

Spis treści

O AUTORZE	15
O KOREKTORZE MERYTORYCZNYM	15
PRZEDMOWA	17
PODZIĘKOWANIA	21
WPROWADZENIE	23

I

CZYM JEST BEZPIECZEŃSTWO INTERFEJSÓW API?	27
--	-----------

O

PRZYGOTOWANIE TESTÓW BEZPIECZEŃSTWA	29
Uzyskanie upoważnienia	30
Modelowanie zagrożeń przed testem interfejsu API	30
Jakie cechy interfejsu API należy testować?	32
Testy mechanizmów uwierzytelniania	32
Zapory WAF	32
Testy aplikacji mobilnych	33
Audyt dokumentacji interfejsu API	33
Testy limitu zapytań	34
Ograniczenia i wykluczenia	35
Testy chmurowych interfejsów API	35
Testy odporności na ataki DoS	36
Raportowanie i testowanie środków zaradczych	37
Uwaga dotycząca programów dla łowców nagród	37
Podsumowanie	39

1	JAK DZIAŁAJĄ APLIKACJE INTERNETOWE?	40
	Podstawy aplikacji internetowych	40
	Adres URL	41
	Zapytania HTTP	42
	Odpowiedzi HTTP	43
	Kody stanu HTTP	44
	Metody HTTP	45
	Połączenia stanowe i bezstanowe	47
	Bazy danych w aplikacjach internetowych	48
	Relacyjne bazy danych	48
	Nierelacyjne bazy danych	49
	Miejsce interfejsów API	50
	Podsumowanie	51
2	ANATOMIA INTERFEJSU API	52
	Jak działają internetowe interfejsy API?	52
	Typy internetowych interfejsów API	55
	REST	55
	GraphQL	59
	Specyfikacje REST API	62
	Formaty wymiany danych	63
	JSON	63
	XML	65
	YAML	66
	Uwierzelnianie	67
	Podstawowe uwierzelnianie	67
	Klucze API	68
	Tokeny JWT	69
	HMAC	70
	OAuth 2.0	71
	Brak uwierzelnienia	73
	Praktyczne ćwiczenie: badanie interfejsu API Twittera	73
	Podsumowanie	75
3	TYPOWE PODATNOŚCI INTERFEJSÓW API	76
	Wycieki informacji	77
	Wadliwa autoryzacja na poziomie obiektu	78
	Wadliwa autoryzacja użytkownika	79
	Nadmierna ekspozycja danych	80
	Brak zasobów i limitu zapytań	81
	Wadliwa autoryzacja na poziomie funkcji	82

Przypisanie masowe 84

Błędna konfiguracja zabezpieczeń 85

Wstrzykiwanie danych 87

Niewłaściwe zarządzanie zasobami 88

Błędy w procedurach biznesowych 89

Podsumowanie 90

II

BUDOWANIE LABORATORIUM TESTOWANIA

INTERFEJSÓW API 91

4

TWÓJ SYSTEM HAKERSKI 93

Kali Linux 93

Analiza aplikacji internetowych za pomocą DevTools 94

Przechwytywanie i modyfikowanie zapytań za pomocą Burp Suite 96

 Konfiguracja FoxyProxy 97

 Instalacja certyfikatu Burp Suite 98

 Korzystanie z programu Burp Suite 99

 Przechwytywanie komunikacji 101

 Modyfikowanie zapytań za pomocą modułu Intruder 103

Wysyłanie zapytań za pomocą programu Postman 106

 Edytor zapytań 107

 Środowisko 110

 Kolekcja 110

 Wysyłanie kolekcji zapytań 113

 Generowanie kodu 114

 Testy 115

Integracja programów Postman i Burp Suite 116

Dodatkowe narzędzia 117

 Przeprowadzanie rekonesansu za pomocą narzędzia OWASP Amass 118

 Wykrywanie punktów końcowych za pomocą programu Kiterunner 119

 Wykrywanie podatności za pomocą Nikto 120

 Wykrywanie podatności za pomocą OWASP ZAP 121

 Zakłócanie za pomocą Wfuzz 121

 Wykrywanie parametrów zapytań za pomocą Arjun 123

Podsumowanie 124

Ćwiczenie 1. Zliczenie kont użytkowników interfejsu API 125

5

PRZYGOTOWANIE PODATNYCH INTERFEJSÓW API 129

Utworzenie hosta z systemem Linux 130

Instalacja środowisk Docker i Docker Compose 130

Instalacja podatnych aplikacji	131
crAPI	131
Pixi	132
Juice Shop	133
DVGA	134
Inne podatne aplikacje	134
Hakowanie interfejsów API w serwisach TryHackMe i HackTheBox	135
Podsumowanie	136
Ćwiczenie 2. Wyszukanie podatnych na ataki interfejsów API	136

