**T.C.**

**SAKARYA ÜNİVERSİTESİ**

**BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ**

BSM 498 BİTİRME ÇALIŞMASI

**WEB SECURİTY PENTEST TOOL**

**UYGULAMASI**

**RAPOR-2**

**B181210030 – VEDAT ARSLAN**

**Fakülte Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ**

**Tez Danışmanı : Prof.(Doç.) Dr. İbrahim Özçelik**

**2023-2024 Bahar Dönemi**

BÖLÜM 2.

KULLANILMAK İSTENEN TEKNOLOJİ VE ORTAMLAR

|  |  |
| --- | --- |
| 2.1. Python…………………………………………………………………… | 2 |
| 2.2. Python Modüller ve Kütüphaneler………………………………………. | 2 |
| 2.2.1 Python Modül Nedir?............................................................................. | 2 |
| 2.2.2 Python Kütüphane Nedir?............................................................... | 2 |
| 2.3. PyQt5 Designer………………………………………………………….. | 3 |
| 2.3.1 PyQt5 Nedir?.................................................................................... | 3 |
| 2.3.2 GUI Geliştirme için PyQt5 Kullanmanın Faydaları……………… | 3 |
| 2.4. Pycharm Community Edition…………………………………………… | 3 |
| 2.5. Damn Vulnerable Web Application (DVWA)…………………………... | 4 |
| 2.6. Nessus…………………………………………………………………… | 5 |
| 2.6.1 Nessus Nedir?................................................................................... | 5 |
| 2.6.2 Nessus’a Ait Bazı Temel Özellikler………………………………. | 6 |
| 2.6.3 Nessus Mimarisi…………………………………………………... | 6 |
| 2.6.4 Neden Nessus?.................................................................................. | 6 |

**BOLÜM 2. KULLANILAN İSTENEN TEKNOLOJİ VE ORTAMLAR.**

**2.1. Python**

Python, sahip olduğu geniş kütüphane sayesinde oldukça popüler hale gelmiş ve kullanım alanlarını da oldukça fazla olması yaygın bir kullanıcı kitlesine ulaşmasını sağlamıştır. Açık kaynaklıdır. Ücretsiz ve sade olması sayesinde diğer programlara göre çok basittir. Kolayca zaman kaybı olmadan hızlıca öğrenilebilir. Ayrı bir derleyiciye ihtiyaç duymaz. Python’da derleme işlemi ortadan kaldırıldığı için hızlı bir şekilde program geliştirilebilir. Daha düzenli bir kod dizilimine sahiptir. Ayrıca basit ve temiz syntaxa (söz dizimi) sahip olması birçok açıdan avantaj sağlamaktadır.

Python’un standart kütüphaneleri birçok Internet protokolünü destekler. Python, uzun süredir kullanılıyor olmasının da avantajı ile geniş bir kullanıcı ağına sahiptir. Bireysel programlamada bilgiye ve gerekli dokümanlara ulaşım kolay olarak gerçekleştirilir.

Desteklediği Platformlar: Unix, Linux, Mac, Windows, vs.

**2.2 Python Modüller ve Kütüphaneler**

**2.2.1. Python Modül Nedir?**

Python uygulamalarında bir takım işlevi yerine getirebilmemizi sağlayan, fonksiyonları ve nitelikleri içinde barındıran araçlara modül denir.

Modüller sayesinde, bir kez yazdığımız kodları pek çok farklı program içinde kullanma imkânı ederiz. Bu imkân bize: Daha az kod yazma, Bir kez yazıp, her yerde çalıştırmamızı ve Daha düzenli, toplu bir şekilde çalışmamızı sağlar.

**2.2.2. Python Kütüphanesi Nedir?**

**Python** kütüphaneleri dediğimiz şey farklı fonksiyonları gerçekleştirebilen, yazılım geliştirme amaçlı kullanılan kaynaklarıdır. Python fazla sayıda kütüphaneye sahip çok fonksiyonlu bir yazılım dilidir. Her biri oldukça yetenekli olan bu kütüphaneleri kullanmak istediğinizde gerekli kodla çağrılarak işlem yapabilirsiniz. Biren fazla kütüphaneyi aynı anda çağırıp kullanmak da mümkündür.

