CAPTURE THE FLAG – RECON 09

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

Link da Challenge: https://pentesterlab.com/exercises/recon_09/course
Nível: Fácil;
Categoria: *Recon*;
Tag: cabeçalho HTTP, navegador (ferramenta de desenvolvedor), pensamento linear.

Neste *Capture The Flag* do **PentesterLab** o objetivo é acessar o cabeçalho HTTP de resposta do servidor para as requisições efetuadas ao site (http://hackycorp.com/).

OBJECTIVE

For this challenge, your goal is to access the headers from responses.

HEADER INSPECTION

When accessing a web server, it often pays off to check the responses' headers. It's common to find information around version and technologies used.

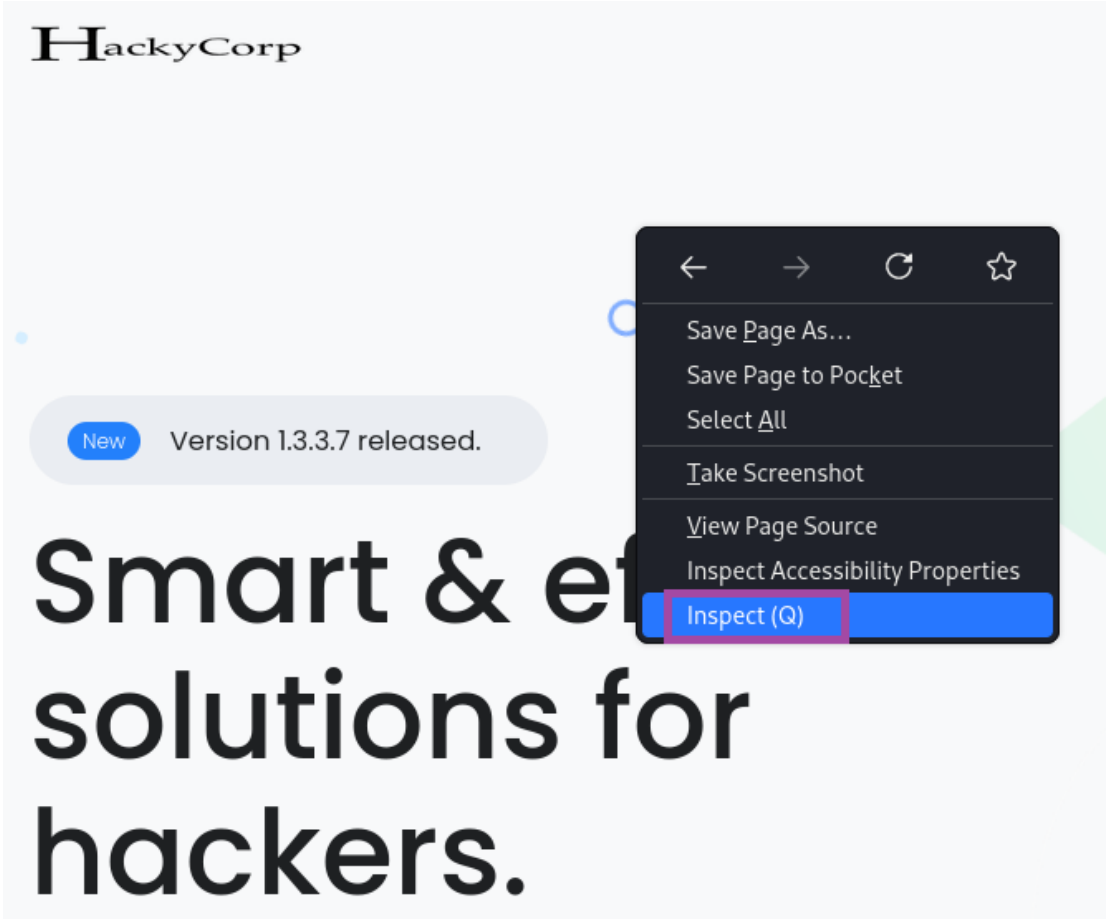
Podemos efetuar a coleta do cabeçalho de resposta HTTP de diferentes formas, porém neste CTF realizarei o acesso utilizando como ferramenta o próprio navegador, neste caso o **Firefox**. Caso você não esteja familiarizado com o assunto recomendo o estudo dos conteúdos abaixo antes de seguir com a leitura.

