BEZPIECZEŃSTWO W TESTACH

Kategoria	Czas trwania	Termin	Cena
Security	20h	ustalamy indywidualnie	ustalamy indywidualnie

Program szkolenia:

Poniżej przedstawiamy przykładowy program szkolenia, który może zostać zmodyfikowany zgodnie z oczekiwaniami oraz poziomem grupy szkoleniowej. Przed przygotowaniem docelowego programu szkolenia, przeprowadzamy rozmowę techniczną, w której bierze udział trener oraz osoba techniczna lub cały zespół developerów reprezentujący klienta, w celu ustalenia szczegółów szkolenia.

1. Wprowadzenie do bezpieczeństwa aplikacji webowych

Architektura aplikacji webowych

- OWASP Top 10 2021
- CWE / CVE / CVSS

2. Zbieranie Informacji

- Information Gathering
- Enumeration

3. Narzędzia

Analiza ruchu sieciowego

- FTP vs HTTP vs HTTPS

Manipulacja zapytaniami HTTP

- modyfikacja zapytania typu GET
- modyfikacja zapytania typy POST/PUT/DELETE

4. Analiza podatności

- (SQLi) SQL i NoSQL injection
- (OSi) OS Command injection
- (UFU) Unrestricted File Upload

5. Wyciek danych

- zawartość logów
- open source code
- inne

6. Low hanging fruit

- Brak poprawnej obsługi błędów

7. Bezpieczeństwo ruchu sieciowego

- TLS/SSL
- Nagłówki HTTP w kontekście bezpieczeństwa
- Same-Origin Policy i Cross-Origin Resource Sharing (CORS)

8. Analiza podatności (atak, obrona, przykład)

- (XSS) Cross-site scriptin
- (XML)
  - (XXE) XML External Entity
  - XML DoS
- (CSRF) Cross-Site Request Forgery
- (LFI) Local File Inclusion
- (RFI) Remote File Inclusion
- (DT) Directory Traversal
- (BF) Brute Force
- (IDOR) Insecure Direct Object Reference
- (SSTI) Server-Side Template Injection
- (SSRF) Server-Side Request Forgery
- (DoS) Denial of Service and Application Denial of Service
- Błędy i podatności w zewnętrznych komponentach (Vulnerable and Outdated Components)

9. Bezpieczeństwo API

- Metody uwierzytelniania i autoryzacji
- Omówienie najczęstszych błędów bezpieczeństwa API
- OWASP API Security Top 10 2019

10. Fuzzowanie aplikacji webowych

11. Aplikacja mobilna

- proxy
- reverse engineering

12. Wprowadzenie do testów penetracyjny (CTF) (+live demo)