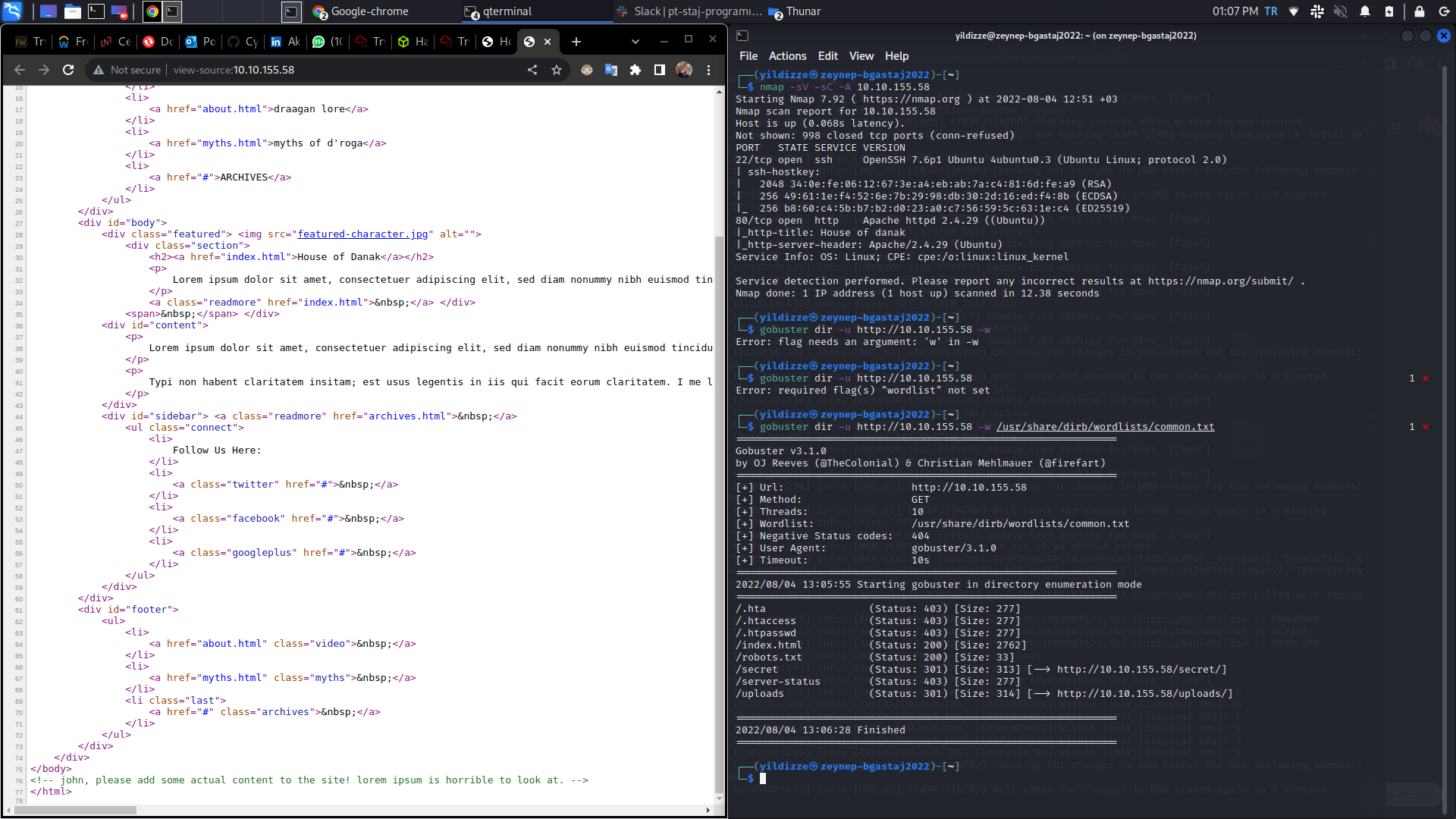
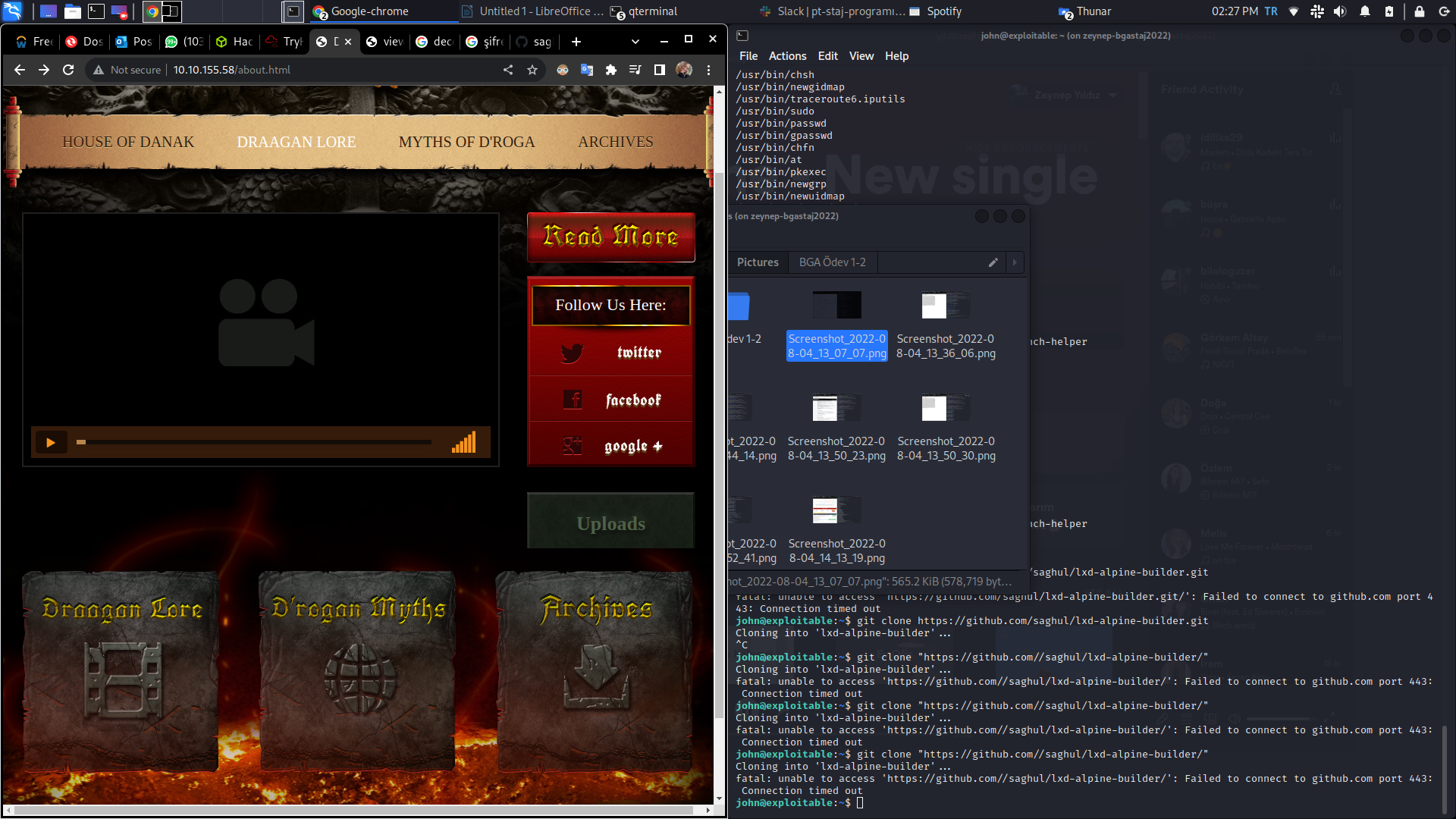
THM GAMING SERVER WRİTEUP

