

Spis treści |

O autorce	13
O recenzentach	14
Słowo wstępne	17
Przedmowa	19

CZĘŚĆ 1. Podstawy zabezpieczeń interfejsów API

ROZDZIAŁ 1

Wprowadzenie do architektury i zabezpieczeń interfejsów API	27
Interfejsy API i ich rola w nowoczesnych aplikacjach	28
Jak działają interfejsy API?	29
Wykorzystanie interfejsów API w nowoczesnych aplikacjach — zalety i korzyści	30
Użycie interfejsów API w rzeczywistych przykładach biznesowych	32
Przegląd zabezpieczeń interfejsów API	33
Dlaczego bezpieczeństwo interfejsów API jest tak istotne?	35
Podstawowe komponenty architektury interfejsów API i protokoły komunikacji	37
Typy interfejsów API i ich zalety	38
Typowe protokoły komunikacyjne i kwestie bezpieczeństwa	41
Podsumowanie	43
Dodatkowe źródła informacji	43

ROZDZIAŁ 2

Ewolucja krajobrazu zagrożeń dotyczących interfejsów API i kwestie bezpieczeństwa	45
Historyczna perspektywa zagrożeń związanych z bezpieczeństwem interfejsów API	46
Początki interfejsów API	46
Powstanie Internetu i sieciowych interfejsów API	46
Pojawienie się stylu architektury REST i nowoczesnych interfejsów API ...	47
Era mikrouslug, urządzeń IoT i przetwarzania w chmurze	47

Współczesny krajobraz zagrożeń związanych z interfejsami API	48
Kluczowe kwestie dotyczące bezpieczeństwa interfejsów API w powiększającym się ekosystemie	49
Nowe trendy w zakresie bezpieczeństwa interfejsów API	51
Architektura zerowego zaufania trust w zabezpieczeniach interfejsów API	52
Wykorzystanie technologii blockchain do wzmocnienia bezpieczeństwa interfejsów API	53
Pojawienie się ataków zautomatyzowanych i botów	54
Kryptografia postkwantowa w zabezpieczeniach interfejsów API	55
Bezpieczeństwo architektury bezserwerowej w kontekście bezpieczeństwa interfejsów API	56
Analityka behawioralna i profilowanie zachowań użytkowników w kontekście bezpieczeństwa interfejsów API	57
Wnioski z rzeczywistych naruszeń danych przez interfejsy API	58
Naruszenie danych firmy Uber (2016 r.)	58
Naruszenie danych firmy Equifax (2017 r.)	60
Naruszenie danych firmy MyFitnessPal (2018 r.)	60
Skandal związany z firmami Facebook i Cambridge Analytica (2018 r.)	61
Podsumowanie	63
Dodatkowe źródła informacji	63

ROZDZIAŁ 3

Objaśnienie 10 największych zagrożeń dotyczących bezpieczeństwa interfejsów API (według organizacji OWASP)	64
Fundacja OWASP i zestawienie API Security Top 10 — oś czasu	65
Analiza zestawienia OWASP API Security Top 10	66
OWASP API 1 — naruszenie autoryzacji na poziomie obiektu	66
OWASP API 2 — naruszenie uwierzytelniania	71
OWASP API 3 — naruszenie autoryzacji na poziomie właściwości obiektu ...	75
OWASP API 4 — nieograniczone wykorzystanie zasobów	77
OWASP API 5 — naruszenie autoryzacji na poziomie funkcji	80
OWASP API 6 — nieograniczony dostęp do poufnych procesów biznesowych	82
OWASP API 7 — fałszowanie żądań po stronie serwera	84
OWASP API 8 — błędna konfiguracja zabezpieczeń	86
OWASP API 9 — niewłaściwe zarządzanie magazynem	90
OWASP API 10 — niezabezpieczone korzystanie z interfejsów API	92
Podsumowanie	93
Dodatkowe źródła informacji	94

CZĘŚĆ 2. Ofensywne naruszanie zabezpieczeń interfejsów API

ROZDZIAŁ 4

Strategie i taktyki ataków dotyczących interfejsów API	97
Wymagania techniczne	98
Testowanie zabezpieczeń interfejsów API — przegląd niezbędnego zestawu narzędzi	98
Przegląd i konfiguracja systemu Kali Linux na maszynie wirtualnej	99
Przeglądarka jako narzędzie do testowania bezpieczeństwa interfejsów API	100
Korzystanie z pakietu Burp Suite i ustawienia usługi proxy	102
Omówienie narzędzi pakietu Burp Suite	103
Konfiguracja rozszerzenia FoxyProxy dla przeglądarki Firefox	105
Konfiguracja certyfikatów pakietu Burp Suite	107
Eksploracja funkcji usługi proxy pakietu Burp Suite	108
Konfiguracja narzędzia Postman do testowania interfejsów API i przechwytywanie ruchu za pomocą pakietu Burp Suite	117
Kolekcje narzędzia Postman	124
Podsumowanie	127
Dodatkowe źródła informacji	127

