Mastering Modern Web Penetration Testing

Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does!

Prakhar Prasad

Packt

BIRMINGHAM - MUMBAI

Mastering Modern Web Penetration Testing

Copyright © 2016 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: October 2016

Production reference: 1251016

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78528-458-8

www.packtpub.com

Credits

Author
Prakhar Prasad

Reviewer
Kubilay Onur Gungor

Commissioning Editor
Julian Ursell

Acquisition Editor
Rahul Nair

Content Development Editor
Amrita Noronha

Technical Editors
Manthan Raja

Copy Editor
Safis Editing

Project Coordinator
Shweta H Birwatkar

Proofreader
Safis Editing

Indexer
Mariammal Chettiyar

Graphics
Disha Haria

Production Coordinator
Arvindkumar Gupta

Cover Work
Arvindkumar Gupta

About the Author

Prakhar Prasad is a web application security researcher and penetration tester from India. He has been a successful participant in various bug bounty programs and has discovered security flaws on websites such as Google, Facebook, Twitter, PayPal, Slack, and many more. He secured the tenth position worldwide in the year 2014 at HackerOne's platform. He is OSCP and OSWP certified, which are some of the most widely respected certifications in the information security industry. He occasionally performs training and security assessment for various government, non-government, and educational organizations.

I am thankful from the bottom of my heart to the editors of this book, Kajal Thapar, Amrita Noronha, and Manthan Raja, for helping and assisting me at various stages of this book. The kick starter behind this book is my dear friend Rafay Baloch, a known name in the ethical-hacking community; he has been a constant source of encouragement and motivation.

The last chapter of this book on API testing is written entirely by Pranav Hivarekar, a renowned researcher in the domain of web application security, who is a very good friend of mine and a down-to-earth human being. I'm immensely thankful to him for coming up with and authoring a guest chapter for this book.

I'll do injustice if I don't mention my family, friends, and loved ones, who have always worked behind the scenes to keep me pumped up and motivated at different stages of this book. This book wouldn't be possible without their efforts.

About the Reviewer

Kubilay Onur Gungor has been working in the cyber security field for more than 8 years. He started his professional career with crypt analysis of encrypted images using chaotic logistic maps.

After working as a QA tester in the Netsparker project, he continued his career in the penetration testing field. He performed many penetration tests and consultancies for the IT infrastructure of many large clients, such as banks, government institutions, and telecommunication companies. After pen testing activities, he worked as a web application security expert and incident management and response expert in Sony Europe and Global Sony Electronics.

He believes in multidisciplinary approach on cyber security and defines it as a struggle. With this approach, he has developed his own unique certification and training program, including penetration testing, malware analysis, incident management and response, cyber terrorism, criminal profiling, unorthodox methods, perception management, and international relations. Currently, this certification program is up and running in Istanbul in the name of Cyber Struggle (`https://cyberstruggle.org`).

Besides security, he holds certificates in foreign policy, brand management, surviving in extreme conditions, international cyber conflicts, anti-terrorism accreditation board, terrorism and counter-terrorism comparing studies.

www.PacktPub.com

eBooks, discount offers, and more

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `customercare@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

Mapt

`https://www.packtpub.com/mapt`

Get the most in-demand software skills with Mapt. Mapt gives you full access to all Packt books and video courses, as well as industry-leading tools to help you plan your personal development and advance your career.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser

Table of Contents

Preface ix

Chapter 1: Common Security Protocols 1

SOP 1

Demonstration of the same-origin policy in Google Chrome 2

Switching origins 3

Quirks with Internet Explorer 4

Cross-domain messaging 4

AJAX and the same-origin policy 5

CORS 6

CORS headers 7

Pre-flight request 7

Simple request 8

URL encoding – percent encoding 8

Unrestricted characters 9

Restricted characters 9

Encoding table 10

Encoding unrestricted characters 11

Double encoding 11

Introducing double encoding 11

IIS 5.0 directory traversal code execution – CVE-2001-0333 12

Using double encoding to evade XSS filters 13

Base64 encoding 14

Character set of Base64 encoding 14

The encoding process 15

Padding in Base64 16

Summary 17

Chapter 2: Information Gathering 19
Information gathering techniques 19
Active techniques 20
Passive techniques 20
Enumerating Domains, Files, and Resources 20
Fierce 21
theHarvester 26
SubBrute 27
CeWL 28
DirBuster 30
WhatWeb 32
Maltego 32
Wolfram Alpha 36
Shodan 37
DNSdumpster 41
Reverse IP Lookup – YouGetSignal 42
Pentest-Tools 43
Google Advanced Search 43
Summary 49
Chapter 3: Cross-Site Scripting 51
Reflected XSS 52
Demonstrating reflected XSS vulnerability 52
Reflected XSS – case study 1 53
Reflected XSS – case study 2 55
Stored XSS 58
Demonstrating stored XSS 58
Stored XSS through Markdown 60
Stored XSS through APIs 61
Stored XSS through spoofed IP addresses 64
Flash-based XSS – ExternalInterface.call() 67
HttpOnly and secure cookie flags 70
DOM-based XSS 71
XSS exploitation – The BeEF 74
Setting Up BeEF 74
Demonstration of the BeEF hook and its components 76
Logs 78
Commands 78
Rider 80
Xssrays 80
IPec 80
Network 81
Summary 81