Öncelikle siteye girerek siteyi biraz kurcalıyoruz.

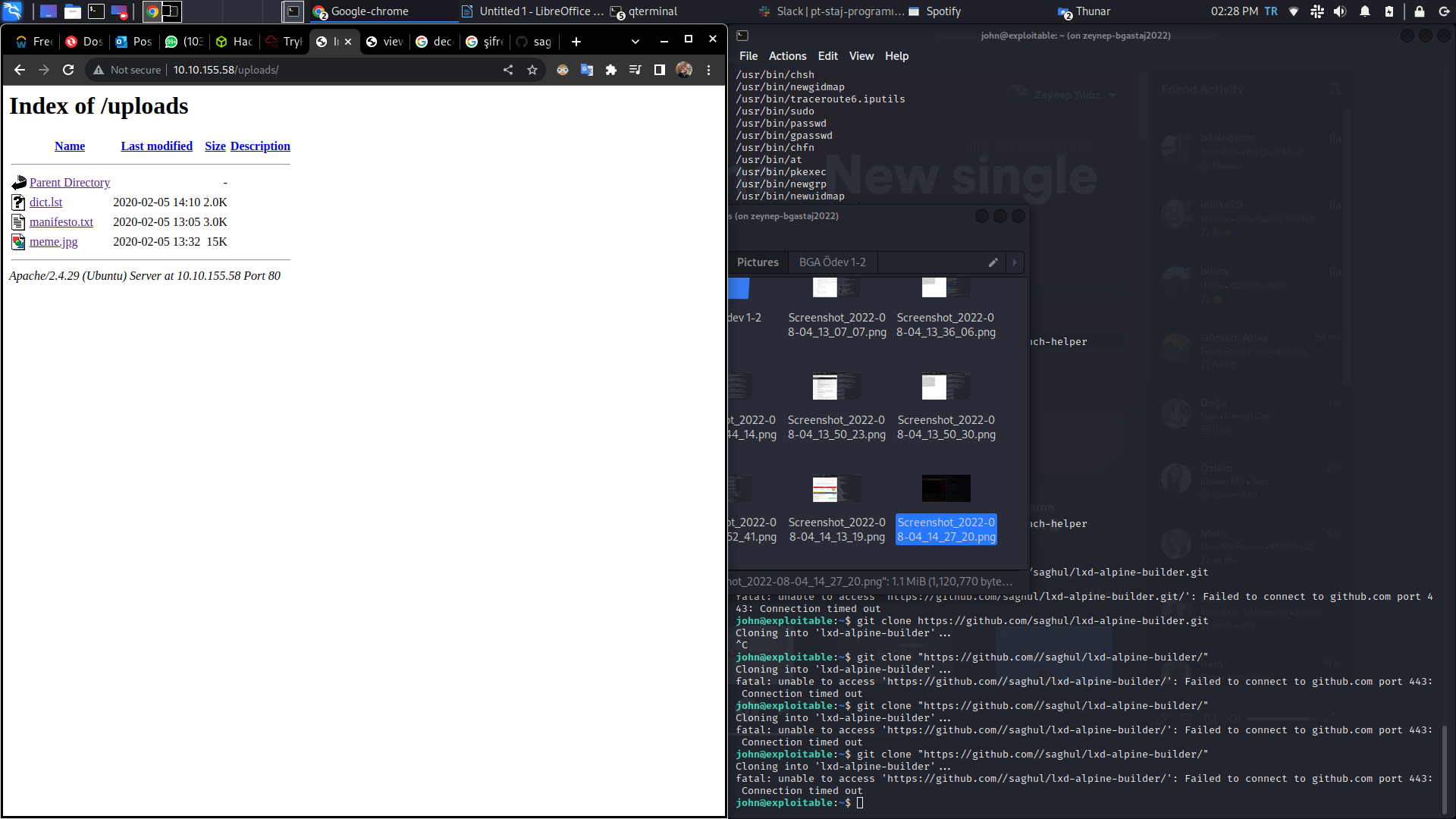
Sourch koduna baktiğimizda “John” diye bir isimle karşılaşıyoruz.



