Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Breaking Crypto the Simple Way – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Breaking Crypto the Simple Way – Gabriel Giardino Sprotte |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/09/2025 |
| **Link** | <https://tryhackme.com/room/breakingcryptothesimpleway> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Gabriel Giardino Sprotte | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 05/09/2025 | 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** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 2](#_Toc2022079500)

[Desenvolvimento 2](#_Toc992143722)

[Pergunta 1 2](#_Toc1702757565)

[Pergunta 2 3](#_Toc2032410099)

[Pergunta 3 4](#_Toc2053703304)

[Pergunta 4 5](#_Toc407853749)

[Pergunta 5 7](#_Toc1500777186)

[Conclusão 8](#_Toc541678796)

[Referências 9](#_Toc1287056854)

Contextualização

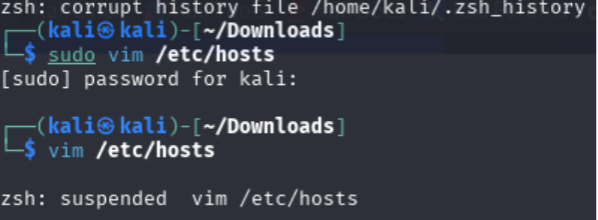
O CTF consiste em uma contextualização básica sobre criptografia.

Desenvolvimento

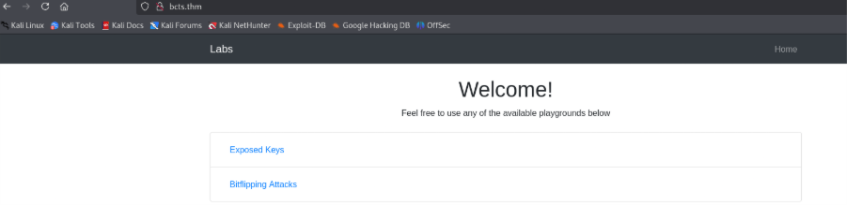
Pergunta 1

**- Inicialização da máquina**

Inicialmente conectamos com a VPN do TryHackMe, e posteriormente seguimos o passo para conseguir entrar no “bcts.thm”, modificando o “/etc/hosts”, colocando o ip gerado pelo TryHackMe, como mostrado a seguir.



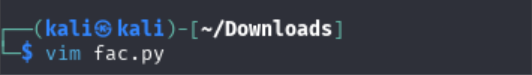
Aqui vemos que agora é possível entrar no site.

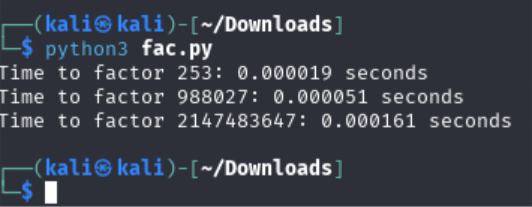


Pergunta 2

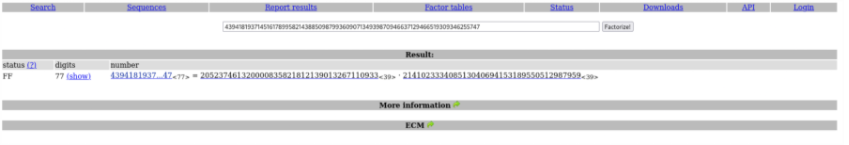
**– What is the flag?**

Este é o exemplo inicial sobre o tema, que é sobre a matemática do RSA, da fatoração de um número “n”, e assim posteriormente mostrando o tempo relativo de cada número.