Dicas de materiais para estudo:

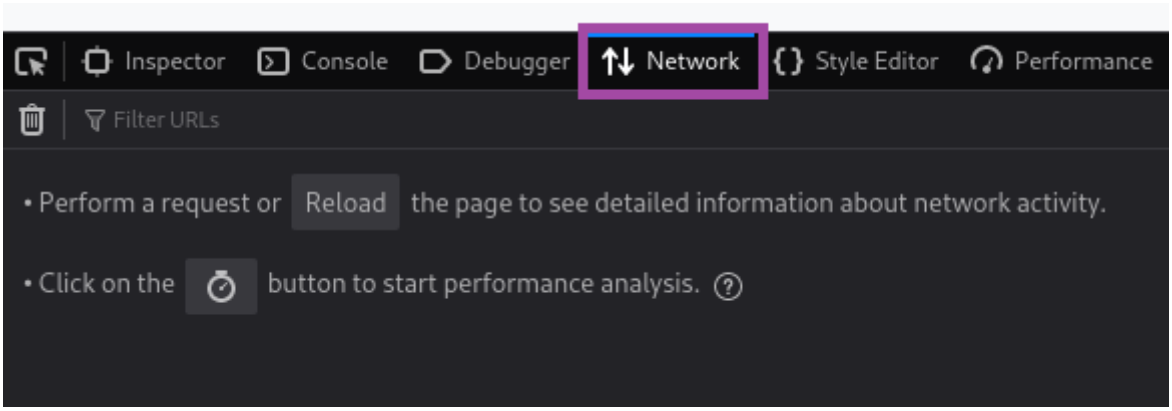
- https://www.youtube.com/watch?v=PcHbyGVoqZk&ab_channel=Refatorando
- https://www.youtube.com/watch?v=2lBJVEYDwlM&ab_channel=DankiCode

Após acessar o site, ao clicar com o botão direito do mouse na página iremos selecionar a opção "***Inspect***" para abrir as opções avançadas e ferramentas de desenvolvedor.

