CYBER SECURITY ACADEMY

WEB IR MOBIŲJŲ APLIKACIJŲ TESTAVIMO WORKSHOP

WEB IR MOBIŲJŲ APLIKACIJŲ TESTAVIMO WORKSHOP

Be web ir mobiliųjų aplikacijų neapsieina nei viena moderni organizacija. Iš jų visuomet tikimasi funkcionalumo, duomenų prieinamumo ir saugumo – tai ypač svarbu verslui ir valstybinėms institucijoms.

Deja, dažniausiai aplikacijos nėra atnaujinamos. Tyrimai rodo, kad web ir mobiliųjų aplikacijų pažeidžiamumai yra veinas tiesiausių kelių siekiant įsilaužti į organizaciją, perimti turimą informaciją ir sukelti nuostolius.

Web ir mobiliųjų aplikacijų saugumo vertinimas ir testavimas yra būtinas žingsnis siekiant apsaugoti savo organizaciją ir jos duomenis.

Suprasti, kaip puolamos aplikacijos būtina tiek programuotojams, tiek saugumo specialistams, nes efektyviai gintis galima tik tada, kai žinai, kaip esi puolamas.

Praktika paremtuose mokymuose išmoksite vertinti aplikacijas kaip tai daro hakeriai ir bandysite jas išnaudoti, kad suprastumėte esamas rizikas. Mokymuose įgausite mobiliųjų ir web aplikacijų testavimui reikalingų žinių, įrankių ir išmoksite tam reikalingų technikų.

Po mokymų gebėsite įvertinti aplikacijų saugumo lygį, nustatyti pagrindinius pažeidžiamumus ir suprasite kaip jie išnaudojami neigiamai paveikti Jūsų organizaciją. Pritaikius šias žinias savo galima apsaugoti ne tik IT infrastruktūrą, bet ir Jūsų klientus bei darbuotojus.

TRUKMĖ: 3 dienos

DĖSTYMO KALBA: lietuvių

KAINA: 1 000 EUR

NUOLAIDOS:

Išankstinės registracijos nuolaida – 15 %

3 ir daugiau žmonių iš vienos įmonės – 20 %

(nuolaidos nesumuojamos)

Rekomendacijos dalyviams:

Siekiant maksimalaus rezultato mokymuose dalyvaujantiems rekomenduojama turėti Linux pagrindus ir gebėti dirbti komandine eilute. Taip pat reikalingos programavimo žinios.

Mokymų metu reikalingas nešiojamasis kompiuteris su šiomis specifikacijomis: kelių branduolių procesorius, 4GB RAM (min 2GB), WLAN, galimybe užkrauti OS iš USB, pageidautinas USBv3 palaikymas (min USBv2).*

* Jei kompiuterio su minėtomis specifikacijomis į mokymus atsinešti nėra galimybės, informuokite CSA ir mes jį parūpinsime (bus taikomas papildomas mokestis).

Lektoriai

Teikia informacijos saugumo valdymo paslaugas, atlieka saugumo auditus, įsiveržimų testavimus, DDoS atsparumo bandymus, teikia konsultacijas ISO 27001 standarto klausimais.

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

WEB IR MOBIŲJŲ APLIKACIJŲ TESTAVIMO WORKSHOP

1-oji diena: Web aplikacijų saugumas

1. OWASP Top 10 Overview
2. Introduction to Burp Suite
3. Vulnerability Classes
   - 3.1. Injection
     - 3.1.1. SQL Injection
     - 3.1.2. ORM Injection
     - 3.1.3. Command Injection
     - 3.1.4. Expression Language Injection
     - 3.1.5. Server-side Template Injection
   - 3.2. Broken Authentication
     - 3.2.1. Improper Authentication
     - 3.2.2. Session Management
     - 3.2.3. OAuth2 Misconfiguration
     - 3.2.4. JWT/JWS Misconfiguration
     - 3.2.5. Insure OTP/2FA Integration
   - 3.3. Sensitive Data Exposure
     - 3.3.1. Password Storage
     - 3.3.2. Weak Encryption
     - 3.3.3. Padding Oracle Attack
     - 3.3.4. Hash Length Extension Attack
   - 3.4. XML External Entities (XXE)
     - 3.4.1. XXE Attack
     - 3.4.2. XML Signature Wrapping
   - 3.5. Security Misconfiguration
     - 3.5.1. Default Configuration
     - 3.5.2. Error Handling
     - 3.5.3. Security Headers
   - 3.6. Broken Access Control
     - 3.6.1. Improper Authorization
     - 3.6.2. Mass Assignment/Auto binding
     - 3.6.3. Cross-Site Request Forgery
     - 3.6.4. Server-Side Request Forgery
     - 3.6.5. File Extension Handling
     - 3.6.6. File Path Traversal
     - 3.6.7. URL Path Traversal
     - 3.6.8. CORS Issues
   - 3.7. Cross-Site Scripting (XSS)
     - 3.7.1. Reflected / Stored / Dom Based XSS
     - 3.7.2. Client-Side Template Injection
   - 3.8. Insecure Deserialization
     - 3.8.1. Deserialization of Untrusted Data
   - 3.9. Using Components with Known Vulnerabilities
     - 3.9.1. Vulnerable Application Libraries
     - 3.9.2. Vulnerable JavaScript Libraries
   - 3.10. .NET Security Considerations
     - 3.10.1. Native Code Vulnerabilities
     - 3.10.2. ASP.NET Request Validation
     - 3.10.3. Viewstate and Event Validation