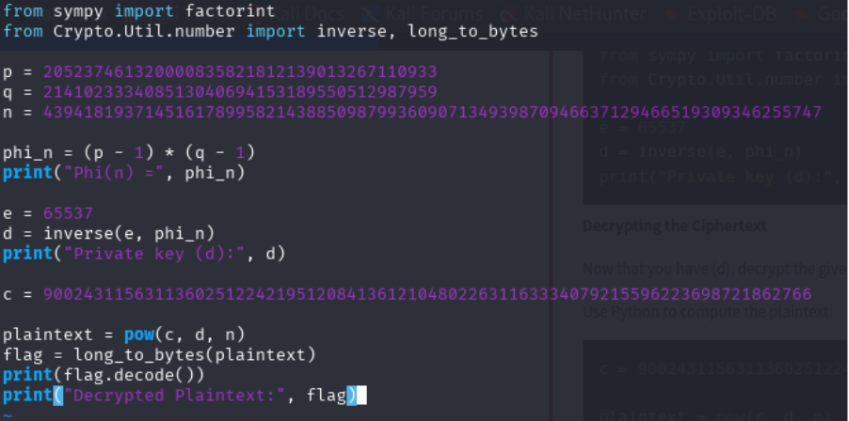




Agora no exercício, utilizando os códigos dados para descriptografar a chave RSA, abaixo está o valor do número P e Q, em base do número N dado.

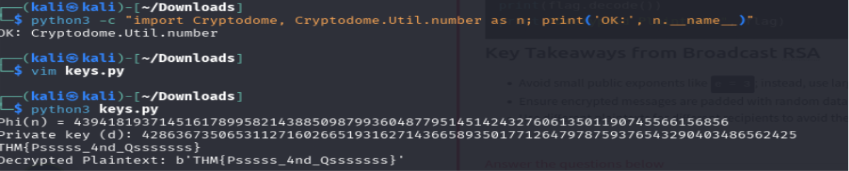


Acima mostra o resultado do site FactorDB, que calcula os números primos de N, sendo o primeiro número dado o P, e o segundo o Q.



Este é o código dado para instruir para fazer o exercício, porém especificamente no meu caso tive que trocar o import para “from Cryptodome.Util.number import inverse, long\_to\_bytes” conseguir funcionar o meu caso.





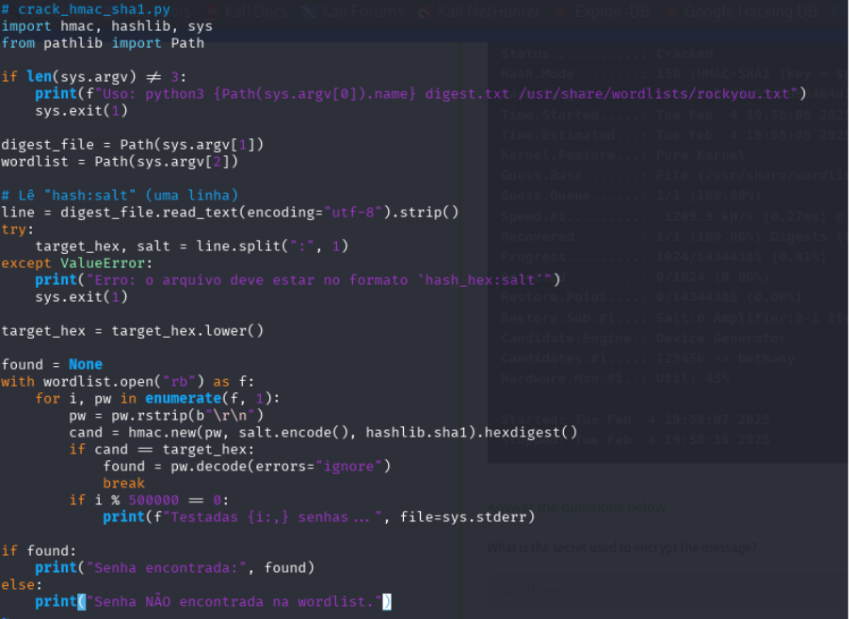
No fim sendo possível responder à questão encontrando a flag “THM{Psssss\_4nd\_Qsssssss}”.

Pergunta 3

**– what is the secret used to encrypt the message?**

A pergunta 3 é sobre hash, que basicamente é sobre criptografar alguma mensagem/transmissão e dentro dela possui vários tipos e com diferentes complexidades.

A parte da resolução é bem rápida, tendo que somente executar dois comandos, porém ao tentar realizar eles, apresentava um erro “Device #1: Not enough allocatable device memory for this attack.”, que basicamente acontece porque ele está usando o backend OpenCL “pocl” (CPU), que no sistema só permite buffers de 256 MB. Para vários modos (inclui o -m 150), isso não é suficiente, e para resolver isto foi criado um código em python que tem a mesma função.



