Secure Web Application Development

A Hands-On Guide with Python and Django

—

Matthew Baker

Apress®

Secure Web Application Development

A Hands-On Guide with Python and Django

Matthew Baker

Apress®

Secure Web Application Development: A Hands-On Guide with Python and Django

Matthew Baker
Kaisten, Aargau, Switzerland

ISBN-13 (pbk): 978-1-4842-8595-4   ISBN-13 (electronic): 978-1-4842-8596-1
https://doi.org/10.1007/978-1-4842-8596-1

Copyright © 2022 by Matthew Baker

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: James Robinson-Prior
Development Editor: James Markham
Coordinating Editor: Gryffin Winkler

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub.

Printed on acid-free paper

To my children Harry and Alexander, who I hope will be the next generation's innovators.

Table of Contents

About the Author xvii

About the Technical Reviewer xix

Acknowledgments xxi

Chapter 1: Introduction...1

1.1 About This Book 1

1.2 Who This Book Is For...3

1.3 Types of Attack..3

Server-Side Attacks...4

Client-Side Attacks 5

1.4 Defense in Depth...6

1.5 Conventions Used in This Book 7

1.6 How This Book Is Organized...7

Chapter 2: The Hands-On Environment..11

2.1 Introducing the Hands-On Environment..11

2.2 Installing a Virtualization Back End (Mac with M1) 12

Install Docker Desktop..13

Install Xcode and Docker Mac Net Connect......................................14

2.3 Installing a Virtualization Back End (All Other Platforms).................15

Install VirtualBox...15

2.4 Install Other Dependencies (All Platforms) 16
- Install Vagrant 16
- Install Web Browsers 16
- Install HTTP Toolkit 16
- Install Windows Terminal (Optional) 17
- Install a Text Editor (Optional) 17

2.5 Downloading and Building the VMs 17
- Running Applications in Vagrant 18
- Building the Vagrant VM 19

2.6 Directory Structure 22

2.7 Using the Hands-On Environment 25
- Using the Vagrant VMs 25
- The Web Server 26
- The Database 26
- MailCatcher 28
- Changing the Code 29
- Starting from Scratch 30

2.8 The Linux Command Line 31
- Command-Line Input 32
- Navigating the Filesystem 32
- Linux Permissions 34
- Set UserID and GroupID Flags 36
- Permissions in Vagrant 37
- Becoming a Different User 37
- Environment Variables 38
- Text Editors 39
- Starting and Stopping Processes 40

Clearing the Terminal....41

Exiting Bash....41

2.9 Summary....42

Chapter 3: Threat Modelling....43

3.1 What Is Threat Modelling?....43

3.2 Asset-Based Threat Modelling....44

Assets....45

Threats....45

Threat Actors....46

3.3 STRIDE....49

3.4 Data-Flow Threat Modelling....50

Data-Flow Diagrams....50

Trust Boundaries....52

3.5 Responding to Threats....53

3.6 Attack Vectors....54

3.7 Attack Surfaces....56

3.8 Summary....58

Chapter 4: Transport and Encryption....59

4.1 The Hypertext Transfer Protocol....59

Requests and Responses....60

Request Methods....65

Response Codes....66

4.2 Symmetric and Public Key Cryptography....70

Types of Encryption....70

Symmetric-Key Algorithms....71

Public-Key Encryption Algorithms....72

Hashing....74

Base64 Encoding 75
Digital Signatures 76
Key Exchange 80
4.3 Authentication and Certificates 82
Proving Authenticity 82
Types of Certificates 86
Popular Authentication Authorities 88
4.4 HTTPS 89
TLS Version 1.2 89
Perfect Forward Secrecy 91
TLS Version 1.3 92
4.5 Summary 92
Chapter 5: Installing and Configuring Services 95
5.1 Designing the Service Architecture 96
5.2 Web Application Frameworks 98
5.3 Man-in-the-Middle Attacks 102
Defending Against Man-in-the-Middle Attacks 106
Session Hijacking Attacks 107
5.4 Denial-of-Service Attacks 108
The Slowloris Attack 109
Consuming Back-End Resources 112
5.5 Setting Up HTTPS 113
HTTPS with Let’s Encrypt 114
Creating a Self-Signed Certificate 115
Browser Requirements for Self-Signed Certificates 122
Permanent Redirects 122

