Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Picker I - PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Picker I – PicoCTF |
| **N° Revisão** | 1 |
| **Data de publicação** | 14/03/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/400?category=3&page=1 |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 14/03/2025 | Produção |
| **1** | 14/03/2025 | Revisão |
| **2** | 14/03/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Média |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Engenharia Reversa, Criptografia, Lógica de Programação |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

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

[Desenvolvimento 3](#_30j0zll)

Servidor 3

Descriptografia6

[Conclusão](#_tyjcwt) 7

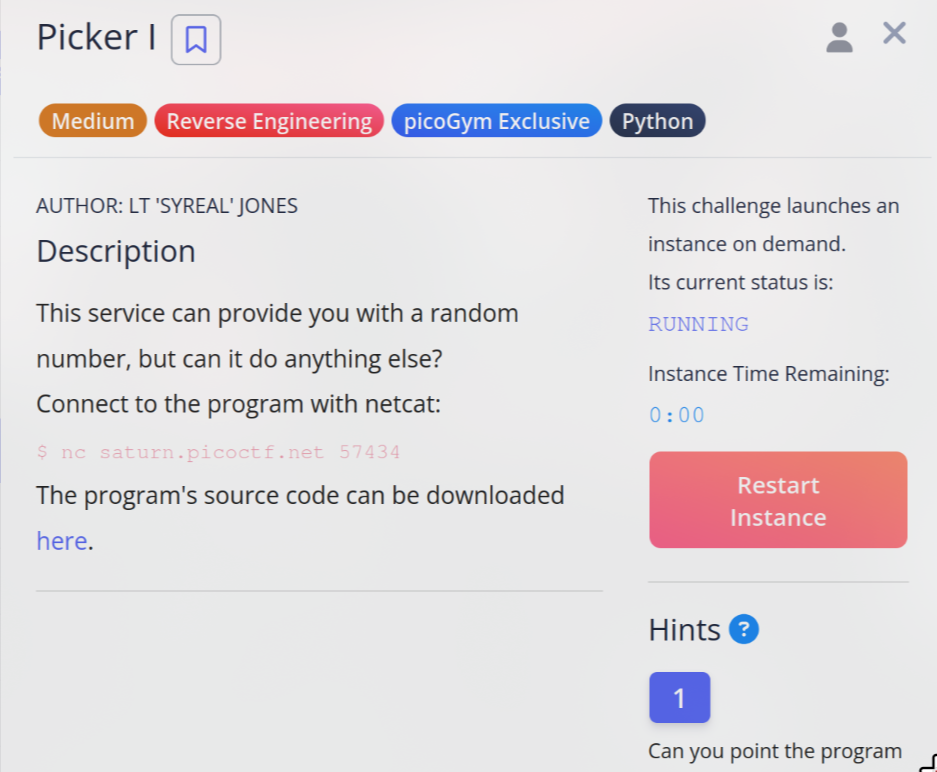
[Referências](#_3dy6vkm) 7

**Contextualização**

O CTF Picker I possui base em análise de código e lógica, exigindo que o usuário busque maneiras de lidar com as funções declaradas no servidor a fim de obter a flag. Pode ser considerado um CTF simples, que demanda apenas de conhecimento em lógica de programação, e um pouco de criptografia, para ser realizado.

