Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Log Hunt - PicoCTF

| **Informações do documento** | |
| --- | --- |
| **Referência** | Renan Schiavotello |
| **N° Revisão** | 1 |
| **Data de publicação** | 20/10/2025 |
| **Link** | [Link para acessar o CTF](https://play.picoctf.org/practice/challenge/527?difficulty=1&page=1&search=&solved=0) |

| **Redação** | Renan Schiavotello | Estudante |
| --- | --- | --- |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

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

| **Informações do CTF** | |
| --- | --- |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | webshell |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

[Contextualização](#_mecptipwlz0) 2

[Desenvolvimento 3](#_2xvtpvhpbim5)

Download the [logs](https://challenge-files.picoctf.net/c_saffron_estate/cbaf5310acc7fcfe879881106e90b1a3de92a961934567f7543bcd96c4aef977/server.log) and figure out the full flag from the fragments. [3](#_q2hj9skrrm4j)

[Conclusão](#_b2sbrgcpd986) 4

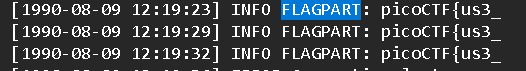
[Referências](#_kzmiwsvo7889) 4

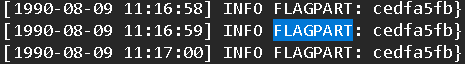
**Contextualização**

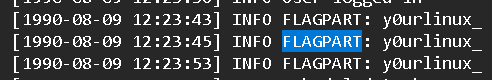
**O enunciado indica que a solução está escondida nos logs. Baixei o arquivo server.log e foquei em encontrar qualquer linha que parecesse conter fragmentos da flag.**

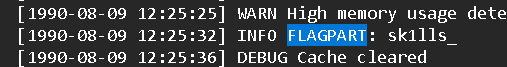
**Desenvolvimento**

1. Varredura por pistas  
    Antes de sair lendo tudo, procurei por marcadores explícitos. Termos como flag, flag, flagpart costumam ser usados para “quebrar” a flag em pedaços. No arquivo, dando um cntrl + f, várias entradas tinham o formato:









1. Confirmando ordem e montando a flag.

esses trechos aparecem durante o arquivo:

INFO FLAGPART: picoCTF{us3\_

INFO FLAGPART: y0urlinux\_

INFO FLAGPART: sk1lls\_

INFO FLAGPART: cedfa5fb}

Fazendo a concatenação obtemos a flag:

****

**Conclusão**

**É um CTF curto e simples que poderia ter sido resolvido utilizando webshell e comandos como por exemplo: grep -n "FLAGPART" server.log**

**Porém eu preferi por comodidade resolver apenas no bloco de notas mesmo.**

**Referências**

* **Plataforma: Pico CTF.**