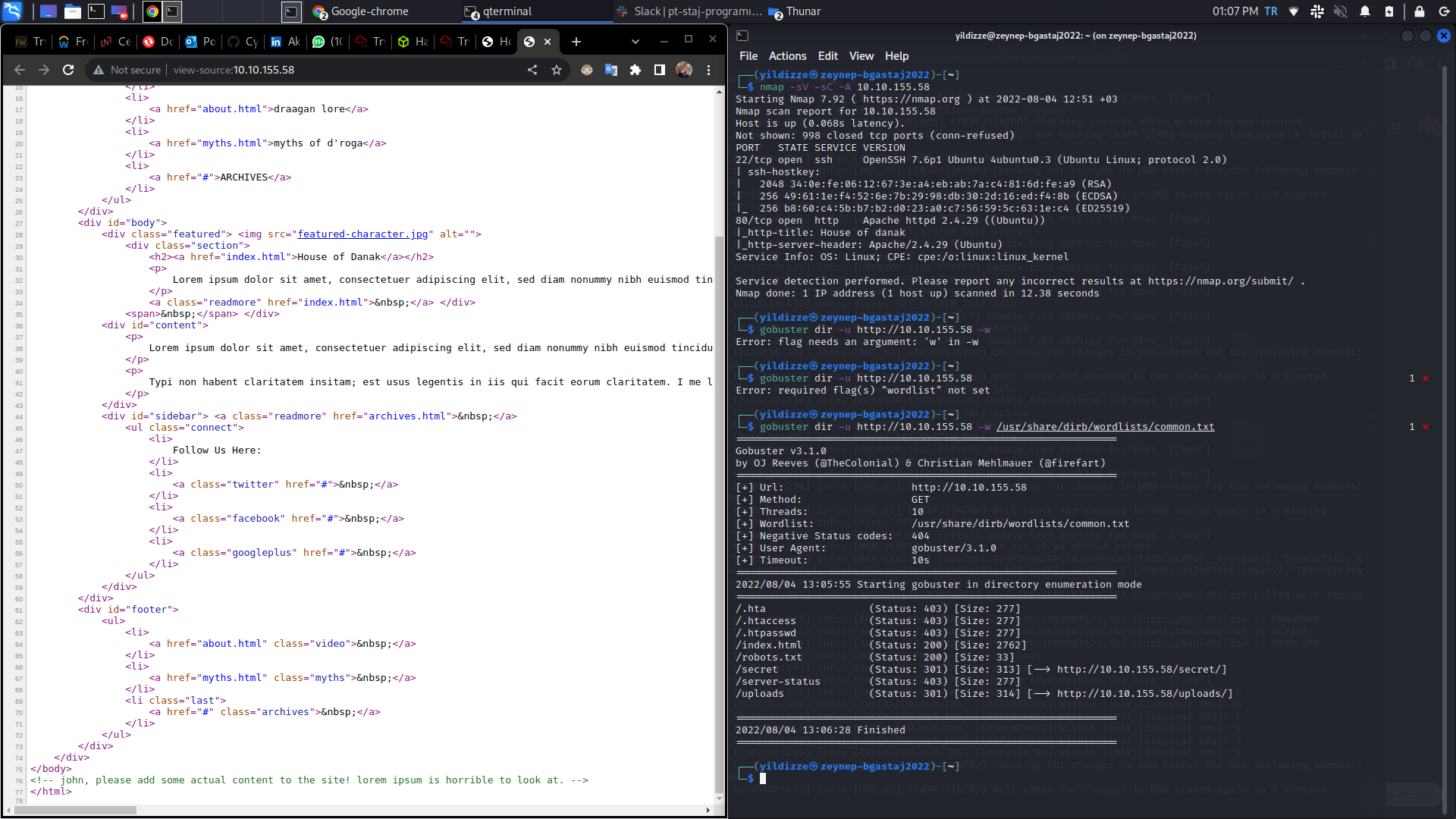
Sitenin içerisindeki yerlere tıklamaya çalıştığımızda bir tanesinden bir yere erişiyoruz. Uploads kısmına tıklıyoruz.



