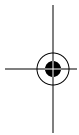


# Table of Contents

<b>Preface</b> .....	<b>xv</b>
<b>1. Apache Security Principles</b> .....	<b>1</b>
Security Definitions	1
Essential Security Principles	3
Common Security Vocabulary	4
Security Process Steps	5
Threat Modeling	5
System-Hardening Matrix	8
Calculating Risk	9
Web Application Architecture Blueprints	10
User View	11
Network View	12
Apache View	13
<b>2. Installation and Configuration</b> .....	<b>15</b>
Installation	16
Source or Binary	16
Static Binary or Dynamic Modules	19
Folder Locations	20
Installation Instructions	21
Configuration and Hardening	26
Setting Up the Server User Account	26
Setting Apache Binary File Permissions	27
Configuring Secure Defaults	27
Enabling CGI Scripts	30

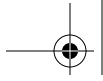


Logging	31
Setting Server Configuration Limits	31
Preventing Information Leaks	33
Changing Web Server Identity	35
Changing the Server Header Field	37
Removing Default Content	39
Putting Apache in Jail	40
Tools of the chroot Trade	42
Using chroot to Put Apache in Jail	45
Using the chroot(2) Patch	49
Using mod_security or mod_chroot	50
<b>3. PHP</b> .....	<b>52</b>
Installation	52
Using PHP as a Module	52
Using PHP as a CGI	54
Choosing Modules	55
Configuration	56
Disabling Undesirable Options	56
Disabling Functions and Classes	59
Restricting Filesystem Access	59
Setting Logging Options	60
Setting Limits	61
Controlling File Uploads	62
Increasing Session Security	62
Setting Safe Mode Options	64
Advanced PHP Hardening	66
PHP 5 SAPI Input Hooks	66
Hardened-PHP	67
<b>4. SSL and TLS</b> .....	<b>69</b>
Cryptography	70
Symmetric Encryption	71
Asymmetric Encryption	73
One-Way Encryption	74
Public-Key Infrastructure	75
How It All Falls into Place	78

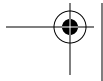
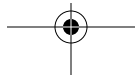
SSL	79
SSL Communication Summary	80
Is SSL Secure?	81
OpenSSL	83
Apache and SSL	86
Installing mod_ssl	86
Generating Keys	87
Generating a Certificate Signing Request	88
Signing Your Own Certificate	89
Getting a Certificate Signed by a CA	90
Configuring SSL	90
Setting Up a Certificate Authority	93
Preparing the CA Certificate for Distribution	96
Issuing Server Certificates	96
Issuing Client Certificates	98
Revoking Certificates	98
Using Client Certificates	99
Performance Considerations	99
OpenSSL Benchmark Script	99
Hardware Acceleration	101
<b>5. Denial of Service Attacks</b> .....	<b>102</b>
Network Attacks	103
Malformed Traffic	104
Brute-Force Attacks	104
SYN Flood Attacks	105
Source Address Spoofing	106
Distributed Denial of Service Attacks	107
Reflection DoS Attacks	108
Self-Inflicted Attacks	109
Badly Configured Apache	109
Poorly Designed Web Applications	111
Real-Life Client Problems	112
Traffic Spikes	113
Content Compression	114
Bandwidth Attacks	114

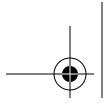
Cyber-Activism	115
The Slashdot Effect	115
Attacks on Apache	116
Apache Vulnerabilities	116
Brute-Force Attacks	117
Programming Model Attacks	118
Local Attacks	119
PAM Limits	120
Process Accounting	120
Kernel Auditing	121
Traffic-Shaping Modules	122
DoS Defense Strategy	123
<b>6. Sharing Servers</b> .....	<b>124</b>
Sharing Problems	124
File Permission Problems	125
Dynamic-Content Problems	127
Sharing Resources	132
Same Domain Name Problems	132
Information Leaks on Execution Boundaries	134
Distributing Configuration Data	137
Securing Dynamic Requests	139
Enabling Script Execution	139
Setting CGI Script Limits	141
Using suEXEC	141
FastCGI	147
Running PHP as a Module	149
Working with Large Numbers of Users	150
Web Shells	150
Dangerous Binaries	151
<b>7. Access Control</b> .....	<b>152</b>
Overview	152
Authentication Methods	154
Basic Authentication	154
Digest Authentication	156
Form-Based Authentication	157

