Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Crypto Failures – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Crypto Failures – Gabriel Giardino Sprotte |
| **N° Revisão** | 1 |
| **Data de publicação** | 21/09/2025 |
| **Link** | <https://tryhackme.com/room/cryptofailures> |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 21/09/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

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

**Sumário**

[Contextualização 2](#_Toc1044849095)

[Desenvolvimento 2](#_Toc1709063961)

[Pergunta 1 2](#_Toc275265700)

[Pergunta 2 6](#_Toc1729753733)

[Conclusão 8](#_Toc1689570429)

[Referências 8](#_Toc1523569552)

Contextualização

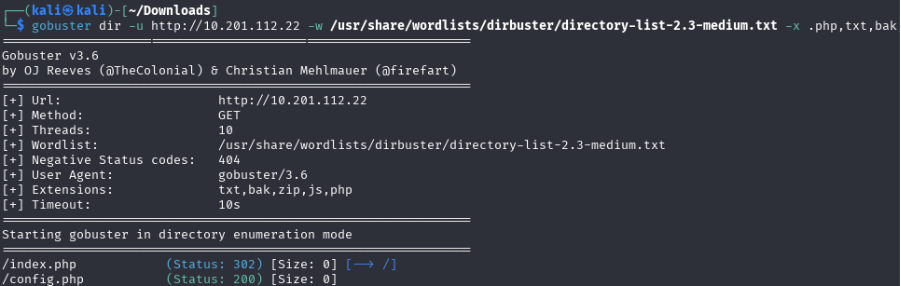
O CTF consiste em descriptografar cookies e conseguir encontrar as flags dentro de um usuário.

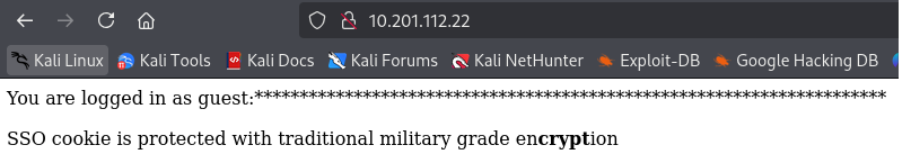
Desenvolvimento

Pergunta 1

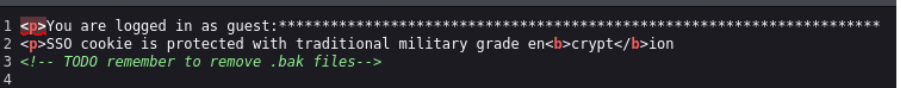
**- What is the value of the web flag?**

Inicialmente temos a página web do ip, junto sendo feito um nmap (possuindo as portas 22(tcp open ssh), 80(tcp open http) abertas), e um gobuster.





Junto com a página web temos também o código fonte que possui uma informação importante, que provavelmente possui um .bak.

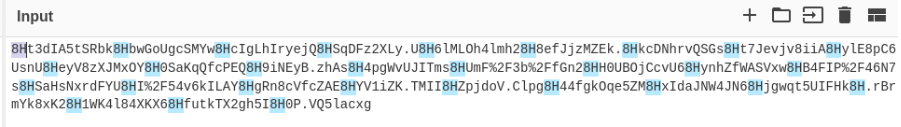


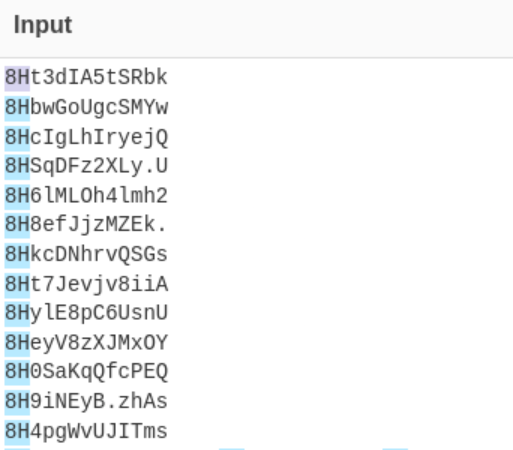
Assim junto com os diretórios encontrados no gobuster e a informação do .bak, tentamos colocar na url, o diretório do “index.php” junto com o bak para ver se é possível pegar alguma informação, e ao baixar ele, abrindo com o vim temos o php que mostra o código.





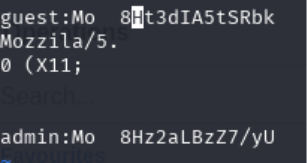
Analisando o código é possível ver a forma de como é feita a criptografa dos cookies, que tendo um usuário (user agent do kali), o “salt” que seria a repetição, e uma chave secreta, é gerada uma combinação padrão que sempre se repete depois de 13 caracteres, abaixo na imagem fica mais fácil de entender



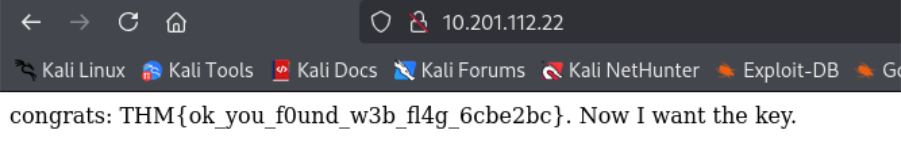


Assim tendo uma repetição sempre no “8H”, sendo a primeira string o valor do usuário, assim fazendo a mesma repetição trocando para admin conseguimos encontrar outro valor para ele.





Portanto ao trocar a primeira repetição que seria do “guest:Mo”, para a do “admin:Mo”, é possível encontrar a flag.



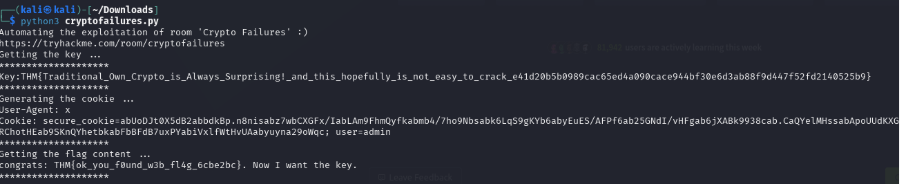
Pergunta 2

**– What is the encryption key?**

Agora temos que descobrir como que esta chave é criptografada, assim pesquisando um script para decodificar ela junto com a inteligência artificial para ajeitar o código para funcionar perfeitamente, temos o seguinte script.



No fim ao compilar ele, conseguimos encontrar a chave para encontrar a flag, assim finalizando o CTF.





Conclusão

O CTF Crypto Failures, é um CTF focado bem na parte de cookies, e tendo que ter uma boa análise para conseguir resolver ele.

Referências

<https://chatgpt.com/>