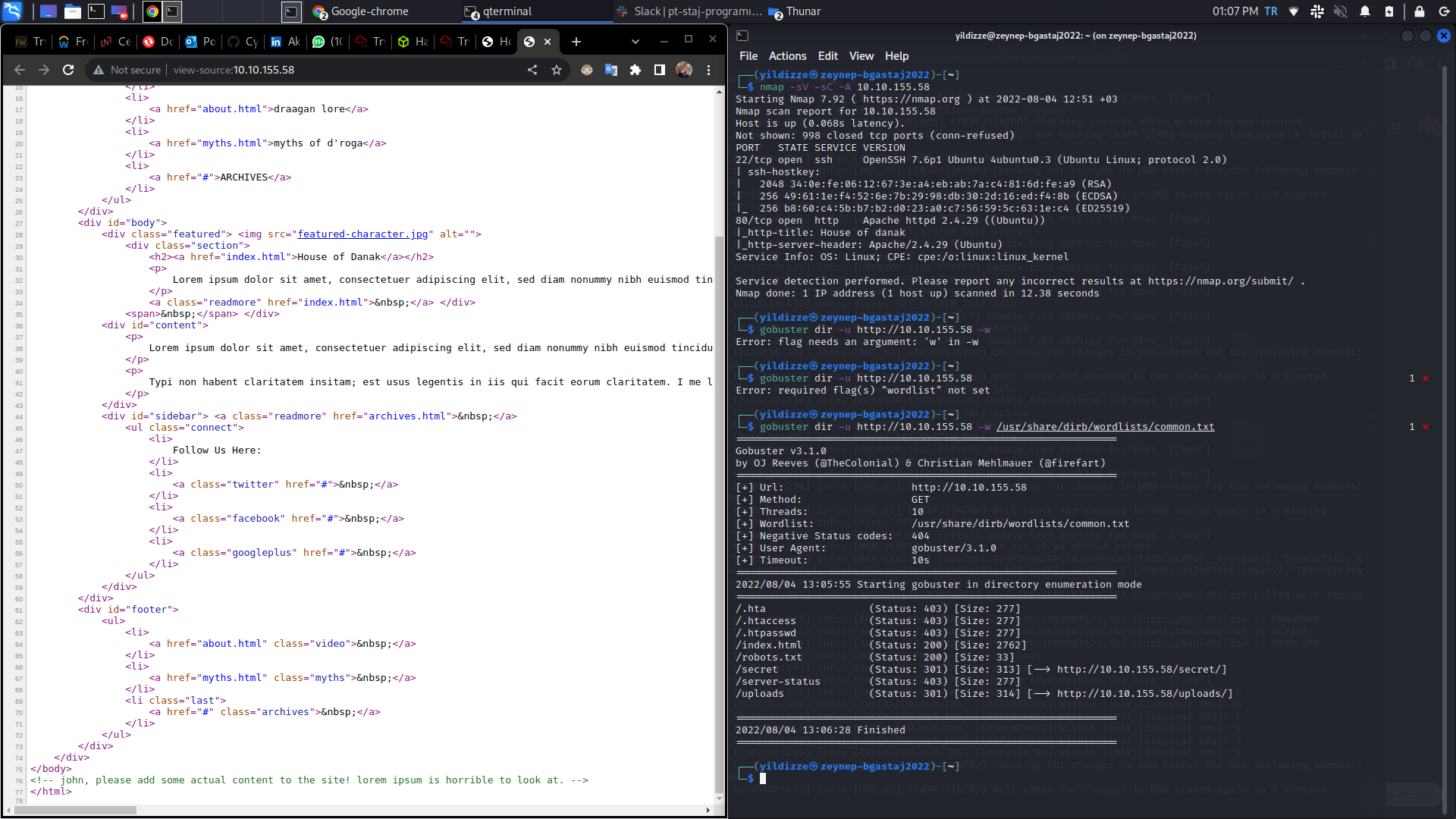
Uploads kısmına tıklayınca böyle bir sayfa ile karşılaşıyoruz. Dict.list kısmında kelime listesinin olduğunu görüyoruz



