

## Szkolenie

# Web Security Testing - Bezpieczeństwo i testowanie Web Aplikacji

[Strona szkolenia](#) | [Terminy szkolenia](#) | [Rejestracja na szkolenie](#) | [Promocje](#)

## Opis szkolenia

**Szkolenie skierowane jest dla wszystkich tych, którzy chcą poznać tajniki testowania aplikacji webowych.**

Osoby bez wiedzy technicznej poznają techniki i metody testowania, a także zapoznają się z narzędziami pomocnymi w testowaniu. Omówione zostaną także popularne ataki na web aplikacje.

### Korzyści po szkoleniu

- usystematyzowanie wiedzy pod kątem bezpieczeństwa Web Aplikacji,
- znajomość popularnych ataków na aplikacje sieciowe i sposoby ich mitygacji,
- zapoznanie się z popularnymi atakami na aplikacje i sposoby ich mitygacji,
- zrozumienie zagrożeń i zdobycie wiedzy na temat najnowszych technik i narzędzi do testowania bezpieczeństwa aplikacji internetowych,
- podniesienie kompetencji technicznych niezbędnych do skutecznej identyfikacji analizy i mitygacji luk w zabezpieczeniach aplikacji webowych,
- wzrost świadomości cyber zagrożeń i usystematyzowanie wiedzy pod kątem popularnych błędów w web aplikacjach.

## Harmonogram szkolenia

### 1. Bezpieczeństwo Web Aplikacji, OWASP

Adres korespondencyjny:

**DAGMA Szkolenia IT** | ul. Bażantów 6a/3 | Katowice (40-668)  
tel. 32 793 11 80 | [szkolenia@dagma.pl](mailto:szkolenia@dagma.pl)  
[szkolenia.dagma.eu](http://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  
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł  
Numer NIP: 634-012-60-68, numer REGON: 008173852

OWASP TOP 10 - analiza krytycznych ryzyk - błędy w tworzeniu/zarządzaniu web aplikacji.

- Broken Access Control
- Cryptographic Failures
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server Side Request Forgery (SSRF)

## 2. Popularne ataki na webaplikacje: przykłady, demonstracje, ćwiczenia, praca własna (laby)

- XSS, reflected, stored, DOM-Based
- Path Traversal
- CSRF/XSRF
- SQL Injection / Blind SQL Injection
- Server-Side Template Injection (SSTI)
- XXE (XML External Entity)
- Http Parameter Manipulation
- Session Attacks - Session Fixation
- Command Injection

## 3. Pentest vs Audyt bezpieczeństwa

## 4. Black box vs Grey box vs White box

## 5. Wprowadzenie do OWASP WEB SECURITY TESTING GUIDE (WSTG)

## 6. Metodologia testowania według WSTG

## 7. WSTG vs inne frameworki - porównanie, plusy i minusy

## 8. Omówienie krytycznych punktów i sposobów testowania według WSTG

## 9. Narzędzia do testowania

## 10. Podsumowanie

Adres korespondencyjny:

**DAGMA Szkolenia IT** | ul. Bażantów 6a/3 | Katowice (40-668)  
tel. 32 793 11 80 | szkolenia@dagma.pl  
[szkolenia.dagma.eu](http://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  
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł  
Numer NIP: 634-012-60-68, numer REGON: 008173852

---

**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  
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł  
Numer NIP: 634-012-60-68, numer REGON: 008173852