Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Wprowadzenie do atakowania i obrony aplikacji webowych

Cele szkolenia

Celem szkolenia z atakowania i ochrony webaplikacji jest poznanie różnych typów ataków poprzez praktyczne ćwiczenia, podczas których uczestnicy sami omijają zabezpieczenia i włamują się do systemu.

Umiejętności

Dzięki szkoleniu uczestnik będzie potrafił:

- *tworzyć bezpieczniejsze aplikacje webowe,*
- *skutecznie naprawiać podatności znalezione w aplikacji,*
- *korzystać z podstawowych narzędzi do przeprowadzenia testów penetracyjnych*
- *samodzielnie testować podatności aplikacji na niektóre ataki i zreprodukować podatności z raportu z testów penetracyjnych,*
- *zrozumieć skutki i ryzyko podatności zgłaszanych podczas testów penetracyjnych lub skanów bezpieczeństwa,*
- *rozumieć zasady etyki związanych z przeprowadzaniem testów penetracyjnych, w tym świadomość granic legalności i moralności, oraz konsekwencji niezgodnego postępowania.*

Profil uczestników

Kurs przeznaczony jest dla osób technicznych, związanych z tworzeniem i utrzymaniem oprogramowania:

- *programistów,*
- *testerów,*
- *dev-opsów*

Nie jest wymagana wstępna wiedza z bezpieczeństwa, ale uczestnik powinien mieć doświadczenie w programowaniu aplikacji webowych i znać następujące pojęcia:

- *metoda HTTP,*
- *nagłówek HTTP,*
- *ciasteczko,*
- *sesja,*
- *model i kontroler,*

- *SQL*

Przygotowanie uczestników

Przed szkoleniem uczestnik musi zainstalować: program Burp Suite Community Edition https://portswigger.net/burp/communitydownload Przeglądarkę z rodziny Chromium, najlepiej Google Chrome albo Brave Dodatek do przeglądarki FoxyProxy https://chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmlnjonogaaifnjlfnp?hl=en , docker

Szczegółowy program szkolenia

1. *Dzień 1*
   - 1.1. *Zapoznanie z narzędziem Burp Suite*
   - 1.2. *Wprowadzenie i praktyczne zadania z podatności SQL injection*
   - 1.3. *Wprowadzenie i praktyczne zadania z podatności Server-Side Template Injection*
   - 1.4. *Wprowadzenie i praktyczne zadania z podatności związanych z uwierzytelnieniem*
   - 1.5. *Hardening - skuteczne zabezpieczanie komponentów firm trzecich*

2. *Dzień 2*
   - 2.1. *Wprowadzenie i praktyczne zadania z podatności związanych z autoryzacją*
   - 2.2. *Wprowadzenie i praktyczne zadania z podatności Cross-site scripting (XSS)*
   - 2.3. *Wprowadzenie i praktyczne zadania z podatności XML External Entities (XXE)*
   - 2.4. *Używanie komponentów ze znanymi podatnościami i błędna konfiguracja*

3. *Dzień 3*
   - 3.1. *Security Headers*
   - 3.2. *Rozszerzenie dotychczasowej wiedzy o narzędzia sqlmap, gobuster, hashcat / jacktheripper, ZAP i inne*
   - 3.3. *Dodatkowe praktyczne przykłady ataków.*

Metoda realizacji szkolenia

Zdalne

Liczba dni, liczba godzin szkoleniowych

3 dni po 4 godziny szkoleniowe

Ścieżka rozwoju po szkoleniu

Po zakończeniu szkolenia rekomendowane jest dalsze doskonalenie w dziedzinie bezpieczeństwa aplikacji webowych poprzez tworzenie bezpiecznych aplikacji i zgłębianie wiedzy na temat projektów organizacji OWASP. Jeżeli uczestnik jest zainteresowany zgłębianiem wiedzy z atakowania aplikacji, sugerowane źródło to PortSwigger WebSec Academy. W szkoleniu praktycznym omówione jest kilka różnych ataków i na każdy z nich poświęcona jest cała godzina zajęć. W celu uzupełnienia wiedzy na temat innych podatności, uczestnik powinien wziąć udział w teoretycznym szkoleniu dostępnym w CSC "Wprowadzenie do bezpieczeństwa aplikacji webowych". Omówione są tam wszystkie podatności z listy OWASP TOP 10 oraz mechanizmy polepszenia bezpieczeństwa aplikacji np. poprzez nagłówki bezpieczeństwa.