

Przedmowa (5)

O książce (7)

1. Wprowadzenie (11)

- Funkcje języka PHP (12)
- Strategie (14)
- Dobre praktyki (17)

2. Formularze i adresy URL (25)

- Formularze i dane (25)
- Ataki semantyczne na adresy URL (28)
- Ataki związane z ładowaniem plików (30)
- Ataki typu cross-site scripting (33)
- Ataki typu CSRF (34)
- Podrabiane zatwierdzenia formularza (38)
- Sfałszowane żądania HTTP (39)

3. Bazy danych i SQL (43)

- Ujawnienie uwierzytelnień dostępu (44)
- Wstrzykiwanie kodu SQL (45)
- Ujawnienie danych przechowywanych w bazie (50)

4. Sesje i cookie (51)

- Kradzież cookie (53)
- Ujawnienie danych sesji (54)
- Zafiksowanie sesji (54)
- Przechwytywanie sesji (58)

5. Pliki dołączane do programów (61)

- Ujawnienie kodu źródłowego (61)
- Adresy URL otwierające tylne drzwi (63)
- Manipulowanie nazwą pliku (63)
- Wstrzykiwanie kodu (65)

6. Pliki i polecenia (67)

- Trawersowanie katalogów (67)
- Zagrożenia związane z plikami zdalnymi (69)
- Wstrzykiwanie poleceń (71)

7. Uwierzytelnianie i autoryzacja (73)

- Łamanie zabezpieczeń metodą brutalnej siły (74)
- Podsluchiwanie haseł (77)
- Ataki metodą powtórzenia (78)
- Trwały login (79)

8. Na wspólnym hoście (85)

- Ujawnienie kodu źródłowego (85)
- Ujawnienie danych sesji (88)
- Wstrzykiwanie sesji (91)
- Przeglądanie systemu plików (93)
- Bezpieczny tryb języka PHP (94)

A Dyrektywy konfiguracyjne (97)

B Funkcje (103)

C Kryptografia (109)

Skorowidz (115)