**Desenvolvimento**

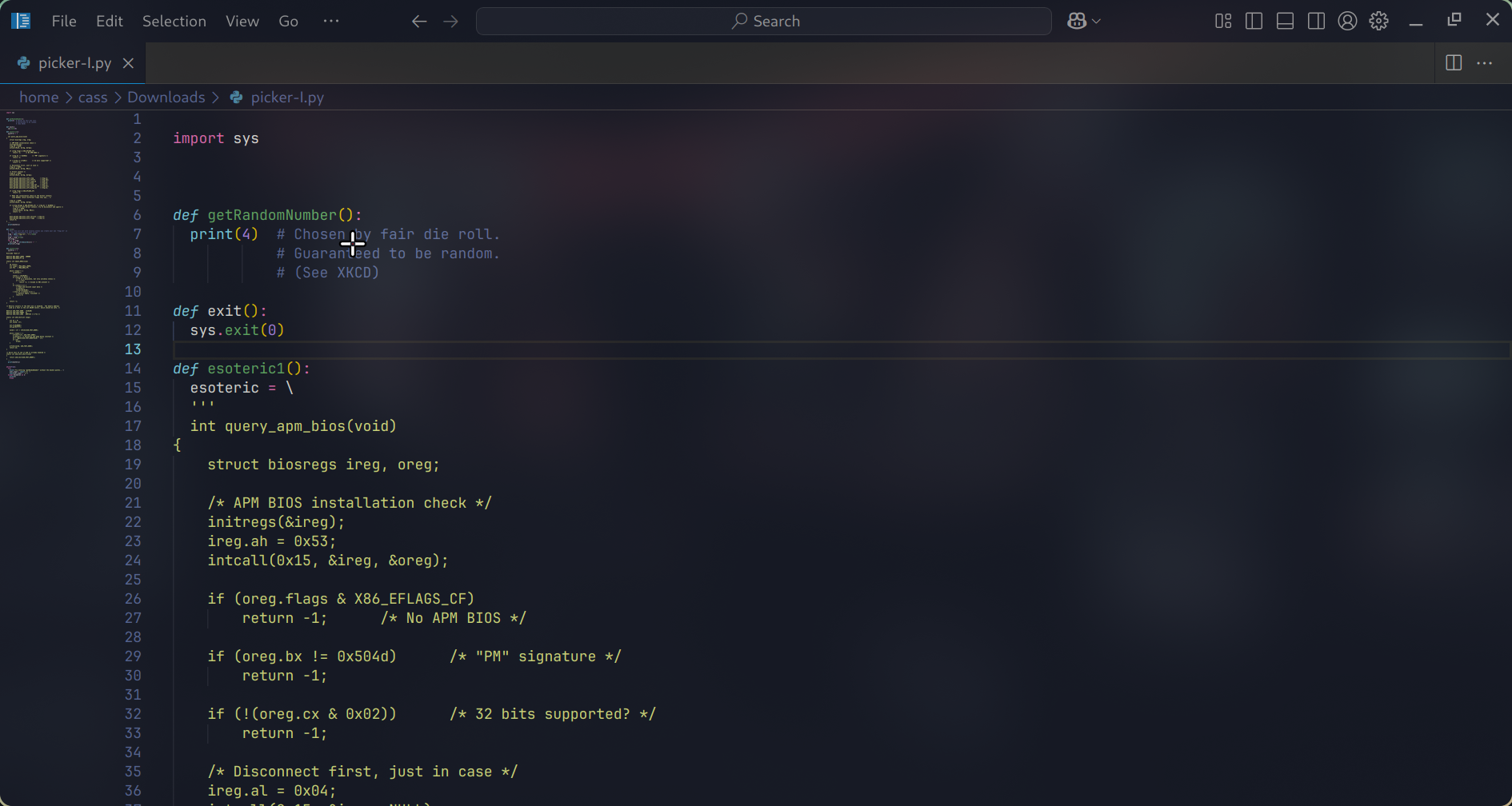
**Servidor**



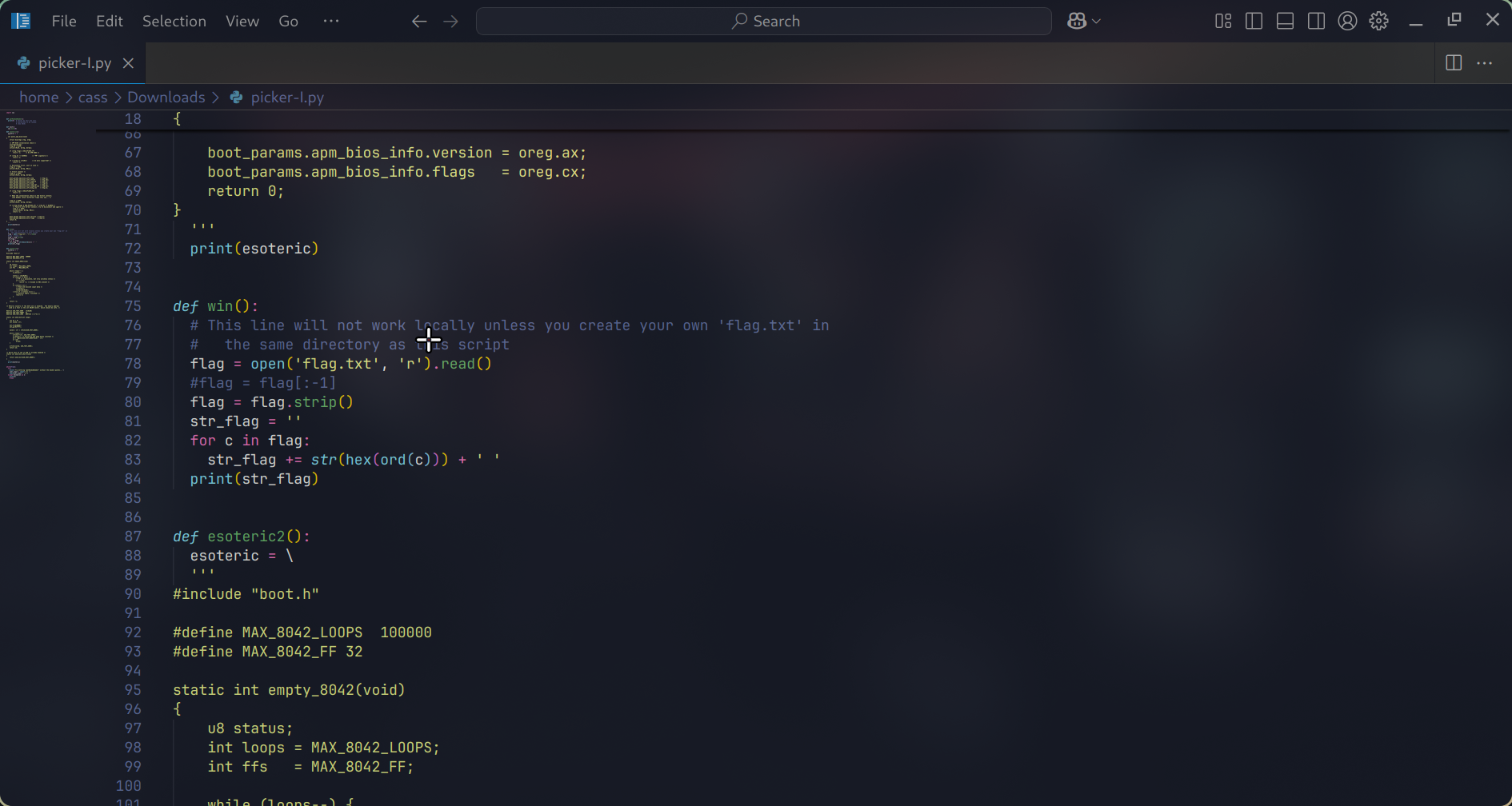
Ao iniciar a instância, obtemos um servidor para se conectar utilizando o *netcat*. Em seguida, ele pede para inserir o texto “getRandomNumber”, e ao inserir, obtemos sempre o número 4.



Ao analisar o código, vemos que essa função realmente retorna sempre o número 4. Também é possível observar algumas outras funções.



Uma destas funções, é a função “win”, que, ao analisar o código, percebemos que ela abre um arquivo chamado flag.txt no servidor e printa cada caractere desta flag em hexadecimal.

