EMA SECURITY

Web Güvenliği Eğitimi

AI-Powered Offensive Services

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Web Güvenliği Eğitimi

Eğitim Açıklaması

Web Uygulama Saldırı ve Savunma Eğitimi, web uygulamaları üzerinde yapılan siber saldırılara karşı savunma tekniklerini öğrenmek isteyenler için idealdir. Katılımcılar, SQL enjeksiyonu, XSS, CSRF gibi yaygın web saldırıları hakkında bilgi edinir ve bu saldırılara karşı alınabilecek önlemleri keşfederler. Ayrıca, güvenli web uygulamaları tasarlama ve mevcut uygulamalarda zafiyetleri tespit etme becerisi kazanacaklardır.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 5 Gün

Eğitim Seviyesi

- Orta
- İleri

Eğitim İçin Ön Gereksinimler

- Web teknolojileri (HTML, CSS, JavaScript) hakkında temel bilgi
- Web uygulamaları ve sunucu yönetimi bilgisi
- Temel güvenlik açıkları ve saldırı teknikleri hakkında bilgi

Eğitimi Kimler Katılmalı?

- Web geliştiriciler ve yazılım mühendisleri
- Web uygulama güvenlik testleri yapmak isteyen IT profesyonelleri
- Güvenlik açıklarını tespit etmek ve koruma sağlamak isteyen siber güvenlik uzmanları

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, web uygulamalarındaki güvenlik açıklarını analiz eder, exploit tekniklerini öğrenir ve bu uygulamaları güvence altına alma yeteneği kazanırlar.

Eğitim İçeriği

- OWASP Top 10 Zafiyetleri ve Gerçek Hayat Uygulamaları
- A01 – Broken Access Control
- Doğrudan nesne erişimi (IDOR)
- Yetki atlatma senaryoları (GET/POST bypass, hidden parametreler)
- Path traversal ve sensitive file erişimi
- Test araçları: Burp Suite, Postman, OWASP ZAP
- A02 – Cryptographic Failures
- Zayıf şifreleme (MD5/SHA1 kullanımı)
- HTTPS yanlış konfigürasyonu (TLS downgrade, Self-signed cert)
- JWT saldırıları (alg:none, weak secret)
- A03 – Injection
- SQL Injection (Classic, Blind, Time-based, OOB)
- Command Injection (OS-level)
- LDAP, XML, SMTP Injection
- SQLMap, Commix, Burp Extension kullanımı
- A04 – Insecure Design
- Güvensiz iş akışı (örnek: parola reset token zayıflığı)
- Masaüstü uygulamalarla entegre web arayüzü zafiyetleri
- A05 – Security Misconfiguration
- Admin panellerine varsayılan erişim
- Geliştirici modları açık uygulamalar
- Açık API uçları (Swagger/OpenAPI zafiyetleri)
- A06 – Vulnerable and Outdated Components
- CVE veritabanından versiyon eşlemesi
- Exploit kullanım örnekleri (Apache Struts RCE, Log4Shell)
- A07 – Identification and Authentication Failures
- Brute-force saldırıları
- Session fixation

Eğitim İçeriği

- 2FA atlatma (OTP reuse, logic flaws)
- A08 – Software and Data Integrity Failures
- Supply chain saldırıları
- CI/CD zafiyetleri (kod inject eden build step'leri)
- A09 – Logging and Monitoring Failures
- Olay izleme eksiklikleri
- Log injection
- WAF/EDR bypass senaryoları
- A10 – Server-Side Request Forgery (SSRF)
- Metadata service erişimi
- Internal scanning
- URL whitelist bypass yöntemleri
- Gelişmiş Saldırı Teknikleri
- DOM-based XSS, CSP bypass
- Prototype Pollution saldırıları
- Subdomain takeover
- Open Redirect abuse
- GraphQL abuse: introspection, mass query injection
- SSRF chaining + RCE örnekleri
- Cloud metadata exfiltration via SSRF (AWS, Azure)
- Kimlik Bilgisi Hırsızlığı ve Hesap Ele Geçirme
- Session hijacking ve cookie stealing
- JWT Manipülasyonu ve Replay saldırıları
- CSRF token atlatma yöntemleri
- OAuth saldırıları: Authorization Code Interception, Token leakage
- Savunma ve Güvenlik Sertleştirme
- Geliştirme Aşamasında
- Güvenli kodlama prensipleri (input/output validation, parameterized query)

Eğitim İçeriği

- Content Security Policy (CSP) konfigürasyonu
- HTTP security headers (HSTS, X-Frame-Options, X-Content-Type)
- Yayın Ortamında
- Web Application Firewall (WAF) konfigürasyonu ve testleri
- Rate-limiting, brute-force koruması (fail2ban, mod_security)
- TLS 1.2+ zorunluluğu, TLS header kontrolleri
- Kaynak Kodu ve CI/CD Güvenliği
- Static Code Analysis (SAST) araçları: SonarQube, Semgrep
- Dependency kontrolü: Snyk, OWASP Dependency-Check
- Secrets tespiti: git-secrets, TruffleHog
- Loglama, İzleme ve Tespit Mekanizmaları
- Nginx/Apache logları üzerinden saldırı tespiti
- WAF log analizi (Cloudflare, ModSecurity, Imperva)
- Uygulama içi loglama best practices
- Log injection saldırılarının tespiti
- ELK, Graylog, Splunk ile görselleştirme ve alarm kuralları
- Olay Müdahalesi ve Saldırı Analizi
- Web shell yüklenmesi ve tespiti
- Webroot dışına dosya bırakma analizleri
- Post-exploitation adımları: credentials.txt, DB dump, .env file theft
- Exploit edilen endpoint analizi: LFI/RCE/SQLi log korelasyonu
- MITRE ATT&CK teknik eşleşmeleri (T1190, T1189, T1059)
- Uygulamalı Senaryolar ve Simülasyonlar
- Juice Shop ve DVWA üzerinden zafiyet sömürme
- SSRF → RCE zincirleme senaryosu
- SQLi + File Write ile web shell bırakma
- Auth bypass ile admin hesabı çalınması
- WAF/Log sistemleri ile saldırı analizi

Sıkça Sorulan Sorular

Web uygulamalarındaki güvenlik açıkları nasıl tespit edilir?

- OWASP Top 10 gibi yaygın web uygulama güvenlik açıkları üzerinde çalışılacak, SQL injection, XSS, CSRF gibi zafiyetlerin tespiti ve exploitation'ı öğretilir.

Web uygulama savunma stratejileri nelerdir?

- Web uygulama güvenliğinde input validation, güvenli kodlama yöntemleri, HTTPS kullanımı ve güvenlik başlıkları gibi savunma teknikleri önemlidir.

Eğitimde hangi web uygulama güvenlik araçları kullanılacak?

- Burp Suite, OWASP ZAP, Nikto gibi araçlar, web uygulamalarındaki güvenlik açıklarını keşfetmek için kullanılacaktır.

Web uygulama saldırıları sırasında hangi etik kurallar uygulanır?

- Web uygulama saldırılarında, yalnızca izinli uygulamalar üzerinde test yapılır ve tespit edilen açıklar raporlanarak çözüm önerileri sunulur.