Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

interencdec – PicoCTF

| **Informações do documento** | |
| --- | --- |
| **Referência** | interencdec – PicoCTF |
| **N° Revisão** | 0 |
| **Data de publicação** | 08/05/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/418 |

| **Redação** | Matheus da Cunha Castilho | Estudante |
| --- | --- | --- |
| **Revisão** | Sérgio Guidi Trovo | Orientador |
| **Aprovação** | Sérgio Guidi Trovo | Diretor |

| **Histórico de revisões** | | |
| --- | --- | --- |
| **N°** | **Entregas** | **Descrição** |
| **0** | 08/05/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

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

**Sumário**

[Contextualização](#_gjdgxs) [3](#_1t3h5sf)

[Desenvolvimento 3](#_30j0zll)

Descriptografia [3](#_2et92p0)

[Conclusão 3](#_tyjcwt)

[Referências 3](#_3dy6vkm)

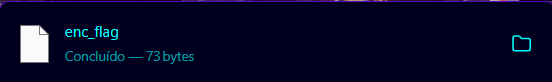
**Contextualização**

O desafio interencdec, disponível na plataforma PicoCTF, propõe uma atividade introdutória de criptografia voltada ao público iniciante em segurança da informação. Seu objetivo é fazer com que o participante identifique e compreenda diferentes camadas de codificação aplicadas a uma mensagem criptografada. Para isso, exige-se a aplicação de conhecimentos básicos como codificação Base64 e Cifra de César.

