Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

findme – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | findme – Matheus da Cunha Castilho |
| **N° Revisão** | 1 |
| **Data de publicação** | 19/04/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/349?category=1&difficulty=2&page=1 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Matheus da Cunha Castilho | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 19/04/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Web Exploitation |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_2dlhfk6i0xjg)

[Desenvolvimento 3](#_rw3isserja6p)

Tela de login 3

Tela principal [3](#_txxqpow7p4gm)

Buscando a flag [3](#_n4v34thnljs4)

[Conclusão 3](#_yenwhptmu3fo)

[Referências 3](#_aetjd1fwg0bo)

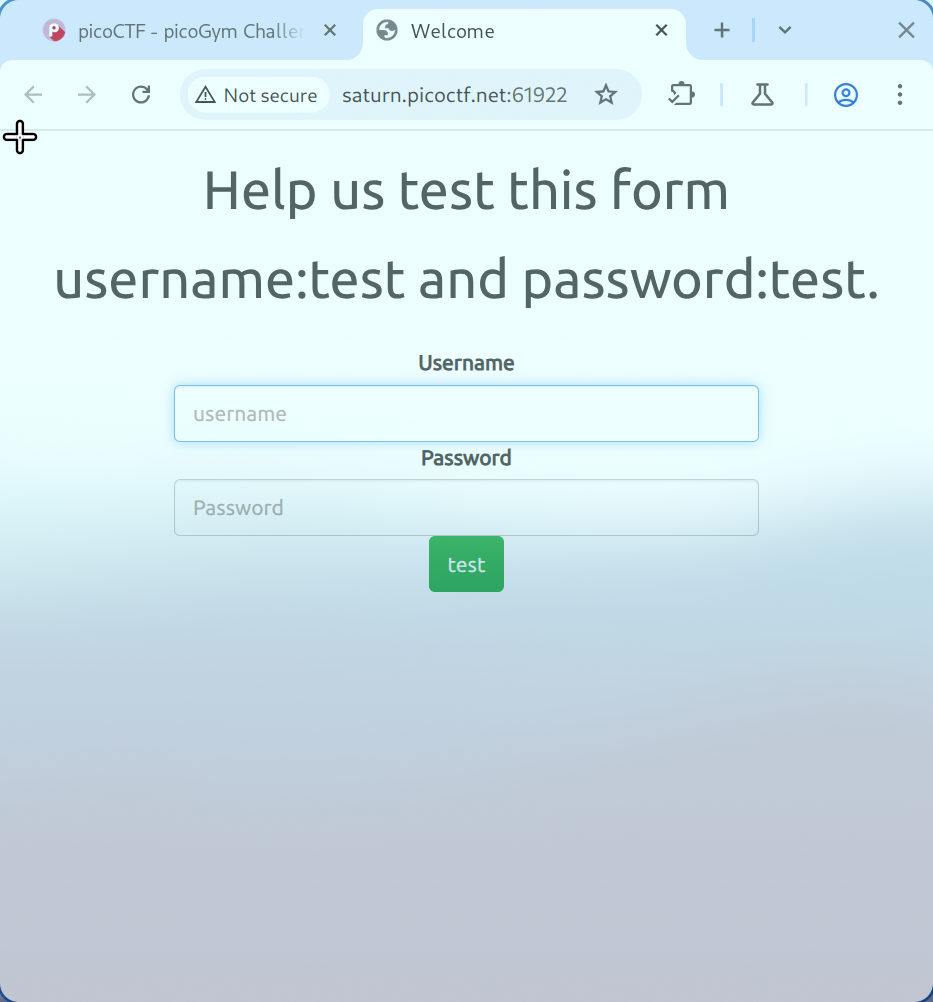
**Contextualização**

O CTF em questão trata de temas básicos da Web Exploitation, exigindo um pouco de interpretação dos textos descritos. É um CTF simples, porém para quem ainda não tem conhecimento de Burp Suite, e no funcionamento de requisições HTTP, pode ser um pouco desafiador.