Daha sonra nmap taraması yapıyoruz. Nmap taraması sonucunda hangi portların açık olduğunun bilgisini almış oluyoruz.

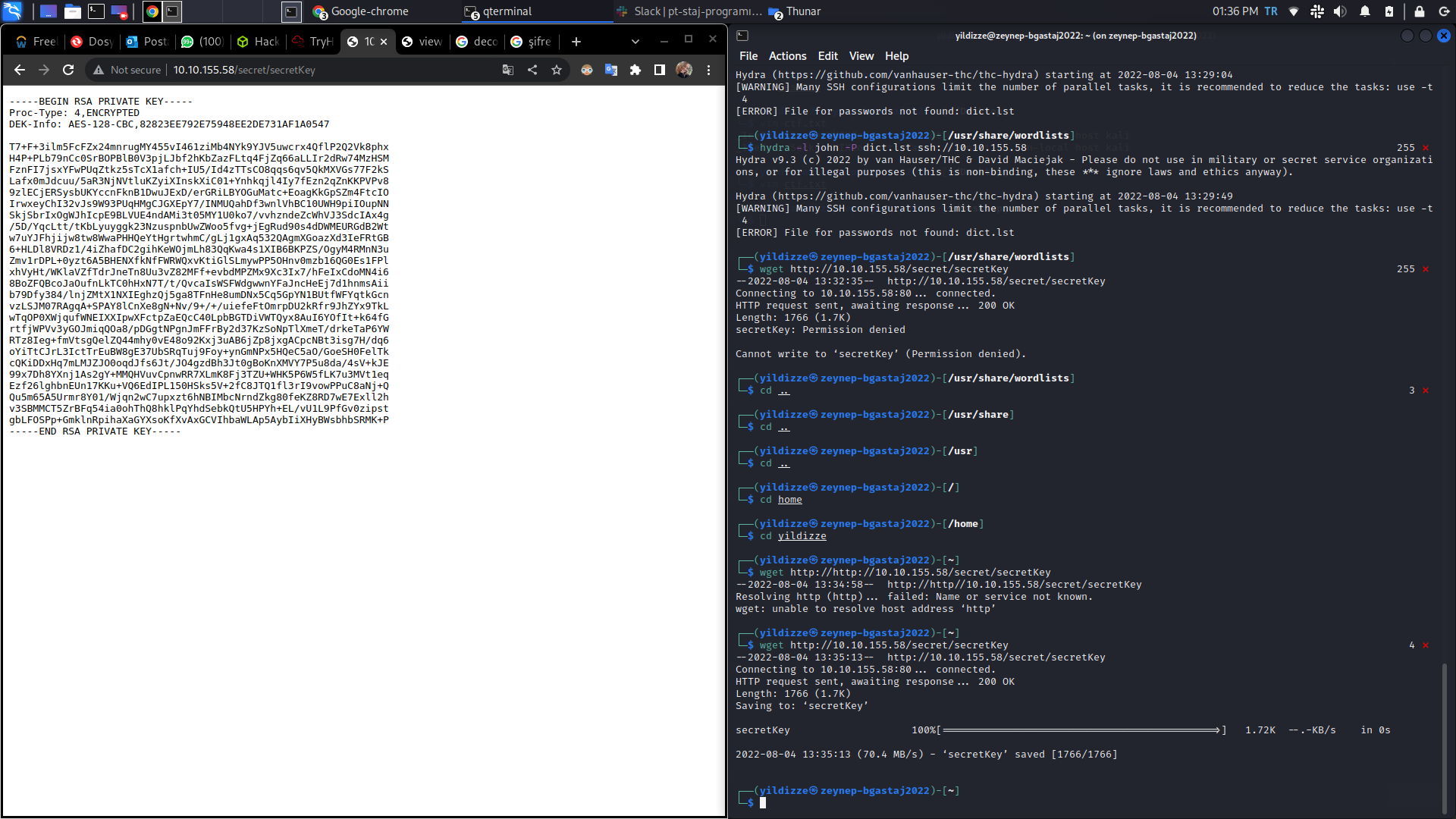


