

# Fundamentos de Segurança Informática

[Painel do utilizador](#)[As minhas unidades curriculares](#)[Fundamentos de Segurança Informática](#)[Aulas Teorico-Práticas](#)[CTF sara a semana #6 \(com início a 22/11\)](#)

## CTF sara a semana #6 (com início a 22/11)

**Matéria relacionada:** usurpação de controlo usando format string vulnerabilities

**Objetivo:** Explorar format string vulnerabilities

**Contexto:**

### Semana 6 - Desafio 1

É fornecido um ficheiro ZIP com um executável (`program`) e o código fonte (`main.c`). A flag encontra-se num ficheiro `flag.txt` que é lido pelo programa. (A flag no zip é dummy, a válida só se encontra no servidor...) Além de tudo isto, fornecemos novamente um script para facilitar o desenvolvimento da exploit, com algumas explicações de como é que o podem usar em parceria com o `gdb`.

#### Tarefas

- Deves começar por correr o `checksec`. Ao contrário da última vez, este programa tem algumas proteções ativas. Deves concluir quais são as proteções e que tipo de ataques é possível fazer.
- De seguida deves analisar o código-fonte e responder às seguintes questões:
  - Qual é a linha do código onde a vulnerabilidade se encontra?
  - O que é que a vulnerabilidade permite fazer?
  - Qual é a funcionalidade que te permite obter a flag?
- Sabendo que a flag se encontra numa variável global ;) e como no `checksec` percebemos que o endereço do programa são estáticos, utiliza o `gdb` para descobrir o endereço de memória da variável onde se encontra a flag.
- Com o endereço da flag e com a vulnerabilidade que encontraste anteriormente, é possível ler a flag da memória e imprimi-la no `stdout`. Esta deve ser submetida no desafio "Semana 6 - Desafio 1".

#### Enunciado CTF

Um possível enunciado num CTF real para este desafio seria o seguinte.

*Continuamos a ter problemas no nosso serviço "FormatRead". Por isso, desativámos a possibilidade de ganhar o desafio, e sairás sempre a perder. Desafio disponível em: `nc ctf-fsi.fe.up.pt 4004`*

### Semana 6 - Desafio 2

É fornecido um ficheiro ZIP com um executável (`program`) e o código fonte (`main.c`). A flag encontra-se no ficheiro `flag.txt`.

#### Tarefas

- Deves começar por correr o `checksec` e analisar o seu output ...
- De seguida, deves analisar o código fonte e responder às seguintes questões:
  - Qual é a linha do código onde a vulnerabilidade se encontra? E o que é que a vulnerabilidade permite fazer?
  - A flag é carregada para memória? Ou existe alguma funcionalidade que podemos utilizar para ter acesso à mesma.
  - Para desbloqueares essa funcionalidade o que é que tens de fazer?
- Deves utilizar a vulnerabilidade que encontraste de forma a re-escrever a variável que te permite ter acesso à flag.

- Finalmente, só tens de abrir o ficheiro `flag.txt` e submeter no desafio "Semana 6 - Desafio 2".

### Enunciado CTF

Um possível enunciado num CTF real para este desafio seria o seguinte.

*O nosso software "FormatWrite" tem uma special feature para fazer administração remota, mas só os nossos técnicos é que a podem usar.  
Desafio disponível em: `nc ctf-fsi.fe.up.pt 4005`*

Última alteração: sexta, 19 de novembro de 2021 às 19:37

[◀ Tarefas para a semana #6 \(com início a 22/11\)](#)

Ir para...

[Tarefas para a semana #8 e #9 \(com início a 6/12 e 13/12\) ▶](#)

Tecnologias Educativas - 20 anos na U.Porto



[Requisitos mínimos utilização](#)

[Portal de e-learning](#)

[Ajuda Moodle](#)

[Inovação Pedagógica](#)

Nome de utilizador: Marcelo Henriques Couto ([Sair](#))

[FEUP-L.EIC021-2021/2022-1S](#)

[Português \(pt\)](#)

[Deutsch \(de\)](#)

[English \(en\)](#)

[Français \(fr\)](#)

[Português \(pt\)](#)

[Obter a Aplicação móvel](#)