ROZDZIAŁ 5

Wykorzystanie luk w interfejsach API	128
Wymagania techniczne	128
Wektory ataku dotyczącego interfejsów API	128
Typy wektorów ataku	129
Ataki z wstrzykiwaniem i danymi losowymi na interfejsy API	134
Ataki z danymi losowymi	135
Ataki ze wstrzykiwaniem	145
Wykorzystywanie luk w interfejsach API związanych z uwierzytelnianiem i autoryzacją	150
Ataki siłowe na hasła	151
Ataki z użyciem tokenów JWT	159
Podsumowanie	166

ROZDZIAŁ 6**Omijanie elementów kontroli uwierzytelniania**

i autoryzacji interfejsów API	167
Wymagania techniczne	168
Wprowadzenie do elementów kontroli uwierzytelniania i autoryzacji w interfejsach API	169
Typowe metody uwierzytelniania i autoryzacji w interfejsach API	170
Omijanie elementów kontroli uwierzytelniania użytkowników	178
Omijanie elementów kontroli uwierzytelniania opartego na tokenach	183
Omijanie elementów kontroli uwierzytelniania opartego na kluczach interfejsu API	187
Omijanie elementów kontroli dostępu opartych na rolach i atrybutach	190
Przykłady rzeczywistych ataków z omijaniem zabezpieczeń interfejsów API	193
Podsumowanie	194
Dodatkowe źródła informacji	194

ROZDZIAŁ 7**Ataki oparte na technikach weryfikacji danych wejściowych**

oraz szyfrowania w interfejsach API	195
Wymagania techniczne	196
Elementy kontrolne weryfikacji poprawności danych wejściowych w interfejsach API	196
Techniki omijania elementów kontrolnych weryfikacji poprawności danych w interfejsach API	201
Wstrzykiwanie kodu SQL	201
Ataki XSS	208
Ataki z użyciem danych XML	212
Wprowadzenie do mechanizmów szyfrowania i odszyfrowywania w interfejsach API	215
Techniki unikania mechanizmów szyfrowania i odszyfrowywania interfejsów API	218
Studium przypadków, czyli rzeczywiste przykłady ataków dotyczących szyfrowania w interfejsach API	220
Podsumowanie	220
Dodatkowe źródła informacji	221

CZĘŚĆ 3. Zaawansowane techniki testowania i naruszania zabezpieczeń interfejsów API

ROZDZIAŁ 8

Testy penetracyjne i ocena podatności interfejsów API 225

Znaczenie oceny podatności interfejsów API	226
Rekonesans i footprinting interfejsów API	228
Techniki rekonesansu i footprintingu interfejsów API	229
Skanowanie i wyliczanie elementów interfejsów API	240
Techniki skanowania i wyliczania interfejsów API	240
Techniki wykorzystania podatności interfejsów API w trakcie ataku i po nim	244
Techniki wykorzystania	245
Techniki wykorzystania po dokonaniu ataku	245
Najlepsze praktyki dotyczące oceny podatności interfejsów API oraz testów penetracyjnych	249
Tworzenie raportów dotyczących podatności interfejsu API oraz ich łagodzenie	249
Przyszłość testów penetracyjnych i oceny podatności interfejsów API	252
Podsumowanie	252
Dodatkowe źródła informacji	252

ROZDZIAŁ 9

Zaawansowane testowanie interfejsów API:

metody, narzędzia i środowiska 253	253
Wymagania techniczne	254
Zautomatyzowane testowanie interfejsów API z wykorzystaniem sztucznej inteligencji	254
Specjalistyczne narzędzia i środowiska używane do testowania interfejsów API z wykorzystaniem sztucznej inteligencji	256
Inne oparte na sztucznej inteligencji narzędzia do automatyzacji zabezpieczeń	261
Testowanie interfejsów API na dużą skalę z użyciem żądań równoległych ...	263
Gatling	264
Sposób użycia narzędzia Gatling do testowania interfejsów API na dużą skalę z wykorzystaniem żądań równoległych	266
Zaawansowane techniki pozyskiwania danych z interfejsów API	267
Stronicowanie	269
Ograniczanie liczby żądań	271
Uwierzytelnianie	273
Zawartość dynamiczna	274