Şimdi sıra gobuster ile tarama yapmaya geldi.

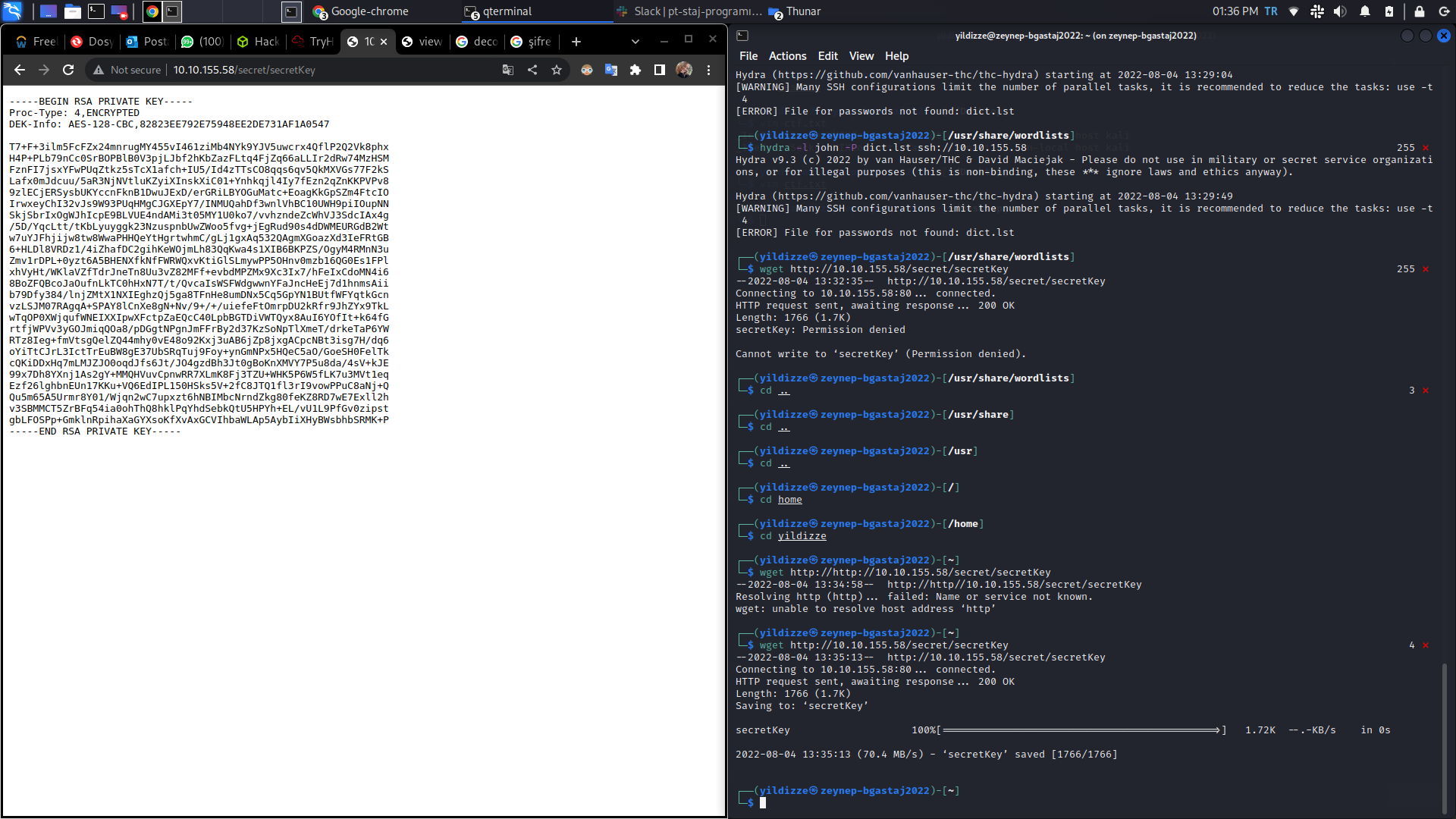


Tarama sonucunda “/secret” isimli bir dizin bulduk.

