



## CAPTURE THE FLAG – RECON 03

Autor: ETR00M

Github: <https://github.com/ETR00M/>

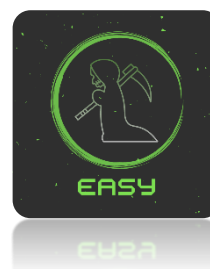
Linkedin: <https://www.linkedin.com/in/ls-anderson/>

Link da Challenge: [https://pentesterlab.com/exercises/recon\\_03/course](https://pentesterlab.com/exercises/recon_03/course)

Nível: fácil;

Categoria: *Recon*;

Tag: páginas web (diretórios comuns), *Directory Listing*, pensamento linear.



Para este Capture The Flag do **PentesterLab** o objetivo é localizar um diretório no servidor que permita a listagem de arquivos (*Directory Listing*) e acessar o arquivo exposto no site (<http://hackycorp.com/>).

### OBJECTIVE

For this challenge, your goal is to find a directory with directory listing in the main website for hackycorp.com.

### DIRECTORY LISTING

When accessing a directory on a webserver, multiple things can happen:

- an "index" file is present and it will get returned. N.B.: the file is not necessarily named `index`, this can be configured. But most of the time, the file will be named `index.html`
- no "index" file is present and the webserver will list the content of the directory. This can obviously leak information.

Indexing directory can be disabled on most webservers. For example, with Apache, you need to use the option: `-Indexes`.

To find directories, with indexing turned on. You need to browse the source of the HTML pages and look at the directories used to store files. Once you have a list of directories, you can access each of them individually.



Para cumprir este desafio primeiramente precisamos entender o que é o *Directory Listing*, o autor do desafio já descreve brevemente como essa falha de configuração ocorre. Quando acessamos um servidor web uma das situações abaixo pode ocorrer:

- O diretório possui uma página HTML (HyperText Markup Language), geralmente nomeada como “index.html”, que será exibida ao acessarmos o servidor a partir de um navegador.
- O diretório não possui uma página HTML a ser exibida, nesse caso o servidor web irá listar todo o conteúdo deste diretório, causando o *Directory Listing* que pode expor dados sensíveis.

Para avançar nesta *challenge* precisamos identificar um diretório em que a listagem de diretórios pode ocorrer, temos diferentes maneiras de fazer isso, porém o autor do desafio nos recomenda a análise do código fonte da aplicação buscando por diretórios utilizados para armazenar arquivos, geralmente esses diretórios não possuem uma página **index.html**, sendo assim, podem gerar o *Directory Listing* caso não sejam devidamente configuradas.

Dicas de materiais para estudo:

- [https://www.youtube.com/watch?v=RSsvxwBpQzg&ab\\_channel=SolydOffensiveSecurity](https://www.youtube.com/watch?v=RSsvxwBpQzg&ab_channel=SolydOffensiveSecurity)

Comando: **view-source:http://hackycorp.com/**

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <title>HackyCorp</title>
  <meta name="keywords" content="Hacky Corp" />
  <meta name="description" content="HACKY CORP">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0">