Access Control in Apache	159
Basic Authentication Using Plaintext Files	159
Basic Authentication Using DBM Files	161
Digest Authentication	162
Certificate-Based Access Control	162
Network Access Control	163
Proxy Access Control	165
Final Access Control Notes	167
Single Sign-on	170
Web Single Sign-on	171
Simple Apache-Only Single Sign-on	172
<b>8. Logging and Monitoring</b> .....	<b>174</b>
Apache Logging Facilities	174
Request Logging	175
Error Logging	179
Special Logging Modules	181
Audit Log	182
Performance Measurement	184
File Upload Interception	185
Application Logs	186
Logging as Much as Possible	186
Log Manipulation	190
Piped Logging	191
Log Rotation	192
Issues with Log Distribution	194
Remote Logging	195
Manual Centralization	195
Syslog Logging	196
Database Logging	198
Distributed Logging with the Spread Toolkit	199
Logging Strategies	201
Log Analysis	201
Monitoring	203
File Integrity	204
Event Monitoring	204
Web Server Status	209

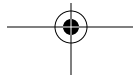


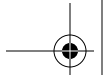
<b>9. Infrastructure .....</b>	<b>218</b>
Application Isolation Strategies	219
Isolating Applications from Servers	219
Isolating Application Modules	219
Utilizing Virtual Servers	220
Host Security	221
Restricting and Securing User Access	221
Deploying Minimal Services	222
Gathering Information and Monitoring Events	223
Securing Network Access	224
Advanced Hardening	226
Keeping Up to Date	227
Network Security	227
Firewall Usage	227
Centralized Logging	228
Network Monitoring	229
External Monitoring	230
Using a Reverse Proxy	231
Apache Reverse Proxy	232
Reverse Proxy by Network Design	235
Reverse Proxy by Redirecting Network Traffic	235
Network Design	236
Reverse Proxy Patterns	237
Advanced Architectures	241
<b>10. Web Application Security .....</b>	<b>250</b>
Session Management Attacks	252
Cookies	252
Session Management Concepts	254
Keeping in Touch With Clients	254
Session Tokens	255
Session Attacks	255
Good Practices	257
Attacks on Clients	258
Typical Client Attack Targets	259
Phishing	259





Application Logic Flaws	260
Cookies and Hidden Fields	261
POST Method	262
Referrer Check Flaws	262
Process State Management	263
Client-Side Validation	264
Information Disclosure	264
HTML Source Code	264
Directory Listings	265
Verbose Error Messages	267
Debug Messages	268
File Disclosure	269
Path Traversal	269
Application Download Flaws	269
Source Code Disclosure	270
Predictable File Locations	271
Injection Flaws	273
SQL Injection	273
Cross-Site Scripting	278
Command Execution	282
Code Execution	283
Preventing Injection Attacks	284
Buffer Overflows	285
Evasion Techniques	286
Simple Evasion Techniques	287
Path Obfuscation	287
URL Encoding	288
Unicode Encoding	289
Null-Byte Attacks	290
SQL Evasion	292
Web Application Security Resources	292
General Resources	292
Web Application Security Resources	293





<b>11. Web Security Assessment</b> .....	<b>294</b>
Black-Box Testing	295
Information Gathering	296
Web Server Analysis	306
Web Application Analysis	314
Attacks Against Access Control	317
Vulnerability Probing	317
White-Box Testing	318
Architecture Review	319
Configuration Review	320
Functional Review	325
Gray-Box Testing	327
<b>12. Web Intrusion Detection</b> .....	<b>328</b>
Evolution of Web Intrusion Detection	328
Is Intrusion Detection the Right Approach?	330
Log-Based Web Intrusion Detection	330
Real-Time Web Intrusion Detection	331
Web Intrusion Detection Features	332
Using mod_security	336
Introduction	337
More Configuration Advice	346
Deployment Guidelines	349
Detecting Common Attacks	352
Advanced Topics	356
<b>Appendix: Tools</b> .....	<b>363</b>
<b>Index</b> .....	<b>381</b>