**2.3 PyQt5 Designer**

**2.3.1. PyQt5 Nedir?**

PyQt5, Qt kitaplıkları için Python bağlamaları kümesidir. Python kullanarak GUI uygulamaları yazmanıza olanak tanır ve güzel kullanıcı arayüzleri oluşturmak için kapsamlı widget ve araç seti sağlar. PyQt5, uygulamaları yazmak, tasarlamak ve hata ayıklamak için Qt Creator IDE'yi kullanır ve sürükle ve bırak arayüzü ile karmaşık uygulamalar geliştirmeyi kolaylaştırır.

**2.3.2.GUI Geliştirme için PyQt5 Kullanmanın Faydaları**

GUI geliştirme için PyQt5'i kullanmanın çapraz platform uyumluluğu, kullanımı kolay ve geniş kullanıcı topluluğu dahil olmak üzere çeşitli avantajları vardır. PyQt5 ile Windows, Linux ve MacOS üzerinde çalışan uygulamalar geliştirerek uygulamalarınızın çeşitli kitleler tarafından erişilebilir olmasını sağlayabilirsiniz. Ayrıca PyQt5'in yeni başlayanlar için bile öğrenilmesi kolaydır, bu da onu GUI geliştirmeye yeni başlayanlar için mükemmel bir seçim haline getirir.

**2.4 Pycharm Community Edition**

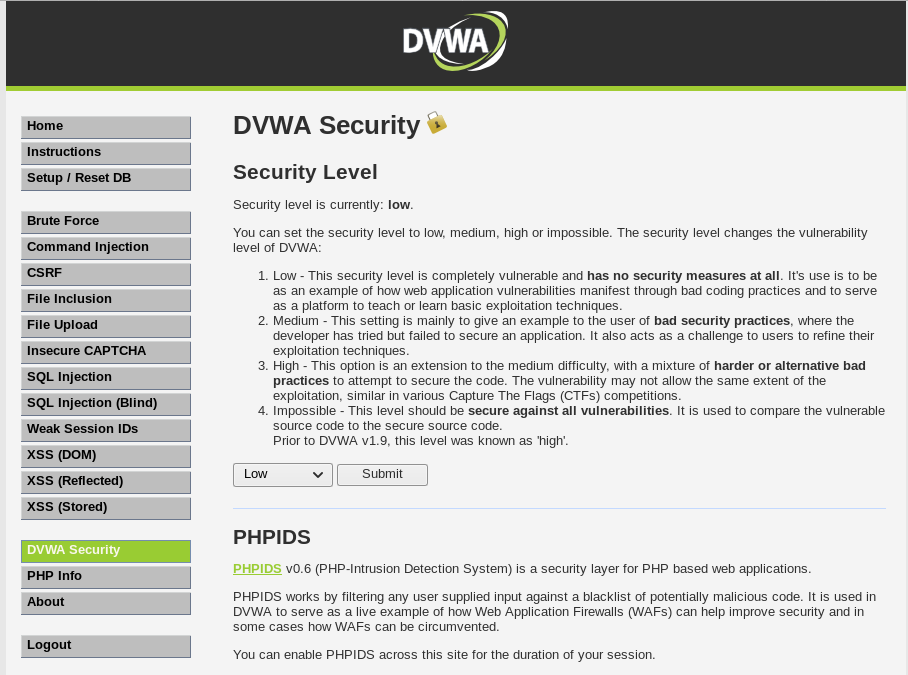
PyCharm Community Edition, Python programcılarına yönelik bir IDE olan PyCharm'ın ücretsiz sürümüdür. PyCharm, geliştiricilerin daha hızlı kod yazmasını, test etmesini, hata ayıklamasını ve dağıtmasını sağlar. Kod tamamlama, refactoring desteği, kod denetimi, sürüm kontrolü, paket yönetimi ve daha fazlası gibi özellikler programcıların daha kısa sürede daha iyi Python kodu yazmasını sağlar. Topluluk sürümü, belirli çerçeveler ve web geliştirme araçları ile entegrasyonu içermez, ancak profesyonel sürüm ise ücretsiz değildir.

