headers)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6.6 Related Vulnerabilities (CVE-2025-55183, CVE-2025-55184)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.6.7 Patching and Remediation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2.7 Blind Deserialization and Mitigation Bypass (Expanded)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 3: Authentication and Authorization Bypass Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.1 JSON Web Token (JWT) Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

JWT Structure:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.1.1 Signature Attacks (`alg=none`, Key Confusion, Null Signature)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.1.2 Weak Secret Brute-Forcing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mechanism:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Tools for Brute-Forcing:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Factors Affecting Success:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Impact:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.1.3 Header Parameter Injection (`kid`, `jku`, `x5u`)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

The Vulnerability:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

`jku` (JWK Set URL) Attack:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

`x5u` (X.509 URL) Attack:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

`kid` (Key ID) Path Traversal / SQL Injection Attack:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

General Best Practices:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.1.4 Replay Attacks and Timing Issues

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Replay Attacks:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Timing Issues (`exp`, `nbf`, `iat`):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Strategies for Replay and Timing Issues:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.2 SAML Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

SAML Flow Overview (SP-Initiated SSO):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

SAML Structure (XML):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.2.1 Signature Wrapping (XML Signature Wrapping - XSW)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.2.2 Assertion Manipulation (Modifying Attributes, Validity Period)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.2.3 Cross-Site Scripting (XSS) via SAML Responses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.3 OAuth 2.0 and OpenID Connect Flaws

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Key Actors in OAuth 2.0 / OIDC:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

OAuth 2.0 Grant Types (Flows):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.3.1 Implicit Grant Flow Issues

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.3.2 Redirect URI Validation Bypass

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.3.3 State Parameter Fixation/Hijacking

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.3.4 Scope Misconfiguration and Privilege Escalation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.3.5 Client Secret Leakage and Consequences

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.4 Multi-Factor Authentication (MFA) Bypass Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.4.1 Exploiting Weak Recovery Mechanisms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.4.2 Rate Limiting and Brute-Force on OTPs

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.4.3 Bypassing MFA During Initial Login Flow

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.4.4 Session Token Reuse After MFA

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.4.5 Social Engineering and Factor Compromise

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.5 Complex Access Control Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.5.1 Horizontal and Vertical Privilege Escalation via Parameter Manipulation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.5.2 Exploiting State Machines and Workflow Logic Flaws

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.5.3 HTTP Method Tampering for Authz Bypass

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.5.4 Insecure Direct Object References (IDOR) in Complex Systems (GUIDs, Hashed IDs)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Overall Mitigation Strategy for Access Control:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6 OAuth 2.1 Implementation Pitfalls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.1 Cross-App OAuth Attack Waves (COAT) and CORF

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.2 Device Flow Exploitation and Vishing (Storm-2372)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.3 Third-Party Integrator Token Compromise

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.4 Open Redirect and Return URL Abuse

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.5 Domain Resurrection and Mutable Claims

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.6 Cross-Tenant nOAuth Abuse (Microsoft Entra)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.7 DPoP Token Misuse and Missing `cnf` Validation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.8 Client Configuration Confusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.9 Audience Injection in Client Assertions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.10 Integration Platform Privileged Scope Over-Granting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.6.11 Detection Engineering for OAuth Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3.7 OAuth Implementation Best Practices Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 4: Exploiting Complex Client-Side Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.1 Advanced Cross-Site Scripting (XSS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.1.1 DOM-Based XSS Deep Dive (Sources, Sinks, Taint Tracking)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.1.2 Mutation XSS (mXSS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

The Problem: Sanitization vs. Browser Parsing Quirks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Example Scenario (Conceptual):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Key Characteristics of mXSS:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Discovering mXSS:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Impact:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.1.3 XSS in Uncommon Contexts (SVG, MathML, Service Workers, WebSockets)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

1. XSS within SVG (Scalable Vector Graphics)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

2. XSS within MathML (Mathematical Markup Language)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

3. XSS via Service Workers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4. XSS via WebSockets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

General Principle:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.1.4 Bypassing Content Security Policy (CSP)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Understanding CSP Directives:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Common Source Values:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

CSP Bypass Techniques:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Developing Secure CSPs:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.1.5 Exploiting PostMessage Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

How `postMessage` Works:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Vulnerabilities in `postMessage` Implementation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Finding `postMessage` Vulnerabilities:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.1.6 Universal XSS (UXSS) and Browser-Level Flaws (Conceptual)

Key Differences from Standard XSS:

Root Causes and Conceptual Examples:

Impact:

Mitigation and Responsibility:

Conclusion on UXSS:

4.2 JavaScript Prototype Pollution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Understanding Prototypes in JavaScript:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