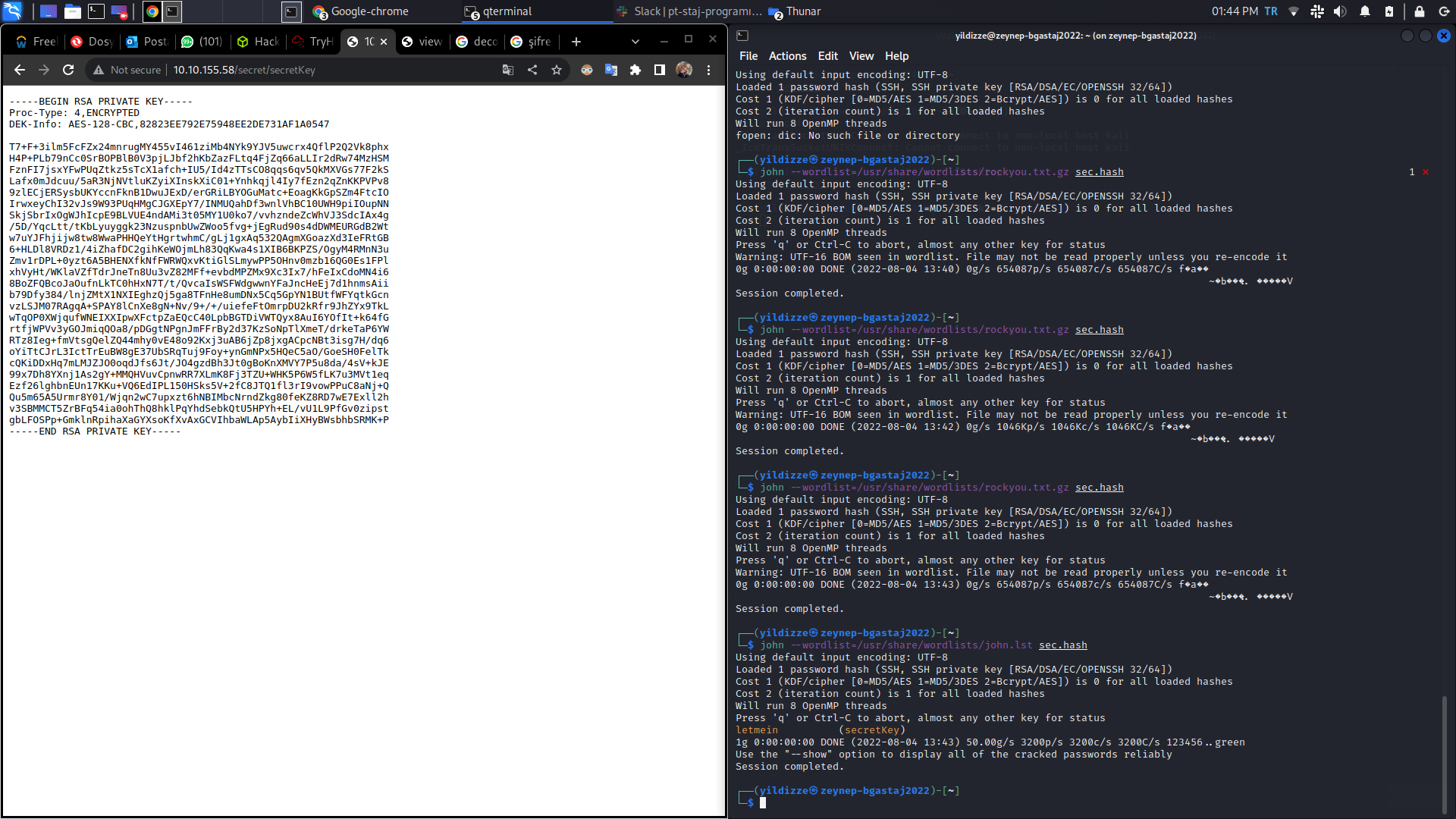
Dizinin içene girdiğimizde ise “secretKey” diye bir dosya ile karşılaşıyoruz. İçerisine girdiğimizde hashlenmiş bir metin ile karşılaşıyoruz.



