

Gilberto Najera-Gutierrez, Juned Ahmed Ansari 著

Kali Linux Web渗透测试

第3版（影印版）

Web Penetration Testing with Kali Linux, 3rd Edition

Kali Linux Web 渗透测试 第3版 (影印版)

Web Penetration Testing with
Kali Linux, 3rd Edition

Gilberto Najera-Gutierrez,
Juned Ahmed Ansari 著

南京 东南大学出版社

图书在版编目(CIP)数据

Kali Linux Web 渗透测试:第3版:英文/(澳)吉尔博托·N.古铁雷斯(Gilberto Najera-Gutierrez),(印)琼·A.安萨里(Juned Ahmed Ansari)著. —影印本. —南京:东南大学出版社,2019.5

书名原文:Web Penetration Testing with Kali Linux, 3rd Edition

ISBN 978-7-5641-8323-3

I. ①K… II. ①吉… ②琼… III. ①Linux 操作系统—安全技术—英文 IV. ①TP316.89

中国版本图书馆 CIP 数据核字(2019)第 046193 号
图字:10-2018-501 号

© 2018 by PACKT Publishing Ltd.

Reprint of the English Edition, jointly published by PACKT Publishing Ltd and Southeast University Press, 2019.
Authorized reprint of the original English edition, 2018 PACKT Publishing Ltd, the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 PACKT Publishing Ltd 出版 2018。

英文影印版由东南大学出版社出版 2019。此影印版的出版和销售得到出版权和销售权的所有者——PACKT Publishing Ltd 的许可。

版权所有,未得书面许可,本书的任何部分和全部不得以任何形式重制。

Kali Linux Web 渗透测试 第3版(影印版)

出版发行:东南大学出版社

地 址:南京四牌楼2号 邮编:210096

出 版 人:江建中

网 址:<http://www.seupress.com>

电子邮件:press@seupress.com

印 刷:常州市武进第三印刷有限公司

开 本:787毫米×980毫米 16开本

印 张:26.75

字 数:524千字

版 次:2019年5月第1版

印 次:2019年5月第1次印刷

书 号:ISBN 978-7-5641-8323-3

定 价:106.00元

本社图书若有印装质量问题,请直接与营销部联系。电话(传真):025-83791830

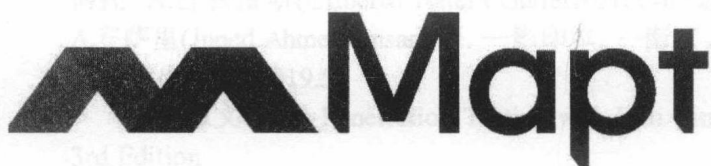
To Leticia and Alexa, thank you for making my life much more joyful than I could have imagined.

A mi madre, con todo el amor, admiración y respeto. Gracias por guiarme con el mejor de los ejemplos y por enseñarme a nunca dejar de aprender, a trabajar duro y a vivir con honestidad.

– Gilberto Najera-Gutierrez

I want to dedicate this book to my parents, Abdul Rashid and Sherbano, and sisters, Tasneem and Lubna. Thank you all for your encouragement on every small step that I took forward. Thank you mom and dad for all the sacrifices and for always believing in me. I also want to thank my seniors, for their mentorship, and my friends and colleagues, for supporting me over the years.

– Juned Ahmed Ansari



mapt.io

Mapt is an online digital library that gives you full access to over 5,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Mapt is fully searchable
- Copy and paste, print, and bookmark content

PacktPub.com

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 service@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.

Contributors

About the authors

Gilberto Najera-Gutierrez is an experienced penetration tester currently working for one of the top security testing service providers in Australia. He obtained leading security and penetration testing certifications, namely Offensive Security Certified Professional (OSCP), EC-Council Certified Security Administrator (ECSA), and GIAC Exploit Researcher and Advanced Penetration Tester (GXPN); he also holds a Master's degree in Computer Science with specialization in Artificial Intelligence.

Gilberto has been working as a penetration tester since 2013, and he has been a security enthusiast for almost 20 years. He has successfully conducted penetration tests on networks and applications of some of the biggest corporations, government agencies, and financial institutions in Mexico and Australia.

Juned Ahmed Ansari (@junedlive) is a cyber security researcher based out of Mumbai. He currently leads the penetration testing and offensive security team in a prodigious MNC. Juned has worked as a consultant for large private sector enterprises, guiding them on their cyber security program. He has also worked with start-ups, helping them make their final product secure.

Juned has conducted several training sessions on advanced penetration testing, which were focused on teaching students stealth and evasion techniques in highly secure environments. His primary focus areas are penetration testing, threat intelligence, and application security research. He holds leading security certifications, namely GXPN, CISSP, CCSK, and CISA. Juned enjoys contributing to public groups and forums and occasionally blogs at <http://securebits.in>.

About the reviewer

Daniel W. Dieterle is an internationally published security author, researcher, and technical editor. He has over 20 years of IT experience and has provided various levels of support and service to hundreds of companies, ranging from small businesses to large corporations. Daniel authors and runs the CYBER ARMS - Computer Security blog (<https://cyberarms.wordpress.com/>) and an Internet of Things projects- and security-based blog (<https://dantheiotman.com/>).

