

BRIEF CONTENTS

Acknowledgments	xvii
Introduction	xix
Chapter 1: Let's Hack a Website	1
PART I: THE BASICS.	5
Chapter 2: How the Internet Works	7
Chapter 3: How Browsers Work	15
Chapter 4: How Web Servers Work	23
Chapter 5: How Programmers Work	35
PART II: THE THREATS	47
Chapter 6: Injection Attacks	49
Chapter 7: Cross-Site Scripting Attacks	65
Chapter 8: Cross-Site Request Forgery Attacks	75
Chapter 9: Compromising Authentication	81
Chapter 10: Session Hijacking	93
Chapter 11: Permissions	103
Chapter 12: Information Leaks	113
Chapter 13: Encryption	117
Chapter 14: Third-Party Code	131
Chapter 15: XML Attacks	145
Chapter 16: Don't Be an Accessory	153
Chapter 17: Denial-of-Service Attacks	163
Chapter 18: Summing Up	169
Index	173

CONTENTS IN DETAIL

ACKNOWLEDGMENTS

xvii

INTRODUCTION

xix

About This Book	xx
Who Should Read This Book	xx
A Brief History of the Internet	xx
Scripting in the Browser	xxi
A New Challenger Enters the Arena	xxi
Machines for Writing HTML	xxii
A Series of Tubes	xxii
What to Worry About First	xxiii
What's in This Book	xxiii

1

LET'S HACK A WEBSITE

1

Software Exploits and the Dark Web	1
How to Hack a Website	3

PART I: THE BASICS

5

2

HOW THE INTERNET WORKS

7

The Internet Protocol Suite	7
Internet Protocol Addresses	8
The Domain Name System	9
Application Layer Protocols	9
HyperText Transfer Protocol	10
Stateful Connections	13
Encryption	14
Summary	14

3

HOW BROWSERS WORK

15

Web Page Rendering	15
The Rendering Pipeline: An Overview	16
The Document Object Model	17
Styling Information	17

JavaScript	18
Before and After Rendering: Everything Else the Browser Does.	20
Summary	20

4 HOW WEB SERVERS WORK 23

Static and Dynamic Resources	24
Static Resources	24
URL Resolution	24
Content Delivery Networks	26
Content Management Systems	26
Dynamic Resources	27
Templates	28
Databases	28
Distributed Caches	30
Web Programming Languages	31
Summary	34

5 HOW PROGRAMMERS WORK 35

Phase 1: Design and Analysis	36
Phase 2: Writing Code	37
Distributed vs. Centralized Version Control	37
Branching and Merging Code	38
Phase 3: Pre-Release Testing	38
Coverage and Continuous Integration	39
Test Environments	39
Phase 4: The Release Process	40
Options for Standardized Deployment During Releases	41
The Build Process	42
Database Migration Scripts	43
Phase 5: Post-Release Testing and Observation	43
Penetration Testing	44
Monitoring, Logging, and Error Reporting	44
Dependency Management	45
Summary	45

PART II: THE THREATS 47

6 INJECTION ATTACKS 49

SQL Injection	50
What Is SQL?	50
Anatomy of a SQL Injection Attack	51
Mitigation 1: Use Parameterized Statements	52
Mitigation 2: Use Object-Relational Mapping	54
Bonus Mitigation: Use Defense in Depth	55

Command Injection	56
Anatomy of a Command Injection Attack	56
Mitigation: Escape Control Characters	57
Remote Code Execution	59
Anatomy of a Remote Code Execution Attack	59
Mitigation: Disable Code Execution During Deserialization	59
File Upload Vulnerabilities	60
Anatomy of a File Upload Attack	60
Mitigations	61
Summary	63

7 CROSS-SITE SCRIPTING ATTACKS 65

Stored Cross-Site Scripting Attacks	66
Mitigation 1: Escape HTML Characters	67
Mitigation 2: Implement a Content Security Policy	69
Reflected Cross-Site Scripting Attacks	70
Mitigation: Escape Dynamic Content from HTTP Requests	71
DOM-Based Cross-Site Scripting Attacks	71
Mitigation: Escaping Dynamic Content from URI Fragments	73
Summary	73

8 CROSS-SITE REQUEST FORGERY ATTACKS 75

Anatomy of a CSRF Attack	76
Mitigation 1: Follow REST Principles	76
Mitigation 2: Implement Anti-CSRF Cookies	77
Mitigation 3: Use the SameSite Cookie Attribute	78
Bonus Mitigation: Require Reauthentication for Sensitive Actions	79
Summary	79