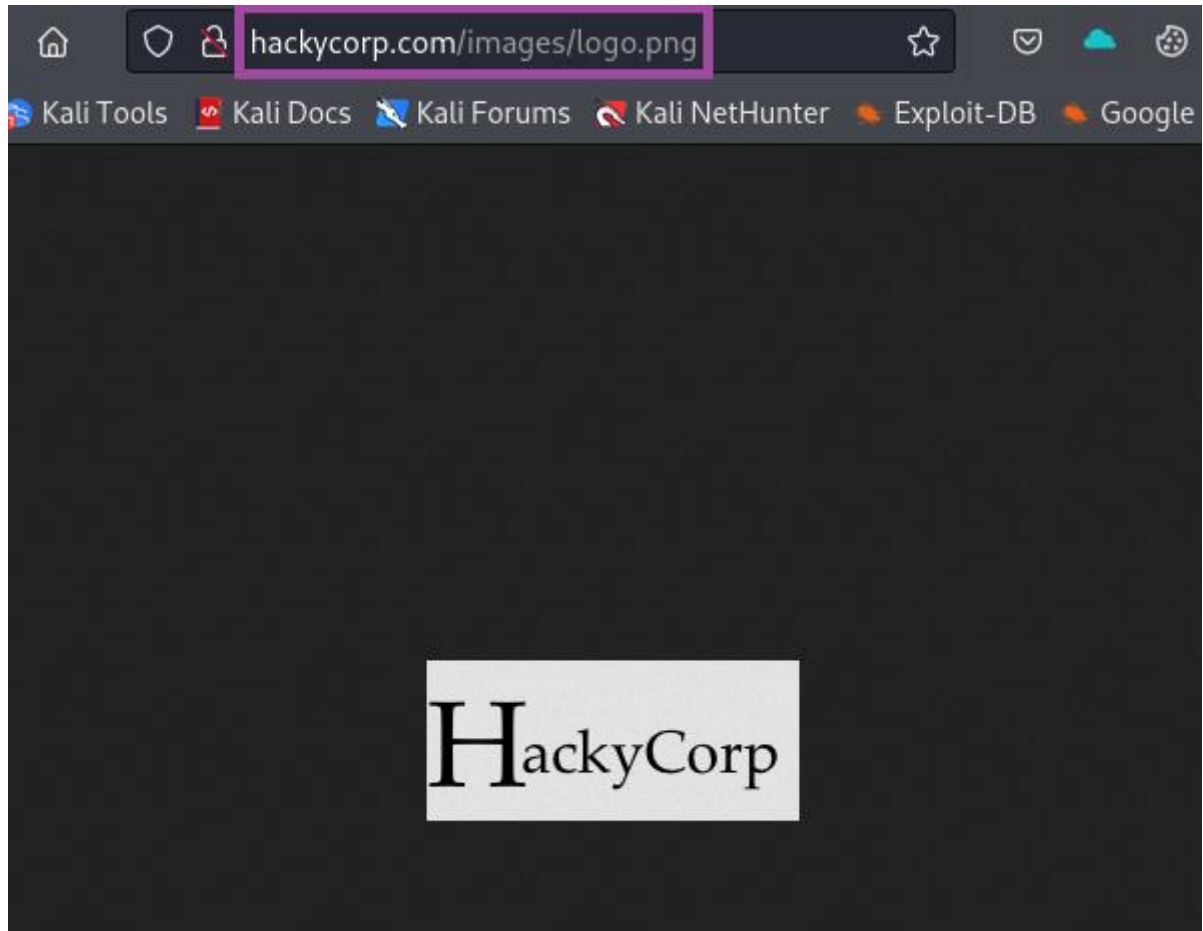
  <!-- Web Fonts -->
  <link href="https://fonts.googleapis.com/css?family=Poppins:300,400,500,600" rel="stylesheet">

  <!-- Libs CSS -->
  <link href="//assets.hackycorp.com/vendor/bootstrap/css/bootstrap.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/vendor/font-awesome/css/all.min.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/vendor/font-awesome/css/fontawesome.min.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/vendor/streamline-icon/css/streamline-icon.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/vendor/cubeportfolio/css/cubeportfolio.min.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/vendor/aos/aos.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/css/header.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/css/style.css" rel="stylesheet" />
  <link href="//assets.hackycorp.com/css/utilities.css" rel="stylesheet" />

