



CAPTURE THE FLAG – RECON 02

Autor: ETR00M

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

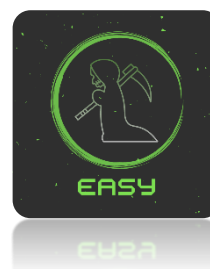
Linkedin: <https://www.linkedin.com/in/ls-anderson/>

Link da Challenge: https://pentesterlab.com/exercises/recon_02/course

Nível: fácil;

Categoria: *Recon*;

Tag: páginas web (arquivo security.txt), pensamento linear.



Para este Capture The Flag do **PentesterLab** o objetivo é localizar e acessar o arquivo “security.txt” do site (<http://hackycorp.com/>).

OBJECTIVE

For this challenge, your goal is to retrieve the security.txt from the main website for hackycorp.com.

THE SECURITY.TXT FILE

The security.txt file is used to tell security researchers how they can disclose vulnerabilities for a website. You can learn more about it here: securitytxt.org and on Wikipedia: [Security.txt](https://en.wikipedia.org/wiki/Security.txt).

Durante a fase de reconhecimento e levantamento de informações iniciais é muito importante conhecer os padrões de desenvolvimento, diretórios e arquivos comuns passíveis de serem encontrados em uma aplicação web.

Dentre estes arquivos está o “security.txt”, caso você não tenha conhecimento sobre o que o arquivo “security.txt”, qual sua função e onde ele está localizado recomendo o estudo deste assunto antes de seguir com o *writeup*.

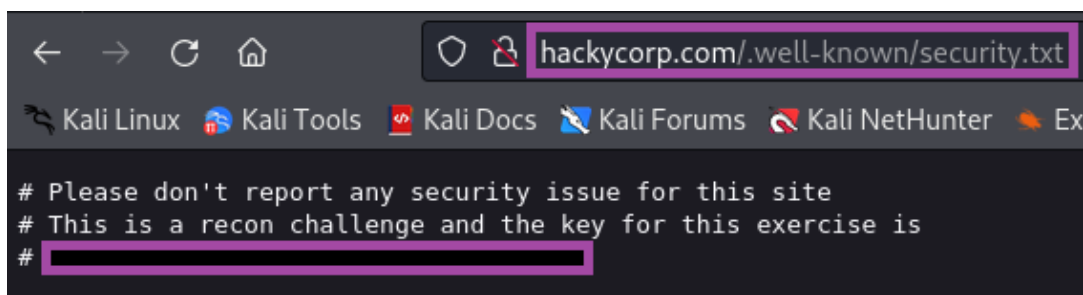


Dicas de materiais para estudo:

- https://www.youtube.com/watch?v=qLLZH9yj_NU&ab_channel=CTHub

O arquivo “**security.txt**” contém informações relevantes para que um pesquisador de segurança possa contatar o time de segurança responsável pela avaliação e correção de falhas nas aplicações web de uma organização, para completar esta *challenge* basta acessar esse arquivo em seu diretório padrão:

Comando: **http://hackycorp.com/.well-known/security.txt**



Após abrir com sucesso o arquivo “**security.txt**” receberemos a *flag* como retorno da requisição, agora basta submetermos ela na guia **Scoring** da plataforma para completar 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