Aula TP - 27/05/2019

Estes exercícios já não têm um cariz de avaliação.

Nota:

Grave os ficheiros na diretoria Aula 13 para a sua máquina local na diretoria /home/user/Aulas/Aula13 .

Exercícios

1. Validação de Input

Experiência 1.1

Analise os ficheiros InputValidation.cpp e InputValidation.java.

1. Explique os dois problemas: (i) utilização do cin/Scanner para leitura, (ii) acesso ao array
2. O que alterava?

Experiência 1.2

Analise o ficheiro WhileEx.java.

1. Qual o(s) problema(s) no input do programa?
2. Altere o programa de modo a validar todo o input e recuperar apropriadamente dos erros.

Experiência 1.3

Analise o ficheiro Input.cpp.

1. Qual o(s) problema(s) no input do programa ?
2. Altere o programa de modo a validar todo o input e recuperar apropriadamente dos erros.

Experiência 1.4

Analise o ficheiro Input.java.

1. Qual o(s) problema(s) no input do programa ?
2. Altere o programa de modo a validar todo o input e recuperar apropriadamente dos erros.

Experiência 1.5

Analise o programa filetype.c que imprime no ecran o tipo de ficheiro passado como argumento.

1. Existem pelo menos dois tipos de vulnerabilidades estudadas na aula teórica de "Validação de Input" que podem ser exploradas. Identifique-as.

2. Forneça o código/passos/linha de comando que permitem explorar cada uma das vulnerabilidades identificadas na linha anterior.
3. O que aconteceria se o seu programa tivesse permissões *setuid root*?

Experiência 1.6

Analise o programa readfile.c que imprime no ecran o conteúdo do ficheiro passado como argumento, a que acrescenta o sufixo ".txt" de modo a garantir que só deixa ler ficheiros em texto.

1. Existem pelo uma vulnerabilidade estudada na aula teórica de "Validação de Input" (em conjunto com outra que já estudou) que permite que o programa imprima ficheiros que não terminam em ".txt". Explique.
2. Indique a linha de comando necessária para aceder ao ficheiro */etc/passwd*.

Experiência 1.7

Analise o ficheiro string_formato.c com o exemplo de vulnerabilidade de string de formato dado na aula, e o ficheiro string_formato2.c já sem essa vulnerabilidade.

1. Faça algumas experiências com vários valores de input tanto com o programa com vulnerabilidades como sem vulnerabilidades e tire as suas conclusões.

2. Princípios de projeto de software

Experiência 2.1

Considere os princípios de projeto de software e indique, justificando, qual (ou quais) dos princípios é o mais diretamente violado em cada uma das seguintes situações:

- Uma empresa que produz componentes relacionadas com segurança não divulga detalhes sobre o projeto/desenho desses componentes, alegadamente por “razões de segurança”
- Uma aplicação descarrega código da Internet e inicia a sua execução sem perguntar ao utilizador se quer iniciar a execução desse código.