BO·TT·EGA
IT minds

Program szkolenia:

OWASP Top 10 z przykładami w ASP.NET MVC

Informacje:

Nazwa:	**OWASP Top 10 z przykładami w ASP.NET MVC**
Kod:	**sec-OWASP**
Kategoria:	Bezpieczeństwo
Grupa docelowa:	architekci testerzy
Czas trwania:	2 dni
Forma:	50% wykłady / 50% praktyczne demonstracje

Niniejsze szkolenie stanowi łagodne wprowadzenie do tematyki bezpieczeństwa aplikacji Webowych. Lista 10 najpowszechniejszych zagrożeń dla tego typu aplikacji publikowana przez organizację OWASP jest najpopularniejszym w branży IT opracowaniem tego typu i stanowi pierwszy przystanek na drodze do systemó wolnych od dziur.

Dla każdego z zagrożeń przedstawimy:

- Mechanizm działania
- Sposoby wykrycia
- Sposoby przeciwdziałania
- Przykładowy scenariusz ataku

Wybrane zagrożenia zostanę zilustrowane studiami konkretnych przypadków firm i instytucji, które padły ofiarą ataków.

Szkolenie przeznaczone jest dla wszystkich osób związanych z wytwarzaniem aplikacji opartych o technologie Webowe.

Zalety szkolenia:

- Informacje na temat zagrożeń dla aplikacji Webowych podane w łatwej i zrozumiałej formie
- Przykłady firm i organizacji, które padły ofiarą przedstawionych zagrożeń
- Praktyczne demonstracje ataków na aplikację ASP.NET MVC

BO·TT·EGA
IT minds

Szczegółowy program:

1. OWASP Top 10

- 1.1. Jak powstaje lista?
- 1.2. Jaki jest cel istnienia listy?

2. WebGoat - nasz kozioł ofiarny

- 2.1. Narzędzia, których będziemy potrzebowali
- 2.2. Budujemy kod źródłowy i uruchamiamy aplikację

3. Zagrożenia - krok po kroku

- 3.1. Wstrzykiwanie poleceń SQL
  - 3.1.1. Zapobiegamy atakowi SQL injection: ADO.NET
  - 3.1.2. Zapobiegamy atakowi SQL injection: Entity Framework
- 3.2. Nieprawidłowe uwierzytelnianie i zarządzanie sesjami
  - 3.2.1. Framework ASP.NET Identity
  - 3.2.2. Zarządzanie stanem sesji w ASP.NET MVC
- 3.3. Cross-Site Scripting (XSS)
  - 3.3.1. Zabezpieczamy wynikowy kod HTML za pomocą klasy AntiXssEncoder
- 3.4. Niezabezpieczony dostęp do danych
  - 3.4.1. Kontrola dostępu za pomocą atrybutu [Authorize]
  - 3.4.2. Obfuskacja i mapowanie referencji do danych
- 3.5. Błędna konfiguracja funkcji bezpieczeństwa
  - 3.5.1. "Utwardzamy" Web.config
  - 3.5.2. Wyłączamy funkcje diagnostyczne
  - 3.5.3. Chronimy połączenie przeglądarki z serwerem za pomocą HTTPS
- 3.6. Ujawnianie danych wrażliwych

BO·TT·EGA
IT minds