
Spis treści

Wstęp	13
1. Historia bezpieczeństwa oprogramowania	29
Początki hakerstwa	29
Enigma — ok. 1930 r.	30
Automatyczne łamanie kodu Enigmy — ok. 1940 r.	33
Poznaj Bombę	34
Phreaking telefonów — ok. 1950 r.	36
Technologia antyphreakingowa — ok. 1960 r.	37
Początki hakowania komputerów — ok. 1980 r.	38
Rozwój sieci WWW — ok. 2000 r.	40
Hakerzy w nowoczesnej erze — po ok. 2015 r.	42
Podsumowanie	45

Część I. Rozpoznanie

2. Wstęp do rekonesansu aplikacji internetowych	49
Zbieranie informacji	49
Mapowanie aplikacji internetowej	51
Podsumowanie	53
3. Struktura nowoczesnej aplikacji internetowej	55
Nowoczesne aplikacje kontra aplikacje starszego typu	55
API typu REST	57
JavaScript Object Notation	59
JavaScript	61
Zmienne i zakres	62
Funkcje	64
Kontekst	64

Dziedziczenie prototypowe	65
Asynchroniczność	67
Hierarchia DOM przeglądarki	70
Platformy SPA	72
Systemy uwierzytelniania i autoryzacji	73
Uwierzytelnianie	73
Autoryzacja	74
Serwery WWW	74
Bazy danych po stronie serwera	75
Magazyny danych po stronie klienta	76
Podsumowanie	77
4. Znajdowanie subdomen	79
Wiele aplikacji na domenę	79
Wbudowane w przeglądarkę narzędzia do analizy sieci	80
Wykorzystanie rekordów publicznych	82
Archiwa silnika wyszukiwania	83
Przypadkowe archiwa	85
Migawki z serwisów społecznościowych	86
Ataki transferu stref	89
Szukanie subdomen metodą brute force	91
Ataki słownikowe	96
5. Analiza API	99
Wykrywanie punktu końcowego	99
Mechanizmy uwierzytelniania	102
Struktury punktów końcowych	104
Popularne struktury	104
Struktura specyficzna dla aplikacji	105
Podsumowanie	106
6. Znajdowanie zewnętrznych zależności	107
Wykrywanie platform po stronie klienta	107
Wykrywanie platform SPA	107
Wykrywanie bibliotek JavaScriptu	109
Wykrywanie bibliotek CSS	111
Wykrywanie platform po stronie serwera	111
Wykrywanie nagłówków	112
Domyślne komunikaty błędów i strony 404	112
Wykrywanie baz danych	114
Podsumowanie	116

7. Identyfikowanie słabych punktów w architekturze aplikacji	117
Sygnały świadczące o bezpiecznej lub niezabezpieczonej architekturze	118
Wiele warstw bezpieczeństwa	121
Zapóżyczenia i ponowne odkrywanie	122
Podsumowanie	124
8. Podsumowanie części I	125

Część II. Ofensywa

9. Wstęp do hakowania aplikacji internetowych	129
Sposób myślenia hakera	129
Rozpoznanie stosowane	130
10. Ataki Cross-Site Scripting (XSS)	133
Wykrywanie i eksploatacja XSS	133
Zapisane ataki XSS	137
Odbite ataki XSS	138
Ataki XSS oparte na hierarchii DOM	140
Ataki XSS oparte na mutacji	143
Podsumowanie	144
11. Cross-Site Request Forgery (CSRF)	147
Manipulowanie parametrami zapytania	147
Inne dane wysyłane żądaniami GET	151
Ataki CSRF na punkty końcowe POST	152
Podsumowanie	154
12. XML External Entity (XXE)	155
Bezpośrednie ataki XXE	155
Pośrednie ataki XXE	158
Podsumowanie	160
13. Wstrzykiwanie	161
Wstrzykiwanie SQL-a	161
Wstrzykiwanie kodu	164
Wstrzykiwanie polecenia	168
Podsumowanie	171

14. Denial of Service (DoS)	173
Ataki DoS wykorzystujące wyrażenia regularne (ReDoS)	173
Logiczne ataki DoS	176
Rozproszone ataki DoS	179
Podsumowanie	180
15. Ataki z wykorzystaniem zewnętrznych zależności	181
Metody integracji	183
Gałęzie i rozwidlenia	183
Integracje z własnym hostingiem	184
Integracja z kodem źródłowym	185
Menedżery pakietów	185
JavaScript	186
Java	188
Inne języki	188
Baza danych Common Vulnerabilities and Exposures	189
Podsumowanie	190
16. Podsumowanie części II	191