  <!-- Skin -->
  <link rel="stylesheet" href="//assets.hackycorp.com/css/skin/default.css">
```



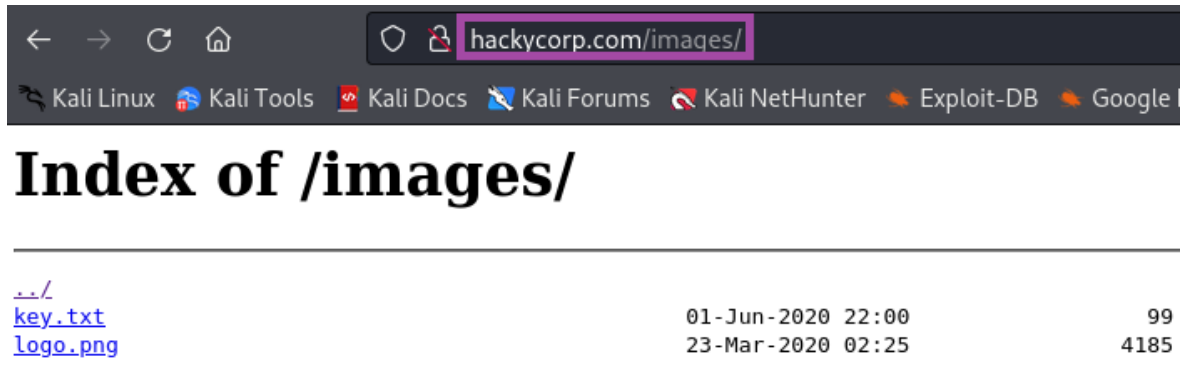
Ao analisarmos o código fonte da página identificaremos referências a diferentes diretórios, um bom lugar para efetuar a busca inicial pelo *Directory Listing* é em diretórios que armazenam imagens, podemos buscar no código essas referências e testarmos os links no navegador:



Ao remover o nome do arquivo “**logo.png**” do fim da URL como resultado podemos identificar que o diretório *images* não possui uma página “*index.html*”, dessa forma todo seu conteúdo é listado evidenciando o *Directory Listing*:

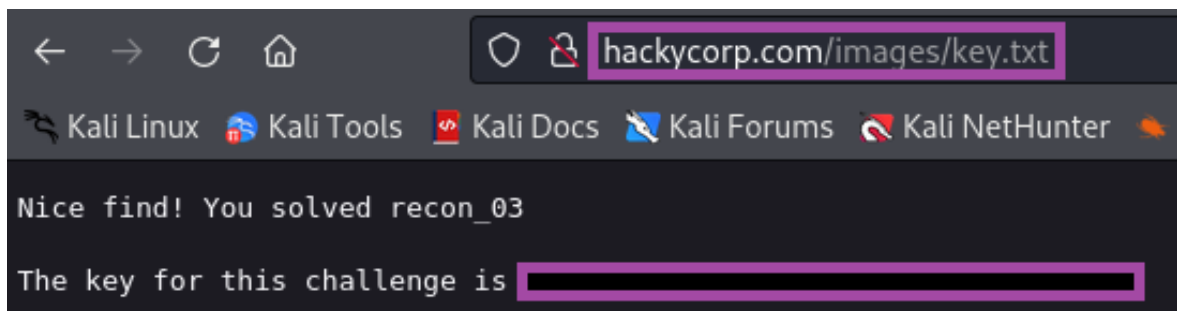


Comando: `http://hackycorp.com/images/`



../		
<a href="#">key.txt</a>	01-Jun-2020 22:00	99
<a href="#">logo.png</a>	23-Mar-2020 02:25	4185

Ao acessar o diretório *images* a partir do navegador temos como retorno a listagem de dois arquivos: “*key.txt*” e “*logo.png*”. No conteúdo do arquivo “*key.txt*” localizaremos a *flag* para concluir este desafio.



Agora basta submetermos a *flag* na plataforma do **PentesterLab** para concluir o desafio:

To mark this exercise as completed, you need to submit the key that you will get by finishing this exercise:

Submit

The domain you're targeting is hackycorp.com



Congrats you have already finished this exercise!

You scored this exercise (last 5 events):

- less than a minute ago