

Spis treści

O autorach 11

O korektorze merytorycznym 12

Przedmowa 13

Rozdział 1. Wprowadzenie do testów penetracyjnych i aplikacji sieciowych 19

Aktywne testowanie zabezpieczeń 20

Różne metodyki testowania 20

Co należy brać pod uwagę podczas przeprowadzania testów penetracyjnych 22

Reguły prowadzenia testu penetracyjnego 22

Ograniczenia testów penetracyjnych 24

Dlaczego należy testować aplikacje sieciowe 26

Dlaczego aplikacje sieciowe należy chronić przed atakami 27

Kali Linux 28

Aplikacje sieciowe - wprowadzenie dla pentesterów 28

Protokół HTTP 29

Żądania i odpowiedzi HTTP 29

Obsługa sesji HTTP 33

Dane HTML w odpowiedzi HTTP 36

Wielowarstwowe aplikacje sieciowe 37

Podsumowanie 46

Rozdział 2. Konfiguracja środowiska testowego z systemem Kali Linux 47

Kali Linux 48

Udoskonalenia wprowadzone w systemie Kali Linux 48

Instalowanie systemu Kali Linux 49

Instalacja systemu Kali Linux na platformie VirtualBox 51

Najważniejsze narzędzia w systemie Kali Linux 58

Narzędzia do identyfikacji frameworków i systemów CMS 59

Serwery proxy aplikacji sieciowych 60

Roboty sieciowe i siłowe przeszukiwanie struktury katalogów 64

Sieciowe skanery podatności i luk w zabezpieczeniach 65

Inne narzędzia 66

Podatne aplikacje i serwery, których można użyć do ćwiczeń 70

Projekt OWASP Broken Web Applications 70

Hackazon 72

Web Security Dojo 72

Inne zasoby 73

Podsumowanie 73

Rozdział 3. Rekonesans i profilowanie serwerów WWW 75

Rekonesans 76

Rekonesans pasywny kontra rekonesans aktywny 77

Gromadzenie informacji 77

Szczegółowe informacje o rejestracji domeny 78

Identyfikacja powiązanych hostów za pomocą DNS 80

Używanie wyszukiwarek i publicznych usług sieciowych do zbierania informacji 86

Narzędzie Recon-ng - system gromadzenia informacji 89

Skanowanie - badanie celu 94

Skanowanie portów za pomocą skanera Nmap 95

Profilowanie serwera 98

Skanowanie serwerów sieciowych w poszukiwaniu luk i błędów konfiguracyjnych 106

Zastosowanie robotów indeksujących do przeszukiwania aplikacji sieciowych (web spidering)

Podsumowanie 119

Rozdział 4. Podatności uwierzytelniania i zarządzania sesjami 121

Schematy uwierzytelniania w aplikacjach internetowych 122

Uwierzytelnianie na poziomie platformy 122

Uwierzytelnianie oparte na formularzach 125

Uwierzytelnianie dwuskładnikowe 126

OAuth 127

Mechanizmy zarządzania sesjami 127

Sesje oparte na uwierzytelnianiu platformy 127

Identyfikatory sesji 127

Typowe błędy uwierzytelniania w aplikacjach internetowych 129

Brak uwierzytelnienia lub nieprawidłowa weryfikacja uwierzytelniania 129

Wyszukiwanie nazw kont użytkowników 129

Pozyskiwanie haseł za pomocą ataków typu brute force i ataków słownikowych 134

Mechanizm resetowania hasła 144

Luki w implementacjach mechanizmu 2FA 145

Wykrywanie i wykorzystywanie niewłaściwego zarządzania sesjami 146

Zastosowanie modułu Burp Sequencer do oceny jakości identyfikatorów sesji 147

Przewidywanie wartości identyfikatorów sesji 149

Ataki typu Session Fixation 154

Zapobieganie atakom na uwierzytelnianie i sesje 157

Wytyczne dotyczące uwierzytelniania 157

Wskazówki dotyczące zarządzania sesjami 159

Podsumowanie 160

Rozdział 5. Wykrywanie i wykorzystywanie podatności pozwalających na wstrzykiwanie kodu 161

Wstrzykiwanie poleceń 162

Identyfikacja parametrów do wstrzykiwania danych 164

Wykorzystywanie luki Shellshock 167

Wstrzykiwanie zapytań SQL 172

Podstawowe zagadnienia związane z językiem SQL 173

Przykład kodu podatnego na atak ze wstrzykiwaniem kodu 174

Metodologia testowania podatności na wstrzykiwanie kodu SQL 175

Pobieranie danych za pomocą wstrzykiwania kodu SQL 178

Automatyzacja procesu wykorzystywania luk typu SQL injection 187

Możliwości ataków z wykorzystaniem wstrzykiwania kodu SQL 194

Wstrzykiwanie kodu XML 195

Ataki typu XPath injection 195

Ataki ze wstrzykiwaniem kodu XML External Entity 199

Ataki typu Entity Expansion 201

Ataki ze wstrzykiwaniem kodu NoSQL 202

Testowanie podatności na wstrzykiwanie kodu NoSQL 203

Wykorzystywanie możliwości wstrzykiwania kodu NoSQL 203

Łagodzenie skutków i zapobieganie podatnościom na wstrzykiwanie kodu 205

Podsumowanie 206

Rozdział 6. Wyszukiwanie i wykorzystywanie podatności typu Cross-site scripting (XSS) 207