**2.5 Damn Vulnerable Web Application (DVWA)**

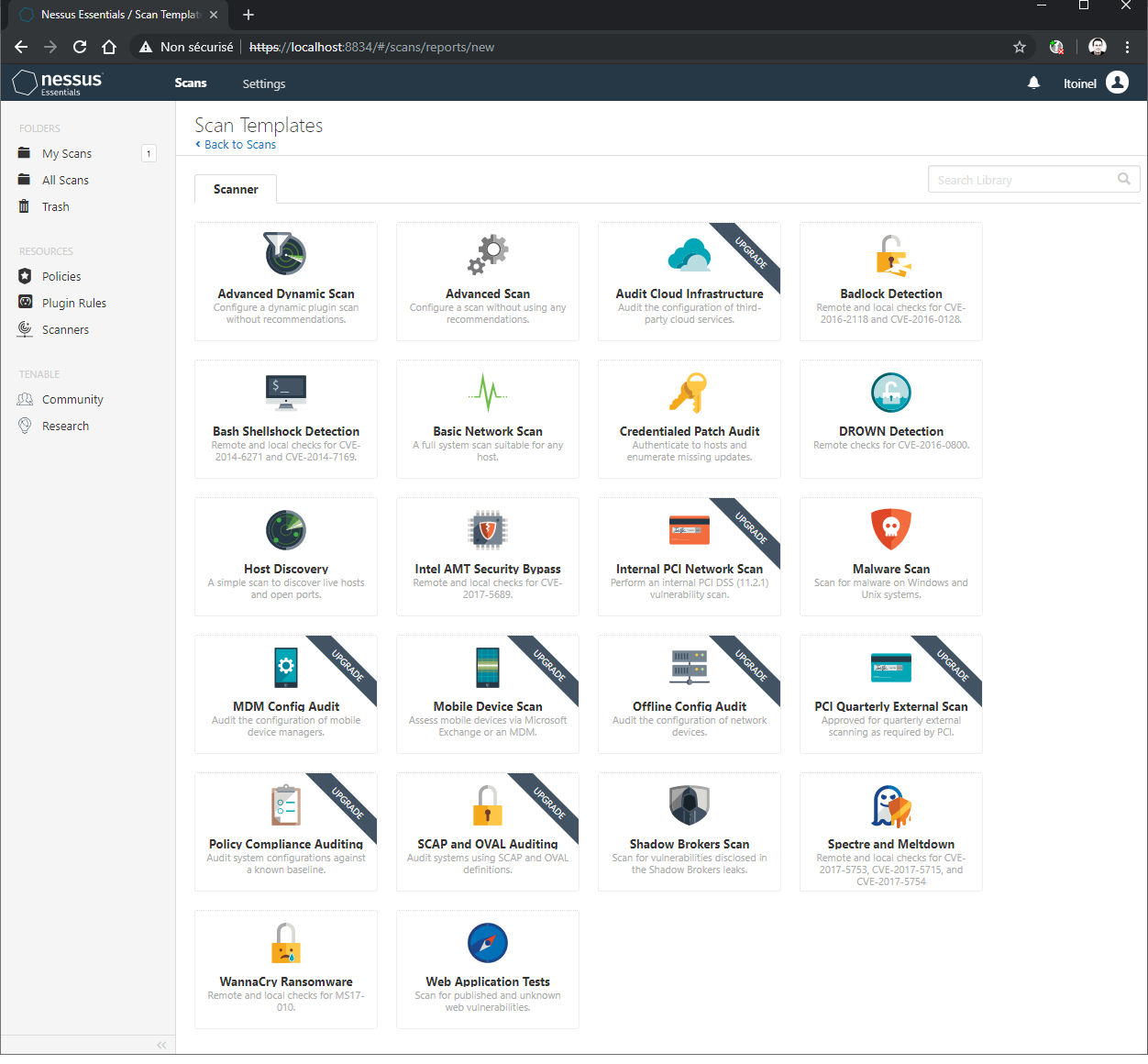
Web uygulama güvenliği alanında kendini geliştirmek isteyen pentesterlar, güvenlik ile uğraşan ya da bu konuda meraklı kimseler için PHP ile oluşturulmuş içinde belli web zafiyetlerini barındıran bir eğitim sistemidir.

