Universidade do Minho
Criptografia e Segurança da Informação
Departamento de Informática

Engenharia de Segurança

TP6 - Aula 9

Grupo 7
Carlos Pinto Pedrosa A77320
José Francisco Gonçalves Petejo e Igreja Matos A77688
7 de Abril de 2019

Conteúdo

1 Vulnerabilidade de codificação

1.1 Pergunta 1.1

Através da informação sobre o número de linhas de código, é possível concluir que o *facebook* possui 62 milhoões de linhas de código. Visto que se trata de um serviço com capacidades de segurança que têm vindo a ser questionadas ao longo dos anos, iremos considerar um rácio de bugs de 30 por cada 1000 linhas de código, sendo assim, a estimativa seria de 1.86 milhoões de *bugs*. Para software de automóveis, cerca de 15 bugs por 1000 linhas logo, e considerando 100 milhões de linhas de código, estima-se 1.5 milhões de bug. O *Linux 3.1* possui 15 milhões de linhas de código e estimando 20 bugs por 1000 linhas, estima-se 300.000 *bugs* Por fim, os serviços de internet da *google* possuem 2 biliões de linhas de código, e como se trata de um serviço do mais alto nivel consideramos 10 bugs por 1000 linhas, estima-se 20 milhões de *bugs*.

Perceber quanto destes *bugs* se tratam de vulnerabilidades é uma tarefa extremamente complicada, visto que não existem estimativas próximas, então teria de se analisar e testar o código múltiplas vezes para as encontrar.

1.2 Pergunta 1.2

1.2.1 Vulnerabilidades de Projeto

- Incomplete Blacklist - Quando um determinado projeto possui uma *lista negra* de valores que não podem ser aceites, mas a identificação desses valores não contém todos esses valores.

- Improper Authentication - Esta vulnerabilidade consiste numa inexistência do processo de verificação de autenticação para provar que esse utilizador representa de facto o utilizador que demontra ser.

1.2.2 Vulnerabilidades de Codificação

- SQL Injection - A não validação dos inputs inseridos pelo utilizador correta, neste caso através da utilização de *magic quotes* de php permite ao atacante obter permissões de administrador do sistema

- Improper Verification of Cryptographic Signature - A verificação incorreta da assinatura criptográfica pode levar a roubos de identidade e deixar o sistema vulnerável.

1.2.3 Vulnerabilidades Operacionais

- CWE-303: Incorrect Implementation of Authentication Algorithm - Uma falha da implementação do algoritmo de autenticação leva à possibilidade de um adversário poder ultrapassar esse mecanismo de segurança e entrar no sistema, deixando o vulnerável

- CWE-1068: Inconsistency Between Implementation and Documented Design - Esta falha representa algo por vezes menosprezado pelas equipas informáticas responsáveis pelo desenvolvimento do projeto, a documentação. A incosistência desta com o produto desenvolvido dificulta a capacidade de manter o software atualizado, afetando indiretamente possíveis vulnerabilidades, visto que torna-se mais dispendioso corrigir potenciais erros.

1.3 Pergunta 1.3

Uma vulnerabilidade de dia zero trata-se de uma vulnerabilidade não conhecida pela comunidade informática, mas sim por um grupo restrito de pessoas, quer sejam atacantes na *dark-web* ou segurança informática do sistema militar de um país. As outras vulnerabilidades estudadas ao longo desta ficha, são vulnerabilidades que a comunidade informática já conhece e as catalogou corretamente.