Universidade do Minho

Mestrado Integrado em Engenharia Informática

Engenharia de Segurança

Aula 10 - Vulnerabilidade de inteiros

Grupo 8

João de Macedo
A76268

João Aloísio
A77953

Nelson Gonçalves
A78173

1 de Maio de 2020

1 Pergunta 1.1

1.1 Qual a vulnerabilidade que existe na função vulneravel() e quais os efeitos da mesma?

Na função *vulneravel* existe uma vulnerabilidade que consiste na declaração das variáveis i e j como inteiros, sendo que estes podem ser incrementados até o tamanha de x e y que são do tipo *size_t*. O nosso compilador diz nos que *size_t* tem 8 bytes de tamanho enquanto que um inteiro tem 4 bytes. Sendo assim, quando as variáveis i e j ultrapassarem o valor permitido para um inteiro, no caso em que x e y sejam maiores que esse valor, vai ocorrer um overflow de inteiro. Isto poderá causar um comportamento inesperado do programa, visto que pode causar um erro como pode chegar apenas ao valor máximo de um inteiro e abortar o ciclo.

1.2 Complete o main() de modo a demonstrar essa vulnerabilidade.

A resolução encontra-se no ficheiro *over_vuln.c*.

1.3 Ao executar dá algum erro? Qual?

Para poder correr o código foi comentado a linha em que escrevia na matriz. Após correr este inteiro i só vai até o seu valor máximo, ou seja, 2147483647 como se pode ver na figura:

2 Pergunta 1.2

2.1 Qual a vulnerabilidade que existe na função vulneravel() e quais os efeitos da mesma?

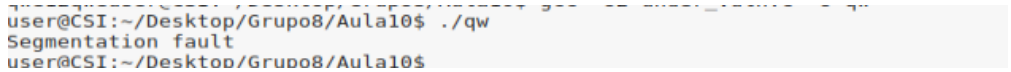
Nesta função a vulnerabilidade existente consiste na verificação tamanho < MAX_SIZE não é verificado para valores negativos, sendo que na instrução a seguir irá tentar alocar memória para a variável destino com um númeor de bytes negativo. Ocorrerá um erro em que irá parar com o programa.

2.2 Complete o main() de modo a demonstrar essa vulnerabilidade.

A resolução encontra-se no ficheiro *under_vuln.c*.

2.3 Ao executar dá algum erro? Qual?

Ao executar o código ocorre *segmentation fault* como se pode comprovar com a imagem:



2.4 Utilize as várias técnicas de programação defensiva introduzidas na aula teórica para mitigar as vulnerabilidades.

A tecnica utilizada para mitigar a vulnerabilidade acima foi a validação do input e a validação de possíveis underflows. A resolução encontra-se no ficheiro under_solu.c