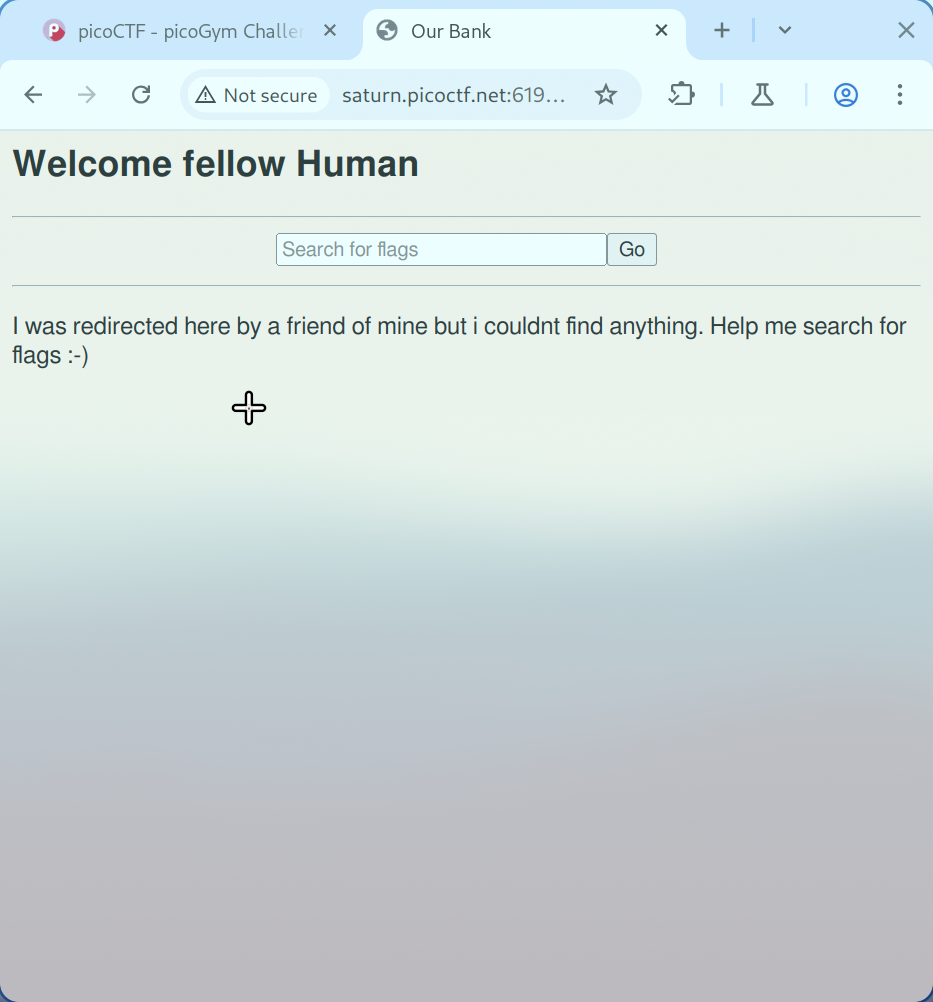
**Desenvolvimento**

**Tela de login**

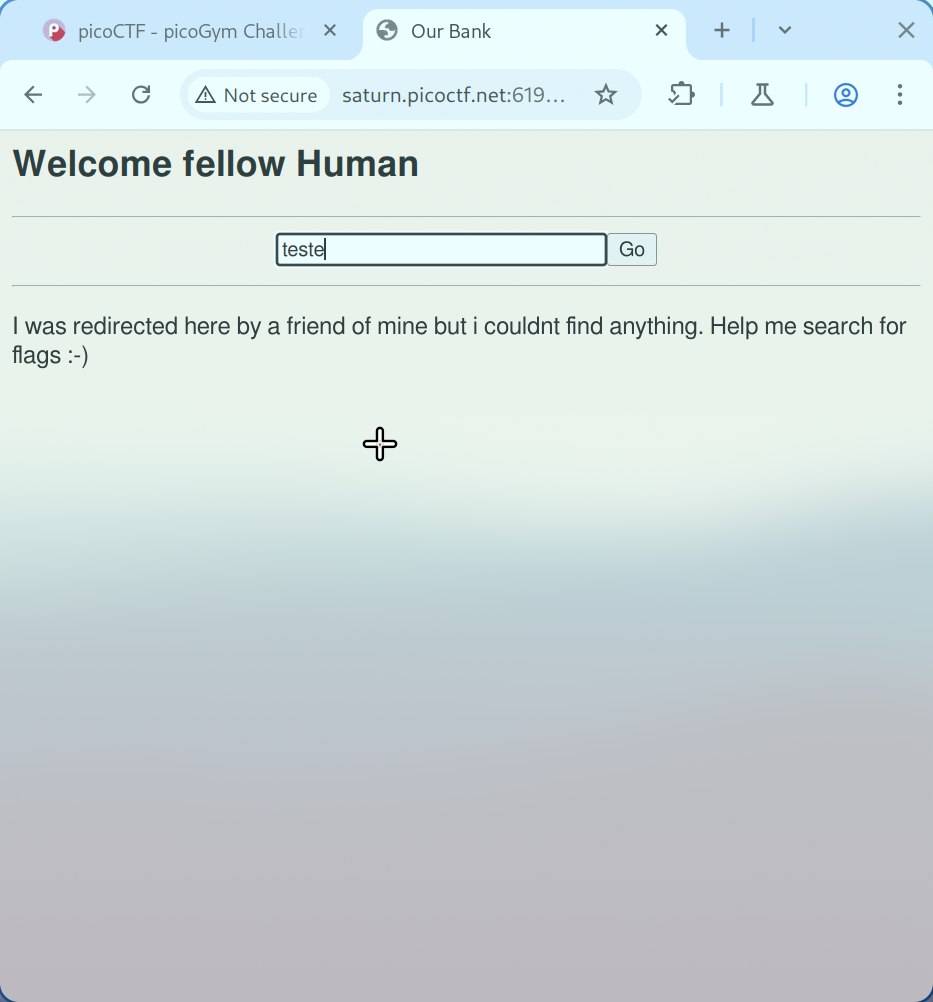
Ao iniciar o CTF, é possível encontrar uma tela de login contendo