5.6 Reverse Proxies and Tunnels 125

Reverse Proxies 125

SSH Tunnels 129

5.7 Server Configuration 135

Hiding Service Details 135

Host Firewalls 138

TCP Wrappers 140

Using a Host Firewall and TCP Wrappers Together 142

Hiding Errors 142

Custom 404 and 500 Pages 144

Default Passwords 146

5.8 Database Configuration 147

Database Password Management 148

Access to the Database Host and Port 149

Postgres Configuration 150

Web-Based Administration Consoles 153

5.9 Securing the Filesystem 154

The Web Server's Public Path 154

Code Directories 157

Upload Directories 158

Django Static Directories 159

Secrets 160

5.10 Summary 161

Chapter 6: APIs and Endpoints 163

6.1 URLs 163

6.2 REST APIs 164

`GET` Requests 165

`POST` Requests 166

PUT Requests 166

PATCH Requests 166

DELETE Requests 168

REST APIs in Django 170

6.3 Unit Testing Permissions.. 175

6.4 Deserialization Attacks... 179

XML Attacks... 180

Function Calls and Creation.. 184

Defending Against Deserialization Attacks 185

6.5 Summary.. 186

Chapter 7: Cookies and User Input 187

7.1 Types of User Input.. 187

7.2 Cookies 188

The Expires and Max-Age Attributes 190

Domain and Path.. 190

The Secure and HttpOnly Attributes 190

The SameSite Cookie Setting... 191

Session ID Cookies 192

Session IDs and the SameSite Setting....................................... 194

7.3 Injection Attacks... 195

7.4 SQL Injection 196

Schema Discovery.. 198

Finding SQL Injection Vulnerabilities 200

Defending Against SQL Injection 200

7.5 Command Injection 205

Back Doors 207

Defending Against Command Injection...................................... 208

Combining SQL and Command Injection 209

7.6 Server-Side Request Forgery....211

Defending Against Server-Side Request Forgery....212

7.7 Cross-Site Scripting (XSS)....212

Reflected XSS....213

Stored XSS....217

DOM-Based XSS....220

Defending Against Cross-Site Scripting....221

HTML Injection....225

7.8 Content Sniffing....225

7.9 Summary....227

Chapter 8: Cross-Site Requests....229

8.1 Cross-Origin Resource Sharing (CORS)....229

CORS and Credentials....232

Setting CORS Headers....234

8.2 Cross-Site Request Forgery (CSRF)....239

CSRF Tokens....242

CSRF Tokens in Django....244

CSRF Attacks....245

CSRF and CORS....251

CSRF and Cookie Security....252

CSRF Summary....252

8.3 Clickjacking and Frame Security....254

8.4 Content Security Policy (CSP)....255

Inline Scripts and Styles....260

CSP Reporting....263

CSP in Django....264

Nonces in Django....266

8.5 Subresource Integrity (SRI) 269
8.6 Summary....270
Chapter 9: Password Management....271
9.1 Storing Passwords 272
Brute-Force Attacks....273
Rainbow Table Attacks....274
Salted Hashes....274
HMAC and PBKDF2 Password Security 276
9.2 Password Policies 279
9.3 Password Reset 281
Password Reset in Django....283
9.4 Passwords and Source Code Control....283
9.5 Summary....285
Chapter 10: Authentication and Authorization 287
10.1 Authentication vs. Authorization 287
10.2 Username and Password Authentication 288
HTTP Authentication 289
Form-Based Authentication....294
Disadvantages of Form-Based Authentication 297
10.3 One-Time Passwords....298
HMAC-Based One-Time Passwords....299
Time-Based One-Time Passwords 300
Sending OTPs via SMS 300
Google Authenticator 301
Installing the Secret Key....302

10.4 Authentication with Public-Key Cryptography 311
Registration 312
Authentication 314
10.5 Biometric Authentication..315
Biometric Authentication with WebAuthn 316
10.6 Role-Based Authorization..329
Role-Based Authorization in Django 330
10.7 JSON Web Tokens (JWTs)..335
Storing and Transmitting JWTs..337
Revoking JWTs 338
10.8 API Keys 340
Sending API Keys..342
API Keys in Django..342
10.9 Summary..349
Chapter 11: OAuth2...351
11.1 OAuth2 Terminology 352
11.2 Authorization Code Flow 355
Attacks Prevented by the Authorization Code Flow 359
Authorization Code Flow in Django..362
11.3 Implicit Flow..370
11.4 Authorization Code with PKCE Flow 372
11.5 Password Flow..374
11.6 Client Credentials Flow 376
11.7 Device Flow..377
11.8 Refresh Token Flow..379

11.9 OpenID Connect 380

OIDC Authorization Code Flow 380

OIDC in Django..382

11.10 Summary..396

Chapter 12: Logging and Monitoring 399

12.1 Logging, Aggregating, and Analytics 400

12.2 The ELK Stack 401

Loading Log Files with Logstash 401

12.3 Creating Custom Log Files 410

12.4 Creating Alerts for Security Events 419

12.5 Summary..424

Chapter 13: Third-Party and Supply Chain Security 427

13.1 Staff Member Security 428

OSINT Threats to Staff Members 428

Defenses Against OSINT Attacks 430

13.2 Third-Party Code 431

Back-End Dependencies 431

Front-End Dependencies 433

13.3 Supply Chain Security 434

The in-toto Framework..437

Using SLSA and in-toto..439

13.4 Summary..439

Chapter 14: Further Resources..441

14.1 Vulnerability Databases..441

14.2 News and Alerts Sites 443

14.3 The OWASP Top Ten..444

Broken Access Control......445
Cryptographic Failures......445
Injection......446
Insecure Design......446
Security Misconfiguration......446
Vulnerable and Outdated Components......447
Identification and Authentication Failures......447
Software and Data Integrity Failures......448
Security Logging and Monitoring Failures......448
Server-Side Request Forgery......448
14.4 Summary......449
Bibliography......453
Index......457