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit authors.packtpub.com and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

Preface	1
Chapter 1: Introduction to Penetration Testing and Web Applications	9
Proactive security testing	10
Different testing methodologies	10
Ethical hacking	11
Penetration testing	11
Vulnerability assessment	11
Security audits	12
Considerations when performing penetration testing	12
Rules of Engagement	12
The type and scope of testing	12
Client contact details	13
Client IT team notifications	14
Sensitive data handling	14
Status meeting and reports	14
The limitations of penetration testing	15
The need for testing web applications	17
Reasons to guard against attacks on web applications	18
Kali Linux	18
A web application overview for penetration testers	19
HTTP protocol	19
Knowing an HTTP request and response	20
The request header	21
The response header	22
HTTP methods	23
The GET method	23
The POST method	24
The HEAD method	24
The TRACE method	24
The PUT and DELETE methods	25
The OPTIONS method	25
Keeping sessions in HTTP	25
Cookies	26

Cookie flow between server and client	26
Persistent and nonpersistent cookies	27
Cookie parameters	28
HTML data in HTTP response	28
The server-side code	29
Multilayer web application	29
Three-layer web application design	29
Web services	31
Introducing SOAP and REST web services	31
HTTP methods in web services	33
XML and JSON	33
AJAX	34
Building blocks of AJAX	35
The AJAX workflow	36
HTML5	38
WebSockets	38
Summary	39
Chapter 2: Setting Up Your Lab with Kali Linux	41
Kali Linux	42
Latest improvements in Kali Linux	42
Installing Kali Linux	43
Virtualizing Kali Linux versus installing it on physical hardware	45
Installing on VirtualBox	46
Creating the virtual machine	46
Installing the system	49
Important tools in Kali Linux	56
CMS & Framework Identification	58
WPScan	58
JoomScan	58
CMSmap	59
Web Application Proxies	59
Burp Proxy	59
Customizing client interception	61
Modifying requests on the fly	61
Burp Proxy with HTTPS websites	62
Zed Attack Proxy	63
ProxyStrike	64
Web Crawlers and Directory Bruteforce	64

DIRB	64
DirBuster	64
Uniscan	65
Web Vulnerability Scanners	65
Nikto	65
w3af	66
Skipfish	66
Other tools	66
OpenVAS	66
Database exploitation	69
Web application fuzzers	69
Using Tor for penetration testing	69
Vulnerable applications and servers to practice on	71
OWASP Broken Web Applications	71
Hackazon	73
Web Security Dojo	73
Other resources	73
Summary	74
Chapter 3: Reconnaissance and Profiling the Web Server	75
Reconnaissance	76
Passive reconnaissance versus active reconnaissance	77
Information gathering	77
Domain registration details	78
Whois – extracting domain information	78
Identifying related hosts using DNS	80
Zone transfer using dig	81
DNS enumeration	83
DNSEnum	84
Fierce	85
DNSRecon	87
Brute force DNS records using Nmap	88
Using search engines and public sites to gather information	88
Google dorks	89
Shodan	90
theHarvester	91
Maltego	93
Recon-ng – a framework for information gathering	94

Domain enumeration using Recon-ng	95
Sub-level and top-level domain enumeration	95
Reporting modules	97
Scanning – probing the target	99
Port scanning using Nmap	100
Different options for port scan	100
Evading firewalls and IPS using Nmap	102
Identifying the operating system	103
Profiling the server	104
Identifying virtual hosts	104
Locating virtual hosts using search engines	105
Identifying load balancers	106
Cookie-based load balancer	106
Other ways of identifying load balancers	107
Application version fingerprinting	108
The Nmap version scan	108
The Amap version scan	109
Fingerprinting the web application framework	110
The HTTP header	111
The WhatWeb scanner	112
Scanning web servers for vulnerabilities and misconfigurations	113
Identifying HTTP methods using Nmap	113
Testing web servers using auxiliary modules in Metasploit	114
Identifying HTTPS configuration and issues	114
OpenSSL client	115
Scanning TLS/SSL configuration with SSLScan	118
Scanning TLS/SSL configuration with SSLyze	119
Testing TLS/SSL configuration using Nmap	120
Spidering web applications	121
Burp Spider	121
Application login	125
Directory brute forcing	125
DIRB	126
ZAP's forced browse	127
Summary	128
Chapter 4: Authentication and Session Management Flaws	131
Authentication schemes in web applications	132
Platform authentication	132
Basic	132

Digest	134
NTLM	134
Kerberos	134
HTTP Negotiate	135
Drawbacks of platform authentication	135
Form-based authentication	136
Two-factor Authentication	137
OAuth	137
Session management mechanisms	138
Sessions based on platform authentication	138
Session identifiers	138
Common authentication flaws in web applications	140
Lack of authentication or incorrect authorization verification	140
Username enumeration	140
Discovering passwords by brute force and dictionary attacks	148
Attacking basic authentication with THC Hydra	149
Attacking form-based authentication	152
Using Burp Suite Intruder	153
Using THC Hydra	158
The password reset functionality	159
Recovery instead of reset	159
Common password reset flaws	160
Vulnerabilities in 2FA implementations	161
Detecting and exploiting improper session management	162
Using Burp Sequencer to evaluate the quality of session IDs	162
Predicting session IDs	166
Session Fixation	172
Preventing authentication and session attacks	177
Authentication guidelines	177
Session management guidelines	179
Summary	180
Chapter 5: Detecting and Exploiting Injection-Based Flaws	181
Command injection	182
Identifying parameters to inject data	185
Error-based and blind command injection	185
Metacharacters for command separator	186

