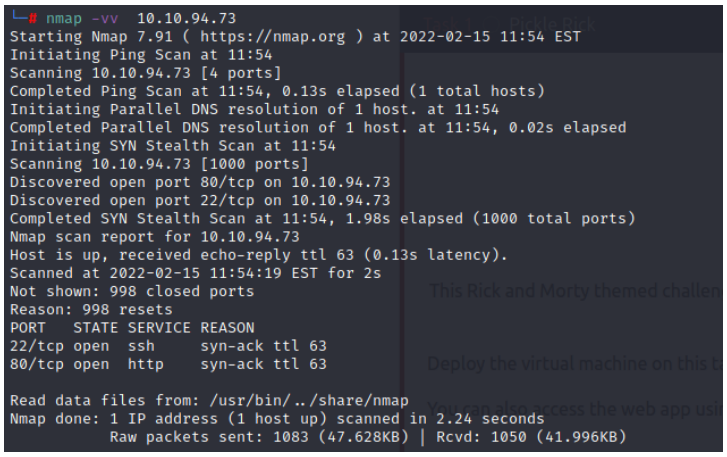
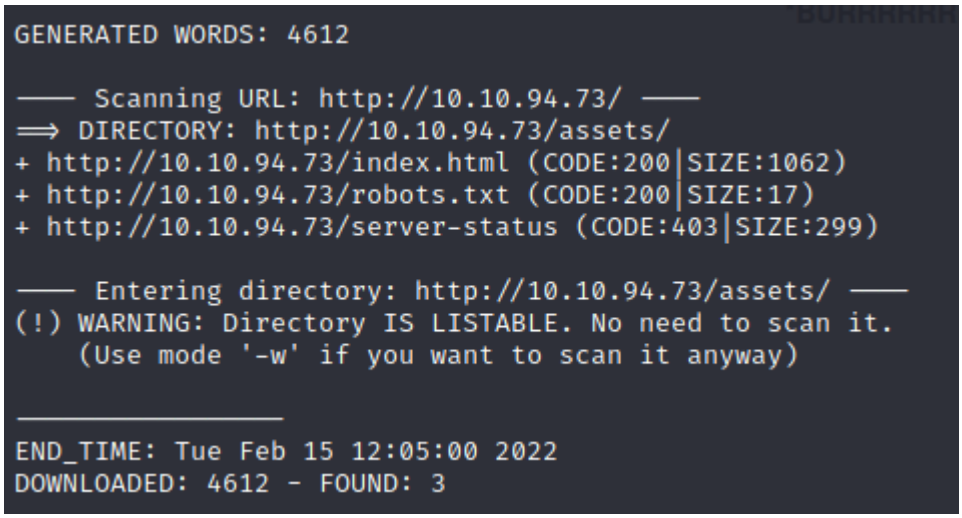
Pickle Rick Write UP

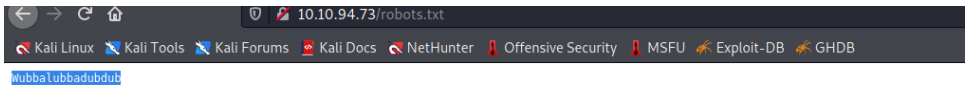
Try Hack Me' den IP yi aldıktan sonra IP'ye nmap atıyoruz, nmap attıktan sonra 80 ve 22 portunun açık olduğunu görüyoruz , IP'mizi bu sefer arama motorunda aratıp siteye gidiyoruz bu sırada dirb kullanarak sitedeki dizin veya dosyalara bakıyoruz .



Burda bazı dosyaları görüyoruz. Bu dizinleri denemeye başlıyoruz.



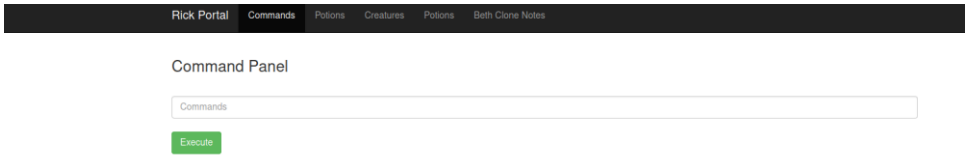
IP' mizin robots.txt yazan dosyasına girdiğimizde bir yazı karşımıza geliyor.



