Web Hacking Black Belt Edition Eğitimi

Süre: **5 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Web Hacking Black Belt Edition, modern web uygulamalarını, API'leri ve bunlarla ilişkili endpoint'leri hedef alan ileri seviye güvenlik açıklarını anlamaya ve test etmeye odaklanan yoğun bir uygulama güvenliği eğitimidir.

Program; belirli application security alanlarına, gelişmiş zafiyet tespit yöntemlerine ve istismar tekniklerine odaklanır. Katılımcılar gerçek ürünlerde karşılaşılmış, bug bounty programlarında raporlanmış ve klasik otomatik güvenlik tarayıcılarının çoğu zaman gözden kaçırabildiği güvenlik sorunlarını inceleme fırsatı bulur.

Eğitim boyunca güncel ve sıra dışı web güvenliği vakaları ele alınır. Katılımcılar ayrıca state-of-the-art Hacklab ortamından yararlanarak konuları uygulamalı şekilde pekiştirir.

Programın öne çıkan başlıkları arasında modern JWT, SAML ve OAuth sorunları, business logic açıkları, kriptografik zafiyetler, serialization ve template injection kaynaklı RCE senaryoları, DNS kanalları üzerinden istismar, ileri seviye SSRF, HPP, XXE ve SQL Injection konuları, serverless güvenlik problemleri, web caching açıkları ve attack chaining örnekleri bulunur.

Eğitimden maksimum fayda sağlamak için katılımcıların Burp Suite kullanımına önceden aşina olmaları önerilir.

Kimler Katılmalı

Bu eğitim özellikle aşağıdaki profiller için uygundur:

- Web geliştiriciler
- Orta seviye penetration tester'lar
- DevOps mühendisleri
- Network mühendisleri
- Security researcher ve analyst'ler
- Security architect'ler
- Bilgi güvenliği profesyonelleri
- Web güvenliği konusunda yetkinliğini ileri seviyeye taşımak isteyenler

Web Hacking Black Belt Edition Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Neler Öğreneceksiniz

Eğitimin sonunda katılımcılar:

- Otomatik tarama araçlarının gözden kaçırabildiği karmaşık web güvenlik açıklarını tespit etmeye ve güvenli test ortamlarında doğrulamaya yönelik teknikleri uygulayabilir.
- Test yaklaşımını gerçek saldırgan davranışları ve kullanılan araçlarla ilişkilendirerek organizasyonun karşı karşıya olduğu tehditlere daha uygun güvenlik değerlendirmeleri yapabilir.
- Standart payload'ların ötesine geçerek offensive security araçlarını belirli test senaryolarına göre uyarlayabilir.
- Güvenlik açıklarının ortaya çıkmasına neden olabilecek koşulların azaltılması veya ortadan kaldırılması için öneriler geliştirebilir.
- Web güvenlik açıklarının iş üzerindeki potansiyel etkisini anlayabilir ve bunu ilgili paydaşlara aktarabilir.
- Güvenlik ekipleri içerisinde daha fazla sorumluluk üstlenebilir ve organizasyon genelinde güvenlik farkındalığının gelişmesine katkıda bulunabilir.

Eğitim İçeriği

Eğitim Yapısı

Eğitim içeriği, web hacking dünyasında öne çıkan güncel saldırı ve güvenlik araştırmalarından seçilmiş ileri seviye konular üzerine kuruludur.

Katılımcılara özel olarak hazırlanmış bir Kali image sağlanır. Bu ortamda, eğitim kapsamında ele alınan zafiyetleri daha hızlı analiz etmeyi ve test etmeyi destekleyen çeşitli araç ve eklentiler bulunur.

Eğitim gerçek penetration testing deneyimine sahip bir uzman tarafından verilir. Gerçek dünya vaka örnekleri, uygulamalı hacking lab ortamı, çeşitli script ve araçlar ile öğrenci dokümanları eğitim boyunca katılımcılara destek olur.