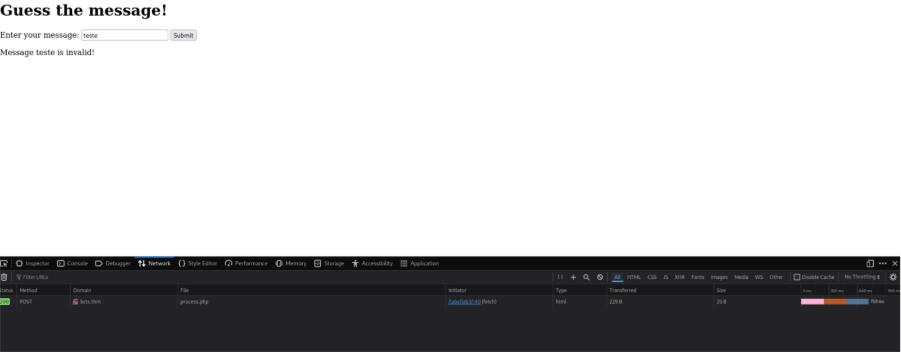


Assim encontrando a resposta sunshine.

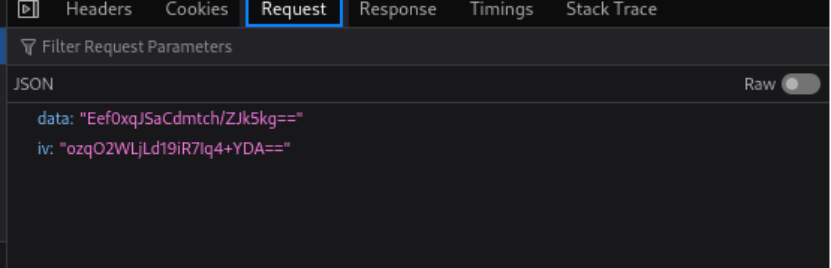
Pergunta 4

**– what is the flag?**

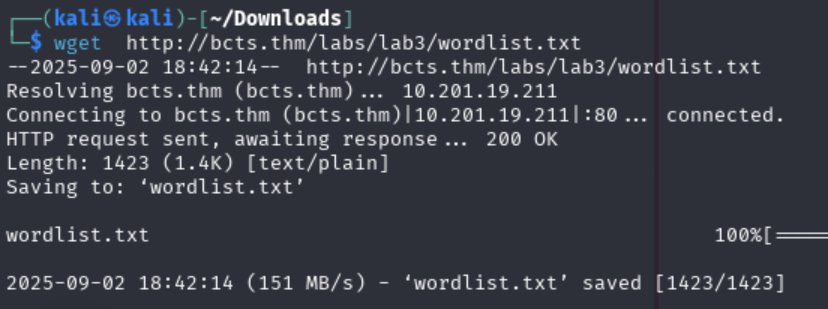
Inicialmente temos a imagem do site abaixo



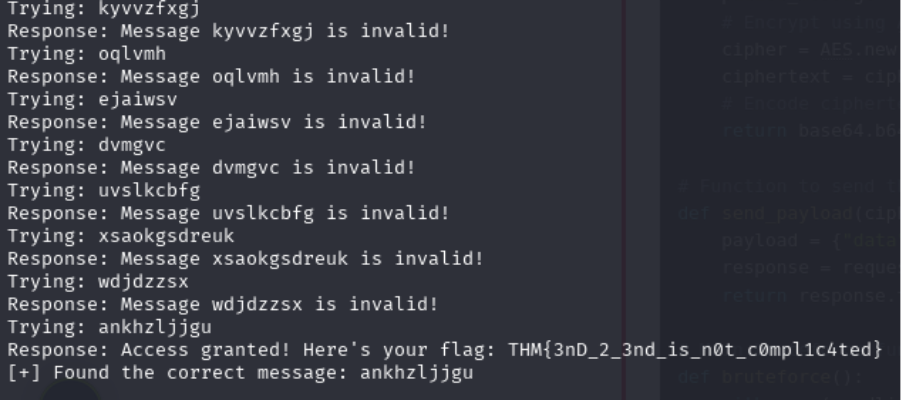
Que ao escrever uma mensagem, aparece uma mensagem criptografada na parte da requisição.



