WEB APPLICATION HACKING AND SECURITY EĞİTİMİ
5 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

Web Application Hacking and Security Eğitimi, web uygulamalarının güvenlik zafiyetlerini anlama, tespit etme ve bu zafiyetlere karşı koruma stratejilerini öğrenmeyi hedefler. Kapsamlı bir eğitim programıdır. Bu eğitim, katılımcılara web uygulamalarının güvenlik açıklarını keşfetme yetenekleri sağlar. Aynı zamanda web uygulamalarını güvence altına alma ve siber saldırılara karşı savunma becerilerini geliştirir.

Güncel web teknolojilerine ve yaygın web uygulama güvenlik açıklarına odaklanır. Katılımcılar, web uygulamalarının nasıl çalıştığını ve güvenlik açıklarını anlamak için temel web teknolojilerine hakim olurlar. Ayrıca, eğitim katılımcılara yaygın güvenlik açıkları olan enjeksiyon saldırıları, kimlik doğrulama zafiyetleri, veritabanı saldırıları öğrenir. Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) gibi konulara yoğunlaşılarak, bu açıkları tespit etme ve önleme stratejileri öğretilir.

Web Application Hacking and Security Eğitimi aynı zamanda katılımcıları etik hacker (ethical hacker) rolüne hazırlar. Bu eğitim sürecinde, katılımcılar siber güvenlik alanında önemli beceriler kazanır. Katılımcılar sızma testleri gerçekleştirme, zafiyet tarama araçları kullanmayı ve saldırı senaryoları oluşturmayı öğrenirler. Eğitim, katılımcıların web uygulamalarının güvenliğini sağlamak için gerekli bilgi ve becerileri kazanmalarını hedefler.

Sonrasında katılımcılar, web uygulamalarını güvence altına alma konusunu öğrenir. Bu, güvenlik duvarları, oturum yönetimi, yetkilendirme mekanizmaları gibi koruma önlemlerinin nasıl uygulanacağını ve güvenlik açıklarını önlemenin yollarını öğrenmeyi içerir. Katılımcılar, gerçek dünya senaryolarına dayanan örnekler ve proje çalışmaları ile bu becerileri pratik olarak geliştirirler.

Design Patterns in C# eğitimi, katılımcıları hem yazılım geliştirme hem de etik hacker alanında yetkinleştirerek kapsamlı bir beceri seti sunar. Bu sayede, katılımcılar yazılım projelerini daha güvenli ve sürdürülebilir hale getirmeyi öğrenir. Aynı zamanda güvenlik açıklarını tespit etme ve çözme konusunda uzmanlaşabilirler.

Web Application Hacking and Security Eğitimi, web uygulama güvenliği konusunda bilgi ve beceri sahibi olmak isteyen güvenlik profesyonelleri, yazılım geliştiriciler ve sistem yöneticileri için önemli bir kaynaktır. Bu eğitim, katılımcıları web uygulamalarının güvenlik açıklarını anlama, siber saldırıları tespit etme ve koruma stratejileri oluşturma konusunda yetkinleştirir.

Neler Öğreneceksiniz?

Web Application Hacking and Security Eğitimi kapsamında aşağıdaki konuları öğrenme fırsatı bulacaksınız:

- Web Uygulama Güvenliği Temelleri: Web uygulama güvenliği ile ilgili temel kavramları öğreneceksiniz. Web uygulama mimarisi, HTTP protokolü, güvenlik katmanları gibi konular üzerinde durulacaktır.

- Web Uygulama Güvenlik Açıkları: Web uygulamalarının yaygın güvenlik açıklarını öğreneceksiniz. Enjeksiyon saldırıları, kimlik doğrulama zafiyetleri, veritabanı saldırıları, XSS ve CSRF gibi konulara yoğunlaşarak, bu açıkları tespit etme ve önleme stratejilerini öğreneceksiniz.
- Web Uygulama Zafiyet Taramaları: Web uygulamalarında zafiyet taramaları gerçekleştirme becerilerinizi geliştireceksiniz. Zafiyet tarama araçlarını kullanarak web uygulamalarındaki güvenlik açıklarını tespit etme ve raporlama yapma yeteneklerinizi geliştireceksiniz.
- Sızma Testleri: Etik hacker (ethical hacker) rolüne odaklanarak web uygulamalarında sızma testleri gerçekleştirme becerilerinizi geliştireceksiniz. Saldırı senaryoları oluşturma, güvenlik açıklarını istismar etme ve sızma testi raporları hazırlama gibi konulara odaklanacaksınız.
- Web Uygulama Güvenliği Koruma Önlemleri: Web uygulamalarını güvence altına alma konusunda bilgi sahibi olacaksınız. Güvenlik duvarları, oturum yönetimi, yetkilendirme mekanizmaları, geliştirme standartları ve kod inceleme gibi konular üzerinde çalışarak web uygulamalarınızı koruma altına alma yeteneklerinizi geliştireceksiniz.

Web Application Hacking and Security Eğitimi, web uygulama güvenliği konusunda bilgi ve beceri sahibi olmak isteyen güvenlik profesyonelleri, yazılım geliştiriciler ve sistem yöneticileri için önemli bir kaynaktır. Bu eğitim, katılımcıları web uygulamalarının güvenlik açıklarını tespit etme, siber saldırıları önleme ve web uygulama güvenliği konusunda savunma stratejileri oluşturma konusunda yetkinleştirir.

