Fundamentos de Segurança Informática

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

Semana #10 - Desafio 1

Na porta 5002 do servidor ctf-fsi.fe.up.pt, encontra-se um servidor web.
Neste serviço podes fazer um pedido ao administrador para que te dê acesso à flag. O adminstrador vê todos os pedidos, mas não existe registo de alguma vez ter dado a flag a alguém. O teu objetivo é dar uma boa justificação ;) de forma a convencer o administrador a fornecer flag.

O administrador irá visitar a página com a tua justificação (que é exatamente igual à que tu vês no entanto com os dois botões ativos) e marcará o pedido como não aceite ao clicar no "Mark request as read", isto faz com que uma mensagem te apareça a dizer que o teu pedido não foi aprovado. A página faz *refresh* de 5 em 5 segundos e a resposta do administrador ao teu pedido pode demorar até 2 minutos.

Tarefas

- Explora a plataforma como um utilizador comum, faz um pedido e espera que este seja visto pelo administrador.
- Verifica se existe alguma vulnerabilidade no formulário de submissão da justificação. Qual é? Consegues usá-la para que o teu pedido seja aprovado?
- Cria uma exploit que explore esta vulnerabilidade e faça com que o teu pedido seja aprovado. Envia-a para o administrador. A flag que obtiveres é para ser submetida no desafio *Semanas #10 - Desafio 1*.

Enunciado CTF

Um possível enunciado para este desafio num CTF real seria:

Criámos um novo serviço que oferece uma flag às melhores jusitificações. Estás convidado a tentar a tua sorte. Disponível em: http://ctf-fsi.fe.up.pt:5002

Semanas #10 - Desafio 2

São fornecidos dois ficheiros: um executável (`program`) e o código fonte (`main.c`). Nota que não deves compilar o ficheiro `main.c`: deves utilizar o executável que é te dado que corresponde ao programa `main.c` compilado e que é extamente o mesmo que se encontra no servidor.

Deves utilizar e adaptar o script que te foi dado anteriormente para resolver este desafio.

Tarefas

- Deves começar por correr o `checksec` e analisar quais são as suas proteções e que tipo de ataques é possível fazer.
- De seguida, deves analisar o código-fonte e responder às seguinte questões:
  - Qual é a linha do código onde a vulnerabilidade se encontra?
  - O que é que a vulnerabilidade permite fazer?
- Cria uma exploit que te permita chamar uma shell no servidor de forma a obter a flag que se encontra no *working directory* do programa.
- Submete a flag no desafio *"Semanas 10 - Desafio 2"*.

Enunciado CTF

Um possível enunciado para este desafio num CTF real seria: Tens uma stack com permissão de execução e um buffer overflow. O que é será que podes fazer? Disponível em: `nc ctf-fsi.fe.up.pt 4001`

Última alteração: quarta, 12 de janeiro de 2022 às 12:35

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

Ir para...

Tarefas para a semana #11 (com início a 10/1/2022) ►