Część III. Obrona

17. Zabezpieczanie nowoczesnych aplikacji internetowych	195
Defensywna architektura oprogramowania	196
Wyczerpujące inspekcje kodu	196
Wykrywanie luk	197
Analiza luk	198
Zarządzanie lukami	198
Testy regresyjne	199
Strategie łagodzenia ryzyka	199
Rekonesans stosowany i techniki ofensywne	199
18. Architektura bezpiecznej aplikacji	201
Analizowanie wymagań dotyczących funkcji	201
Uwierzytelnianie i autoryzacja	202
Protokoły Secure Sockets Layer i Transport Layer Security	203
Bezpieczne dane dostępne	203
Haszowanie danych dostępowych	205
Uwierzytelnianie dwuskładnikowe	207
Dane osobowe i finansowe	208
Wyszukiwanie	209
Podsumowanie	209

19. Przegląd kodu pod kątem bezpieczeństwa	211
Jak zacząć inspekcję kodu	212
Archetypowe luki kontra błędy we własnej logice	213
Od czego zacząć inspekcję pod kątem bezpieczeństwa	214
Antywzorce bezpiecznego kodowania	216
Czarne listy	216
Szablonowy kod	217
Antywzorzec domyślnego zaufania	218
Separacja klienta i serwera	218
Podsumowanie	219
20. Wykrywanie luk	221
Automatyzacja bezpieczeństwa	221
Analiza statyczna	222
Analiza dynamiczna	223
Testowanie regresji dotyczącej luk	224
Programy odpowiedzialnego ujawniania luk	227
Programy dla łowców błędów	227
Zewnętrzne testy penetracyjne	228
Podsumowanie	229
21. Zarządzanie lukami	231
Odtwarzanie luk	231
Ocena dotkliwości luki	232
Common Vulnerability Scoring System	232
CVSS: Base Scoring	233
CVSS: Temporal Scoring	235
CVSS: Environmental Scoring	236
Zaawansowana punktacja luk	237
Poza selekcją i oceną punktową	238
Podsumowanie	238
22. Obrona przed atakami XSS	239
Najlepsze praktyki tworzenia kodu odpornego na ataki XSS	239
Czyszczenie danych wpisanych przez użytkownika	241
DOMParser	242
SVG	242
Blob	243
Czyszczenie hiperłączy	243
Kodowanie encji znakowych HTML-a	244
CSS	245

Zasady Content Security Policy stosowane w celu zapobiegania atakom XSS	246
Źródło skryptu	246
Flagi unsafe-eval i unsafe-inline	247
Implementowanie CSP	247
Podsumowanie	248
23. Obrona przed atakami CSRF	249
Weryfikacja nagłówka	249
Tokeny CSRF	250
Bezstanowe tokeny CSRF	251
Najlepsze praktyki zapobiegające atakom CSRF	252
Bezstanowe żądania GET	252
Łagodzenie ryzyka atakami CSRF na poziomie aplikacji	253
Podsumowanie	255
24. Obrona przed atakami XXE	257
Weryfikacja innych formatów danych	257
Zaawansowane ryzyka XXE	259
Podsumowanie	259
25. Ochrona przed wstrzykiwaniem	261
Ochrona przed wstrzykiwaniem SQL-a	261
Wykrywanie wstrzykiwania SQL-a	261
Zapytania parametryzowane	263
Metody obrony specyficzne dla baz danych	264
Ogólne metody ochrony przed wstrzykiwaniem	265
Potencjalne cele wstrzykiwania	265
Zasada najmniejszych uprawnień	266
Tworzenie białej listy poleceń	266
Podsumowanie	268
26. Ochrona przed atakami DoS	269
Ochrona przed atakami DoS na funkcje parsujące wyrażenia regularne	269
Ochrona przed atakami DoS wymierzonymi w logikę	270
Ochrona przed atakami DDoS	271
Łagodzenie skutków ataków DDoS	271
Podsumowanie	272
27. Zabezpieczanie zewnętrznych zależności	273
Ocena drzewa zależności	273
Modelowanie drzewa zależności	274
Drzewa zależności w rzeczywistym świecie	274
Analiza automatyczna	275

Techniki bezpiecznej integracji	275
Podział odpowiedzialności	275
Bezpieczne zarządzanie pakietami	276
Podsumowanie	277
28. Podsumowanie części III	279
Historia bezpieczeństwa oprogramowania	279
Rekonesans aplikacji internetowych	280
Ofensywa	282
Obrona	283
29. Podsumowanie	287