Ön Koşullar

Web Application Hacking and Security Eğitimine katılmadan önce aşağıdaki ön koşulları sağlamanız önerilir:

- Temel Bilgisayar Ağı Bilgisi: Temel ağ kavramlarına ve ağ yapılandırmasına aşina olmanız beklenir. IP adreslemesi, ağ protokolleri, ağ güvenliği önlemleri gibi konularda bilgi sahibi olmanız önemlidir.
- Web Teknolojileri Bilgisi: Web uygulamalarının temel çalışma prensipleri, HTTP protokolü, HTML, CSS, JavaScript gibi web teknolojileri hakkında temel bir anlayışa sahip olmanız beklenir.
- Temel Programlama Bilgisi: Web uygulamalarının arkasındaki programlama konseptlerine aşina olmanız faydalı olacaktır. En az bir programlama dilinde temel düzeyde bilgi sahibi olmanız önerilir.
- Güvenlik Kavramlarına Hakimiyet: Temel güvenlik kavramlarına aşina olmanız beklenir. Şifreleme, yetkilendirme, kimlik doğrulama, zayıf nokta analizi gibi temel güvenlik prensiplerini anlamak önemlidir.
- İşletim Sistemi Bilgisi: Web uygulamalarının yaygın olarak kullanıldığı işletim sistemlerine dair temel bilgiye sahip olmanız beklenir. Özellikle web sunucusu konfigürasyonu ve yönetimi hakkında bilgi sahibi olmanız faydalı olacaktır.

Bu ön koşulları sağlamak, Web Application Hacking and Security Eğitimi'nden daha fazla fayda sağlamanıza yardımcı olacaktır. Eğer bu ön koşullara tam olarak sahip değilseniz, ilgili konuları

önceden araştırarak veya temel eğitimleri alarak hazırlık yapmanız önerilir. Böylece eğitim sürecinde daha iyi anlayış ve deneyim kazanabilirsiniz.

Kimler Katılmalı

Web Application Hacking and Security Eğitimi, aşağıdaki kişiler için uygundur:

- Güvenlik Profesyonelleri: Güvenlik alanında çalışan veya çalışmayı hedefleyen profesyoneller, web uygulama güvenliği konusunda bilgi ve beceri sahibi olmak için bu eğitime katılabilirler. Bu eğitim, güvenlik uzmanlarının web uygulamalarının güvenlik açıklarını tespit etme, düzeltme ve saldırılara karşı savunma becerilerini geliştirir.
- Yazılım Geliştiricileri: Yazılım geliştirme alanında çalışanlar, web uygulamalarının güvenliğini artırmak ve güvenlik açıklarını tespit etme konusunda bilgi ve beceri kazanmak için bu eğitime katılabilirler. Bu eğitim, yazılım geliştiricilerin web uygulama güvenliği konusunda bilinçlenmelerini ve güvenli kodlama tekniklerini öğrenmelerini sağlar.
- Sistem ve Ağ Yöneticileri: Sistem yöneticileri ve ağ yöneticileri, web uygulama güvenliği konusunda bilgi sahibi olmak ve güvenlik önlemlerini uygulama konusunda bu eğitime katılabilirler. Bu eğitim, yöneticilerin web uygulamalarını siber saldırılara karşı koruma, güvenlik açıklarını tespit etme ve savunma stratejileri geliştirme yeteneklerini geliştirir.
- Etik Hackerlar (Ethical Hackers): Etik hackerlar, web uygulama güvenliği konusunda bilgi ve beceri sahibi olmak ve sızma testleri gerçekleştirme yeteneklerini geliştirmek için bu eğitime katılabilirler. Bu eğitim, etik hackerlara web uygulamalarını hedef alan saldırıları tespit etme, zafiyet taraması yapma ve saldırılara karşı savunma stratejileri geliştirme konusunda yetkinlik kazandırır.

Web Application Hacking and Security Eğitimi, web uygulama güvenliği konusunda bilgi ve beceri sahibi olmak isteyen herkes için uygundur. Bu eğitim, web uygulamalarının güvenlik açıklarını tespit etme, saldırılara karşı korunma ve güvenli bir web ortamı oluşturma konularında yetkinlik kazanmanızı sağlar.

Outline

Module 1: Introduction to Web Application Security

- Overview of web application security concepts and challenges
- Common web vulnerabilities and their impact
- Introduction to the ethical hacking approach

Module 2: Web Application Architecture and Technologies

- Understanding web application architecture
- Overview of client-side technologies (HTML, CSS, JavaScript)
- Backend technologies (server-side scripting languages, frameworks, databases)

Module 3: Information Gathering and Footprinting

- Techniques for gathering information about the target web application
- Footprinting, reconnaissance, and enumeration

- Utilizing search engines, social engineering, and public resources

Module 4: Web Application Scanning and Enumeration

- Web vulnerability scanning tools and techniques
- Identifying open ports, services, and vulnerabilities
- Mapping the attack surface and analyzing application functionality

Module 5: Web Application Attacks and Exploitation

- Injection attacks (SQL injection, XSS, command injection)
- Authentication and session attacks
- Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks

Module 6: Web Application Security Testing

- Manual and automated security testing techniques
- Exploiting vulnerabilities to gain unauthorized access
- Analyzing application responses and identifying security flaws

Module 7: Web Application Security Controls and Best Practices

- Secure coding practices and security frameworks
- Implementing secure authentication and access controls
- Web application firewall (WAF) and intrusion prevention systems

Module 8: Web Application Security Reporting and Mitigation

- Documenting vulnerabilities and security findings
- Prioritizing and categorizing identified risks
- Providing recommendations and countermeasures for mitigation

Module 9: Web Application Security in Practice

- Real-world case studies and examples of web application attacks
- Learning from notable security breaches and incidents
- Emerging trends and future challenges in web application security

Module 10: Legal and Ethical Considerations

- Understanding the legal and ethical aspects of web application security testing
- Compliance with laws, regulations, and industry standards
- Ethical hacking guidelines and responsible disclosure practices