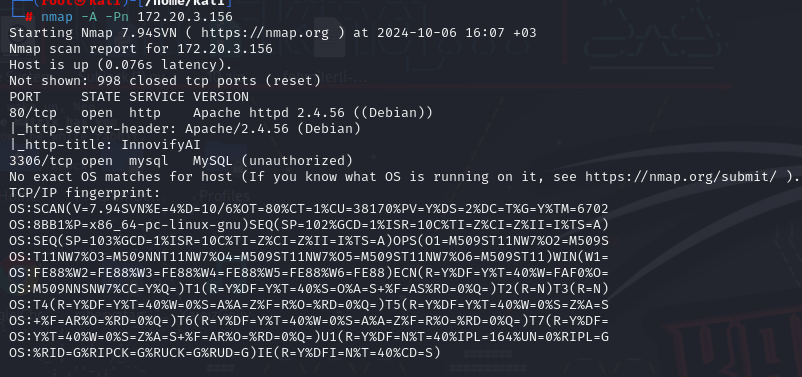
**BEE WRİTE-UP**

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

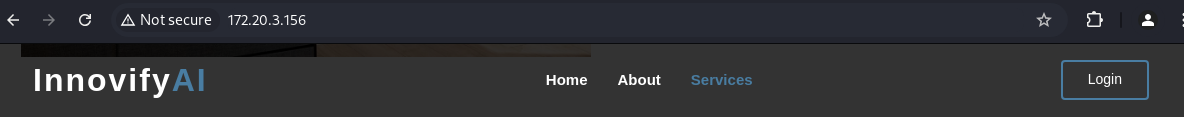
**SORU 1:** Hangi port(lar) açıktır?

Nmap taraması yaparak bu sorunun cevabını bulmaya çalışacağım.

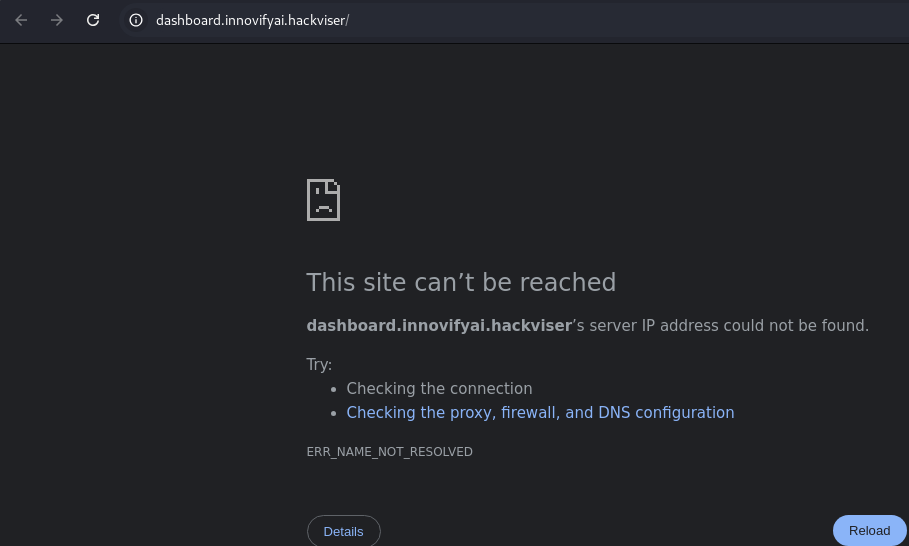


**80**(http) ve **3306**(mysql) portlarının açık olduğunu bulduk.

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

****

Siteyi incelerken login sayfası görüyorum. Gitmek istediğimde gidemiyorum.

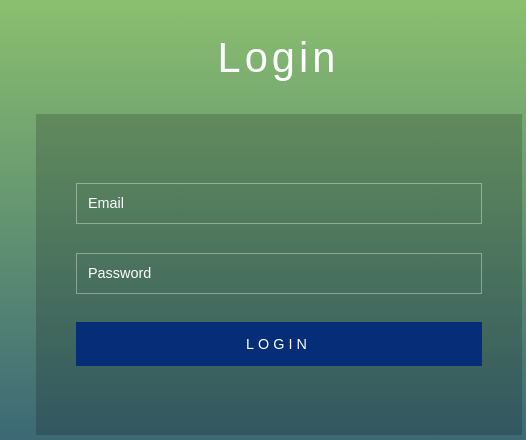


Burada url kısmını hosts dosyamıza eklememiz gerekiyor sayfanın çalışması için.

**http://dashboard.innovifyai.hackviser/**

/etc/hosts dosyamıza şu şekilde kaydediyoruz.



 Ve sayfaya eriştrik.

**SORU 3:** Hangi zafiyet ile login panelini bypass ettiniz?

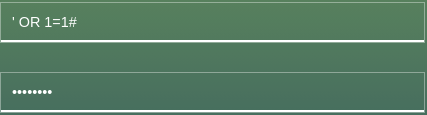
Login sayfalarında aklıma ilk gelen SQL Injection oluyor. Zaten 3306 portunda da açık vardı. Deneme yapıyorum. Benden sürekli e posta girmemi istiyor. Payload deneyemiyorum. Sayfayı incele kısmından email type kısmını text olarak değiştirip deneyeceğim.





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.

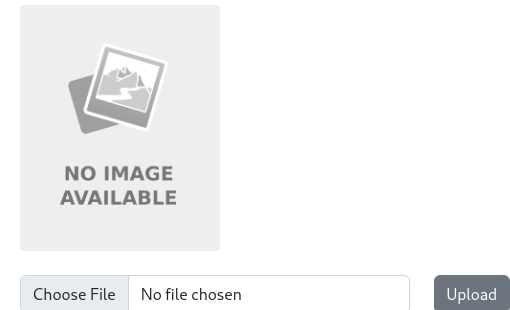
Şimdi ayarlar kısmına gidiyoruz.



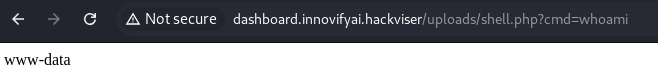
Cevap: **settings.php**

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

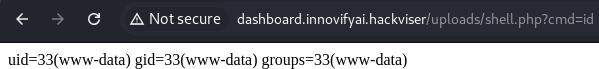
Bu soruyu çözmek için file upload açığını kullanacağız. Ayarlar kısmında fotoğraf yükleme kısmı var.

 Buraya yükleyeceğimiz kötü amaçlı kod ile soruyu çözebiliriz.

 Kodunu barındıran Shell.php dosyasını yüklüyorum.

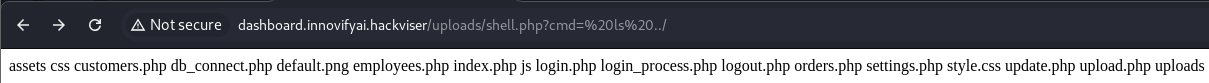


Burada Shell dosyamızın başarılı ile yüklenip çalıştığını görüyoruz.



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

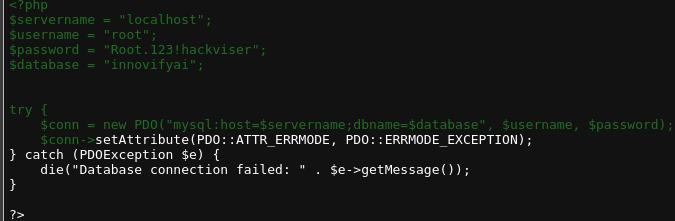
**SORU 6:** MySQL parolası nedir?

****

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.

 Burada istediğimiz şifreyi elde ettik.

Cevap: **Root.123!hackviser**