# Contents

## Introduction

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Web Browser Security</strong></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>A Principal Principle</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Exploring the Browser</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Symbiosis with the Web Application</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Same Origin Policy</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>HTTP Headers</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Markup Languages</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Cascading Style Sheets</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Scripting</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Document Object Model</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Rendering Engines</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Geolocation</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Web Storage</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Cross-origin Resource Sharing</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>HTML5</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Evolutionary Pressures</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>HTTP Headers</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Reflected XSS Filtering</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Sandboxing</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Anti-phishing and Anti-malware</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Mixed Content</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Core Security Problems</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Attack Surface</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Surrendering Control</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>TCP Protocol Control</td>
<td>20</td>
</tr>
</tbody>
</table>
### Contents

- Encrypted Communication 20
- Same Origin Policy 21
- Fallacies 21
- Browser Hacking Methodology 22
- Summary 28
- Questions 28
- Notes 29

#### Chapter 2 Initiating Control 31
- Understanding Control Initiation 32
- Control Initiation Techniques 32
  - Using Cross-site Scripting Attacks 32
  - Using Compromised Web Applications 46
  - Using Advertising Networks 46
  - Using Social Engineering Attacks 47
  - Using Man-in-the-Middle Attacks 59
- Summary 72
- Questions 73
- Notes 73

#### Chapter 3 Retaining Control 77
- Understanding Control Retention 78
- Exploring Communication Techniques 79
  - Using XMLHttpRequest Polling 80
  - Using Cross-origin Resource Sharing 83
  - Using WebSocket Communication 84
  - Using Messaging Communication 86
  - Using DNS Tunnel Communication 89
- Exploring Persistence Techniques 96
  - UsingIFrames 96
  - Using Browser Events 98
  - Using Pop-Under Windows 101
  - Using Man-in-the-Browser Attacks 104
- Evading Detection 110
  - Evasion using Encoding 111
  - Evasion using Obfuscation 116
- Summary 125
- Questions 126
- Notes 127

#### Chapter 4 Bypassing the Same Origin Policy 129
- Understanding the Same Origin Policy 130
  - Understanding the SOP with the DOM 130
  - Understanding the SOP with CORS 131
  - Understanding the SOP with Plugins 132
  - Understanding the SOP with UI Redressing 133
  - Understanding the SOP with Browser History 133
Exploring SOP Bypasses
  Bypassing SOP in Java
  Bypassing SOP in Adobe Reader
  Bypassing SOP in Adobe Flash
  Bypassing SOP in Silverlight
  Bypassing SOP in Internet Explorer
  Bypassing SOP in Safari
  Bypassing SOP in Firefox
  Bypassing SOP in Opera
  Bypassing SOP in Cloud Storage
  Bypassing SOP in CORS

Exploiting SOP Bypasses
  Proxying Requests
  Exploiting UI Redressing Attacks
  Exploiting Browser History

Summary
Questions
Notes

Chapter 5  Attacking Users

Defacing Content
Capture User Input
  Using Focus Events
  Using Keyboard Events
  Using Mouse and Pointer Events
  Using Form Events
  Using IFrame Key Logging

Social Engineering
  Using TabNabbing
  Using the Fullscreen
  Abusing UI Expectations
  Using Signed Java Applets

Privacy Attacks
  Non-cookie Session Tracking
  Bypassing Anonymization
  Attacking Password Managers
  Controlling the Webcam and Microphone

Summary
Questions
Notes

Chapter 6  Attacking Browsers

Fingerprinting Browsers
  Fingerprinting using HTTP Headers
  Fingerprinting using DOM Properties
  Fingerprinting using Software Bugs
  Fingerprinting using Quirks
### Chapter 8  Attacking Plugins

- Understanding Plugin Anatomy 372
  - How Plugins Differ from Extensions 372
  - How Plugins Differ from Standard Programs 374
  - Calling Plugins 374
  - How Plugins are Blocked 376
- Fingerprinting Plugins 377
  - Detecting Plugins 377
  - Automatic Plugin Detection 379
  - Detecting Plugins in BeEF 380
- Attacking Plugins 382
  - Bypassing Click to Play 382
  - Attacking Java 388
  - Attacking Flash 400
  - Attacking ActiveX Controls 403
  - Attacking PDF Readers 408
  - Attacking Media Plugins 410
- Summary 415
- Questions 416
- Notes 416

### Chapter 9  Attacking Web Applications

- Sending Cross-origin Requests 422
  - Enumerating Cross-origin Quirks 422
  - Preflight Requests 425
  - Implications 425
- Cross-origin Web Application Detection 426
  - Discovering Intranet Device IP Addresses 426
  - Enumerating Internal Domain Names 427
- Cross-origin Web Application Fingerprinting 429
  - Requesting Known Resources 430
- Cross-origin Authentication Detection 436
- Exploiting Cross-site Request Forgery 440
  - Understanding Cross-site Request Forgery 440
  - Attacking Password Reset with XSRF 443
  - Using CSRF Tokens for Protection 444
- Cross-origin Resource Detection 445
- Cross-origin Web Application Vulnerability Detection 450
  - SQL Injection Vulnerabilities 450
  - Detecting Cross-site Scripting Vulnerabilities 465
- Proxying through the Browser 469
  - Browsing through a Browser 472
  - Burp through a Browser 477
  - Sqlmap through a Browser 480
  - Browser through Flash 482
- Launching Denial-of-Service Attacks 487
  - Web Application Pinch Points 487
  - DDoS Using Multiple Hooked Browsers 489
Launching Web Application Exploits 493
Cross-origin DNS Hijack 493
Cross-origin JBoss JMX Remote Command Execution 495
Cross-origin GlassFish Remote Command Execution 497
Cross-origin m0n0wall Remote Command Execution 501
Cross-origin Embedded Device Command Execution 502

Summary 508
Questions 508
Notes 509

Chapter 10  Attacking Networks 513

Identifying Targets 514
Identifying the Hooked Browser’s Internal IP 514
Identifying the Hooked Browser’s Subnet 520
Ping Sweeping 523
Ping Sweeping using XMLHttpRequest 523
Ping Sweeping using Java 528
Port Scanning 531
Bypassing Port Banning 532
Port Scanning using the IMG Tag 537
Distributed Port Scanning 539
Fingerprinting Non-HTTP Services 542
Attacking Non-HTTP Services 545
NAT Pinning 545
Achieving Inter-protocol Communication 549
Achieving Inter-protocol Exploitation 564
Getting Shells using BeEF Bind 579
The BeEF Bind Shellcode 579
Using BeEF Bind in your Exploits 585
Using BeEF Bind as a Web Shell 596
Summary 599
Questions 600
Notes 601

Chapter 11  Epilogue: Final Thoughts 605

Index 609