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

WEB IR MOBIŲJŲ APLIKACIJŲ TESTAVIMO WORKSHOP

2-oji diena: iOS aplikacijų saugumas

1. iOS Fundamentals
   - 1.1. iOS Security Model
   - 1.2. Application Model
2. Reversing Engineering
   - 2.1. IPA File Structure
   - 2.2. Device Jailbreaking
   - 2.3. Static Analysis Tools
   - 2.4. Dynamic Analysis Tools
   - 2.5. Log Monitoring
   - 2.6. Network Traffic Analysis
   - 2.7. HTTPS Traffic Interception
   - 2.8. Jailbreak Detection Bypass
   - 2.9. SSL Certificate Pinning Bypass
3. Application Security
   - 3.1. Insecure Data Storage
     - 3.1.1. Insecure Data Stored in Database
     - 3.1.2. Sensitive Data in Property List Files
     - 3.1.3. Keychain
     - 3.1.4. Insecure Snapshot
     - 3.1.5. Sensitive Information in clipboard
     - 3.1.6. Sensitive Data in Log Files
   - 3.2. Insecure Communication
     - 3.2.1. Use of Plaintext Protocols
     - 3.2.2. Certificate Validation
     - 3.2.3. Certificate Pinning
   - 3.3. Insecure Cryptography
     - 3.3.1. Insecure Key and Credentials Management
     - 3.3.2. Insecure Cryptographic Algorithms
   - 3.4. Insecure IPC Mechanisms
     - 3.4.1. URL Scheme Attacks
   - 3.5. Insecure User Input Handling
     - 3.5.1. UIWebView JavaScript injection
     - 3.5.2. SQL Injection
     - 3.5.3. XML Parsing
   - 3.6. Memory Corruption
     - 3.6.1. Format Strings
     - 3.6.2. Use-After-Free
   - 3.7. Client Code Quality
     - 3.7.1. App Signing
     - 3.7.2. Activation of Security Features
   - 3.8. Code Tampering
     - 3.8.1. Jailbreak Detection

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

WEB IR MOBIŲJŲ APLIKACIJŲ TESTAVIMO WORKSHOP

3-oji diena: Android aplikacijų saugumas

1. Android Fundamentals
   - 1.1. Android Security Model
   - 1.2. Application Model
2. Reverse Engineering
   - 2.1. APK File Structure
   - 2.2. Device Rooting/Emulators
   - 2.3. Static Analysis Tools
   - 2.4. ProGuard Deobfuscation
   - 2.5. Dynamic Analysis Tools
   - 2.6. Log Monitoring
   - 2.7. Network Traffic Analysis
   - 2.8. HTTPS Traffic Interception
   - 2.9. Root Detection Bypass
   - 2.10. Certificate Pinning Bypass
3. Application Security
   - 3.1. Insecure Data Storage
     - 3.1.1. Insecure Shared Preferences Files
     - 3.1.2. Insecure Files in Internal Storage
     - 3.1.3. Insecure Files in External Storage
     - 3.1.4. Insecure Database Files
     - 3.1.5. Data Leakage via Logging
     - 3.1.6. Data Leakage via Clipboard
     - 3.1.7. Data Leakage via Backup Functionality
     - 3.1.8. Data Leakage via Auto-generated Screenshots
   - 3.2. Insecure Communication
     - 3.2.1. Use of Plaintext Protocols
     - 3.2.2. Certificate Validation
     - 3.2.3. Certificate Pinning
   - 3.3. Insufficient Cryptography
     - 3.3.1. Insecure Key and Credentials Management
     - 3.3.2. Insecure Cryptographic Algorithms
   - 3.4. Insecure IPC Mechanisms
     - 3.4.1. Insecure Activities
     - 3.4.2. Insecure Content Providers
     - 3.4.3. Insecure Broadcast Receivers
     - 3.4.4. Insecure Services
     - 3.4.5. Custom URL Schemes
     - 3.4.6. Intent Sniffing
   - 3.5. Insecure User Input Handling
     - 3.5.1. WebView JavaScript injection
     - 3.5.2. SQL Injection
     - 3.5.3. XML Parsing
   - 3.6. Code Tampering
     - 3.6.1. Root Detection
     - 3.6.2. Debuggable Application

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt