Hackviser Ödevi

---ISINMALAR---

1-Arrow(uzaktan bilgisayar erişimi)

İlk olarak hedef makinanın açık portlarını bulmak için nmap taraması yapıyoruz ve 23 portunda telnet çalıştığını ve açık olduğunu görüyoruz telnet ip komutu ile bağlantı gerçekleştiriyoruz kullanıcı adı ve şifrenin root olduğu ipucu olarak verilmişti. Giriş yaptıktan sonra bulunduğumuz dizini görmek için pwd komutunu çalıştırıyoruz.

2-File Hunter

İlk olarak nmap taraması yapıyoruz ve 21 portunda ftp servisinin çalıştığını görüyoruz .Bağlanmayı denemek için ftp {ip adresi} komutu ile bağlanmayı deniyoruz. Giriş yaptığımızda gelen Anonymous ismi ile giriş yapıyoruz. Görev 4 de istendiği üzere help komutu ile çalıştırabileceğimiz komutları görüntüledikten sonra ls komutu ile dosyaları görüntülüyoruz. Userlist adlı dosyayı indirip içini açarak okuma işlemini gerçekleştiriyoruz.

3-Secure Command(uzaktan bilgisayar erişimi)

Port taraması yapıyoruz ve 22 portunda ssh servisinin çalıştığını görüyoruz. Görev 3 de verilen bilgiler ile ssh servisine bağlanıyoruz. Bağlandıktan sonra yetki yükseltme yapmamız gerekiyor root kullanıcısının parolası da root olarak bırakılmış roota geçiyoruz.

4-Query Gate (sql injection)

MySQL sunucusuna bağlanarak hedef veritabanı üzerinde bilgi toplama görevlerini yerine getirdim. root kullanıcısı ile sunucuya bağlanarak MySQL komut satırına erişim sağladım. Bu süreçte, veritabanına parola olmadan bağlanabilmemin, hedef sunucuda bir yapılandırma hatası olduğunu fark ettim. Veritabanlarına bağlanıp tablo ve veri sorgulamaları yaparak başarılı sonuçlar elde ettim. Özellikle, SHOW DATABASES ve USE komutlarını kullanarak belirli bir veritabanı üzerinde çalışmayı öğrendim.Sonuç olarak, hedef veritabanında yer alan tabloları keşfettim ve bu tablolardan birinde yer alan verilerle beyaz şapkalı hacker'ın bilgilerine ulaşmayı başardım.

5- Discover Lernaean(uzaktan komut çalıştırma)

İlk olarak, hedef makine üzerinde bir port taraması yapmak için **nmap** aracını kullandım ve 22 numaralı portta **SSH** servisinin, 80 numaralı portta ise **Apache HTTP** sunucusunun çalıştığını tespit ettim. Tarayıcı üzerinden 80 portunu ziyaret ettiğimde Apache'nin varsayılan sayfasını görüntüledim.Daha sonra, **dirbuster** ve **gobuster** gibi araçlar kullanarak dizin taraması yaptım. Bu tarama sonucunda **/filemanager** dizinini keşfettim. Tarayıcı ile bu dizine girdiğimde beni "Tiny File Manager" sayfası karşıladı. Görevde istenildiği gibi kullanıcı adı ve parola bulmak için araştırma yaptım ve varsayılan giriş bilgilerini denemeye karar verdim. **user:12345** bilgileri ile başarılı bir şekilde giriş yaptım ve hedef bilgisayarın dosya sistemine erişim sağladım.Sonrasında, sistemdeki kullanıcıları görmek için **/etc/passwd** dosyasını inceledim ve en son eklenen kullanıcının **rock** olduğunu öğrendim. 22 numaralı portta **SSH** servisi çalıştığını bildiğim için, rock kullanıcısı ile SSH bağlantısı yapmayı denedim. Ancak parola gerektiği için **hydra** aracı ile SSH brute-force saldırısı yaparak rock kullanıcısının parolasını buldum.

SSH ile rock kullanıcısı olarak hedef makineye bağlandıktan sonra, kullanıcının daha önce çalıştırdığı komutları görmek için **.bash_history** dosyasını okudum ve ilk çalıştırdığı komutu başarılı bir şekilde buldum.

6-Bee(File Upload)

İlk olarak, hedef makine üzerinde bir port taraması gerçekleştirdim ve 80 numaralı portta bir HTTP sunucusunun çalıştığını tespit ettim. Tarayıcıdan bu sunucuya eriştiğimde basit bir web sitesi ile karşılaştım. Sayfayı inceledikten sonra giriş ekranını fark ettim, ancak site DNS çözümleme hatası veriyordu. Bu sorunu çözmek için **/etc/hosts** dosyasına DNS kaydı ekledim ve siteye başarılı bir şekilde eriştim.Giriş ekranında bir SQL Injection zafiyeti olabileceğini düşündüm ve bunu test etmek için bazı SQL payload'ları denedim. İlk denemelerimde

"Email or password incorrect" hatası aldım. Fakat e-posta alanındaki HTML özelliklerini değiştirerek istediğim SQL kodunu girebildim. Bu sayede SQL Injection zafiyetini tespit ettim ve login panelini bypass ederek admin paneline giriş yapmayı başardım. Kullanılan SQL Injection payload'u sayesinde login kontrolünü atlatabildim.Admin panelini inceledikten sonra bir dosya yükleme alanı keşfettim. Dosya yükleme alanında bir zafiyet olup olmadığını anlamak için önce test amaçlı bir **.txt** dosyası yüklemeyi denedim ve başarılı oldum. Bu durum, dosya yükleme zafiyetini doğruladı. Ardından, bir **PHP web shell** hazırlayarak sunucuya yükledim ve web shell aracılığıyla sunucuda komut çalıştırma yetkisi kazandım. İlk olarak **whoami** komutunu çalıştırarak sunucuya erişimimi doğruladım.Sonrasında, MySQL parolasını bulmak için başka bir web shell hazırladım ve **db_connect.php** dosyasını inceledim. Bu dosyanın kaynak kodunu görüntüleyerek veritabanı bağlantı bilgilerine ulaşmayı başardım ve görevde istenen bilgilere eriştim.Sonuç olarak, SQL Injection ve dosya yükleme zafiyetlerinden faydalanarak hedef makinede tam erişim sağlayarak tüm görevleri başarıyla tamamladım.

7-Leaf(Server-Side Template Injection)

İlk olarak nmap taraması yapıyoruz ve açık olan portlardan bir web uygulamasının ve bir MySQL sunucusunun çalıştığını görüyoruz. Tarayıcıda açarak websitenin başlığının “Modish Tech” olduğunu öğreniyoruz. Ürünlerin detay sayfasında id isimli bir GET parametresi kullanıldığını fark ediyoruz. SSTI (Server Side Template Injection) zafiyetinin varlığını kontrol etmek için {{7*7}} payloadını deniyoruz ve sonuç olarak ekranda 49 çıktısını görüyoruz.Bu sonuç bize, hedef makinede Jinja2 veya Twig template motorlarından birinin çalıştığını gösteriyor. Daha detaylı testler sonucunda Twig template motoru olduğunu tespit ediyoruz. Makineye sızmak için Twig payloadlarını kullanarak shell alıyoruz. Komut çalıştırmak için Netcat ile bir port açarak {{['nc -nvlp 1337 -e /bin/bash']|filter('system')}} payloadını çalıştırıyoruz ve shell erişimi sağlıyoruz. Ardından hedef makinede gerekli bilgileri elde ediyoruz.

8-Venomous(Local File Inclusion)

İlk adımda nmap taraması yaparak 80 portunun açık olduğunu ve bir HTTP sunucusunun çalıştığını görüyoruz. Web sunucusunun Nginx olduğunu -sV parametresiyle öğreniyoruz. Websitesine göz attığımızda, fatura görüntülemek için kullanılan bir GET parametresi olduğunu fark ediyoruz. Bu parametreyi kullanarak LFI (Local File Inclusion) zafiyetini tespit ediyoruz ve /etc/passwd dosyasına erişiyoruz.Log poisoning ile sunucu üzerinde komut çalıştırmayı hedefliyoruz. Nginx erişim loglarına zararlı kod enjekte ediyoruz ve Netcat aracılığıyla reverse shell alıyoruz. Hedef makineye sızmayı başardıktan sonra gerekli dosya bilgilerine ulaşarak görevleri tamamlıyoruz.

Web Uygulama Güvenliği Laboratuvarları

---XSS—

1-Reflected XSS

Ekranda çıkan alana <img src onerror=alert()> payloadını yazdım

2-Stored XSS

Verilen bilgiler ile giriş yapıp mesaj kutusuna <img src onerror=alert()> payloadını yapıştırdım

3-Dom Based XSS

Verilen bilgiler url den gönderildiği için url kısmına alert('XSS Vulnerability'); payloadı yerleştiriyoruz

---SQL Injection---

1-Basic SQL Injection

admin' or 1 -- - payloadını kullanıcı adı kısmına girerek giriş yaptım

2-Union-Based SQL Injection

' UNION SELECT 1,2,3,4 -- - payloadını girdim ve sonuç döndürdü sonra ' UNION SELECT 1,2,3,database() -- - yazarak veritabanı adını aldım(ecliptica_cars)

----Unrestricted File Upload---

1-Basic Unrestricted File Upload

Shell.php osyamı yükledim cd … komutu ile üst dizine çıktım sonrasında cat ile dosya içeriğini okudum

2-MIME Type Filter Bypass

---Insecure Direct Object References (IDOR)---

1-Invoices

url deki adres 1003 yaptım ve bilgilere eriştim

2-Ticket Sales

Bilet adedi girdikten sonra burp ile isteği yakalayıp bilet fiyatını 1 birim yapıyorum

3-Change Password

Test kullanıcısına giriş yaptım şifre değiştirirken burp ile yakalayıp userid yi 1 yaparak admin kullanıcısının şifresini değiştirdim

---Command Injection---

1-Basic Command Injection

Girdi yerine asd | hostname komutu ile buldum

2-Command Injection Filter Bypass

Blacklistte olmayan bir komut bulamadım

---File Inclusion---

1-Basic Local File Inclusion

Url kısmındaki page=/etc/passwd yazıyoruz ve getiriyor

2-Local File Inclusion Filter Bypass

Yapamadım

3-Basic Remote File Inclusion

Hacker box ile php dosyasını yazdım ve php dosyasını internete açtım url kısmından yönlendirdim ve hostname : hackerbox olarak çıktı aldım ama cevp dopru değil anlamadım

---XML External Entity Injection (XXE)---

Yapamadım 😟

----Cross Site Request Forgery (CSRF) ----

1-Change Password

Şifre değiştirme işlemini url den yapıyor şifreyi 123 yaptım url deki linki desteğe atarak onun da şifresini değiştirmesini sağladım

2-Money Transfer

https://awaited-bulleteer.europe1.hackviser.space/index.php?transfer_amount=10&receiver=user
url de gönderirken bu parametreler ile gönderiyor burp suit ile yakalayıp yukarıdaki linki oluşturup yolladım ve para geldi

---Broken Authentication---

1-Dictionary Attack

Intruder ile şifreyi denedim girdi fakat şifrenin ne olduğunu bulamadı turbo intruder ile denedim yine girdi admin kullanıcısına ama olumlu sonuç dönmedi

2-Execution After Redirect (EAR)

Yapamadım .