Exploiting shellshock	188
Getting a reverse shell	188
Exploitation using Metasploit	193
SQL injection	195
An SQL primer	195
The SELECT statement	196
Vulnerable code	197
SQL injection testing methodology	198
Extracting data with SQL injection	201
Getting basic environment information	203
Blind SQL injection	206
Automating exploitation	212
sqlninja	213
BBQSQL	215
sqlmap	216
Attack potential of the SQL injection flaw	222
XML injection	222
XPath injection	222
XPath injection with XCat	226
The XML External Entity injection	228
The Entity Expansion attack	230
NoSQL injection	232
Testing for NoSQL injection	233
Exploiting NoSQL injection	233
Mitigation and prevention of injection vulnerabilities	235
Summary	236
Chapter 6: Finding and Exploiting Cross-Site Scripting (XSS) Vulnerabilities	237
An overview of Cross-Site Scripting	238
Persistent XSS	240
Reflected XSS	242
DOM-based XSS	242
XSS using the POST method	244
Exploiting Cross-Site Scripting	245
Cookie stealing	245
Website defacing	247

Key loggers	249
Taking control of the user's browser with BeEF-XSS	252
Scanning for XSS flaws	256
XSSer	256
XSS-Sniper	258
Preventing and mitigating Cross-Site Scripting	259
Summary	260
Chapter 7: Cross-Site Request Forgery, Identification, and Exploitation	261
Testing for CSRF flaws	262
Exploiting a CSRF flaw	265
Exploiting CSRF in a POST request	265
CSRF on web services	268
Using Cross-Site Scripting to bypass CSRF protections	271
Preventing CSRF	275
Summary	276
Chapter 8: Attacking Flaws in Cryptographic Implementations	277
A cryptography primer	278
Algorithms and modes	278
Asymmetric encryption versus symmetric encryption	279
Symmetric encryption algorithm	279
Stream and block ciphers	280
Initialization Vectors	281
Block cipher modes	281
Hashing functions	282
Salt values	282
Secure communication over SSL/TLS	283
Secure communication in web applications	284
TLS encryption process	285
Identifying weak implementations of SSL/TLS	286
The OpenSSL command-line tool	286
SSLScan	290
SSLYze	292
Testing SSL configuration using Nmap	293
Exploiting Heartbleed	295

POODLE	298
Custom encryption protocols	299
Identifying encrypted and hashed information	300
Hashing algorithms	300
hash-identifier	301
Frequency analysis	302
Entropy analysis	306
Identifying the encryption algorithm	308
Common flaws in sensitive data storage and transmission	309
Using offline cracking tools	310
Using John the Ripper	311
Using Hashcat	313
Preventing flaws in cryptographic implementations	315
Summary	316
Chapter 9: AJAX, HTML5, and Client-Side Attacks	317
Crawling AJAX applications	317
AJAX Crawling Tool	318
Sprajax	319
The AJAX Spider – OWASP ZAP	320
Analyzing the client-side code and storage	322
Browser developer tools	322
The Inspector panel	323
The Debugger panel	324
The Console panel	325
The Network panel	326
The Storage panel	327
The DOM panel	327
HTML5 for penetration testers	328
New XSS vectors	328
New elements	328
New properties	328
Local storage and client databases	329
Web Storage	329
IndexedDB	330
Web Messaging	331
WebSockets	331

Intercepting and modifying WebSockets	335
Other relevant features of HTML5	338
Cross-Origin Resource Sharing (CORS)	338
Geolocation	338
Web Workers	338
Bypassing client-side controls	339
Mitigating AJAX, HTML5, and client-side vulnerabilities	344
Summary	344
Chapter 10: Other Common Security Flaws in Web Applications	345
Insecure direct object references	346
Direct object references in web services	348
Path traversal	349
File inclusion vulnerabilities	353
Local File Inclusion	353
Remote File Inclusion	356
HTTP parameter pollution	357
Information disclosure	358
Mitigation	362
Insecure direct object references	362
File inclusion attacks	363
HTTP parameter pollution	363
Information disclosure	363
Summary	364
Chapter 11: Using Automated Scanners on Web Applications	365
Considerations before using an automated scanner	365
Web application vulnerability scanners in Kali Linux	366
Nikto	367
Skipfish	369
Wapiti	372
OWASP-ZAP scanner	374
Content Management Systems scanners	377
WPScan	377
JoomScan	379
CMSmap	380
Fuzzing web applications	381

Using the OWASP-ZAP fuzzer	382
Burp Intruder	388
Post-scanning actions	394
Summary	394
Other Books You May Enjoy	397
Index	401