

Spis treści

O autorze (7)

O redaktorze merytorycznym (9)

Wstęp (11)

Rozdział 1. Typowe protokoły bezpieczeństwa (17)

SOP (17)

CORS (21)

Kodowanie URL, czyli kodowanie z procentem (24)

Podwójne kodowanie (26)

Kodowanie Base64 (28)

Podsumowanie (31)

Rozdział 2. Zbieranie informacji (33)

Techniki zbierania informacji (33)

Wyliczanie domen, plików i zasobów (34)

Fierce (35)

theHarvester (38)

SubBrute (39)

CeWL (41)

DirBuster (42)

WhatWeb (44)

Shodan (48)

DNSdumpster (50)

Wyszukiwanie domen po odwróconym adresie IP - YouGetSignal (50)

Pentest-Tools (52)

Zaawansowane wyszukiwanie Google (52)

Podsumowanie (56)

Rozdział 3. Ataki XSS (57)

Odbity XSS (58)

Zapisany XSS (62)

Ataki XSS wykorzystujące Flasha - funkcja ExternalInterface.call() (70)

Znaczniki HttpOnly i bezpieczne pliki cookie (71)

Ataki XSS bazujące na obiektach DOM (72)

Narzędzie BeEF, czyli wykorzystywanie podatności XSS (75)

Podsumowanie (81)

Rozdział 4. Atak CSRF (83)

Wprowadzenie do CSRF (84)

Wykonywanie ataku CSRF dla żądań POST (85)

W jaki sposób programiści zapobiegają CSRF? (86)

Podatność CSRF PayPala dotycząca zmiany numerów telefonów (87)

Wykorzystanie podatności na atak CSRF w żądaniach typu JSON (88)

Wykorzystanie ataku XSS do wykradania tokenów CSRF (90)

Wykorzystanie słabości tokena CSRF (91)

Flash na ratunek (92)

Podsumowanie (96)

Rozdział 5. Wykorzystanie wstrzykiwania SQL (97)

Instalacja SQLMap w systemie Kali Linux (98)

Wprowadzenie do SQLMap (99)

Pobieranie danych - scenariusz z wykorzystywaniem błędu (102)

SQLMap i modyfikacja adresów URL (106)

Przyspieszamy cały proces (107)

Pobieranie danych z bazy w scenariuszach wykorzystujących czas lub działających na ślepo (109)

Odczyt i zapis plików (111)

Obsługa wstrzykiwania w żądaniu POST (115)

Wstrzykiwanie SQL do stron wymagających logowania (118)

Powłoka SQL (119)

Powłoka poleceń (119)

Unikanie filtrów - skrypty modyfikujące (121)

Konfiguracja serwera pośredniczącego (124)

Podsumowanie (124)

Rozdział 6. Podatności na atak związane z przesyłaniem plików (127)

Podatność na atak związana z przesyłaniem plików - wprowadzenie (128)

Zdalne wykonywanie kodu (129)

Powrót do XSS (134)

Ataki typu DoS (136)

Obejście zabezpieczeń związanych z przesyłaniem plików (138)

Podsumowanie (146)

Rozdział 7. Metasploit i sieć WWW (149)

Moduły Metasploit (149)

Użycie Msfconsole (151)

Wykorzystanie modułów pomocniczych związanych z aplikacjami internetowymi (153)

Wykorzystanie WMAP (157)

Generowanie w Metasploit ładunków dla aplikacji internetowych (161)

Podsumowanie (166)

Rozdział 8. Ataki XML (167)

Podstawy formatu XML (168)

Atak XXE (172)

XML do kwadratu (178)

Podsumowanie (180)

Rozdział 9. Nowe wektory ataków (181)

Atak SSRF (181)

Atak IDOR (188)

Przebijanie DOM (194)

Atak RPO (196)

Podmiana interfejsu użytkownika (201)

Wstrzykiwanie obiektów PHP (204)

Podsumowanie (209)

Rozdział 10. Bezpieczeństwo OAuth 2.0 (211)

Wprowadzenie do modelu OAuth 2.0 (212)

Otrzymywanie upoważnień (215)

Użycie OAuth dla zabawy i zysku (219)

Podsumowanie (223)

Rozdział 11. Metodologia testowania API (225)

 Zrozumieć API typu REST (225)

 Konfiguracja środowiska testowego (230)

 Nauka API (232)

 Podstawowa metodologia testowania API dla programistów (237)

Skorowidz (243)