instruções para iniciar a sessão.



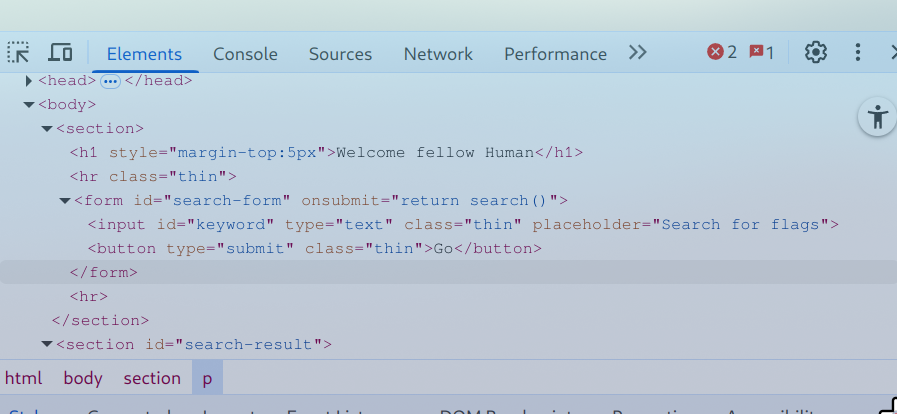
**Tela Principal**



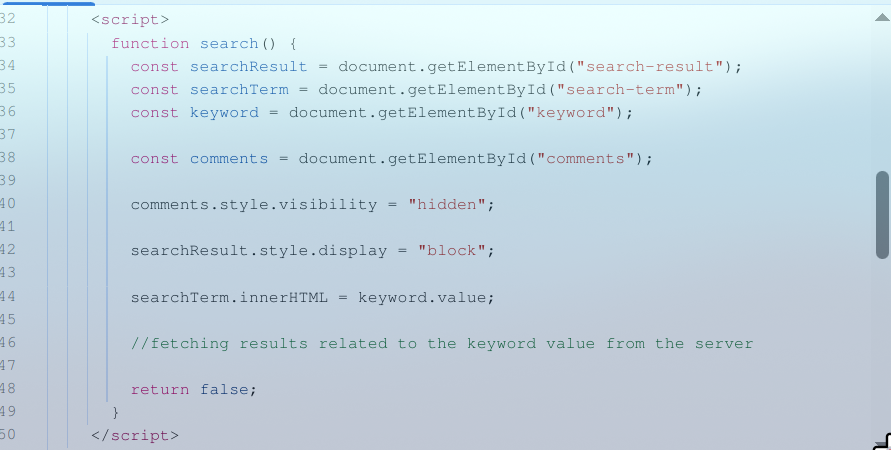
Ao tentar pesquisar algo, nada acontece.