III

ATAKOWANIE INTERFEJSÓW API141

6

ODKRYWANIE INTERFEJSÓW API	143
Rekonesans pasywny	144
Proces rekonesansu pasywnego	144
Hakowanie za pomocą Google	145
Katalog interfejsów API — ProgrammableWeb	147
Shodan	149
OWASP Amass	151
Informacje eksponowane w serwisie GitHub	153
Rekonesans aktywny	155
Proces rekonesansu aktywnego	156
Ogólne skanowanie za pomocą Nmap	158
Wyszukiwanie ukrytych ścieżek w pliku robots.txt	159
Wyszukiwanie poufnych informacji za pomocą Chrome DevTools	159
Weryfikacja interfejsu API za pomocą Burp Suite	162
Skanowanie identyfikatorów URI za pomocą OWASP ZAP	164
Wyszukiwanie identyfikatorów URI metodą brutalnej siły za pomocą programu Gobuster	166
Wykrywanie zasobów interfejsów API za pomocą narzędzia Kiterunner	168
Podsumowanie	169
Ćwiczenie 3. Rekonesans aktywny w teście czarnej skrzynki	170

7

ANALIZA PUNKTÓW KOŃCOWYCH	175
Pozyskiwanie informacji o zapytaniach	176
Wyszukiwanie informacji w dokumentacji	176
Import specyfikacji interfejsu API	179
Inżynieria odwrotna interfejsu API	181
Konfiguracja uwierzytelnienia w programie Postman	185
Analiza funkcjonalności interfejsu	187
Testowanie interfejsu zgodnie z przeznaczeniem	187
Wykonywanie operacji jako uwierzytelniony użytkownik	188
Analiza odpowiedzi	189

Wyszukiwanie wycieków informacji	190
Wyszukiwanie błędów w konfiguracji zabezpieczeń	191
Szczegółowe komunikaty o błędach	191
Stabe algorytmy szyfrowania	192
Problematyczna konfiguracja	192
Wyszukiwanie nadmiernej ekspozycji danych	193
Wyszukiwanie błędów w procedurach biznesowych	194
Podsumowanie	195
Ćwiczenie 4. Utworzenie kolekcji crAPI i identyfikacja nadmiernej ekspozycji danych	195

8

ATAKOWANIE PROCESU UWIERZYTELNIANIA UŻYTKOWNIKÓW200

Typowe ataki na procesy uwierzytelniania użytkowników	201
Łamanie poświadczeń metodą brutalnej siły	201
Reset hasła i atakowanie procesu uwierzytelnienia wieloskładnikowego metodą brutalnej siły	202
Rozpylanie hasel	204
Kodowanie Base64 w atakach metodą brutalnej siły	206
Falszowanie tokenów	207
Analiza ręcznie załadowanej listy tokenów	208
Analiza przechwytywanych tokenów	210
Generowanie prawdopodobnych tokenów	211
Łamanie tokenów JWT	213
Identyfikacja i analiza tokenów JWT	213
Eliminacja algorytmu kodowania	216
Podmiana algorytmu	216
Łamanie tokenu JWT	217
Podsumowanie	218
Ćwiczenie 5. Łamanie podpisu tokenu JWT w aplikacji crAPI	218

9

ZAKŁÓCANIE INTERFEJSU API222

Skuteczne zakłócanie interfejsów API	222
Dobór ładunków zakłócających	224
Wykrywanie anomalii	225
Zakłócanie interfejsu wszерz i w głąb	227
Zakłócanie interfejsu wszерz za pomocą programu Postman	228
Zakłócanie interfejsu w głąb za pomocą programu Burp Suite	230
Zakłócanie interfejsu w głąb za pomocą programu Wfuzz	232
Zakłócanie interfejsu wszерz i identyfikowanie niewłaściwego zarządzania zasobami	235
Testowanie metod HTTP za pomocą programu Wfuzz	237
Głębsze zakłócanie interfejsu i omijanie weryfikacji danych wejściowych	238
Zakłócanie interfejsu i przetwarzanie katalogów	239
Podsumowanie	239
Ćwiczenie 6. Zakłócanie interfejsu wszерz i niewłaściwe zarządzanie zasobami	240