Ayrıca eğitim sonunda, sınıf içi egzersizlerin nasıl çözüleceğini adım adım gösteren ayrıntılı cevap dokümanları sağlanır.

Lab Setup ve Architecture Overview

- Laboratuvar ortamının tanıtımı
- Eğitim mimarisinin genel yapısı

Burp Suite Özelliklerine Giriş

- Eğitimde kullanılacak temel Burp Suite özellikleri

Authentication ve SSO Saldırıları

- Token hijacking saldırıları
- Logical bypass ve boundary conditions

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Two-Factor Authentication bypass
- Subdomain takeover üzerinden authentication bypass
- JWT/JWS token saldırıları
- SAML authorization bypass
- OAuth güvenlik problemleri

Password Reset Saldırıları

- Session poisoning
- Host Header validation bypass
- Yaygın password reset hatalarına ilişkin vaka analizleri

Business Logic ve Authorization Açıkları

- Mass Assignment
- Invite ve Promo Code bypass
- Replay Attack
- API Authorization bypass
- HTTP Parameter Pollution (HPP)

XML External Entity (XXE)

- XXE temelleri
- OOB kanalları üzerinden gelişmiş XXE senaryoları
- SAML üzerinden XXE
- File parsing süreçlerinde XXE

Kriptografik Açıklar

- Known Plaintext Attack
- Hatalı password reset senaryoları
- Padding Oracle Attack
- Hash length extension saldırıları
- .NET Machine Key üzerinden authentication bypass
- Fixed IV kullanılan padding oracle senaryoları

Remote Code Execution (RCE)

- Java Serialization
- .NET Serialization
- PHP Serialization
- Python Serialization
- Server-Side Template Injection
- OOB kanallarında code injection senaryoları

SQL Injection Masterclass

- Second-order injection
- Out-of-Band exploitation
- Kriptografi üzerinden SQL Injection
- PowerShell üzerinden OS code execution
- Gelişmiş SQL Injection konuları
- Advanced SQLMap kullanımı ve WAF bypass

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- GraphQL penetration testing

Zorlu File Upload Senaryoları

- Malicious file extensions
- File validation kontrollerini aşma senaryoları
- Hardened web server ortamları
- File metadata üzerinden SQL Injection

Server-Side Request Forgery (SSRF)

- Internal network sorgulama senaryoları
- Template ve extension hedefli SSRF
- SSRF filter bypass teknikleri
- Vaka çalışmaları

Cloud Ortamlarına Yönelik Saldırılar

- SSRF exploitation
- Serverless exploitation
- Cloud döneminde Google Dorking
- Cognito yanlış yapılandırmaları ve data exfiltration
- Cloud-hosted uygulamalarda post-exploitation teknikleri
- Çeşitli vaka analizleri

Hardened CMS Ortamları

- Farklı CMS yapılarını tanımlama ve değerlendirme
- Hardened WordPress, Joomla ve SharePoint ortamları

Web Caching Attacks

- Web cache kaynaklı güvenlik problemleri ve saldırı senaryoları

Diğer Güvenlik Açıkları

- Unicode normalization saldırıları
- Second-order IDOR
- Yanlış yapılandırılmış code control sistemleri
- HTTP Desync saldırıları

Attack Chaining

- Çok katmanlı güvenlik açıklarının zincirlenmesi
- N-tier vulnerability chaining
- RCE ile sonuçlanan çok aşamalı saldırı senaryoları

Vaka Çalışmaları

- Gerçek hayattan çeşitli web güvenliği örnekleri
- Sıra dışı XSS ve CSRF senaryoları

B33r-101

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Eğitim içeriğinde yer alan özel bölüm

Sınav ve Değerlendirme

Bu eğitim programı kapsamında resmi bir sınav bulunmaktadır.

Sınav NotSoSecure tarafından sağlanır ve eğitim ücretine dahildir. Sınav formatı, süresi, soru sayısı ve geçme puanı gibi ayrıntılar değerlendirme öncesinde QA account manager veya eğitmen tarafından katılımcılarla paylaşılır.