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

COMARCH
Szkolenia

Bezpieczeństwo aplikacji internetowych

Podstawy zabezpieczania aplikacji webowych

Cele szkolenia

Szkolenie ma na celu zapoznanie uczestników z zagrożeniami aplikacji internetowych wynikającymi z ich szczególnej architektury. Po zakończeniu szkolenia jego uczestnik będzie potrafił zidentyfikować i zneutralizować potencjalne problemy bezpieczeństwa aplikacji internetowych.

Umiejętności

Dzięki szkoleniu uczestnik będzie potrafił:

Identyfikować zagrożenia bezpieczeństwa związane z aplikacjami internetowymi

Unikać błędów podczas tworzenia aplikacji internetowych powodujących luki bezpieczeństwa

Wytłumaczyć dlaczego bezpieczeństwo aplikacji jest ważne i dlaczego jest często bagatelizowane

Skonfigurować używane oprogramowanie pod względem bezpieczeństwa, rozumiejąc cel i zastosowanie występujących w nim zabezpieczeń

Skonfigurować bezpieczny system uwierzytelniania użytkowników z użyciem aktualnych praktyk projektowych i specyfikacji

Profil uczestników

Szkolenie przeznaczone jest dla osób znających podstawy działania aplikacji internetowych chcących się dowiedzieć jakie zagrożenia bezpieczeństwa występują w tego typu aplikacjach i jak się przed nimi zabezpieczać.

Przygotowanie uczestników

Od uczestników szkolenia wymagana jest znajomość zasad programowania oraz sposobu działania sieci WWW. Przydatna jest też choćby podstawowa znajomość języka Java.

Szczegółowy program szkolenia

Architektury aplikacji internetowych i źródła zagrożeń
- Od aplikacji UTC do RIA
- Podstawowe problemy bezpieczeństwa: sesje, cookies, tokeny
- Problemy bezpieczeństwa w aplikacjach responsywnych

- Klasyfikacje zagrożeń: STRIDE, OWASP
- Najprostsze ataki fałszujące request

Ataki typu injection

- SQL Injection
- Blind Injection
- Code Injection
- Command Injection

Ataki XSS

- Scenariusz ataku – reflected XSS, persistent XSS
- Możliwości i ograniczenia Javascript, Source & Sink
- DOM-based XSS
- Problemy z czyszczeniem danych
- Etapy czyszczenia danych i ich ograniczenia

Ograniczenia kodu w Javascript

- Same Origin Policy
- CORS – działanie i konfiguracja
- Preflight

Cross-site Request Forgery (CSRF)

- Zasada działania
- Możliwości
- Sposoby zabezpieczenia

Nagłówki request i response dotyczące zabezpieczeń

- Cache
- Zabezpieczenie przed click-jacking
- Specjalne nagłówki serwerów i przeglądarek
- Content Security Policy

Socjotechnika i phishing

- Człowiek jako podstawowe słabe ogniwo
- Możliwości preparowania linków

Uwierzytelnianie

- Klasyczne ataki na sesje I zabezpieczenia przed nimi
- Zabezpieczanie za pomocą JWT – zalety i wady
- OAuth 2
- OpenID Connect

Metoda realizacji szkolenia

Szkolenie realizowane jest w formie naprzemiennie następującej po sobie części teoretycznej w postaci mini wykładów oraz części praktycznej w postaci ćwiczeń komputerowych. Szkolenie łączy w sobie fachową wiedzę merytoryczną z praktycznymi przykładami jej wykorzystania w środowisku pracy. Ćwiczenia skonstruowane są w sposób, który wspiera utrwalenie nabytej wiedzy, oraz przyszłe twórcze wykorzystanie jej w dalszym rozwoju umiejętności.

Liczba dni, liczba godzin szkoleniowych

2 dni, 16 godzin szkoleniowych

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

Ścieżka rozwoju po szkoleniu

- *Wzorce projektowe. Praktyczne zastosowania wzorców projektowych z przykładami w języku Java.*
- *Obsługa baz danych w języku Java. Podstawy specyfikacji JPA na przykładzie Hibernate.*
- *Tworzenie efektywnych aplikacji JAVA.*