10

EKSPLORACJA PROCESU AUTORYZACJI UŻYTKOWNIKÓW244

Identyfikacja podatności BOLA	244
Określenie identyfikatora zasobu	245
Test A-B podatności BOLA	246
Test podatności BOLA z użyciem kanału bocznego	247
Identyfikacja podatności BFLA	248
Test A-B-A podatności BFLA	249
Testowanie podatności BFLA za pomocą programu Postman	249
Wskazówki dotyczące hakowania procesu autoryzacji	252
Zmienne kolekcji w programie Postman	252
Wyszukiwanie i zmienianie zapytań w programie Burp Suite	252
Podsumowanie	252
Ćwiczenie 7. Lokalizacja pojazdu innego użytkownika	253

11

PRZYPISANIE MASOWE258

Identyfikowanie przypisania masowego	258
Rejestrowanie konta	259
Nieautoryzowany dostęp do zasobów innej organizacji	259
Identyfikacja kluczy	260
Wyszukiwanie kluczy w dokumentacji	260
Zakładanie niezrozumiałych kluczy	261
Losowe testowanie podatności na przypisanie masowe	262
Testowanie podatności na przypisanie masowe za pomocą programów Arjun i Burp Suite Intruder	262
Test podatności BFLA i przypisania masowego	263
Podsumowanie	264
Ćwiczenie 8. Modyfikacja ceny produktu w sklepie internetowym	265

12

WSTRZYKIWANIE DANYCH269

Identyfikacja podatności na wstrzykiwanie danych	270
Skrypty międzydomenowe (XSS)	270
Skrypty międzyinterfejsowe (XAS)	272
Wstrzykiwanie zapytań SQL	273
Specjalne ciągi znaków w zapytaniach SQL	275
SQLmap	276
Wstrzykiwanie zapytań NoSQL	277
Wstrzykiwanie poleceń systemu operacyjnego	279
Podsumowanie	281
Ćwiczenie 9. Wyłudzenie kuponów poprzez wstrzykiwanie zapytań NoSQL	281

IV

HAKOWANIE INTERFEJSÓW API W PRAKTYCE 287

13

OMIJANIE ZABEZPIECZEŃ I TESTOWANIE LIMITU ZAPYTAŃ 289

Omijanie mechanizmów ochrony	290
Jak funkcjonuje mechanizm ochrony?	290
Wykrywanie mechanizmów ochrony	291
Fikcyjne konta	292
Techniki uników	292
Omijanie zabezpieczeń za pomocą programu Burp Suite	294
Omijanie zabezpieczeń za pomocą programu Wfuzz	296
Testowanie limitu zapytań	298
Przestrzeganie łagodnych limitów	298
Modyfikacja ścieżki URL	300
Fałszowanie nagłówka pochodzenia	301
Rotacja adresów IP w Burp Suite	302
Podsumowanie	306

14

ATAKOWANIE INTERFEJSU GRAPHQL API 307

Zapytania GraphQL i środowisko IDE	307
Aktywny rekonesans aplikacji DVGA	309
Skanowanie	309
Badanie za pomocą przeglądarki	310
Badanie za pomocą narzędzi DevTools	311
Inżynieria odwrotna interfejsu GraphQL API	312
Identyfikacja punktu końcowego metodą brutalnej siły	313
Modyfikacja nagłówka w celu uzyskania dostępu do środowiska GraphQL	314
Inżynieria odwrotna interfejsu GraphQL API	316
Inżynieria odwrotna interfejsu przy użyciu zapytania introspekcyjnego	318
Analiza interfejsu GraphQL API	319
Tworzenie zapytań za pomocą eksploratora dokumentacji	319
Rozszerzenie InQL programu Burp Suite	321
Zakłócanie i wstrzykiwanie poleceń	323
Podsumowanie	328

15

WŁAMANIA DO INTERFEJSÓW API I POLOWANIA NA NAGRODY 329

Włamania	330
Peloton	330
Poczta Stanów Zjednoczonych	331
T-Mobile	333

Połowania na nagrody	334
Cena dobrego klucza API	335
Błąd w procesie autoryzacji w prywatnym interfejsie API	336
Starbucks — włamanie, którego nie było	337
Podatność BOLA interfejsu GraphQL API w serwisie Instagram	339
Podsumowanie	341
 ZAKOŃCZENIE	 343
 A	
LISTA KONTROLNA HAKERA	345
 B	
DODATKOWE MATERIAŁY	348
 SKOROWIDZ	 353