9 COMPROMISING AUTHENTICATION 81

Implementing Authentication	82
HTTP-Native Authentication	82
Non-Native Authentication	83
Brute-Force Attacks	83
Mitigation 1: Use Third-Party Authentication	84
Mitigation 2: Integrate with Single Sign-On	84
Mitigation 3: Secure Your Own Authentication System	85
Requiring Usernames, Email Address, or Both	85
Requiring Complex Passwords	87
Securely Storing Passwords	88
Requiring Multifactor Authentication	89
Implementing and Securing the Logout Function	90
Preventing User Enumeration	91
Summary	92

10		
SESSION HIJACKING		93
How Sessions Work		94
Server-Side Sessions		94
Client-Side Sessions		96
How Attackers Hijack Sessions		97
Cookie Theft		97
Session Fixation		99
Taking Advantage of Weak Session IDs		100
Summary		100

11		
PERMISSIONS		103
Privilege Escalation		104
Access Control		104
Designing an Authorization Model		105
Implementing Access Control		106
Testing Access Control		107
Adding Audit Trails		107
Avoiding Common Oversights		108
Directory Traversal		108
Filepaths and Relative Filepaths		108
Anatomy of a Directory Traversal Attack		109
Mitigation 1: Trust Your Web Server		110
Mitigation 2: Use a Hosting Service		110
Mitigation 3: Use Indirect File References		111
Mitigation 4: Sanitize File References		111
Summary		112

12		
INFORMATION LEAKS		113
Mitigation 1: Disable Telltale Server Headers		114
Mitigation 2: Use Clean URLs		114
Mitigation 3: Use Generic Cookie Parameters		114
Mitigation 4: Disable Client-Side Error Reporting		115
Mitigation 5: Minify or Obfuscate Your JavaScript Files		115
Mitigation 6: Sanitize Your Client-Side Files		116
Stay on Top of Security Advisories		116
Summary		116

13		
ENCRYPTION		117
Encryption in the Internet Protocol		118
Encryption Algorithms, Hashing, and Message Authentication Codes		118
The TLS Handshake		120
Enabling HTTPS		122
Digital Certificates		122
Obtaining a Digital Certificate		123
Installing a Digital Certificate		125

Attacking HTTP (and HTTPS)	127
Wireless Routers	128
Wi-Fi Hotspots	128
Internet Service Providers	128
Government Agencies	129
Summary	129

14 **THIRD-PARTY CODE** **131**

Securing Dependencies	132
Know What Code You Are Running	132
Be Able to Deploy New Versions Quickly	134
Stay Alert to Security Issues	135
Know When to Upgrade	136
Securing Configuration	136
Disable Default Credentials	137
Disable Open Directory Listings	137
Protect Your Configuration Information	137
Harden Test Environments	138
Secure Administrative Frontends	138
Securing the Services That You Use	138
Protect Your API Keys	139
Secure Your Webhooks	139
Secure Content Served by Third Parties	140
Services as an Attack Vector	140
Be Wary of Malvertising	141
Avoid Malware Delivery	141
Use a Reputable Ad Platform	142
Use SafeFrame	142
Tailor Your Ad Preferences	143
Review and Report Suspicious Ads	143
Summary	143

15 **XML ATTACKS** **145**

The Uses of XML	146
Validating XML	147
Document Type Definitions	147
XML Bombs	148
XML External Entity Attacks	149
How Hackers Exploit External Entities	150
Securing Your XML Parser	150
Python	151
Ruby	151
Node.js	151
Java	151
.NET	151
Other Considerations	152
Summary	152

16

DON'T BE AN ACCESSORY

153

Email Fraud	154
Implement the Sender Policy Framework	155
Implement DomainKeys Identified Mail	155
Securing Your Email: Practical Steps	156
Disguising Malicious Links in Email.	156
Open Redirects	157
Preventing Open Redirects	157
Other Considerations	158
Clickjacking	158
Preventing Clickjacking	158
Server-Side Request Forgery	159
Protecting Against Server-Side Forgery.	160
Botnets	160
Protecting Against Malware Infection.	160
Summary	161

17

DENIAL-OF-SERVICE ATTACKS

163

Denial-of-Service Attack Types	164
Internet Control Message Protocol Attacks	164
Transmission Control Protocol Attacks	164
Application Layer Attacks.	165
Reflected and Amplified Attacks	165
Distributed Denial-of-Service Attacks	165
Unintentional Denial-of-Service Attacks.	166
Denial-of-Service Attack Mitigation	166
Firewalls and Intrusion Prevention Systems	166
Distributed Denial-of-Service Protection Services	167
Building for Scale	167
Summary	168

18

SUMMING UP

169

INDEX

173