Ayrıca bu sistem üzerinde 3 farklı zorluk seviyesi bulunmaktadır. Bunlar Low, medium ve high şeklindedir.

DVWA uygulamasını Windows işletim sisteminde çalıştırabilmek için XAMPP adli bir yazılımı makinemize kurmamız gerekmektedir. XAMPP bilgisayarımızda PHP ile yazılmış web uygulamalarını çalıştırabileceğimiz bir platformdur.



**2.6 Nessus**

****

**2.6.1. Nessus Nedir?**

Nessus, 2 milyondan fazla kullanıcısı olan, dünyanın en çok kullanılan güvenlik açığı tarama programıdır. Nessus ile fiziksel, sanal ve bulut ortamlarında güvenlik zafiyetlerinin tespiti, değerlendirilmesi ve kötü amaçlı yazılımların hızlı ve doğru bir şekilde tespiti için kullanılır. Ayrıca, bilişim altyapılarının güvenlik açısından denetlenmesi ve güvenlik seviyelerinin tespit edilerek açıklıklarının kapatılması gibi çalışmaları kapsayan penetrasyon/sızma testi hizmeti kurumların gerçekleşecek siber saldırılara karşı hazırlıklı ve dayanıklı olmalarını sağlar. Nessus, sizin belirttiğiniz ağlar arası ve web uygulamaları arasında ağları tarayıp bulabildiği açıkları bize raporlayan bir penetration test uygulamasıdır. Örnek olarak kendi şirket ağınızı içerden ve dışardan tarayarak firewall’unuzda, açık portlarınızda vs. olan açıkları yakalayıp onları düzeltmenize olanak sağlar. Cihazlarda hangi işletim sisteminin çalıştığını, hangi servislerin hangi portlar üzerinde çalıştığını, işletim sistemi ve servislere ait açıklıklar, yazılım bileşenleri ve ağ protokollerinin sahip olduğu zafiyetler ve uyumluluk gereksinimlerinin ne durumda olduğu gibi kriterlere göre hedef cihazların sahip oldukları açıklıklarla ilgili geniş kapsamlı raporlama sunar.

**2.6.2. Nessus’a Ait Bazı Temel Özellikler**

* Geniş ve kapsamlı bir tarama sağlar.
* Saldırıları sınıflandırma özelliği ile ölçeklendirilebilir bir yapı sunar.
* Düşük maliyet sunar.
* Her geçen gün gelişen saldırı teknik ve taktiklere karşı güncel çözümler ve tarama teknikleri sunmaktadır.
* Çoklu tarayıcı yönetimi ve zafiyet analizi sağlar.

**2.6.3. Nessus Mimarisi**

Nesus bir İstemci-Sunucu (Client-Server) modeline dayanır. Nessus istemcileri, başlatılmasına izin verilmeden önce sunucuya kimlik doğrulanması yapılmalıdır. Bu mimari, Nessus kurulumları yönetmeyi kolaylaştırır.

**2.6.4. Neden Nessus?**

* Bugün 20.000 ’den fazla kuruluş Nessus Professional’ı kullanmakta ve dünya çapında 1,5 milyondan fazla kullanıcısı bulunmaktadır.
* Yüksek hızlı hassas tarama ve düşük false-positives.
* Düşük maliyetli güvenlik açığı taraması.
* Rekabetçi çözümlerden daha fazla teknoloji ve daha fazla güvenlik açığının kapsamı için destek.
* IP adresi taramaları için sınırsız yetkilendirme.
* Metasploit, Core Impact, Canvas, ExploitHub gibi popüler test araçlarıyla tarama verilerini ilişkilendirebilme.
* Kolay kurulumu ve bakım kolaylığı
* Yüzbinlerce sistem ölçeklenebilirliği