The Vulnerability:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.2.1 Identifying Vulnerable Code Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.2.2 Client-Side Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Finding Gadgets:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.2.3 Server-Side Exploitation (Context)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.3 DOM Clobbering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

The Mechanism: Named Access on `window` and `document`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

The Vulnerability:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Example Scenario:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Key Clobbering Patterns and Targets:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.3.1 Overwriting Global Variables and Functions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.3.2 Bypassing Security Checks (DOMPurify, etc.)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.3.3 Chaining with Other Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.4 Advanced Cross-Site Request Forgery (CSRF)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Classic CSRF Recap:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.4.1 CSRF against JSON Endpoints

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.4.2 Bypassing Referer Checks and Origin Headers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.4.3 Login/Logout CSRF Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.4.4 Exploiting CSRF in APIs without Standard Browser Protections

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

General CSRF Best Practices:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.5 Clickjacking and UI Redressing: Advanced Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Classic Clickjacking Recap:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.5.1 Bypassing Frame-Busting Scripts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.5.2 Drag-and-Drop Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.5.3 Exploiting Nested Contexts and Partial Overlays

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

4.5.4 Content Security Policy `frame-ancestors` Bypass (Misconfigurations)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Conclusion on Clickjacking:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 5: Server-Side Request Forgery (SSRF) - In Depth

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.1 Identifying SSRF Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.1.1 Explicit SSRF (URL Parameters)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.1.2 Blind SSRF (No Direct Response)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.1.3 SSRF via Uncommon Protocols (`gopher://`, `dict://`, `file://`)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

SSRF via Data Formats and Headers:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.2 Exploitation Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.2.1 Internal Network Scanning and Port Enumeration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.2.2 Interacting with Internal Services

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.2.3 Reading Local Files (`file://` wrapper)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.2.4 Cloud Instance Metadata Abuse

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.2.5 Chaining SSRF with Other Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

5.3 Bypassing SSRF Filters

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Common Filtering Strategies:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Bypass Techniques:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Testing Bypass Techniques:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation (Building Robust Filters):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 6: Deserialization Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.1 Understanding Serialization and Deserialization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.1.1 Common Formats

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.1.2 The Concept of Gadget Chains

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.2 Java Deserialization Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.2.1 Identifying Vulnerable Libraries (e.g., Apache Commons Collections)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Identifying Vulnerable Applications:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.2.2 Using Tools like `ysoserial`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.2.3 Exploiting Custom Serializable Objects

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.2.4 Targeting RMI, JMX, JMS Endpoints

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Strategies for Java Deserialization:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.3 PHP Deserialization (Object Injection)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.3.1 Identifying `unserialize()` Usage

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

PHP Serialized Format Recap:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.3.2 Finding POP (Property Oriented Programming) Gadgets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.3.3 Exploiting Phar Deserialization (`phar://` wrapper)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation for General PHP Deserialization:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.4 Python Deserialization (Pickle)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.4.1 The `pickle` Module Dangers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Python Pickle Format (Conceptual):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Identifying Vulnerable Code:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.4.2 Crafting Malicious Pickle Payloads (`__reduce__`)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation (Crucial):

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.5 .NET Deserialization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.5.1 Targeting `BinaryFormatter`, `LosFormatter`, `JSON.NET`, `XmlSerializer`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.5.2 Using Tools like `ysoserial.net`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Strategies for .NET Deserialization:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

6.6 Blind Deserialization and Mitigation Bypass

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Blind Deserialization Exploitation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Bypass Techniques:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Conclusion on Blind Exploitation and Bypasses:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 7: Attacking APIs and Microservices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.1 REST API Security Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.1.1 Authentication/Authorization Flaws (API Keys, JWT, OAuth)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.1.2 Rate Limiting and Resource Exhaustion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.1.3 Mass Assignment Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.1.4 Injection Vulnerabilities in API Parameters

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.1.5 SSRF via API Endpoints

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.2 GraphQL Security Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

GraphQL Fundamentals:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.2.1 Introspection Query Abuse

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.2.2 Denial of Service via Deeply Nested/Complex Queries

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.2.3 Authorization Bypass in Resolvers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.2.4 Batching Attack Amplification

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.2.5 Injection within GraphQL Arguments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.3 Attacking gRPC and Protocol Buffers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

gRPC Fundamentals:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.3.1 Service Discovery and Method Enumeration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.3.2 Manipulating Protobuf Payloads

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.3.3 Authentication and Authorization Issues

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.3.4 Exploiting Server Reflection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.3.5 Denial of Service

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.3.6 Traditional Injection (via Protobuf Data)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Strategies Specific to gRPC:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.4 API Gateway and Service Mesh Security Issues

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.4.1 Misconfigurations in Routing and Authentication (API Gateways / Ingress)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.4.2 Bypassing Security Policies at the Gateway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