Wget yardımı ile secretKey’i çekiyoruz çekiyoruz



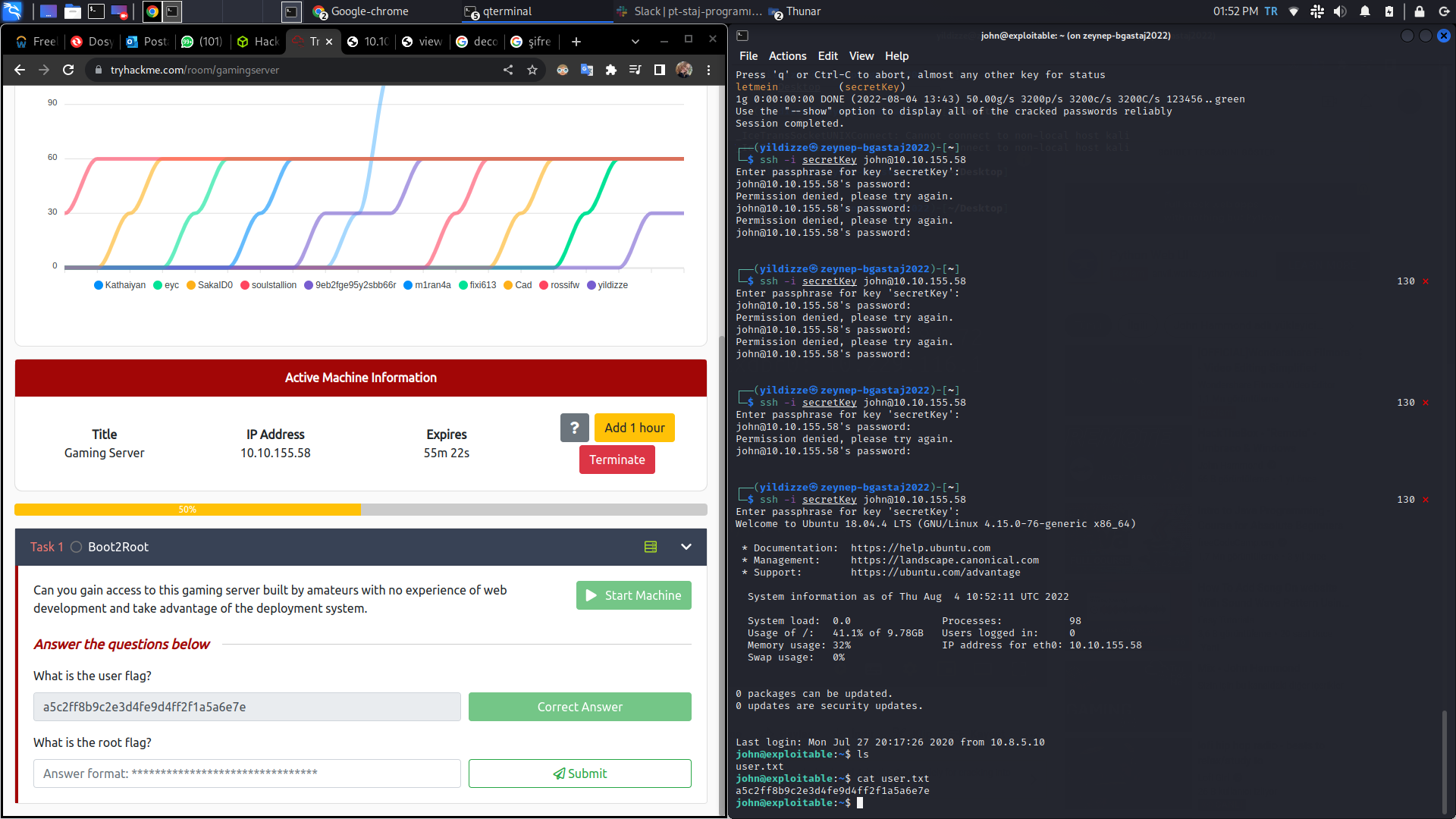
John yardımı ile şifreyi kırıyoruz.



Ve şifreyi bulduk!

Şifre: letmein

Şimdi de sıra ssh ile bağlanmaya geldi. Ssh bağlantısını gerçekleştiriyoruz ve ls komutu ile içerisindeki dosyaları görüyoruz. User.txt diye bil dosya buluyoruz. İçine girdiğimizde flag’ı buluyoruz.



**User Flag: a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e**

**(Makinenin süresi bittiği için tekrar başlatmam gerekiyor ve IP adresim bu sebeple değişiyor!)**

LXD yardımı ile ilerlememiz gerekmekte ancak git clone ile çekemedim timeout hatası aldım. İnternette araştırdım sorunu çözemedim.