E vendo o código fonte da página, apresenta uma parte que a mensagem é alguma coisa aleatória que contém 16 bits, e com isso para facilitar é disponibilizado uma wordlist que possui varia alternativas delas.



E junto com o código disponibilizado foi possível encontrar qual é a mensagem certa.



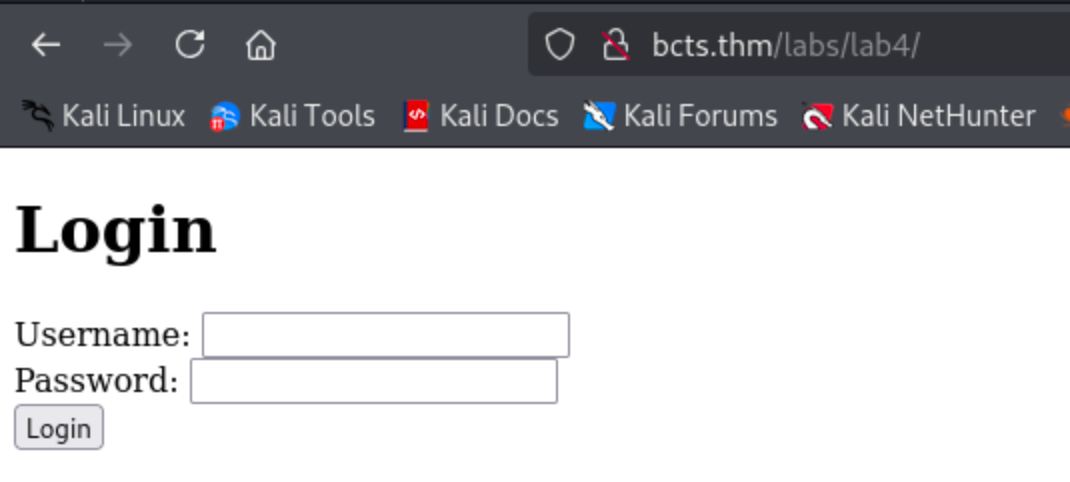
No fim colocando na página apresenta também a resposta.