Chapter 4: Cross-Site Request Forgery 83
Introducing CSRF 84
Exploiting POST-request based CSRF 86
How developers prevent CSRF? 86
PayPal's CSRF vulnerability to change phone numbers 87
Exploiting CSRF in JSON requests 90
Using XSS to steal anti-CSRF tokens 92
Exploring pseudo anti-CSRF tokens 93
Flash comes to the rescue 94
Rosetta Flash 97
Defeating XMLHTTPRequest-based CSRF protection 98
Summary 99
Chapter 5: Exploiting SQL Injection 101
Installation of SQLMap under Kali Linux 102
Introduction to SQLMap 103
Injection techniques 106
Dumping the data – in an error-based scenario 107
Interacting with the wizard 110
Dump everything! 112
SQLMap and URL rewriting 112
Speeding up the process! 113
Multi-threading 113
NULL connection 114
HTTP persistent connections 114
Output prediction 114
Basic optimization flags 115
Dumping the data – in blind and time-based scenarios 115
Reading and writing files 117
Checking privileges 118
Reading files 118
Writing files 119
Handling injections in a POST request 122
SQL injection inside a login-based portal 125
SQL shell 125
Command shell 127
Evasion – tamper scripts 128
Configuring with proxies 132
Summary 133

Chapter 6: File Upload Vulnerabilities 135
Introducing file upload vulnerability 136
Remote code execution 137
Multi-functional web shells 139
Netcat accessible reverse shell 142
The return of XSS 143
SWF – the flash 143
SVG images 145
Denial of Service 146
Malicious JPEG file – pixel flood 146
Malicious GIF file – frame flood 146
Malicious zTXT field of PNG files 146
Bypassing upload protections 147
Case-sensitive blacklist extension check bypass 147
MIME content type verification bypass 149
Apache's htaccess trick to execute benign files as PHP 151
SetHandler method 152
The AddType method 152
Bypassing image content verification 153
Summary 156
Chapter 7: Metasploit and Web 157
Discovering Metasploit modules 158
Interacting with Msfconsole 160
Using Auxiliary Modules related to Web Applications 162
Understanding WMAP – Metasploit's Web Application Security Scanner 167
Generating Web backdoor payload with Metasploit 171
Summary 178
Chapter 8: XML Attacks 179
XML 101 – the basics 180
XML elements 180
XML Attributes 181
XML DTD and entities 181
Internal DTD 181
External DTD 182
Entities 183
Entity declaration 183
XXE attack 184
Reading files 186
PHP Base64 conversion URI as an alternative 187

SSRF through XXE 188
Remote code execution 190
Denial of Service through XXE 191
XML quadratic blowup 192
XML billion laughs 193
The quadratic blowup 194
WordPress 3.9 quadratic blowup vulnerability – Case Study 194
Summary 195
Chapter 9: Emerging Attack Vectors 197
Server Side Request Forgery 197
Demonstrating SSRF 198
Protocol Handlers for SSRF URLs 201
Case Study – MailChimp port scan SSRF 203
Open port – with non-HTTP service 203
Open port – with HTTP service 204
Closed port – with HTTP service 204
Insecure Direct Object Reference 205
The basics of IDOR 205
Case studies 206
IDOR in Flipkart to delete saved shipping addresses 207
IDOR in HackerOne to leak private response template data 208
DOM clobbering 211
Case study – breaking GitHub's Gist comment system through DOM clobbering 213
Relative Path Overwrite 214
Controlling CSS 217
Internet Explorer 218
UI redressing 220
PHP Object Injection 224
PHP serialization 225
PHP magic functions 226
Object injection 227
Summary 229
Chapter 10: OAuth 2.0 Security 231
Introducing the OAuth 2.0 model 232
OAuth 2.0 roles 232
Resource owner 233
Client 233
Resource server 234
Authorization server 234

The application 234
Redirect URI 235
Access token 235
Client ID 235
Client secret 235
Receiving grants 236
Authorization grant 236
Implicit grant 239
Exploiting OAuth for fun and profit 239
Open redirect – the malformed URL 240
Hijacking the OAuth flow – fiddling with redirect URI 241
Directory traversal tricks 241
Domain tricks 242
Flow hijack through open redirect on client 243
Force a malicious app installation 244
Summary 245
Chapter 11: API Testing Methodology 247
Understanding REST APIs 247
REST API concepts 247
URIs 248
URI format 248
Modelling of resource 248
Stitching things together 248
REST API and HTTP 249
Request methods 250
Response codes 250
Headers 251
Setting up the testing environment 252
Analyzing the API 252
Basic HTTP authentication 252
Access token 253
Cookies 253
Tools 254
Burp Suite 254
REST API clients 254
Custom API explorers 255
Learning the API 255
Developer documentation 255
Understanding requests/responses 257
Learning scopes 258
Learning roles 260

Basic methodology to test developer APIs **261**

Listing endpoints 261

Firing different request methods 261

Exploiting API bugs 262

Scope based testing 262

Roles based testing 264

Insecure direct object reference testing 266

Summary **267**

Index **269**