

Spis treści

Wstęp	5
Rozdział 1. Kontrola dostępu do danych i funkcji	7
Modyfikacje elementów interfejsu	7
Zabezpieczanie dostępu do danych	13
Kwestia enumeracji zasobów	15
Kontrola dostępu do funkcji	18
Modyfikowanie żądań HTTP	22
Rozdział 2. SQL Injection	27
Co to jest SQL Injection?	27
Atak na logowanie	27
Dostęp do ukrytych danych	34
Nieautoryzowane modyfikowanie danych	39
Ślepy atak (Blind SQL Injection)	40
Ataki specyficzne dla platformy	44
Sposoby obrony	47
Filtry i ścisłe typowanie	48
Białe i czarne listy	49
Eskejpowanie	50
Zapytania parametryzowane	51
Odpowiednie uprawnienia	54
Automatyczne wyszukiwanie błędów	54
Rozdział 3. Przechowywanie haseł użytkowników	59
Hasła niekodowane	59
Szyfrowanie symetryczne	62
Korzystanie z funkcji skrótu	64
Solenie haseł	65
Rozdział 4. Ataki na logowanie	71
Przesyłanie danych	71
Blokowanie kont	72
Opóźnianie prób logowania	77
Logowanie i CAPTCHA	80
Informacje dla użytkownika	85
Łączenie różnych metod	88

Rozdział 5. Ataki typu XSS	89
Czym jest Cross-site scripting?	89
Jak powstaje błąd typu XSS?	89
Skutki ataku typu Persistent XSS	94
Atak typu Reflected XSS	97
Sposoby obrony	100
Rozdział 6. Dane z zewnętrznych źródeł	105
Gadżety na stronach WWW	105
Rozdział 7. Ataki CSRF i błędy transakcyjne	115
Geneza ataku	115
Przykład serwisu podatnego na atak	115
Błędy transakcyjne	120
Atak CSRF	124
Tokeny jako ochrona przed CSRF	128
Rozdział 8. Ataki Path Traversal	133
Specyfika ataku	133
Serwis pobierania plików podatny na atak	133
Identyfikatory zamiast nazw plików	138
Nie tylko pobieranie plików	141
Rozdział 9. Brak właściwej autoryzacji	147
Uwierzytelnienie i autoryzacja	147
Uwierzytelnienie to nie wszystko	147
Autoryzacja wykonywanych operacji	152
Rozdział 10. Dane u klienta	161
Logowanie raz jeszcze	161
Dane uwierzytelniające w cookie	165
Koszyk w sklepie internetowym	168
Rozdział 11. Ataki na sesję	181
Porywanie sesji	181
Fiksacja i adopcja	182
Przykład strony podatnej na złożony atak	183
Rozdział 12. Ładowanie plików na serwer	191
Serwis z obrazami	191
Czy to działa?	197
Atak na aplikację	198
Jak poprawić aplikację?	202
Skorowidz	205