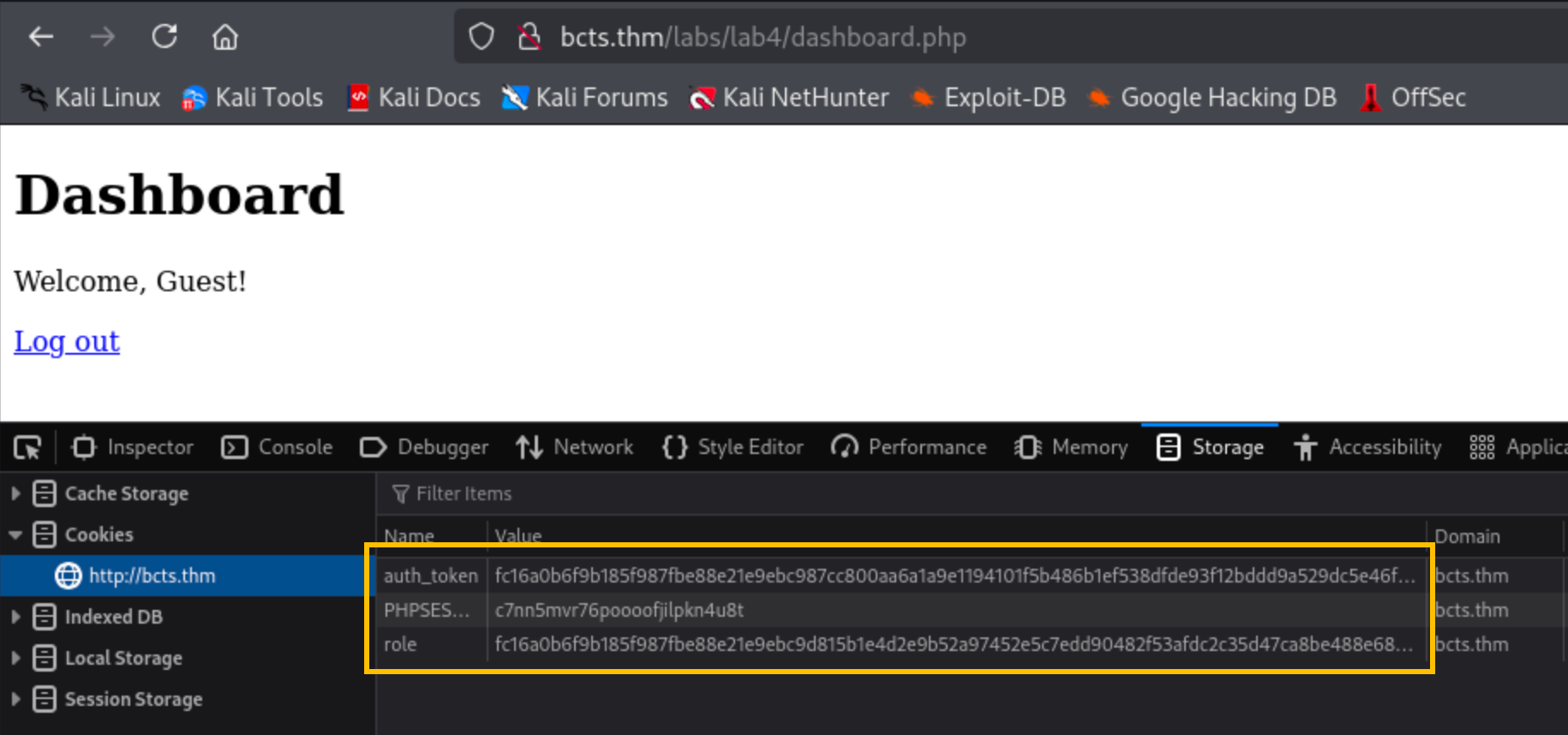
Pergunta 5

**– what is the flag?**

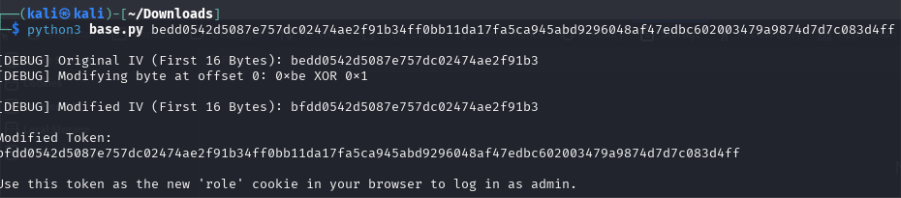
Agora por fim na última pergunta que é sobre bitflip com cookies.



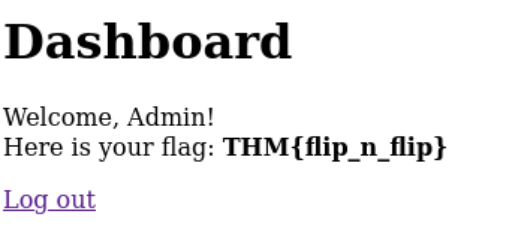
Aqui é a interface do lab4, que nele conseguimos fazer um login com usuário e senha, que ao entrar, indo na parte dos cookies, vemos que na parte do role, que seria nossa senha.



E neste caso, a codificação dele funciona de uma forma trocando o bit da senha criptografada, por exemplo de 0 para 1, e flipando este valor com XOR com 16 bits assim para depois fazer a troca, é possível identificar a senha do usuário do admin.



Na imagem acima, ela mostra a nossa senha antiga e após trocar o bit dela a nova modificada.



Portanto no fim sendo possível entrar no usuário do admin e finalizando o CTF.



Conclusão

O CTF Breaking Crypto the Simple Way, é um CTF bem simples, porém muito didático e um bom começo para aprender sobre criptografia.

Referências

<https://factordb.com/>