SECURITUM

# SZKOLENIE

# Bezpieczeństwo aplikacji WWW

Grupa docelowa

programiści | testerzy | pentesterzy

Poziom zaawansowania

★ ★ ★

## O SZKOLENIU

- Ponad 30 ćwiczeń warsztatowych
- Nauka metod wykrywania i ochrony przed podatnościami
- Doświadczony trener
- Praca na realnych aplikacjach w LAB
- 30-minutowe wprowadzenie dla początkujących (przed szkoleniem)

DODATKOWE INFORMACJE

FORMULARZ ZGŁOSZENIOWY

## UCZESTNICY O SZKOLENIU

*Najlepsze szkolenie na jakim byłem.*

*Było fajne: zrozumiałe, w odpowiedniej szybkości, by każdy zdążył zrobić ćwiczenie ze wsparciem prowadzącego.*

*Tematyka i ćwiczenia zostały jednak tak skonstruowane, że każdy – niezależnie od swojego poziomu – mógł się z satysfakcją wyżyć. Michał bardzo fajnie tłumaczył i podpowiadał, ale nie prowadził za rączkę.*

*Szkolenie bardzo dobre. Zaleta: możliwość praktyki, co ułatwia zrozumienie i zapamiętanie.*

*Trzy dni wypełnione od rana do późnego popołudnia ćwiczeniami wraz z przystępnie wytłumaczoną teorią, do tego świetny sposób prowadzenia zajęć i przygotowanie techniczne.*

## RAMOWY PROGRAM SZKOLENIA

### Wprowadzenie do tematyki testowania bezpieczeństwa aplikacji webowych

- Czym są testy penetracyjne aplikacji WWW?
- Różnice pomiędzy testem penetracyjnym a audytem bezpieczeństwa
- Prezentacja przykładowego raportu z testów penetracyjnych
- Najistotniejsze klasy podatności występujące w aplikacjach webowych
- Omówienie dokumentów OWASP Top Ten, OWASP ASVS (Application Security Verification Standard), OWASP Testing Guide
- Dalsze źródła wiedzy: serwisy on-line, literatura, narzędzia

### Narzędzia wspierające testowanie bezpieczeństwa aplikacji

- Realizacja w pełni automatycznych testów aplikacji webowych – w tym generacja automatycznego raportu
- Automatyzacja testów (sprawne przygotowanie proof of concept ataku)
- Wykrywanie contentu na serwerze (metody bruteforce oraz zoptymalizowane bruteforce)
- Zastosowanie narzędzi do realizacji ataków typu bruteforce na uwierzytelnienie

### Podatność SQL injection

- 10-minutowe wprowadzenie do języka SQL
- 6–7 przykładów tej podatności w różnych miejscach aplikacji – nauka wykrywania podatności, przygotowania proof of contept (nieautoryzowane pobranie danych z bazy, wykonanie kodu w systemie operacyjnym), nauka łatania podatności
- Techniki omijania filtrów
- Blind SQL injection – prezentacja sposobów wykrywania oraz narzędzi umożliwiających atak
- Przykłady na kilku różnych bazach danych (wskazanie elementów charakterystycznych dla SQL Server, Oracle, MySQL, PostgreSQL, DB2, SQLite)

### Wykrywanie, wykorzystywanie oraz ochrona przed podatnościami

- Path traversal – wykonanie kodu w systemie operacyjnym z wykorzystaniem ze zmiennych środowiskowych CGI
- Problemy z XXE (XML External Entity)
- LDAP injection (wariant w systemach Linux oraz Windows)
- XPATH injection
- OS Command injection (4 warianty) – w tym błąd w jednej z bibliotek JAVA
- XSS – przejęcie dostępu administracyjnego w systemie blogowym / omijanie filtrów
- CSRF

### Ataki na system uwierzytelnienia i autoryzacji

- Badanie kilku aspektów bezpieczeństwa ścieżki logowania
- Badanie wykorzystanych mechanizmów autoryzacji
- Badanie statystyczne losowości identyfikatorów sesji
- Techniki bruteforce

### Całościowy test bezpieczeństwa aplikacji w LAB – podsumowanie zdobytej wiedzy

- Wykrycie 6–7 klas podatności
- Przełamanie zabezpieczeń aplikacji
- Wskazanie metod ochrony

## SZKOLENIE POLECAJĄ

ROSWALTO

sekurak.pl

programista

# TRENER


**Michał Bentkowski**


- 11 miejsce w globalnym rankingu Hall of Fame Google – Application Security
- Lokalizował błędy klienckie w domenie google.com czy Google Docs – zgłaszając przeszło 20 błędów z pulą wypłaty kilkadziesiąt tysięcy dolarów
- Wskazywał błędy w najpopularniejszych przeglądarkach: Firefox (CVE-2015-7188) czy Internet Explorer (CVE-2015-6139)
- Prelegent na konferencjach: KrakYourNet (2016), OWASP@Kraków (2015), 4Developers (2016) oraz na Sekurak Hacking Party
- Autor tekstów w serwisie: sekurak.pl, sekurak/offline oraz w magazynie „Programista”
- Konsultant d/s bezpieczeństwa IT w firmie Securitum (ponad 5 lat doświadczenia w testach aplikacji mobilnych i webowych)

## PUBLIKACJE

- *Ominięcie Same-Origin Policy w Firefoksie*
- *XSS-y w Google Caja*
- *Wyciek danych z Facebooka*

# ZAPISZ SIĘ

FORMULARZ ZGŁOSZENIOWY

DODATKOWE INFORMACJE


< SZKOLENIA@SECURITUM.PL >