31/05/2023 – PicoCTF – GET aHEAD

Link: <https://play.picoctf.org/practice/challenge/132?page=1&search=>

1. Utilizar Burp Suite para alterar as requisições ao site. Ao fazer uma requisição, clicando em “Choose Red” no site, tem-se a seguinte requisição:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Ao mandar ao “Repeater”:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Ao abrir a aba do Repeater:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Por conta das dicas e do nome do desafio, tem-se uma relação com o método HTTP “HEAD”. Ao trocar o método de “GET” para “HEAD”, e fazer uma requisição, tem-se:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Portanto, a flag é: $flag