CAPTURE THE FLAG – RECON 01

Autor: ETR00M
Github: https://github.com/ETR00M/
Linkedin: https://www.linkedin.com/in/ls-anderson/

Link da Challenge: https://pentesterlab.com/exercises/recon_01/course
Nível: fácil;
Categoria: *Recon*;
Tag: páginas web (erro 404), pensamento linear.

Para este Capture The Flag do **PentesterLab** o objetivo é gerar um erro 404 no site (http://hackycorp.com/).

OBJECTIVE

For this challenge, your goal is to generate a 404/"Not Found" error on the main website for hackycorp.com.

THE 404 PAGES

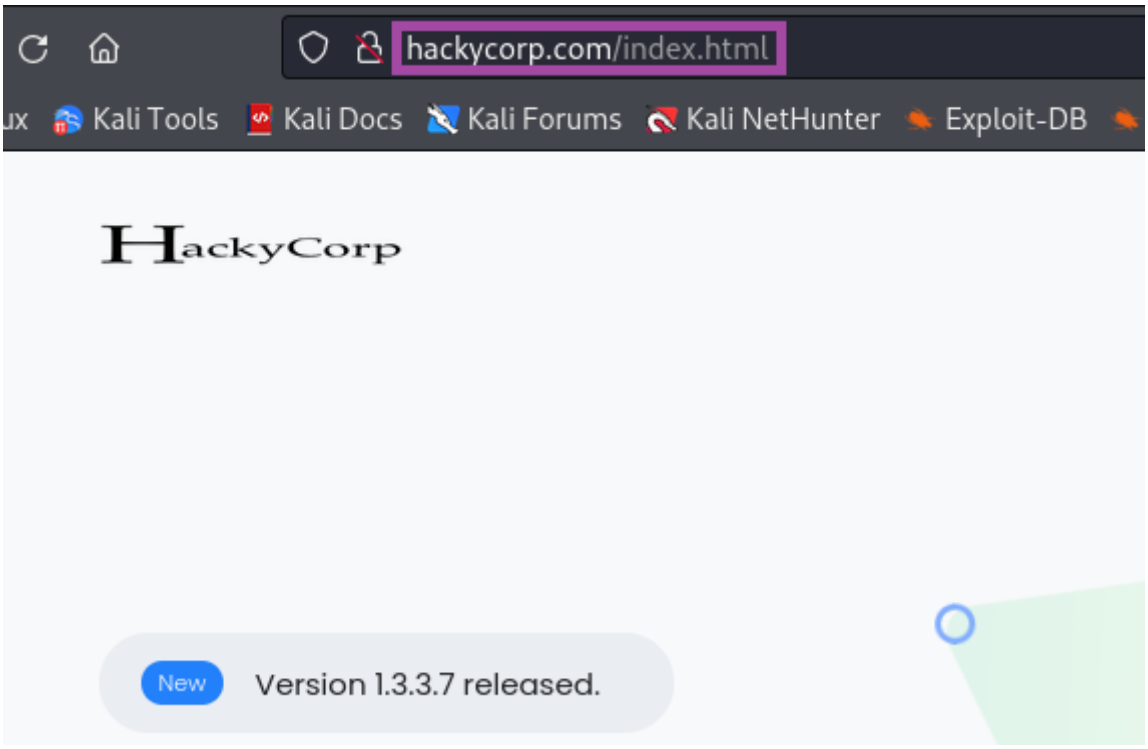
Not Found/404 pages can leak information about the web stack used by a company or application. It also allows you to detect files that exists when you start bruteforcing directory. This is why it is important to check what the 404 page looks like.

Durante a fase de reconhecimento e levantamento de informações iniciais é importante forçar a aplicação a lidar com erros para identificar seu comportamento e existência de controles em caso de falhas. Nesta *challenge* precisaremos gerar um erro de ***Page Not Found*** (404) na aplicação, caso você não conheça esse erro, ou não saiba como gerá-lo, recomendo o estudo do assunto antes de seguir com a leitura do *writeup*.

Dicas de materiais para estudo:

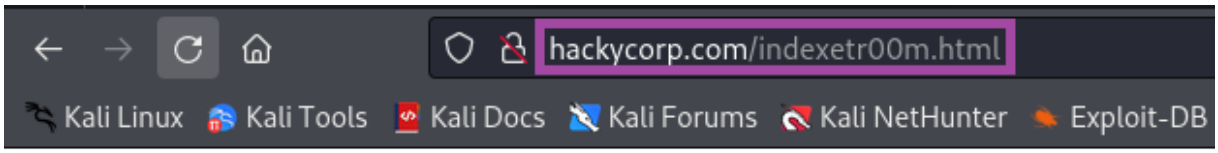
- https://www.youtube.com/watch?v=1Vp5O8Je7hs&ab_channel=Dicion%C3%A1riodeInform%C3%A1tica
- https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Status
- https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Status#respostas_de_erro_do_cliente

Por padrão, o arquivo "**index.html**" contém a página principal de uma aplicação web conforme mostrado na imagem abaixo, sendo assim, geraremos um erro "**404**" a partir dessas informações já conhecidas e esperadas em qualquer site.



Irei acrescentar um "**etr00m**" ao final de index fazendo com que o site busque pelo arquivo "**indexetr00m.html**", gerando erro pela não localização da página solicitada, ou seja, tendo como código de retorno: "**404 – *Page Not Found***", quaisquer outros nomes de arquivos que forem buscados e não sejam localizados no servidor gerarão o mesmo resultado.

Comando: **http://hackycorp.com/indexetr00m.html**



404 page! You solved recon_01

The key for this challenge is: [redacted]

Após gerar com sucesso o erro **404** no site recebemos a *flag* como resultado, agora basta submetermos ela na guia **Scoring** da plataforma para completar o desafio.