



Kratak sadržaj

POGLAVLJE 1

Uvod u penetraciono testiranje i veb aplikacije 9

POGLAVLJE 2

Podešavanje laboratorije pomoću Kali Linuxa 41

POGLAVLJE 3

Izviđanje i profilisanje veb servera 75

POGLAVLJE 4

Nedostaci provere identiteta i upravljanja sesijom 131

POGLAVLJE 5

Detektovanje i eksploatacija ranjivosti zasnovanih na injektiranju 181

POGLAVLJE 6

Pronalaženje i eksploatacija CrossSite Scripting (XSS) ranjivosti 237

POGLAVLJE 7

Cross-Site Request Forgery, identifikacija i eksploatacija 261

POGLAVLJE 8

Napadanje nedostataka u kriptografskim implementacijama 277

POGLAVLJE 9

AJAX, HTML5 napadi i napadi na strani klijenta 317

POGLAVLJE 10

Ostali uobičajeni bezbednosni nedostaci u veb aplikacijama 345

POGLAVLJE 11

Upotreba automatizovanih skenera u veb aplikacijama 365

INDEKS 397





Sadržaj

Uvod	1
-------------------	----------

POGLAVLJE 1

Uvod u penetraciono testiranje i veb aplikacije	9
--	----------

Proaktivno testiranje bezbednosti	10
Različite metodologije testiranja.....	10
Etičko hakovanje.....	11
Penetraciono testiranje.....	11
Procena ranjivosti.....	11
Provere bezbednosti.....	12
Razmatranja prilikom izvršavanja penetracionog testiranja	12
Pravila angažovanja	12
Tip i oblast važenja testiranja.....	12
Detalji o kontaktu klijenta	13
Obaveštenja IT tima klijenta	14
Obrađa poverljivih podataka	14
Obaveštenja o statusu i izveštaji.....	14
Ograničenja penetracionog testiranja	15
Potreba za testiranjem veb aplikacija.....	17
Razlozi za zaštitu od napada u veb aplikacijama.....	18
Kali Linux.....	18
Pregled veb aplikacije za izvršioce penetracionog testa	19
HTTP protokol	19
Poznavanje HTTP zahteva i odgovora.....	20
Zaglavlje zahteva.....	21
Zaglavlje odgovora.....	22
HTTP metodi	23
Zadržavanje sesija u HTTP-u	25
„Kolačići“	26
Tok „kolačića“ između servera i klijenta	26
Trajni i privremeni „kolačići“	27
Parametri „kolačića“	28

HTML podaci u HTTP odgovoru.....	28
Kod na strani servera.....	29
Višeslojna veb aplikacija.....	29
Dizajn troslojne veb aplikacije	29
Veb servisi	31
Predstavljanje SOAP i REST veb servisa.....	31
HTTP metodi u veb servisima.....	33
XML i JSON.....	33
AJAX	34
HTML5	38
WebSocket.....	38
Rezime	39

POGLAVLJE 2

Podešavanje laboratorije pomoću Kali Linuxa 41

Kali Linux.....	42
Najnovija poboljšanja u Kali Linuxu	42
Instaliranje Kali Linuxa.....	43
Virtuelizacija Kali Linuxa u odnosu na instaliranje na računar	45
Instaliranje na VirtualBox.....	46
Važne alatke u Kali Linuxu	56
CMS & Framework Identification.....	58
WPScan	58
JoomScan.....	58
CMSmap	59
Posrednici za veb aplikaciju	59
Burp Proxy.....	59
Zed Attack Proxy.....	63
ProxyStrike	64
Pretraživači Veba i pronalaženje direktorijuma	64
DIRB	64
DirBuster.....	64
Uniscan.....	65
Skeneri ranjivosti Veba.....	65
Nikto.....	65
w3af.....	66
Skipfish.....	66
Ostale alatke	66
OpenVAS	66
Eksploatacija baze podataka	69
Fuzzeri veb aplikacije.....	69
Upotreba Tora za penetraciono testiranje	69
Ranjive aplikacije i serveri za vežbu	71
OWASP Broken Web Applications	71
Hackazon.....	73
Web Security Dojo	73
Ostali izvori.....	73
Rezime	74