Przegląd podatności typu Cross-site scripting 208

Ataki typu Persistent XSS 210

Ataki typu Reflected XSS 211

Ataki typu DOM-based XSS 211

Ataki typu XSS z użyciem metody POST 213

Wykorzystywanie podatności typu Cross-site scripting 214

Wykradanie plików cookie 214

Podmiana zawartości witryny 216

Keylogger - rejestrowanie naciśnień klawiszy 217

Przejmowanie kontroli nad przeglądarką użytkownika za pomocą pakietu BeEF-XSS 220

Skanowanie w poszukiwaniu luk typu XSS 223

XSSer 223

XSS-Sniper 225

Zapobieganie skutkom ataków typu Cross-site scripting 226

Podsumowanie 227

Rozdział 7. Wyszukiwanie i wykorzystywanie podatności typu Cross-site request forgery (CSRF/XSRF) 229

Wyszukiwanie podatności typu CSRF 230

Wykorzystywanie podatności typu CSRF 233

Wykorzystywanie podatności CSRF z użyciem żądania POST 233

Ataki typu CSRF na usługi sieciowe 236

Zastosowanie podatności XSS do ominięcia zabezpieczeń przed atakami CSRF 238

Zapobieganie atakom CSRF 242

Podsumowanie 243

Rozdział 8. Ataki z wykorzystaniem podatności kryptograficznych 245

Podstawowe zagadnienia związane z kryptografią 246

Algorytmy i tryby szyfrowania 247

Funkcje haszujące 250

Bezpieczna komunikacja z użyciem protokołu SSL/TLS 251

Bezpieczna komunikacja w aplikacjach sieciowych 252

Identyfikacja słabych implementacji SSL/TLS 254

Polecenie OpenSSL 254

SSLScan 257

SSLyze 258

Testowanie konfiguracji SSL za pomocą skanera Nmap 259

Wykorzystywanie luki Heartbleed 261

Luka POODLE 263

Niestandardowe protokoły szyfrowania 264

Identyfikacja zaszyfrowanych i zakodowanych informacji 264

Najczęstsze błędy popełniane podczas przechowywania i przesyłania poufnych danych 272

Używanie narzędzi do łamania haseł offline 273

Zapobieganie błędom w implementacjach kryptograficznych 277

Podsumowanie 278

Rozdział 9. AJAX, HTML5 i ataki po stronie klienta 279

Przeszukiwanie aplikacji AJAX 279

AJAX Crawling Tool 280

Sprajax 281

AJAX Spider - OWASP ZAP 281

Analizowanie magazynu danych i kodu po stronie klienta 283

Narzędzia programistyczne przeglądarki sieciowej 284

HTML5 dla pentesterów 288

Nowe wektory ataków XSS 288

Lokalne magazyny danych i bazy klienta 289

Web Messaging 291

WebSockets 291

Inne ważne cechy HTML5 296

Omijanie mechanizmów kontroli działających po stronie klienta 297

Łagodzenie skutków luk w zabezpieczeniach AJAX, HTML5 i innych podatności po stronie klienta

Podsumowanie 302

Rozdział 10. Inne często spotykane podatności aplikacji sieciowych 303

Niezabezpieczone bezpośrednie odwołania do obiektów 304

 Bezpośrednie odwołania do obiektów w usługach sieciowych 306

 Ataki typu path traversal 306

Ataki typu file inclusion 308

 Ataki typu Local File Inclusion 309

 Ataki typu Remote File Inclusion 312

Ataki typu HTTP parameter pollution 312

Wycieki informacji 313

Zapobieganie atakom 316

 Niezabezpieczone bezpośrednie odwołania do obiektów 316

 Ataki typu file inclusion 316

 Ataki typu HTTP parameter pollution 317

 Wycieki informacji 317

Podsumowanie 317

Rozdział 11. Skanowanie aplikacji sieciowych przy użyciu zautomatyzowanych skanerów podatności 319

Zanim zaczniesz używać automatycznego skanera podatności 320

Skanery podatności aplikacji sieciowych dostępne w systemie Kali Linux 321

 Nikto 321

 Skipfish 323

 Wapiti 325

 Skaner OWASP ZAP 327

Skanery podatności dla systemów CMS 329

 WPScan 330

JoomScan 331

CMSmap 332

Fuzzing aplikacji internetowych 333

Korzystanie z fuzzera OWASP ZAP 334

Moduł Burp Intruder 338

Postępowanie po zakończeniu skanowania 342

Podsumowanie 342

Skorowidz 345