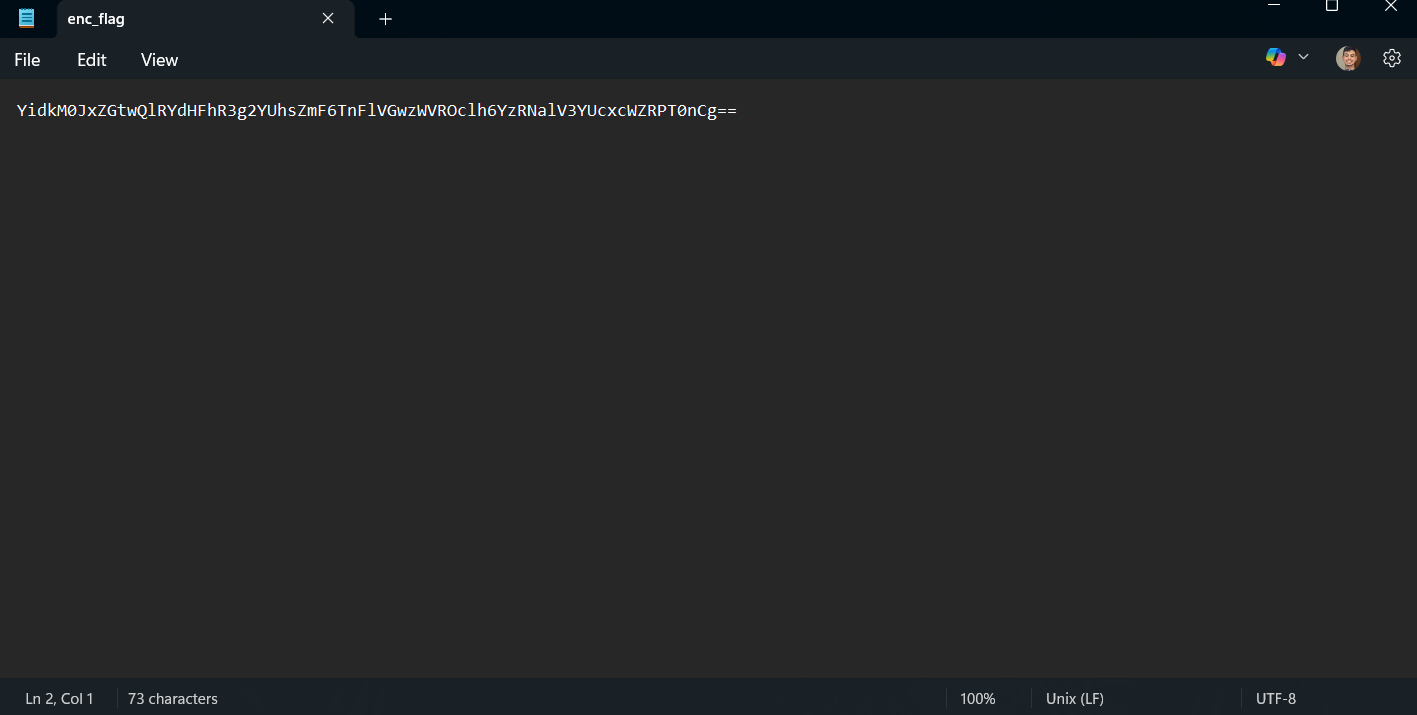
**Desenvolvimento**

**Descriptografia**

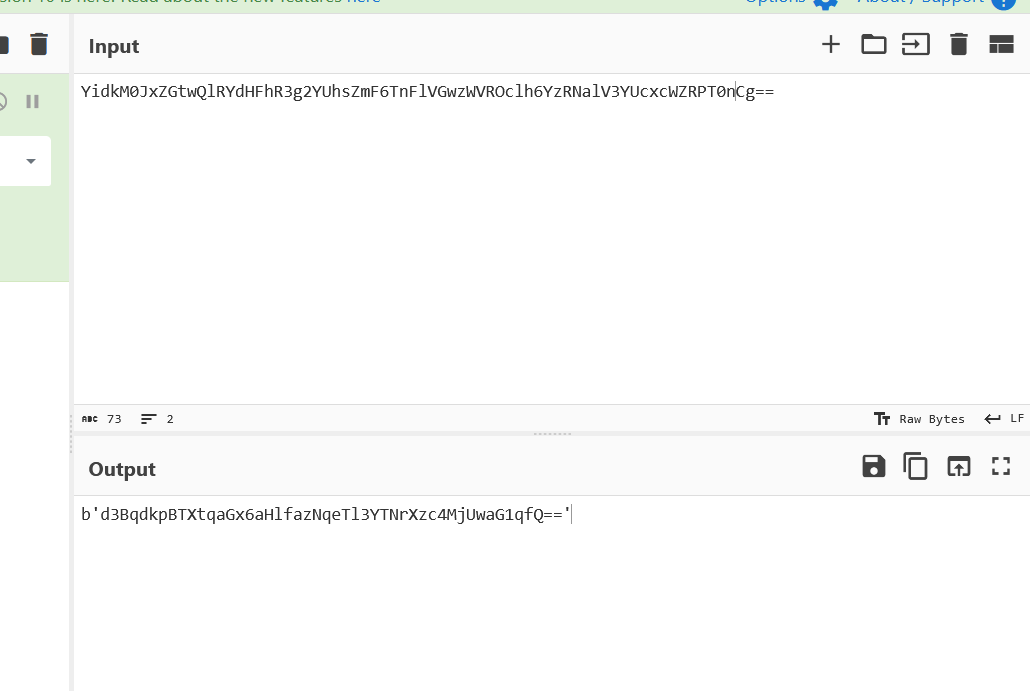
Ao iniciar o CTF, nos deparamos com o seguinte arquivo:



Ao abrí-lo com um editor de texto, foi possível observar o seguinte texto criptografado