7.4.3 Service Mesh Security Issues (e.g., Istio, Linkerd)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Testing and Mitigation Strategies:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 8: Exploiting Business Logic Flaws

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.1 Identifying Logic Flaws

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.1.1 Understanding Application Workflows

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.1.2 Threat Modeling Business Processes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.1.3 Looking for Assumptions and Edge Cases

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.2 Common Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.2.1 Parameter Tampering for Unauthorized Actions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.2.2 Exploiting Weak Validation Logic

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.2.3 Circumventing Multi-Step Processes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.2.4 Price Manipulation and Discount Abuse (Revisited)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.2.5 Feature Abuse

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation for Business Logic Flaws:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.3 Race Conditions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.3.1 Identifying Potential Race Conditions (TOCTOU - Time-of-Check to Time-of-Use)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.3.2 Exploitation Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

8.3.3 Tools and Techniques for Triggering Race Conditions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation Strategies:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 9: Web Cache Poisoning and Deception

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.1 Understanding Web Caching Mechanisms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.2 Cache Poisoning Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.2.1 Exploiting Unkeyed Inputs (Headers, Cookies)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.2.2 HTTP Request Smuggling for Cache Poisoning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.2.3 Chaining with XSS or Open Redirects

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation for Cache Poisoning:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.3 Cache Deception Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation for Cache Deception:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.4 Edge Side Includes (ESI) Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.4.1 Identifying ESI Usage:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

9.4.2 Exploiting ESI for SSRF and XSS:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 10: HTTP Request Smuggling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.1 Understanding Ambiguous Requests (CL.TE, TE.CL, TE.TE)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.1.1 CL.TE: Front-End uses `Content-Length`, Back-End uses `Transfer-Encoding`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.1.2 TE.CL: Front-End uses `Transfer-Encoding`, Back-End uses `Content-Length`

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.1.3 TE.TE: Front-End and Back-End both use `Transfer-Encoding`, but one can be Downgraded/Obfuscated

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.2 Identifying Request Smuggling Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.3 Exploitation Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.3.1 Bypassing Front-End Security Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.3.2 Session Hijacking / Request Hijacking

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.3.3 Web Cache Poisoning via Request Smuggling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.3.4 Cross-Site Scripting (XSS) via Smuggled Requests

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Mitigation:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.4 HTTP/3 QUIC Request Smuggling and TOCTOU (QUIC-er Races)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.4.1 The QUIC-er Races Paper: HTTP/3 TOCTOU Vulnerabilities (Springer, April 2026)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.4.2 Single Datagram Attack (SDA) Mechanics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.4.3 Critical Concurrency Threshold (N=100)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.4.4 The Smothering Effect: Database-Level Lost Updates

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.4.5 H3SpaceX Framework and Experimental Results

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.4.6 Intermediary De-multiplexing as Synchronization Catalyst

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.5 HTTP/3 Impact on Traditional Attack Vectors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.5.1 Reduced Visibility for Network Security Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.5.2 New SSRF Considerations in UDP-Based Environments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

10.5.3 WAF and IDS Blind Spots

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 11: Cloud-Native Application Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

11.1 Serverless (FaaS) Security Issues

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

11.2 Container Security (Docker, Kubernetes)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

11.3 Cloud Storage Misconfigurations (S3, Azure Blob, GCS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

11.4 Infrastructure as Code (IaC) Security Review

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 12: Advanced Evasion Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.1 Bypassing Web Application Firewalls (WAFs)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.2 Bypassing Client-Side Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.3 Rate Limit Bypass Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Conclusion on Evasion:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4 WAFFLED: Parsing Discrepancy-Based WAF Bypass

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.1 WAFFLED Research Overview (Northeastern/Dartmouth, March 2026)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.2 Targeted WAFs and Frameworks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.3 Multipart/form-data Bypasses (351 instances)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.4 application/xml Bypasses (299 instances)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.5 application/json Bypasses (557 instances, largest category)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.6 Real-World Validation on 100 High-Ranking Websites

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.7 HTTP-Normalizer: RFC Grammar Enforcement as Mitigation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.4.8 Mitigation Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

12.5 AI-Powered WAF Bypass Optimization

Chapter 13: Exploit Chaining and Post-Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

13.1 The Art of Chaining Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

13.2 Web-Based Post-Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Conclusion:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Chapter 14: Reporting, Remediation, and Future Trends

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

14.1 Writing High-Quality Technical Reports

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

14.2 Advanced Remediation Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

14.3 Emerging Threats and Future Trends

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Concluding Thoughts:

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Appendix A: Tooling Quick Reference

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.

Appendix B: Useful Payloads and Cheat Sheets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/webapplicationattackvectors2026.