Java and Web Application Security Eğitimi

Açıklama

Web uygulamalarını Java kullanarak yazmak eski teknolojilerle uğraşmaktan belgelenmemiş üçüncü taraf bileşenlere, sıkı son teslim tarihlerinden kod sürdürülebilirliğine kadar çeşitli nedenlerden dolayı bazı durumlarda çok karmaşık olabilir. Tüm bunların ötesinde, size şu anda siber saldırganların kodunuzu kırmak için uğraştıklarını söylesek? Kodunuzu kırmada başarılı olabilirler mi?

Bu eğitimde neler öğreneceksiniz?

- Güvenlik, BT güvenliği ve güvenli kodlamanın temel kavramları
- OWASP Top Ten sıralamasının ötesindeki Web güvenlik boşlukları ve bunlardan nasıl kaçınılacağı
- XML güvenliği hakkında bilgiler
- Dağıtım ortamının nasıl güvenli bir şekilde kurulacağı ve işletileceği
- İstemci tarafı güvenlik boşlukları ve güvenli kodlama uygulamaları
- Java geliştirme ortamının çeşitli güvenlik özelliklerini kullanma
- Kriptografı hakkında pratik bilgiler
- Tipik kodlama hataları ve bu hatalardan kaçınma yöntemleri
- Java çerçevesindeki bazı yeni güvenlik boşlukları hakkında çeşitli bilgiler
- Güvenli kodlama uygulamaları hakkında çeşitli kaynaklar ve diğer bilgiler

---

Eğitim İçeriği

IT security and secure coding

- Nature of security
- What is risk?
- IT security vs. secure coding
- From vulnerabilities to botnets and cybercrime
- Nature of security flaws
- Reasons of difficulty
- From an infected computer to targeted attacks
- The Seven Pernicious Kingdoms
- OWASP Top Ten 2017

Web application security

- Injection
- Injection principles
- SQL injection
- Exercise – SQL Injection
- Exercise – SQL injection
- Typical SQL Injection attack methods
- Blind and time-based SQL injection
- SQL injection protection methods
- Other injection flaws
- Command injection
- Case study – ImageMagick
- Broken authentication
- Session handling threats
- Session handling best practices
- Session handling in Java
- Setting cookie attributes – best practices
- Sensitive data exposure
- Transport layer security
- Enforcing HTTPS
- XML external entity (XXE)
- XML Entity introduction
- XML bomb
- Exercise – XML bomb
- XML external entity attack (XXE) – resource inclusion
- XML external entity attack – URL invocation

- XML external entity attack – parameter entities
- Exercise – XXE attack
- Preventing entity-related attacks
- Case study – XXE in Google Toolbar
- Broken access control
- Typical access control weaknesses
- Insecure direct object reference (IDOR)
- Exercise – Insecure direct object reference
- Protection against IDOR
- Case study – Facebook Notes
- Exercise – Authorization bypass
- Security misconfiguration
- Configuration management
- Hardening
- Patch management
- Configuring the environment
- Insecure file uploads
- Exercise – Uploading executable files
- Filtering file uploads – validation and configuration
- Cross-Site Scripting (XSS)
- Persistent XSS
- Reflected XSS
- DOM-based XSS
- Exercise – Cross Site Scripting
- Exploitation: CSS injection
- Exploitation: injecting the tag
- Exercise – HTML injection with base tag
- XSS prevention
- XSS prevention tools in Java and JSP
- Insecure deserialization
- Deserialization basics
- Security challenges of deserialization
- Deserialization in Java
- From deserialization to code execution
- POP payload targeting the Apache Commons gadget (Java)
- Real-world Java examples of deserialization vulnerabilities
- Issues with deserialization – JSON
- Best practices against deserialization vulnerabilities

Client-side security

- JavaScript security
- Same Origin Policy
- Cross Origin Resource Sharing (CORS)
- Exercise – Client-side authentication
- Client-side authentication and password management
- Protecting JavaScript code
- Exercise – JavaScript obfuscation
- Clickjacking
- Exercise – Do you Like me?
- Protection against Clickjacking
- Anti frame-busting – dismissing protection scripts
- Protection against busting frame busting
- AJAX security
- XSS in AJAX
- Script injection attack in AJAX
- Exercise – XSS in AJAX
- XSS protection in Ajax
- Exercise CSRF in AJAX – JavaScript hijacking
- CSRF protection in AJAX
- HTML5 security
- New XSS possibilities in HTML5
- HTML5 clickjacking attack – text field injection
- HTML5 clickjacking – content extraction
- Form tampering
- Exercise – Form tampering
- Cross-origin requests
- HTML proxy with cross-origin request
- Exercise – Client side include

Foundations of Java security

- The Java environment
- Java security
- Low-level security – the Java language and environment
- Java language security
- Type safety
- Automatic memory management

- Java execution overview
- Bytecode Verifier
- Class Loader
- Protecting Java code
- High-level security – access control
- Protection domains
- Security Manager and Access Controller
- Permission checking
- Effects of doPrivileged

Practical cryptography

- Cryptosystems
- Elements of a cryptosystem
- Symmetric-key cryptography
- Providing confidentiality with symmetric cryptography
- Symmetric encryption algorithms
- Block ciphers – modes of operation
- Other cryptographic algorithms
- Hash or message digest
- Hash algorithms
- SHAttered
- Message Authentication Code (MAC)
- Providing integrity and authenticity with a symmetric key
- Random numbers and cryptography
- Cryptographically-strong PRNGs
- Hardware-based TRNGs
- Asymmetric (public-key) cryptography
- Providing confidentiality with public-key encryption
- Rule of thumb – possession of private key
- Combining symmetric and asymmetric algorithms
- Public Key Infrastructure (PKI)

Ön Koşullar

C# Programlama tecrübesi