Zaawansowane techniki wprowadzania danych losowych związane z testowaniem interfejsów API	276
AFL	281
Przykład zastosowania	282
Środowiska testowania interfejsów API	283
Środowisko RestAssured	285
Środowisko WireMock	289
Środowisko Postman	292
Środowisko Karate DSL	294
Środowisko Citrus	295
Podsumowanie	298
Dodatkowe źródła informacji	299

ROZDZIAŁ 10

Wykorzystanie technik obchodzenia	300
Wymagania techniczne	301
Techniki zaciemniania kodu w interfejsach API	301
Zaciemnianie przepływu sterowania	303
Podział kodu	304
Wstrzykiwanie „martwego” kodu	306
Nadmierne wykorzystanie zasobów	307
Techniki wstrzykiwania kodu służące do unikania wykrycia	309
Zanieczyszczanie parametrów	309
Wstrzykiwanie bajtów zerowych	310
Wykorzystanie kodowania i szyfrowania w celu obejścia metod wykrywania	312
Kodowanie	312
Szyfrowanie	313
Kwestie dotyczące metod obrony	314
Steganografia w interfejsach API	316
Zaawansowane przypadki użycia i narzędzia	317
Kwestie dotyczące metod obrony	319
Polimorfizm w interfejsach API	321
Cechy polimorfizmu	321
Narzędzia	323
Kwestie dotyczące metod obrony	325
Wykrywanie technik obchodzenia w interfejsach API i przeciwdziałanie im	326
Kompleksowe rejestrowanie i monitorowanie	327
Analiza behawioralna	327
Wykrywanie oparte na podpisach	328
Dynamiczne generowanie podpisów	328
Uczenie maszynowe i sztuczna inteligencja	329
Praktyki zwiększania bezpieczeństwa ukierunkowane na ludzi	329

Podsumowanie	331
Dodatkowe źródła informacji	332

CZĘŚĆ 4. Zabezpieczenia interfejsów API dla specjalistów technicznych od zarządzania

ROZDZIAŁ 11

Najlepsze praktyki dotyczące projektowania i implementacji bezpiecznych interfejsów API	335
Wymagania techniczne	336
Znaczenie projektowania i implementacji bezpiecznych interfejsów API	336
Projektowanie bezpiecznych interfejsów API	337
Modelowanie zagrożeń	338
Implementacja bezpiecznych interfejsów API	344
Narzędzia	348
Utrzymanie bezpiecznych interfejsów API	350
Narzędzia	352
Podsumowanie	354
Dodatkowe źródła informacji	355

ROZDZIAŁ 12

Wyzwania i rozważania dotyczące zabezpieczeń interfejsów API w dużych przedsiębiorstwach	356
Wymagania techniczne	357
Zarządzanie bezpieczeństwem w różnorodnym ekosystemie interfejsów API	357
Równoważenie bezpieczeństwa i użyteczności	360
Wyzwania	360
Ochrona starszych interfejsów API	364
Zastosowanie bram interfejsów API	364
Implementowanie zapór sieciowych aplikacji internetowych	365
Regularne audyty zabezpieczeń	366
Regularne aktualizacje i poprawki	366
Monitorowanie i rejestrowanie aktywności	367
Szyfrowanie danych	367
Tworzenie bezpiecznych interfejsów API na potrzeby integracji z podmiotami zewnętrznymi	367
Monitorowanie bezpieczeństwa i reagowanie na incydenty w przypadku interfejsów API	370
Monitorowanie zabezpieczeń	371
Reagowanie na incydenty	373

Podsumowanie	375
Dodatkowe źródła informacji	376

ROZDZIAŁ 13

Wprowadzanie inicjatyw związanych ze skutecznym nadzorem nad interfejsami API oraz z zarządzaniem ryzykiem	377
Nadzór nad interfejsami API i zarządzania ryzykiem	378
Kluczowe elementy nadzoru nad interfejsami API i zarządzania ryzykiem	378
Ustanawianie solidnych zasad bezpieczeństwa interfejsów API	383
Określenie celów i zakresu	384
Identyfikacja wymagań dotyczących bezpieczeństwa	384
Uwierzytelnianie i autoryzacja	384
Szyfrowanie danych	385
Weryfikacja i oczyszczanie danych wejściowych	385
Rejestrowanie i monitorowanie	385
Zgodność i nadzór	386
Przeprowadzanie skutecznych ocen ryzyka w przypadku interfejsów API	386
Elementy ryzyka powiązane z interfejsami API	387
Metody i struktury	387
Definiowanie zakresu	387
Identyfikacja i analiza ryzyka	388
Ustalanie priorytetów elementów ryzyka	388
Strategie minimalizujące	389
Dokumentacja i raportowanie	389
Ciągłe monitorowanie i przegląd	390
Struktury zapewniania zgodności w przypadku bezpieczeństwa interfejsów API	390
Zgodność z regulacjami prawnymi	391
Standardy branżowe	400
Audyty i przeglądy zabezpieczeń interfejsów API	401
Cel i zakres	402
Metody i techniki	402
Zgodność i standardy	402
Identyfikacja podatności i zagrożeń	403
Działanie zaradcze i zalecenia	403
Ciągłe monitorowanie i utrzymywanie	403
Typowy proces audytu i przeglądu	403
Podsumowanie	406
Dodatkowe źródła informacji	407

Podsumowanie	375
Dodatkowe źródła informacji	376

ROZDZIAŁ 13

Wprowadzanie inicjatyw związanych ze skutecznym nadzorem nad interfejsami API oraz z zarządzaniem ryzykiem 377

Nadzór nad interfejsami API i zarządzania ryzykiem	378
Kluczowe elementy nadzoru nad interfejsami API i zarządzania ryzykiem	378
Ustanawianie solidnych zasad bezpieczeństwa interfejsów API	383
Określenie celów i zakresu	384
Identyfikacja wymagań dotyczących bezpieczeństwa	384
Uwierzytelnianie i autoryzacja	384
Szyfrowanie danych	385
Weryfikacja i oczyszczanie danych wejściowych	385
Rejestrowanie i monitorowanie	385
Zgodność i nadzór	386
Przeprowadzanie skutecznych ocen ryzyka w przypadku interfejsów API	386
Elementy ryzyka powiązane z interfejsami API	387
Metody i struktury	387
Definiowanie zakresu	387
Identyfikacja i analiza ryzyka	388
Ustalanie priorytetów elementów ryzyka	388
Strategie minimalizujące	389
Dokumentacja i raportowanie	389
Ciągłe monitorowanie i przegląd	390
Struktury zapewniania zgodności w przypadku bezpieczeństwa interfejsów API	390
Zgodność z regulacjami prawnymi	391
Standardy branżowe	400
Audyty i przeglądy zabezpieczeń interfejsów API	401
Cel i zakres	402
Metody i techniki	402
Zgodność i standardy	402
Identyfikacja podatności i zagrożeń	403
Działanie zaradcze i zalecenia	403
Ciągłe monitorowanie i utrzymywanie	403
Typowy proces audytu i przeglądu	403
Podsumowanie	406
Dodatkowe źródła informacji	407

O autorce

Confidence Staveley to wielokrotnie nagradzana liderka w dziedzinie cyberbezpieczeństwa, mająca wykształcenie z zakresu inżynierii oprogramowania, specjalizująca się w dziedzinie bezpieczeństwa aplikacji i strategiach związanych z cyberbezpieczeństwem. Jej wyjątkowa umiejętność przekładania zagadnień ze świata cyberbezpieczeństwa na przystępne informacje sprawia, że trafia do wielu odbiorców. W ramach swojej serii „API Kitchen” prezentowanej w serwisie YouTube autorka objaśnia kwestię bezpieczeństwa interfejsów API z użyciem metafor kulinarnych.

Confidence posiada dyplom zaawansowania w inżynierii oprogramowania, tytuł licencjata z informatyki i informatycznych systemów biznesowych, a także tytuł magistra zarządzania w informatyce uzyskany na uniwersytecie w Bradford. Uzyskała też wiele branżowych certyfikatów, takich jak CISSP, CSSLP oraz CCISO. Oprócz pełnienia ról doradczych w wielu zarządach Confidence jest założycielką fundacji CyberSafe Foundation oraz firmy MerkleFence.

Przede wszystkim chciałabym podziękować moim rodzicom za dar edukacji.

Najwyższy szacunek wyrażam moim mentorom. Jestem głęboko wdzięczna profesorowi Prashantowi Pillaiowi (posiadaczowi brytyjskiego orderu MBE), który pokierował mnie na ścieżkę cyberbezpieczeństwa, oraz doktorowi Obadare Peterowi Adewale, który niestrudzenie pozwala mi „stać na swoich ramionach”.

Dziękuję również moim recenzentom technicznym, Gbolabo Awelewie i Shalomowi Onyibe, którzy mimo bardzo napiętego harmonogramu poświęcili swój czas, aby wesprzeć mnie w tym wyjątkowo ważnym projekcie dzielenia się wiedzą. Szczególne podziękowania kieruję do moich współpracowników — Jonesa Barazy, Catherine Kamau i Detiema Tawo, którzy udzielili mi dużego wsparcia w czasie trwania tego projektu.