SECURITUM

SZKOLENIE

Zaawansowane bezpieczeństwo aplikacji WWW

Grupa docelowa

programiści | testerzy | pentesterzy

Poziom zaawansowania

★ ★ ★

O SZKOLENIU

- Intensywne warsztaty: 85% praktyki
- Ponad 20 ćwiczeń na realnych aplikacjach, w tym niedawno „załatanych”
- Case study najciekawszych / typowych błędów
- Praktyczna prezentacja uniwersalnych metod ochrony przed podatnościami
- Szkolenie prowadzi doświadczony audytor-pentester

DODATKOWE INFORMACJE

FORMULARZ ZGŁOSZENIOWY

UCZESTNICY O SZKOLENIU

Duża ilość praktyki i ciekawe laby.

Dobre połączenie: przygotowanie techniczne i świeże bugi.

Doświadczenie prowadzącego i realne, aktualne przykłady użycia różnych podatności.

Rzadkie połączenie: silne nastawienie na praktykę, wiedza merytoryczna trenera i aktualne przypadki z „życia wzięte”.

Przegląd całego wachlarza ataków, nie tylko SQLi, XSS, pathtraversal, ale też mniej popularnych, szczególnie XXE, XPATH, MongoDB. Świetnie przygotowane ćwiczenia. Widać ogrom pracy włożony w przygotowanie szkolenia.

RAMOWY PROGRAM SZKOLENIA

Bezpieczeństwo webservices / API REST – warsztaty

- Lokalizowanie WebServices
- Generacja komunikatów SOAP na bazie WSDL
- XXE (XML eXternal Entities) a webservices
- XML bomb a webservices
- Praktyczne przykłady API REST oraz podatności

Błędy związane z obsługą XML – warsztaty

- XXE – wariant klasyczny
- XXE – wersja blind
- XML Bomb
- XML injection
- XSLT – OS Command Execution
- XSLT – odczyt plików z FS

Podatności klasy Object Injection – warsztaty

- Wykonanie kodu w OS przy deserializacji w Python
- PHP Object Injection
- Deserializacja w Java

Formaty kompresji a bezpieczeństwo aplikacji

- Shell z wykorzystaniem zip
- Linki symboliczne w zip

Uniwersalne mechanizmy ochrony aplikacji webowych – warsztaty

- Content Security Policy
- HTTP Strict Transport Security
- HTTP Public Key Pinning
- Web Application Firewall
- Monitoring logów serwera WWW z wykorzystaniem OSSEC
- Case study: ochrona przed DoS na aplikację webową

NoSQL injection – warsztaty

- Przegląd baz noSQL
- Przykłady wstrzyknięć do MongoDB
- MongoDB: omijanie uwierzytelnienia
- MongoDB: server-side JavaScript Injection

Case study: podatności w aplikacji Java – warsztaty

- Path traversal / omijanie filtrów
- XXE
- Zdalne wykonanie kodu w OS
- Shell w JSP

Case study: podatności w aplikacji .NET Framework – warsztaty

- Path traversal / omijanie filtrów
- Skanowanie portów poprzez aplikację webową
- Sekwencja kilku podatności od dostępu anonimowego do przejęcia kontroli administracyjnej i wykonania kodu w OS

Case study: podatności w konsoli zarządczej routerów TP-link

- Dwie niezależne metody wstrzykiwania kodu w OS

Ćwiczenie podsumowujące

- Wieloetapowe utrwalenie pozyskanej wiedzy

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 >