POGLAVLJE 3**Izviđanje i profilisanje veb servera 75**

Izviđanje.....	76
Pasivno nasuprot aktivnom izviđanju	77
Sakupljanje informacija.....	77
Detalji o registraciji domena.....	78
Whois – ekstrahovanje informacija o domenu.....	78
Identifikacija povezanih hostova pomoću DNS-a.....	80
Prenos zone pomoću dig.....	81
Popis DNS-a.....	83
Upotreba mehanizama za pretraživanje i javnih sajtova za sakupljanje informacija	88
Google dorks.....	89
Shodan	90
theHarvester.....	91
Maltego.....	93
Recon-ng – radni okvir za sakupljanje informacija	94
Popisivanje domena pomoću alatke Recon-ng	95
Moduli izveštavanja.....	97
Skeniranje – ispitivanje cilja.....	99
Skeniranje porta pomoću Nmapa.....	100
Različite opcije za skeniranje porta.....	100
Izbegavanje zaštitnih barijera i IPS-a pomoću Nmapa	102
Identifikovanje operativnog sistema	103
Profilisanje servera.....	104
Identifikovanje virtuelnih hostova	104
Otkrivanje verzije aplikacije.....	108
Ispitivanje radnog okvira veb aplikacije.....	110
Ispitivanje ranjivosti i pogrešne konfiguracije veb servera	113
Identifikacija HTTP metoda pomoću Nmapa	113
Identifikacija HTTPS konfiguracije i grešaka	114
Ispitivanje veb aplikacija	121
Burp Spider	121
Pogađanje direktorijuma grubom silom	125
Rezime	128

POGLAVLJE 4**Nedostaci provere identiteta i upravljanja sesijom 131**

Šeme provere identiteta u veb aplikacijama.....	132
Provera identiteta platforme	132
Basic	132
Digest.....	134
NTLM.....	134
Kerberos.....	134
HTTP Negotiate.....	135
Mane provere identiteta platforme.....	135
Provera identiteta zasnovana na obrascu.....	136
Provera identiteta zasnovana na dva faktora	137

OAuth	137
Mehanizmi upravljanja sesijom	138
Sesije zasnovane na proveri identiteta platforme	138
Identifikatori sesije	138
Uobičajeni nedostaci provere identiteta u veb aplikacijama	140
Nedostatak provere identiteta ili netačna verifikacija autorizacije.....	140
Popisivanje korisničkih imena	140
Otkrivanje lozinke grubom silom i napadi rečnikom	148
Napad na osnovnu proveru identiteta pomoću alatke THC Hydra.....	149
Napad na proveru identiteta koja je zasnovana na obrascu	152
Funkcionalnost resetovanja lozinke.....	159
Obnavljanje, umesto resetovanja.....	160
Uobičajeni nedostaci resetovanja lozinke.....	160
Ranjivosti u 2FA implementacijama.....	161
Detektovanje i eksploatacija nepravilnog upravljanja sesijom.....	162
Upotreba Burp Sequencera za procenu kvaliteta ID-ova sesije	162
Predviđanje ID-ova sesije	166
Session Fixation	172
Sprečavanje napada provere identiteta i sesije	177
Smernice za proveru identiteta	177
Smernice za upravljanje sesijom	179
Rezime	180

POGLAVLJE 5

Detektovanje i eksploatacija ranjivosti zasnovanih na injektiranju 181

Injektiranje komande	182
Identifikovanje parametara za injektiranje podataka.....	185
Injekcije komande zasnovane na grešci i nevidljive injekcije komande	185
Metaznakovi za razdvajanje komandi.....	186
Eksploatacija shellshocka	188
Dobijanje obrnutog komandnog okruženja	188
Eksploatacija pomoću Metasploita.....	193
SQL injektiranje	195
Osnove SQL-a	195
Iskaz SELECT	196
Ranjivi kod	197
Metodologija testiranja SQL injektiranja.....	198
Ekstrahovanje podataka pomoću SQL injektiranja.....	201
Dobijanje osnovnih informacija o okruženju	203
Nevidljivo SQL injektiranje.....	206
Automatizacija eksploatacije.....	212
Alatka sqlninja	213
BBQSQL	215
Alatka sqlmap	216
Mogućnost napada nedostatka SQL injektiranja	222
XML injektiranje	222
XPath injektiranje.....	222

XPath injektiranje pomoću alatke Xcat	226
XML External Entity injektiranje.....	228
Entity Expansion napad	230
NoSQL injektiranje	232
Testiranje NoSQL injektiranja	233
Eksploatacija NoSQL injektiranja	233
Izbegavanje i prevencija ranjivosti injektiranja	235
Rezime	236

POGLAVLJE 6

Pronalaženje i eksploatacija CrossSite Scripting (XSS) ranjivosti 237

Pregled Cross-Site Scriptinga.....	238
Trajni XSS	240
Reflektovani XSS.....	242
XSS zasnovan na DOM-u	242
XSS pomoću metoda POST	244
Eksploatacija Cross-Site Scripting ranjivosti	245
Krađa „kolačića“	245
Promena prikaza veb sajta.....	247
Program za evidentiranje ključa	249
Preuzimanje kontrole nad pretraživačem korisnika pomoću BeEFXSS-a.....	252
Skeniranje XSS nedostataka	256
XSSer.....	256
XSS-Sniper	258
Sprečavanje i ublažavanje Cross-Site Scripting ranjivosti	259
Rezime	260