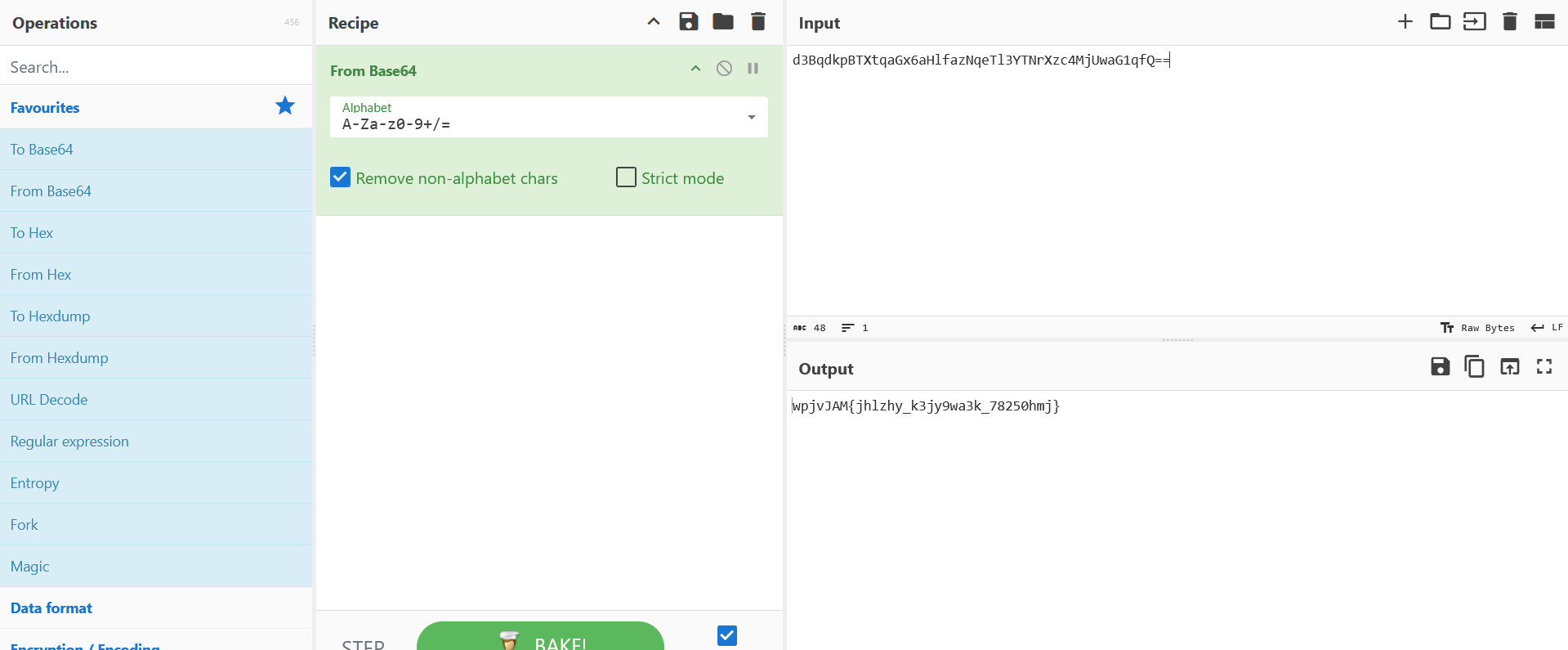


Então, como o texto contém dois sinais de “=” ao final, temos como ponto de partida provavelmente uma criptografia em base64. Então, ao jogá-lo na plataforma CyberChef, para buscar texto criptografado em base64, obtive isto.



Com isso, vemos outros sinais de igual ao final, podendo ser provavelmente outro base64, porém com alguns outros caracteres.

Ao tentar outro base64, me deparei com caracteres não legíveis, ou seja, provavelmente o texto não está devidamente formatado para ser descriptografado utilizando base64. Portanto, deve-se remover os caracteres extras do texto para impedir que ele retorne caracteres não legíveis, mantendo apenas o que está dentro das aspas.



Então, assim já foi possível obter um texto possivelmente no formato da flag, porém com caracteres trocados. Esse tipo de texto é característico de textos criptografados com Cifra de César, portanto podemos colocá-lo em alguma ferramenta com brute-force com Cifra de César para verificar se é possível encontrar textos legíveis. Com isso, obtemos a flag.



**Conclusão**

A resolução do desafio mostrou como é importante seguir etapas e analisar bem o que está sendo apresentado. Usando ferramentas como o CyberChef e o dCode, foi possível entender que a mensagem estava codificada em diferentes camadas, começando com base64 e depois com Cifra de César. Apesar de ser um desafio considerado fácil, ele ajuda a treinar o olhar para identificar padrões e reforçou conhecimentos básicos de criptografia, sendo muito útil para quem está começando na área de segurança da informação.

**Referências**

<https://gchq.github.io/CyberChef/>

<https://www.dcode.fr/>