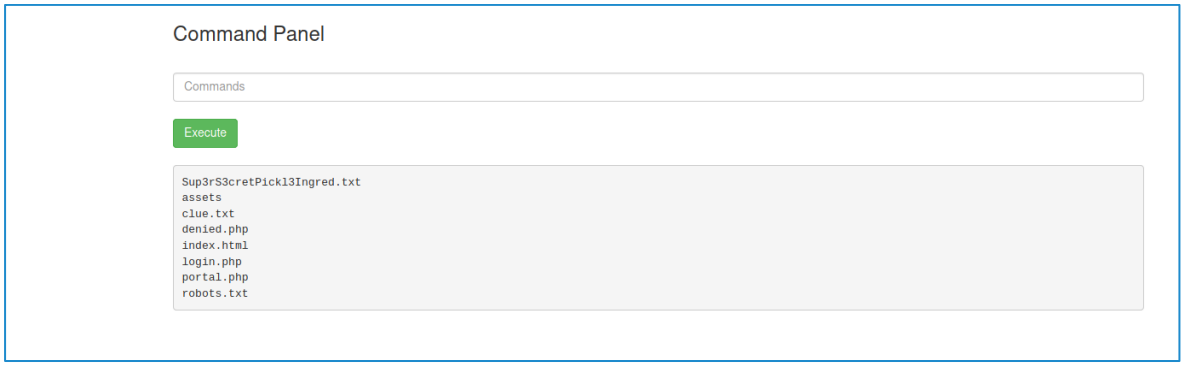
Bu yazıyı koplayıyoruz ve sitemizin index.html ' ine gidiyoruz burda kaynak kodumuzu açtığımızda karşımıza şöyle bir ekran geliyor

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>
    <p>I need you to <b>*BURRRP*</b>...Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: RickRul3s

  -->

</body>
</html>
```

Burda yazan username'i koplayayıp sitemizin login.php'sine gidiyoruz. Burda koplayadığımız kullanıcı adını ve parolayı girdikten sonra karşımıza şöyle bir ekran çıkıyor.



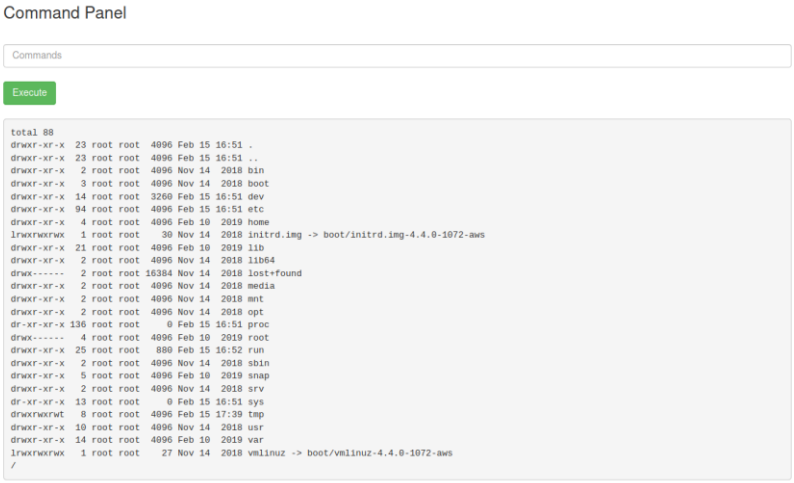
Burda karşımıza bir command panel geliyor bu panele ls komutunu yazdığımızda karşımıza şu ekran geliyor



Bu dosyaları tek tek deniyoruz ve Sup3rS3cretPickl3Ingred.txt açtığımızda ilk key'i alıyoruz

```
mr. meeseek hair
```

İlk key’imizi aldıktan sonra diğer dosyalarımızı deniyoruz. Burda clue.txt yi denerken karşımıza boş bir şey çıkıyor bunun için üst dizinlere çıkıyoruz karşımızıza bu çıkıyor



Sonra gine dizinlere çıkarak 2 Key’i buluyoruz. Sonra yetki alarak clue.txt açarak son keyi buluyoruz.