Fundamentos de Segurança Informática

CTF para as semanas #8 e #9 (com início a 6/12 e 13/12)

Matéria relacionada: segurança web, injeção de comandos

Objetivo: Explorar vulnerabilidades de injeção

Semanas #8 e #9 - Desafio 1

Na porta 5003 do servidor ctf-fsi.fe.up.pt, encontra-se um servidor web em PHP. Este servidor tem uma funcionalidade de login que utiliza uma base de dados sql para guardar os dados dos utilizadores.

O teu objetivo é fazer login utilizando a conta de utilizador `admin`. Quando conseguires fazer login, a flag será apresentada na página web.

É fornecido o código fonte que é utilizado pelo servidor para interagir com a base de dados.

- Nota que não é necessário utilizar ferramentas de análise automática para explorar esta vulnerabilidade.*

Tarefas

- Explorar a aplicação como um utilizador final.
- Identificar na aula teórica sobre ataques web uma vulnerabilidade que permite fazer bypass ao login sem conhecer as credenciais
- Analisar o código fonte e tentar identificar se existe alguma das vulnerabilidades elencadas anteriormente.
- Identificar a linha onde o código está vulnerável e encontrar uma forma de explorar essa vulnerabilidade.
- Explorar a vulnerabilidade de forma a fazer login como utilizador `admin`. Submeter a flag que encontrares no desafio *Semanas #8 e #9 - Desafio 1*.

Enunciado CTF

Um possível enunciado para este desafio num CTF real seria:

Se conseguires fazer login como `admin`, consegues abrir o cofre e descobrir todos os seus segredos. Disponível em: http://ctf-fsi.fe.up.pt:5003

Semanas #8 e #9 - Desafio 2

Na porta 5000 do servidor ctf-fsi.fe.up.pt, encontra-se um servidor web em PHP. Este servidor é equivalente aos que estão disponíveis em muitos routers. Neste caso, a avaliação será feita numa perspetiva black-box, como acontece na maioria das análises a dispositivos *IoT*, onde não temos acesso ao código fonte.

Tarefas

- Que funcionalidades é que estão acessiveis a um utilizador sem este estar autenticado?
- Das funcionalidade que identificaste e do *feedback* que tiveste da sua utilização, pensa como é que estas podem estar implementatadas no servidor. Será que estão a utilizar algum utilitário linux?
- Se sim, que vulnerabilidades podem estar presentes na chamada deste utilitário?
- Verifica se existe alguma vulnerabilidade nesta funcionalidade.

- Identificada a vulnerabilidade, utiliza-a para aceder à flag que se encontra no ficheiro `/flag.txt`. A flag deve ser submetida no desafio *Semanas 8 e 9 - Desafio 2*.

Enunciado CTF

Um possível enunciado para este desafio num CTF real seria:

Olá! Comprei um novo router, diz que suporta 6G e é super rápido... Mas o fabricante é desconhecido e não sei se é seguro para usar em minha casa. Como tens a cadeira de FIS, achas que podes dar uma olhadela nele? Disponível em: http://ctf-fsi.fe.up.pt:5000

Última alteração: segunda, 20 de dezembro de 2021 às 00:53

◄ Tarefas para a semana #8 e #9 (com início a 6/12 e 13/12)

Ir para...

Tarefas para a semana #10 (com início a 3/1/2022) ►