SECURITUM

SZKOLENIE

Bezpieczeństwo frontendu aplikacji WWW

Grupa docelowa

programiści | testerzy | pentesterzy

Poziom zaawansowania

★ ★ ★

O SZKOLENIU

- Praktyczny kurs prowadzony przez znanego badacza bezpieczeństwa
- Dwa dni warsztatów nt. praktycznej strony bezpieczeństwa aplikacji webowych w kontekście podatności po stronie frontendu
- Prezentacja zagrożeń stwarzanych przez popularne frameworki (JavaScript - jQuery / AngularJS / React / itp.) oraz mniej typowych podatności
- Tajniki warsztatu bugbountera, sprytnych metod omijania filtrów oraz metod ochrony

DODATKOWE INFORMACJE

FORMULARZ ZGŁOSZENIOWY

UCZESTNICY O SZKOLENIU

Praktyczne ćwiczenia ataku i dokładnie opisane historie wyśledzenia bugów z Google.

Dużo ciekawych detali dotyczących języków, kontekstów.

Trener kompetentny, dobrze przygotowany, pełen profesjonalizm.

Referencje do bugów, które zostały znalezione w rzeczywistych projektach.

Nacisk na praktyczne ćwiczenia, fajna strona do testowania.

Umiejętnie przekazana wiedza, dobre kierowanie przy pracy na przykładach.

Teoria była prosto opisana w ciekawy sposób. Nie nudziło się. Wszystko zrozumiałem. Notatki online.

RAMOWY PROGRAM SZKOLENIA

Wprowadzenie

- Krótkie wprowadzenie do technologii klienckich (HTML, JS, CSS)
- Najistotniejsze klasy podatności aplikacji webowych od strony klienta
- Omówienie źródeł zdobywania wiedzy

Fundamenty działania przeglądarek internetowych

- Same-Origin Policy
- Mechanizmy przechowywania danych po stronie przeglądarki/serwera (cookies, localStorage, sessionStorage,...)
- Mechanizmy bezpieczeństwa technologii pochodnych (Flash)

Cross-Site Scripting (XSS) – król podatności client-side

- Rodzaje XSS-ów (ze szczególnym uwzględnieniem DOM-based)
- Zaprezentowanie najistotniejszych różnic między popularnymi przeglądarkami w interpretacji JavaScript
- Zaprezentowanie kilku przykładów podatności XSS w różnych kontekstach
- Techniki omijania filtrów
- XSS przez pliki XML, SVG oraz Flash
- Omówienie Same Origin Method Execution (SOME)

Przeprowadzanie ataków bez XSS-a

- Wycieki danych przez „dangling markup"
- Wycieki danych przez CSS-y (atak Relative Path Overwrite)
- Współdzielenie danych pomiędzy domenami (CORS, JSONP)

Elementy API HTML5

- Web Workers
- Service Workers

Zwiększanie bezpieczeństwa frontendu

- Nagłówki bezpieczeństwa (Public-Key-Pins, X-Frame-Options , Strict-Transport-Security i inne)
- Content-Security-Policy (CSP) – remedium na problemy bezpieczeństwa czy piekło wdrożenia?
  - Omówienie podstaw CSP
  - Omówienie różnic pomiędzy poszczególnymi wersjami CSP
  - Sposoby obejścia CSP
- Flagi ciasteczek (HttpOnly, Secure, SameSite)

Problemy bezpieczeństwa popularnych frameworków JS (jQuery, Angular, React, Knockout i inne)

- Błędy bezpieczeństwa samych frameworków
- Wstrzyknięcia szablonów
- Problemy izolacji kontekstu JS

Podsumowanie

- LAB podsumowujący szkolenie, zawierający kilka podatności do samodzielnego wykorzystania
- Podsumowanie wszystkich podatności i metod ochrony
- Wskazanie ogólnych, najlepszych praktyk w zabezpieczaniu frontendu

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

SZKOLENIE POLECAJĄ

ROSWALTO

sekurak.pl

programista

< SZKOLENIA@SECURITUM.PL >