Analisando o código fonte da página, vimos que ao clicar no botão, a função search() é chamada.



Analisando vimos que não há nada de útil por lá, apenas o que uma função de busca realmente faria.

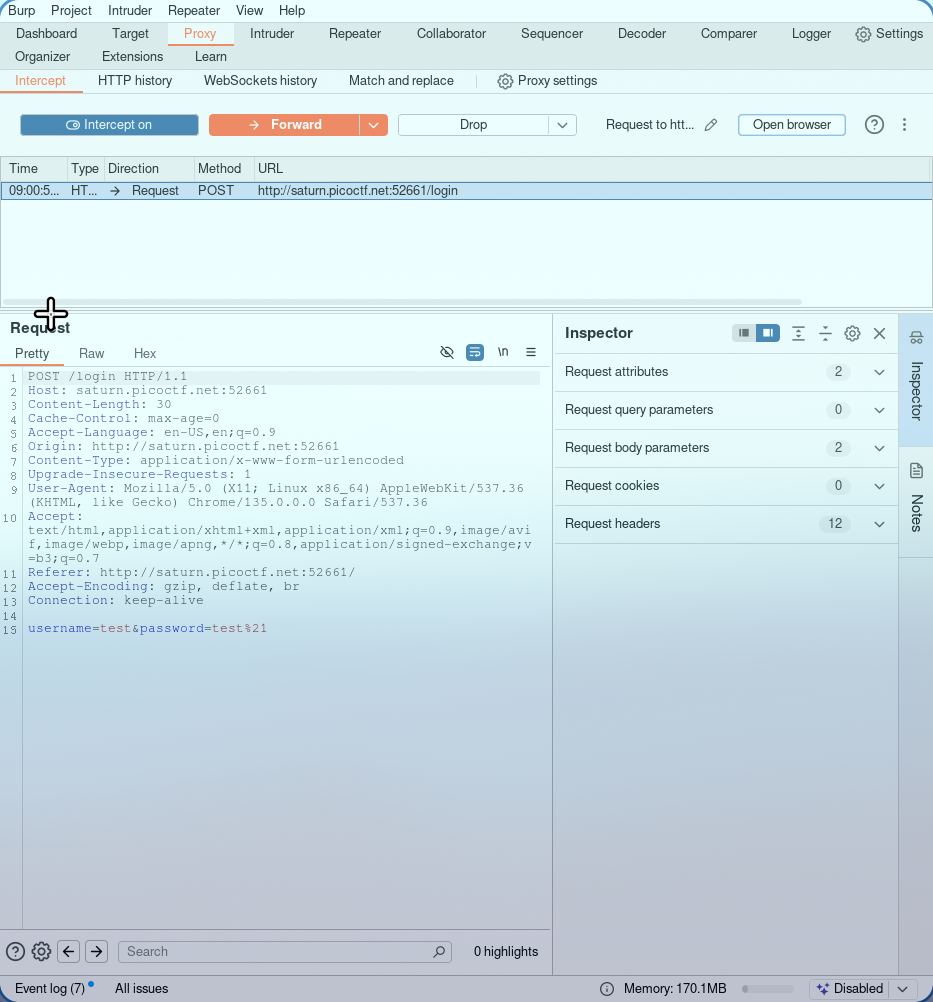


Voltando à tela do PicoCTF, ao olhar as dicas, é possível perceber que a dica refere-se a um redirecionamento, provavelmente entre o login e a tela principal.

