

Program szkolenia:

OWASP Top 10

Informacje:

Nazwa:	OWASP Top 10
Kod:	Arch-Sec-OWASP
Kategoria:	Bezpieczeństwo
Grupa docelowa:	testerzy architekci
Czas trwania:	1 dzień
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 systemów wolnych od dziur.

Dla każdego z zagrożeń przedstawimy:

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

Wybrane zagrożenia zostaną 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

Szczegółowy program:

1. OWASP Top 10

1.1. Jak powstaje lista?

1.2. Jaki jest cel istnienia listy?

2. Zagrożenia - krok po kroku

2.1. Wstrzykiwanie poleceń SQL

2.2. Nieprawidłowe uwierzytelnianie i zarządzanie sesjami

2.3. Cross-Site Scripting (XSS)

2.4. Niezabezpieczony dostęp do danych

2.5. Błędna konfiguracja funkcji bezpieczeństwa

2.6. Ujawnianie danych wrażliwych

2.7. Brak kontroli dostępu na poziomie funkcji

2.8. Cross-Site Request Forgery (XSRF)

2.9. Używanie komponentów ze znanymi dziurami w zabezpieczeniach

2.10. Brak walidacji przekierowań