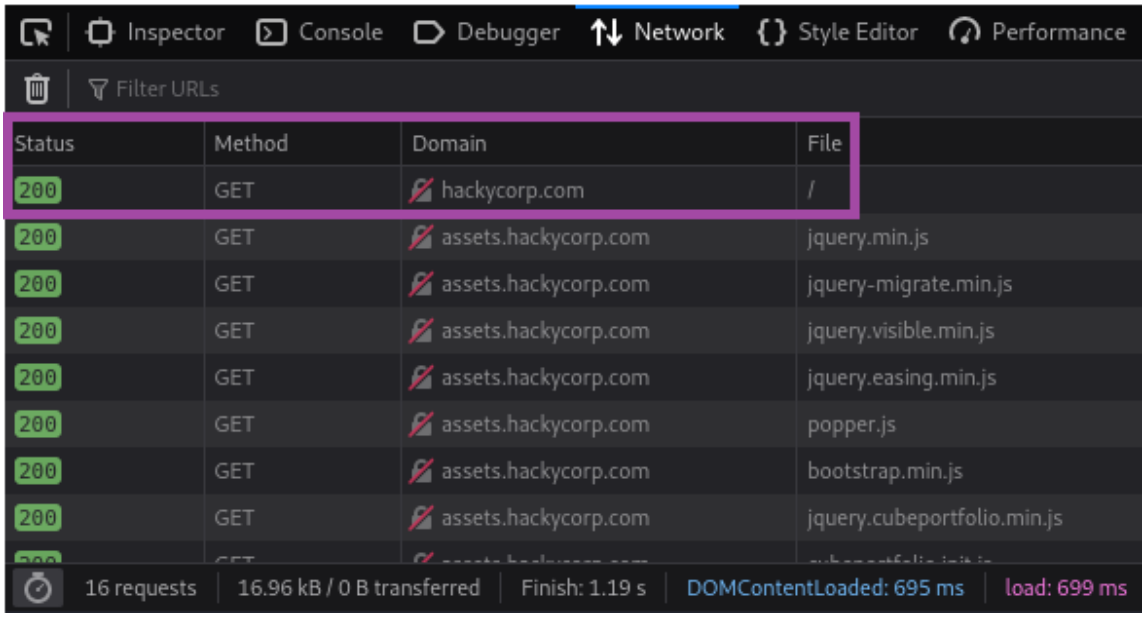
Comando: **http://hackycorp.com**



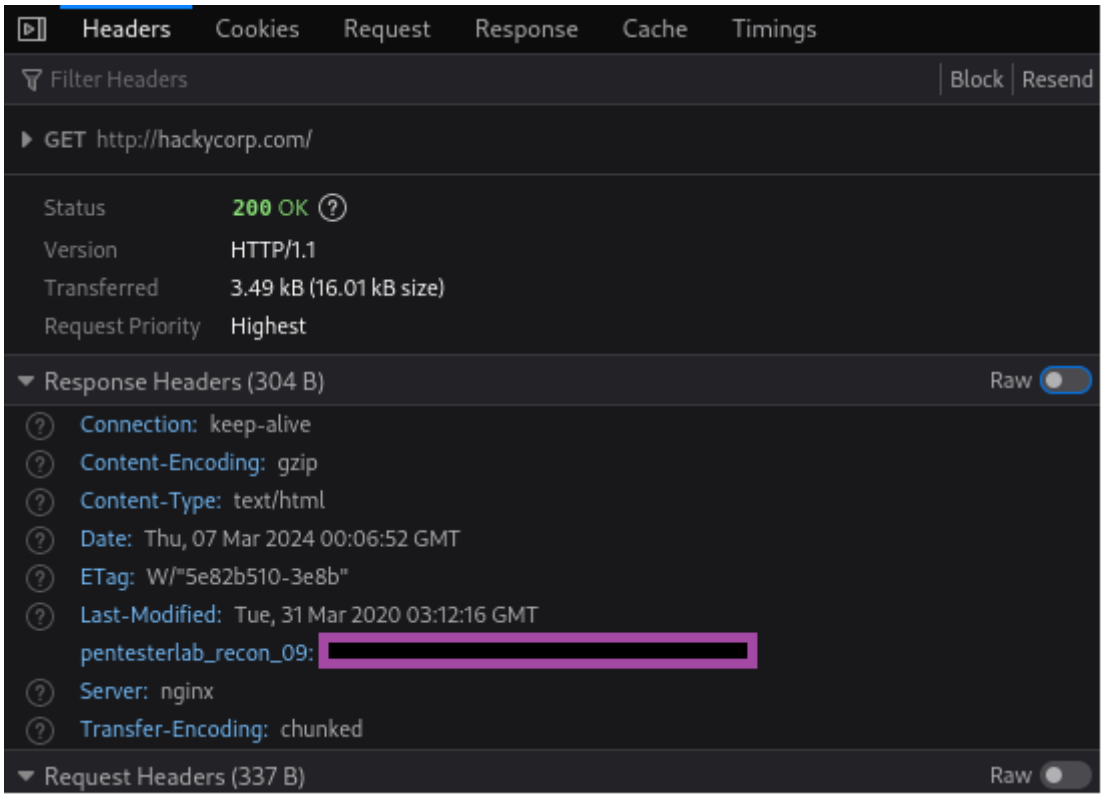
O menu de opções será apresentado na parte inferior no navegador, nela selecionaremos a ferramenta "***Network***" para capturar as comunicações estabelecidas entre o navegador e o servidor de aplicação que estamos acessando.



Conforme indicado na descrição da ferramenta, para efetuar a captura das atividades de rede será necessário atualizar o site ("**F5**"), uma saída semelhante a apresentada abaixo será recebida. Precisaremos avaliar o primeiro resultado referente a requisição ao domínio **hackycorp.com**.



Ao selecionar o domínio será apresentado a guia "**Header**", entre as informações coletadas teremos os dados de requisição e resposta da aplicação, que contém a *flag* da *challenge*.



Agora basta submetermos a *flag* na plataforma para completarmos o desafio de reconhecimento.