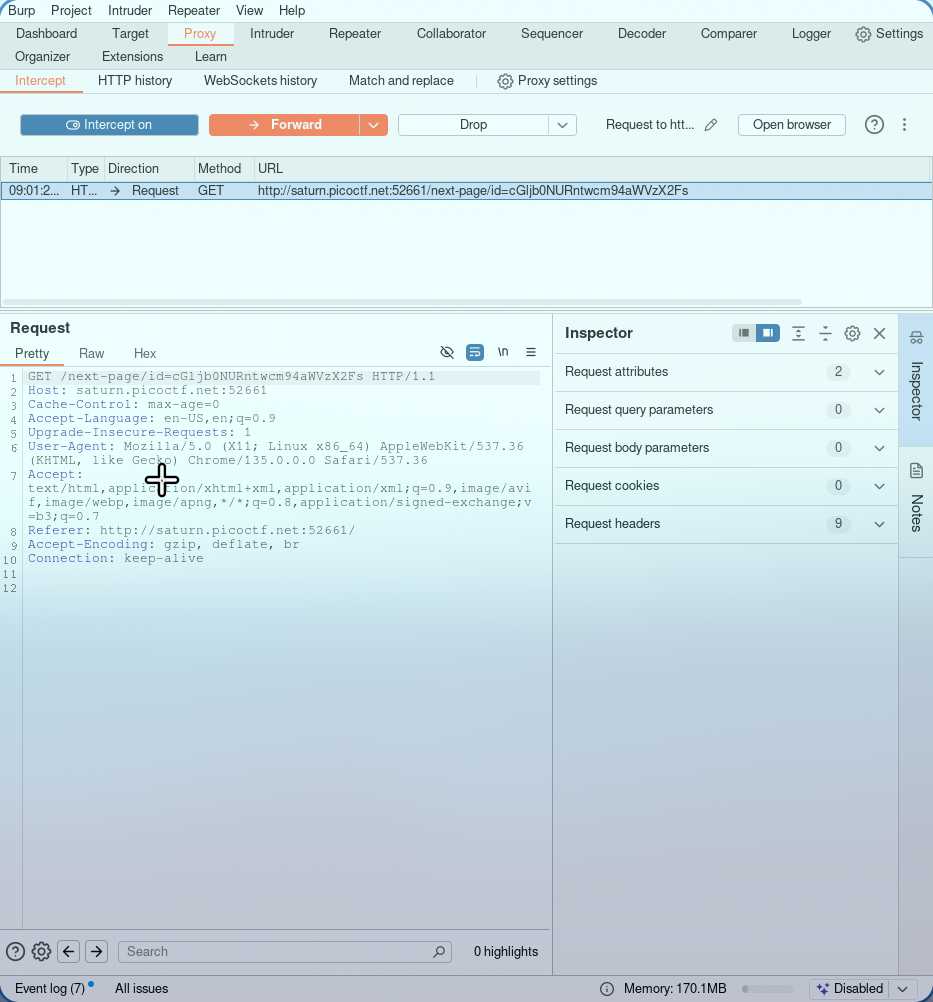


**Buscando a Flag**

Ao utilizar o Burp Suite para interceptar as requisições, não obtemos nada no login, apenas os dados passados.

