Ofensywne Testowanie Web Aplikacji

Odbiorcy: Programiści, Architekci, Testerzy, Administratorzy, DevOps, Bezpiecznicy
Forma: Warsztat (70% praktyki, 30% teorii)
Czas trwania: 2 dni
Wymagania: Laptop, środowisko VM, docker

Testowanie ofensywne jest jedną z podstawowych praktyk zapewniania bezpieczeństwa systemów IT. Szkolenie Ofensywne Testowanie Web Aplikacji (OTWA) zbudowane jest tak, aby Twój zespół wytwórczy nabył umiejętności identyfikacji oraz rozwiązywania typowych problemów bezpieczeństwa web aplikacji.

Agenda

1. Fundamenty teoretyczne
1.1. Triada CIA
1.2. Sposoby oceny bezpieczeństwa systemów IT
1.3. OWASP Top 10 (2021, 2017, 2013)
1.4. OWASP Web Security Testing Guide (WSTG)
1.5. OWASP Application Security Verification Standard (ASVS)
1.6. Black-box, white-box, gray-box
1.7. Penetration Testing Execution Standard (PTES)
2. Fundamenty praktyczne
2.1. Kali Linux
2.2. Firefox Developer Edition
2.3. OWASP Zed Attack Proxy (ZAP)
2.4. Web 101: Podstawy HTTP
2.5. Web 101: Same Origin Policy (SOP)
2.6. Web 101: Document Object Model (DOM)
3. Rekonesans i enumeracja web aplikacji

3.1. Architektura
3.2. Logika biznesowa
3.3. Kod źródłowy
3.4. Stos technologiczny
3.5. Specjalne pliki i ich wyszukiwanie
3.6. Mapowanie web aplikacji
3.7. Web Application Firewalls (WAF)
3.8. Bezpieczeństwo kanału komunikacyjnego na przykładzie HTTPS (SSL/TLS)
4. OWASP Top 10 2021
4.1. Kontrola dostępu
4.2. Wstrzyknięcia
4.3. Podatności wynikające z logiki aplikacji
4.4. Podatności wynikające z konfiguracji
4.5. Podatności w komponentach zewnętrznych
4.6. Uwierzytelnianie
4.7. Problemy z integralnością aplikacji i danych
4.8. Monitorowanie i logowanie
4.9. Server-Side Request Forgery
5. Raportowanie
5.1. Jak pisać i jak czytać raporty z oceny bezpieczeństwa
5.2. Krytyczność podatności i ryzyko
5.3. Common Vulnerability Scoring System (CVSS)
5.4. Common Vulnerabilities and Exposures (CVE)
5.5. Vulnerability Rating Taxonomy (VRT)
5.6. Omówienie przykładowych raportów