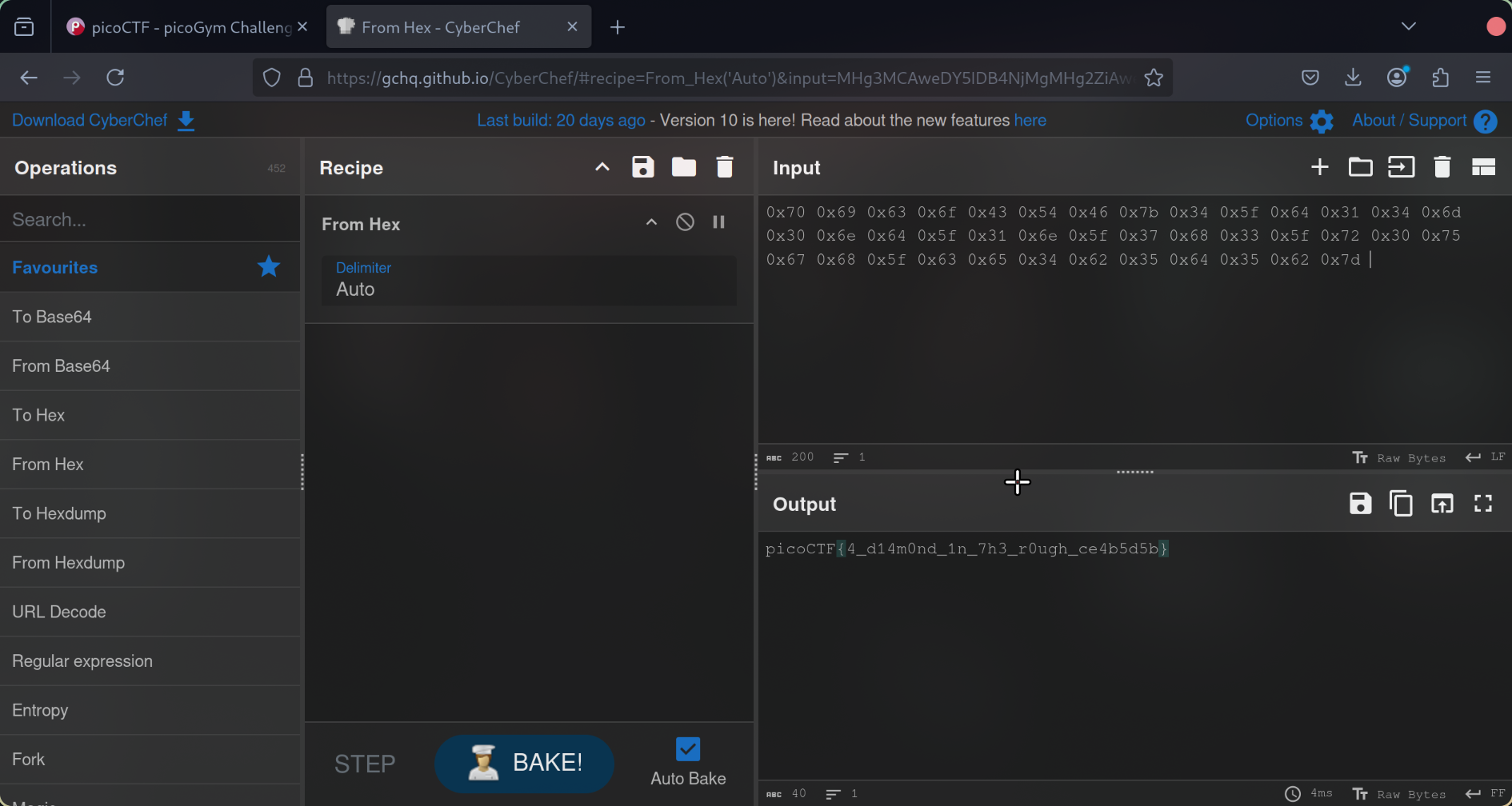


**Descriptografia**

Então, ao executar “win” no terminal com o servidor, obtemos um texto em hexadecimal.



Ao descriptografar, obtemos a flag.





**Conclusão**

O CTF realizado pode ser considerado um exercício básico para introdução à engenharia reversa, por conter tanto princípios de lógica, quanto de análise de código. Além disso, possui um hash simples para descriptografar e obter a flag, necessitando de conhecimentos básicos em hash para realizar. Com isso, conclui-se que o CTF em questão pode ser uma boa porta de entrada para iniciantes em engenharia reversa, e em programação.

**Referências**

<https://docs.oracle.com/cd/E36784_01/html/E36870/netcat-1.html>

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

<https://docs.python.org/3/library/functions.html#open>