POGLAVLJE 7

Cross-Site Request Forgery, identifikacija i eksploatacija 261

Testiranje CSRF nedostataka	262
Eksploatacija CSRF nedostatka	265
Eksploatacija CSRF-a u POST zahtevu.....	265
CSRF na veb servisima.....	268
Upotreba Cross-Site Scripting ranjivosti za zaobilazanje CSRF zaštite.....	271
Sprečavanje CSRF-a	275
Rezime	276

POGLAVLJE 8

Napadanje nedostataka u kriptografskim implementacijama 277

Primer kriptografije.....	278
Algoritmi i režimi.....	278
Asimetrično šifrovanje nasuprot simetričnog	279
Šifre tokova i blokovske šifre.....	280
Inicijalizacioni vektori	281
Režimi blokovske šifre	281
Funkcije heširanja	282

Salt vrednosti	282
Sigurna komunikacija preko SSL/TLS-a	283
Sigurna komunikacija u veb aplikacijama.....	284
Proces TLS šifrovanja.....	285
Identifikacija slabih implementacija SSL/TLS-a	286
OpenSSL alatka komandne linije.....	286
SSLScan.....	290
SSLyze	292
Testiranje SSL konfiguracije pomoću Nmapa.....	293
Eksploatacija ranjivosti Heartbleed	295
POODLE	298
Prilagođeni protokoli šifrovanja.....	299
Identifikacija šifrovane i heširane informacije	300
Algoritmi heširanja	300
Analiza frekvencije.....	302
Analiza entropije	306
Identifikacija algoritma šifrovanja.....	308
Uobičajeni nedostaci u skladištenju i prenosu poverljivih podataka.....	309
Upotreba offline alatki za razbijanje	310
Upotreba alatke John the Ripper	311
Upotreba alatke Hashcat	313
Sprečavanje nedostataka u kriptografskim implementacijama.....	315
Rezime	316

POGLAVLJE 9

AJAX, HTML5 napadi i napadi na strani klijenta 317

Pretraživanje AJAX aplikacija	317
AJAX Crawling Tool.....	318
Sprajax	319
AJAX Spider – OWASP ZAP.....	320
Analiza koda na strani klijenta i skladišta.....	322
Programerske alatke pretraživača	322
Panel Inspector.....	323
Panel Debugger	324
Panel Console	325
Panel Network	326
Panel Storage	327
Panel DOM	327
HTML5 za izvršioce penetracionog testa	328
Novi XSS vektori	328
Novi elementi	328
Nova svojstva.....	328
Lokalno skladište i baze podataka klijenta	329
Web Storage.....	329
IndexedDB	330
Web Messaging	331
WebSockets.....	331
Presretanje i modifikacija WebSocketsa	335

Ostale relevantne funkcije u HTML-u 5	338
Cross-Origin Resource Sharing (CORS)	338
Geolokacija	338
Web Workers	338
Zaobilaženje kontrola na strani klijenta	339
Ublažavanje AJAX i HTML5 ranjivosti i ranjivosti na strani klijenta	344
Rezime	344

POGLAVLJE 10

Ostali uobičajeni bezbednosni nedostaci u veb aplikacijama 345

Nesigurne reference direktnog objekta	346
Reference direktnog objekta u veb servisima	348
Path traversal	349
Ranjivosti uključivanja fajla	353
Local File Inclusion	353
Remote File Inclusion	356
Zagađenje HTTP parametra	357
Otkrivanje informacija	358
Ublažavanje	362
Nesigurne reference direktnog objekta	362
Napadi uključivanja fajla	363
Zagađivanje HTTP parametra	363
Otkrivanje informacija	363
Rezime	364

POGLAVLJE 11

Upotreba automatizovanih skenera u veb aplikacijama 365

Razmatranja pre upotrebe automatizovanog skenera	365
Skeneri ranjivosti veb aplikacije u Kali Linuxu	366
Nikto	367
Skipfish	369
Wapiti	372
OWASP-ZAP skener	374
Skeneri sistema za upravljanje sadržajem	377
WPScan	377
JoomScan	379
CMSmap	380
Rasplinuto testiranje veb aplikacija	381
Upotreba OWASP-ZAP rasplintog testera	382
Burp Intruder	388
Akcije posle skeniranja	394
Rezime	394

INDEKS 397

