WEB UYGULAMA ZAFİYET TARAMASI VE SIZMA EĞİTİMİ

5 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

Web Uygulama Zafiyet Taraması ve Sızma Eğitimi, katılımcılara web uygulamalarındaki olası zafiyetleri bulmayı ve bu zafiyetleri kullanmayı öğretir.

Eğitim genellikle şu konuları ele alır:

- Web Uygulamalarının Yapısı ve İşleyişini Anlama:

Eğitim, katılımcılara web uygulamalarının genel yapısını ve işleyişini anlatır. HTTP protokolü gibi temel konseptler üzerinde durulur.

- Zafiyet Tarama Teknikleri ve Araçlarını Kullanma:

Eğitimde, katılımcılar zafiyet tarama tekniklerini ve popüler tarama araçlarını kullanma becerilerini geliştirirler.

- Sızma Testi Teknikleri ve Araçlarıyla Çalışma:

Katılımcılar, sızma testi teknikleri ve araçları konusunda bilgi ve deneyim kazanırlar. Pratik sızma testleri de yapma fırsatı bulurlar.

- Güvenlik Açığı ve Saldırı Türlerini Tanıma:

Eğitim, XSS, SQL Injection, CSRF gibi çeşitli güvenlik açıkları ve saldırı türlerini tanıtır.

- Zafiyetleri Giderme ve Önleme Stratejileri Uygulama:

Katılımcılar, tespit ettikleri zafiyetleri nasıl giderirler ve gelecekteki zafiyetleri nasıl önlerler, bu konularda bilgi ve deneyim kazanırlar.

Bu eğitimin ardından, katılımcılar, web uygulamalarında detaylı zafiyet taraması gerçekleştirmenin yanı sıra, etkin ve etkileyici sızma testleri yapma becerisine de sahip olacaklar. Her iki beceri de, bir organizasyonun siber güvenliğini sağlama ve olası sızıntıları önleme açısından kritik öneme sahiptir.

Daha sonra, tespit edilen zafiyetleri nasıl giderileceğini öğrenmek de bu eğitimin önemli bir parçasıdır. Katılımcılar, bir zafiyetin ortadan kaldırılması için gereken adımları atmayı öğrenirler. Bunun yanı sıra, tespit edilen zafiyetleri nasıl raporlayacaklarını ve bu raporları nasıl kullanacaklarını da öğrenirler. Bu beceri, siber güvenlik olaylarına hızlı ve etkili bir şekilde yanıt vermek için önemlidir.

İleri seviye eğitimler ise, bu temel becerileri daha derin ve teknik bilgi ile zenginleştirir. Bu eğitimler, belirli araçların veya tekniklerin kullanımına daha çok odaklanır. Örneğin, bir ileri seviye eğitim, belirli bir sızma testi aracının veya zafiyet tarama aracının daha detaylı kullanımını öğretebilir. Bu tür eğitimler, katılımcıların belirli bir teknoloji veya teknik üzerinde uzmanlaşmasına yardımcı olur ve onlara, siber güvenlik alanındaki kariyerlerinde daha fazla uzmanlık ve beceri kazandırır.

Neler Öğreneceksiniz?

Web uygulama zafiyet tarama ve sızma eğitimi sürecinde, şunları öğrenebilirsiniz:

- Web uygulama güvenliği hakkında temel bilgi: Web uygulamalarının nasıl sızdırılabileceği, güvenlik açıklarının neler olabileceği, güvenlik ihlallerinin nasıl önlenebileceği gibi konular.
- Zafiyet tarama teknikleri: Web uygulamalarındaki güvenlik açıklarını tespit etmek için kullanılan zafiyet tarama araçları, metodolojiler ve teknikler.
- Sızma testleri: Web uygulamalarının güvenliğini test etmek için yapılan sızma testlerinin nasıl yapılacağı ve sonuçlarının nasıl yorumlanacağı.
- Güvenli kodlama pratikleri: Güvenli bir web uygulaması geliştirmek için gerekli olan kodlama pratikleri ve uygulamalar.
- Güvenlik politikaları ve yönetimi: Web uygulama güvenliğini koruma amacıyla oluşturulan politikalar, prosedürler ve yönetim uygulamaları.
- Güncel güvenlik tehditleri ve trendleri: Web uygulama güvenliği alanında meydana gelen son gelişmeler ve gelecekte beklenen tehditler.

Bu eğitim sürecinde, teorik bilgi ve uygulamalı çalışmalar yaparak, web uygulama güvenliği hakkında daha derin bir anlayış kazanabileceksiniz.

Ön Koşullar

Web uygulama zafiyet tarama ve sızma eğitimi sürecine katılmak için şu ön koşulların olması beklenir:

- Bilgisayar bilimi veya benzer bir alanda eğitim almış olmak: Web uygulama güvenliği konularını anlamak için programlama dilleri ve bilgisayar sistemlerinin temel işleyişi hakkında bilgiye ihtiyaç duyulur.
- Programlama dilleri: HTML, JavaScript, PHP gibi programlama dillerinde temel düzeyde bilgi sahibi olmak.
- İnternet ve ağ teknolojileri hakkında temel bilgi: HTTP protokolü, IP adresleri, tarama teknikleri gibi konular hakkında temel bilgiye sahip olmak.
- Ağ ve güvenlik hakkında temel bilgi: Firewall, VPN, şifreleme gibi konular hakkında temel bilgiye sahip olmak.

Bu ön koşullar, eğitimi daha verimli hale getirmek ve eğitim sürecinde daha rahat ilerlemek için gereklidir. Ancak, bu ön koşulları tamamlamamış olsanız dahi, eğitim almak isteyen herkesin katılabileceği ve öğrenebileceği bir alandır. Eğitmen, gerektiğinde temel bilgileri vermeye ve yardımcı olmaya hazırdır.

Kimler Katılmalı

Web uygulama zafiyet tarama ve sızma eğitimi, aşağıdaki kişiler için faydalı olabilir:

- Web Uygulama Geliştiricileri: Web uygulamalarını geliştiren kişiler, güvenliği düşünerek nasıl geliştirebileceklerini öğrenmek isteyebilirler.
- Güvenlik Uzmanları: Güvenlik uzmanları, web uygulamalarının zafiyet tarama ve sızma testleri yapmak için gerekli olan teknikleri öğrenmek isteyebilirler.
- İT Yöneticileri: İT yöneticileri, web uygulamalarının güvenliğini garanti altına almak için gerekli olan teknikleri ve yönetim pratiklerini öğrenmek isteyebilirler.
- Hacker'lar ve Sızma Testçileri: Hacker'lar ve sızma testçileri, web uygulamalarının güvenliğini test etmek için gerekli olan teknikleri ve metodolojileri öğrenmek isteyebilirler.
- Bilişim ve İT Okuryazarlığı Arayan Kişiler: Bilişim ve İT sektörüne ilgi duyan ve web uygulama güvenliği hakkında daha fazla bilgi edinmek isteyen herkes bu eğitimi alabilir.

Bu eğitim, web uygulama güvenliği konularına ilgi duyan herkes katılabilir. Katılımcıların ön koşulları ve seviyeleri farklı olabilir, ancak eğitmen her seviyedeki katılımcıya uygun bir şekilde eğitim vermeyi amaçlar