



Cibersegurança de Imersão (CTF)

Dia 01: Doninha – Cella 04

*Resumo: esta célula apresentará configurações incorretas do site que podem levar ao arquivo
exposição.*

Versão: 1.0

Conteúdo

I	Introdução	2
II	Instruções gerais	3
III	Instruções Comuns	4
4	Célula 04	5
V	Submissão e avaliação por pares	6

Capítulo I

Introdução

O que esta célula fará você ver:

- Aprenda segurança básica na web.

Capítulo II

Instruções gerais

A menos que seja explicitamente especificado, as seguintes regras serão aplicadas a cada célula desta Imersão.

- Este assunto é a única fonte confiável. Não confie em nenhum boato.
- Tenha cuidado com os direitos de acesso aos seus arquivos e pastas.
- Suas tarefas serão avaliadas por seus colegas de Imersão.
- Todas as atribuições de shell devem ser executadas usando `/bin/bash`.
- Você não deve deixar em seu repositório remoto quaisquer arquivos que não sejam os explicitamente solicitados pelo exercício.
- Você tem uma pergunta? Pergunte ao seu vizinho esquerdo. Caso contrário, tente a sorte com seu vizinho certo.
- Todas as respostas técnicas que você possa precisar estão disponíveis nas páginas de manual ou no Internet.
- Lembre-se de utilizar o servidor Discord dedicado à sua Imersão.
- Você deve ler atentamente os exemplos. Eles podem revelar requisitos que não são óbvios na descrição da tarefa.


Capítulo III

Instruções Comuns

- É proibido o uso de ferramentas automatizadas, a menos que especificado no assunto.
- Se nenhum outro formato for especificado, o formato do sinalizador será 42SP{this_is_a_test_flag}.
- As avaliações dos pares avaliarão a sua compreensão de como resolver cada desafio, por isso você deve ser capaz de explicar claramente tudo o que fez e os seus pares devem ser capazes de compreender a sua explicação.
- Os exercícios deste projeto seguem uma ordem estrita e você não poderá prosseguir para exercícios adicionais se não tiver concluído os anteriores (por exemplo, Você não pode fazer a célula01 sem completar a célula00).

Capítulo IV

Célula 04

	Célula: 04
Célula 04	
Diretório de entrega: weasel-cell04/ Arquivos para entrega: flag.txt	

Na mesma rede privilegiada onde Marvin capturou os pacotes trocados com o servidor da plataforma de mídia social, o endereço IP local do computador do seu alvo também foi registrado. Esta informação não seria muito significativa a menos que tivéssemos acesso à rede, permitindo-nos interagir com o endereço IP. Graças a Marvin, que plantou discretamente um computador do tamanho de um cartão de crédito na mesma infraestrutura analisada, agora possuímos acesso remoto à rede.

Com esse acesso, podemos realizar uma análise abrangente da rede e tentar nos infiltrar no seu alvo. O IP do seu alvo é 10.51.1.198 e sua missão é determinar se algum serviço está sendo executado no dispositivo do seu alvo.

Você deve conseguir localizar a bandeira.



Listagem de diretório.



O uso de ferramentas automatizadas não criadas por você não é permitido neste exercício.

Você precisará enviar o flag.txt na pasta correta e passar por seus pares.

Capítulo V

Envio e avaliação por pares

- Crie uma nova pasta 'weasel-cell04' e navegue até ela. Coloque seu arquivo 'flag.txt' dentro da pasta e empurre-o.



Observe que durante sua avaliação, qualquer coisa que não esteja presente na pasta da célula não será verificado.