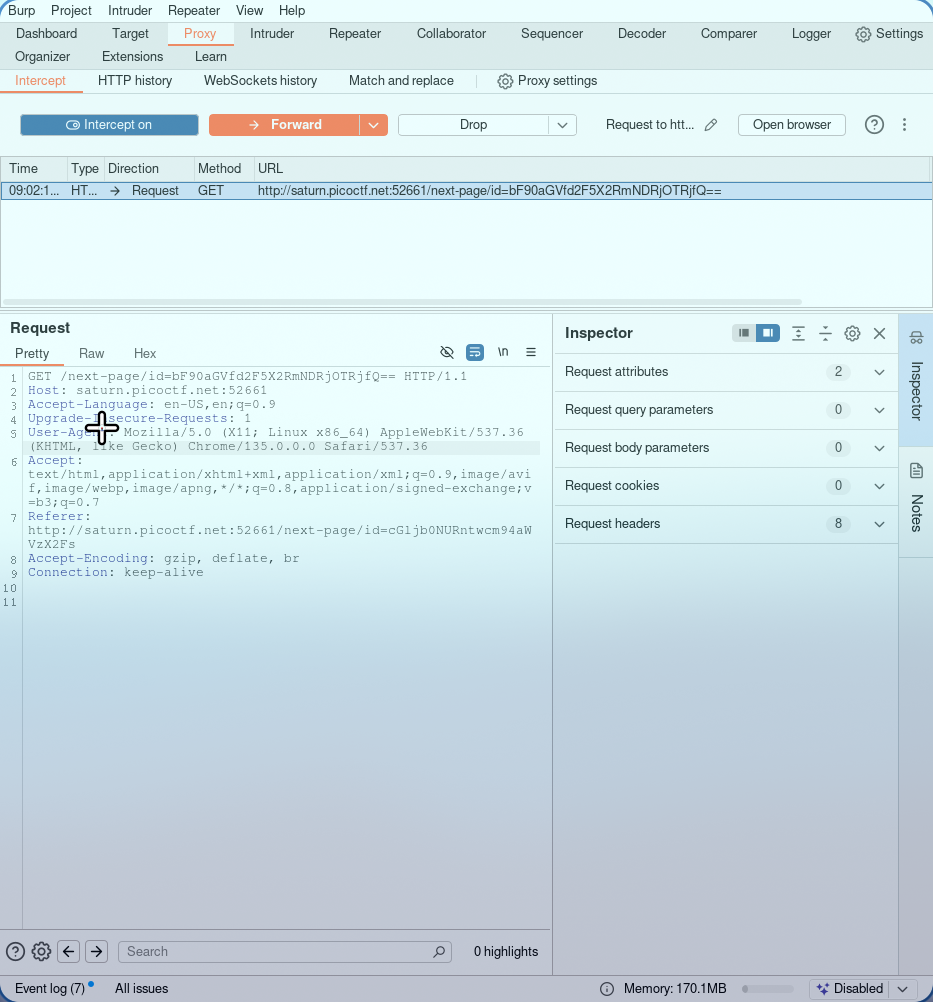


Então, ao seguir com a requisição, outra é recebida pelo Burp Suite.

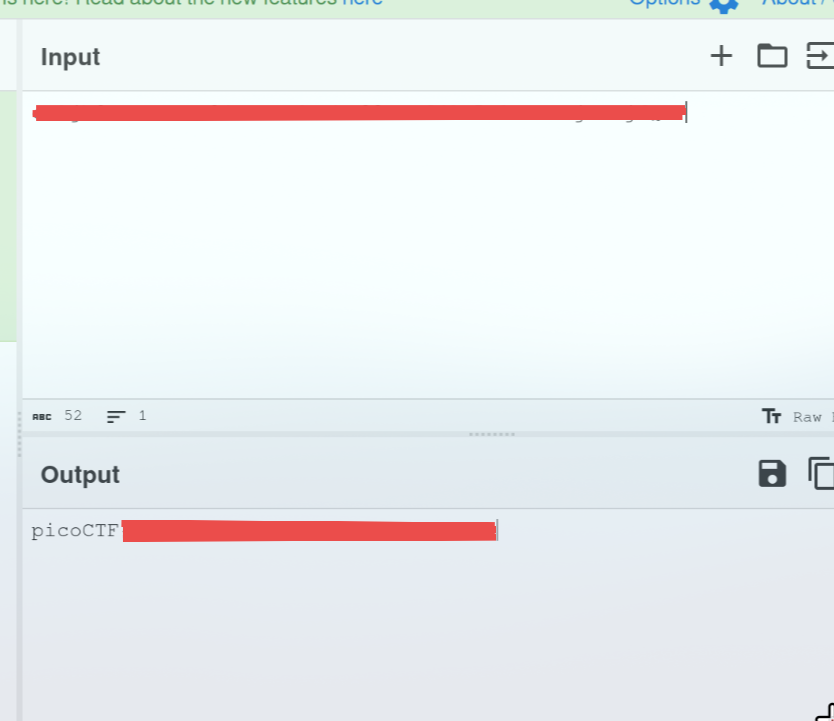


A requisição em questão contém um id criptografado, por isso, pode-se anotá-lo para utilizar depois.

Passando a requisição, é possível obter outro texto criptografado.



Ao juntar os dois textos, percebemos que o texto possui símbolos de igual no final, o que pode significar que é criptografado em base 64.



**Conclusão**

O CTF em questão aborda conceitos de Web Exploitation e pode ser resolvido com relativamente pouco esforço. Apesar de, no início, fazer o usuário buscar pelo sistema principal da tela de busca, ao observar a dica o caminho antes descrito se torna obsoleto. Sabendo que deve-se checar o redirecionamento, ao utilizar o Burp Suite, rapidamente obtemos a flag. Pode ser considerado um CTF médio, pois caso o usuário seja novo em Web Exploitation, a tarefa acaba sendo mais desafiadora.

**Referências**

<https://play.picoctf.org/practice/challenge/349?category=1&difficulty=2&page=1>

<https://portswigger.net/burp>