Szkolenie

Web Security Testing - Bezpieczeństwo i testowanie Web Aplikacji

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie skierowane jest do wszystkich osób, które chcą poznać lub usystematyzować wiedzę z zakresu testowania bezpieczeństwa aplikacji webowych. Program obejmuje zarówno **podstawy bezpieczeństwa aplikacji internetowych**, jak i **praktyczne aspekty testów penetracyjnych**, prowadzone w oparciu o realne scenariusze ataków.

Osoby bez zaawansowanej wiedzy technicznej poznają **techniki i metody testowania**, a także narzędzia wykorzystywane w testach bezpieczeństwa aplikacji webowych. Uczestnicy zapoznają się z **najczęściej występującymi podatnościami**, sposobami ich identyfikacji, wykorzystania oraz mitygacji.

Szkolenie realizowane jest w oparciu o **OWASP Web Security Testing Guide (WSTG)** oraz dobre praktyki testów penetracyjnych, z naciskiem na **manualne testowanie bezpieczeństwa**, rekonesans aplikacji oraz poprawne raportowanie wyników testów.

Forma szkolenia łączy **wykład**, **demonstracje na żywo oraz praktyczne laboratoria**, umożliwiające samodzielną pracę uczestników.

Dla kogo?

- osoby rozpoczynające pracę z testami bezpieczeństwa aplikacji webowych,
- testerzy, administratorzy, programiści chcący lepiej zrozumieć zagrożenia webowe,
- osoby nietechniczne zainteresowane zrozumieniem mechanizmów ataków na aplikacje,
- specjaliści IT chcący usystematyzować wiedzę w oparciu o standardy OWASP.

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Korzyści

Po ukończeniu szkolenia uczestnik:

- posiada **usystematyzowaną wiedzę z zakresu bezpieczeństwa aplikacji webowych**,
- zna **najczęściej występujące podatności** w aplikacjach internetowych oraz metody ich wykrywania,
- potrafi **praktycznie identyfikować i analizować podatności** w aplikacjach webowych,
- rozumie **mechanizmy ataków** oraz ich wpływ na bezpieczeństwo organizacji,
- zna **metody mitygacji i dobre praktyki zabezpieczania aplikacji**,
- potrafi przeprowadzić **rekonesans aplikacji webowej** przed właściwymi testami,
- rozumie różnice między **testami automatycznymi a manualnymi**,
- zna **proces testów bezpieczeństwa aplikacji webowych** – od planowania, przez testy, po raportowanie,
- potrafi przygotować **profesjonalny raport z testów bezpieczeństwa** dla zespołów technicznych i biznesowych,
- zwiększa świadomość zagrożeń wynikających z błędów projektowych i implementacyjnych w aplikacjach webowych.
- rozumie aspekty etyczne i prawne przeprowadzania testów penetracyjnych.

Harmonogram szkolenia

1. Bezpieczeństwo aplikacji webowych – wprowadzenie

- Podstawy bezpieczeństwa aplikacji webowych,
- Aktualne zagrożenia i podatności obserwowane w rzeczywistych aplikacjach webowych,
- Rola testów bezpieczeństwa w cyklu życia aplikacji,
- OWASP jako standard bezpieczeństwa aplikacji webowych.

2. OWASP Top 10 – analiza krytycznych ryzyk

Analiza wszystkich kategorii OWASP Top 10, ze szczególnym naciskiem na błędy projektowe i implementacyjne:

- Broken Access Control,
  - w tym podatności klasy **IDOR**
  - bezpieczeństwo tokenów **JWT**
- Security Misconfiguration,
- Software Supply Chain Failures,

- Cryptographic Failures,
- Injection,
- Insecure Design,
- Authentication Failures,
- Software or Data Integrity Failures,
- Security Logging & Alerting Failures,
- Mishandling of Exceptional Conditions.

Dodatkowo:

- podstawy protokołu **HTTP/HTTPS** w kontekście testów bezpieczeństwa.

3. Rekonesans aplikacji webowych

- Rekonesans aplikacji webowych jako etap testów bezpieczeństwa,
- Pasywne i aktywne zbieranie informacji o celu,
- Analiza komunikacji http,
- Identyfikacja endpointów, parametrów i logiki aplikacji,
- Wprowadzenie do bezpieczeństwa API (REST/JSON) oraz nowoczesnych architektur webowych.

4. Popularne ataki na aplikacje webowe (przykłady, demonstracje, laboratoria)

- Cross-Site Scripting (XSS):
  - Reflected,
  - Stored,
  - DOM-based.
- SQL Injection / Blind SQL Injection / NoSQL Injection,
- Server-Side Template Injection (SSTI),
- XML External Entity (XXE),
- Server-Side Request Forgery (SSRF),
- Path Traversal,
- Command Injection,
- HTTP Parameter Manipulation,
- Ataki na sesje,
- Cross-Site Request Forgery (CSRF/XSRF),
- Bezpieczna obsługa uploadu plików i podatności prowadzące do Remote Code Execution **(RCE)**.

Każda podatność omawiana jest pod kątem:

- mechanizmu działania,
- sposobu identyfikacji,
- potencjalnych skutków,
- metod mitygacji.

5. Pentest vs audyt bezpieczeństwa

- Różnice między testami penetracyjnymi a skanem podatności,
- Zakres, cele i oczekiwania biznesowe,
- Kiedy wybrać pentest, a kiedy skan podatności.

6. Modele testów bezpieczeństwa

- Black box vs Grey box vs White box,
- Zalety i ograniczenia poszczególnych podejść,
- Wpływ modelu testów na wyniki i raport końcowy.

7. OWASP Web Security Testing Guide (WSTG)

- Wprowadzenie do OWASP WSTG,
- Struktura i założenia metodologii,
- Metodologia testowania bezpieczeństwa aplikacji webowych,
- Kluczowe punkty testowe i ich praktyczne zastosowanie,
- WSTG vs inne frameworki – porównanie, plusy i minusy.

8. Narzędzia do testowania bezpieczeństwa

- Przegląd narzędzi wykorzystywanych w testach bezpieczeństwa aplikacji webowych,
- **Burp Suite (Community / Professional)** jako podstawowe narzędzie pracy testera,
- Automatyzacja vs testy manualne – kiedy i jakich narzędzi używać,
- Ograniczenia narzędzi automatycznych.

9. Dokumentacja i raportowanie

- Struktura profesjonalnego raportu z testów bezpieczeństwa,
- Najczęstsze błędy raportowe,
- Jak komunikować wyniki testów zespołom technicznym i biznesowym,
- Klasyfikacja podatności według skali CVSS (jak oceniać krytyczność błędów).

10. Podsumowanie i ćwiczenie końcowe

- Podsumowanie kluczowych zagadnień,
- Sesja pytań i odpowiedzi.

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.