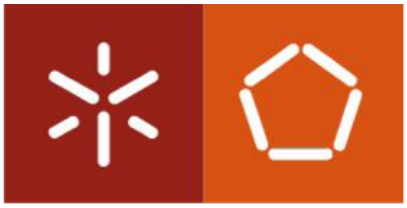

Universidade do Minho
Departamento de Informática
Mestrado Integrado em Engenharia Informática

Engenharia de Segurança

Aula 8

Diana Lopes, nº a74944
Gabriela Vaz, nº a74899

Conteúdo

0.1 Pergunta P1.1

De acordo com `https://informationisbeautiful.net/visualizations/million-lines-of-code` sabemos que:

- o Facebook tem 61 milhões de linhas de código;
- software de automóveis tem 100 milhões de linhas de código;
- o Linux 3.1 tem 15 milhões de linhas de código;
- os serviços de internet da Google têm 2 biliões de linhas de código.

Assim, tendo em conta que qualquer pacote de *software* tem entre 5 a 50 *bugs* por cada mil linhas de código, facilmente se conclui que a qualquer pacote de *software* tem entre $(linhasdecodigo) * 5/1000$ e $(linhasdecodigo) * 50/1000$ *bugs*. Ou seja,

- o Facebook tem entre 305000 e 3050000 *bugs*;
- *software* de automóveis tem entre 500000 e 5000000 *bugs*;
- o Linux 3.1 tem entre 75000 e 750000 *bugs*;
- os serviços de internet da Google têm entre 1000000 e 10000000 *bugs* (assumindo que 1 bilião corresponde a mil milhões).

Não há forma de relacionar o número de *bugs* com o número de vulnerabilidades.

0.2 Pergunta P1.2

CWE VIEW: Weaknesses Introduced During Design

View ID: 701
Type: Implicit

Objective

This view (slice) lists weaknesses that can be introduced during design.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Modes_Of_Introduction/Introduction/Phase='Architecture and Design']

Membership

Nature	Type	ID	Name
HasMember	V	6	J2EE Misconfiguration: Insufficient Session-ID Length
HasMember	V	7	J2EE Misconfiguration: Missing Custom Error Page
HasMember	V	8	J2EE Misconfiguration: Entity Bean Declared Remote
HasMember	V	9	J2EE Misconfiguration: Weak Access Permissions for EJB Methods
HasMember	V	13	ASP.NET Misconfiguration: Password in Configuration File
HasMember	C	20	Improper Input Validation
HasMember	C	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
HasMember	V	24	Path Traversal: '../filedir'
HasMember	B	36	Absolute Path Traversal
HasMember	B	66	Improper Handling of File Names that Identify Virtual Resources
HasMember	V	67	Improper Handling of Windows Device Names
HasMember	V	69	Improper Handling of Windows ::DATA Alternate Data Stream
HasMember	V	72	Improper Handling of Apple HFS+ Alternate Data Stream Path
HasMember	C	73	External Control of File Name or Path
HasMember	C	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Figura 1: `https://cwe.mitre.org/data/definitions/701.html`

CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length

Weakness ID: 6
Abstraction: Variant
Structure: Simple
Status: Incomplete

Presentation Filter: Basic

Description

The J2EE application is configured to use an insufficient session ID length.

Extended Description

If an attacker can guess or steal a session ID, then they may be able to take over the user's session (called session hijacking). The number of possible session IDs increases with increased session ID length, making it more difficult to guess or steal a session ID.

Relationships

Figura 2: Vulnerabilidade de Projeto.

0.3 Pergunta P1.3

As vulnerabilidades dia-zero são vulnerabilidades desconhecidas pelo *software*. Por causa dessa característica, os interessados em corrigir essa vulnerabilidade não podem atuar, pois não têm conhecimento sobre ela. É isto que faz com que este tipo de vulnerabilidades seja mais perigoso do que as outras vulnerabilidades, que podem ser corrigidas mal são descobertas.

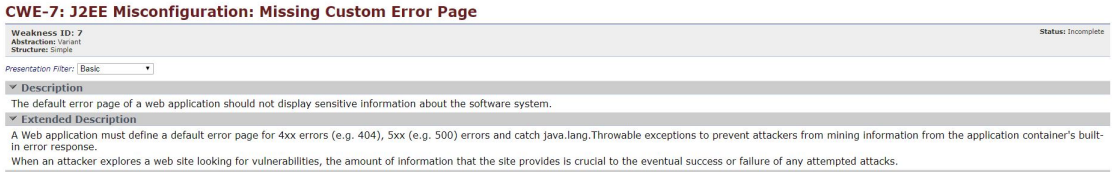

Figura 3: Vulnerabilidade de Projeto.

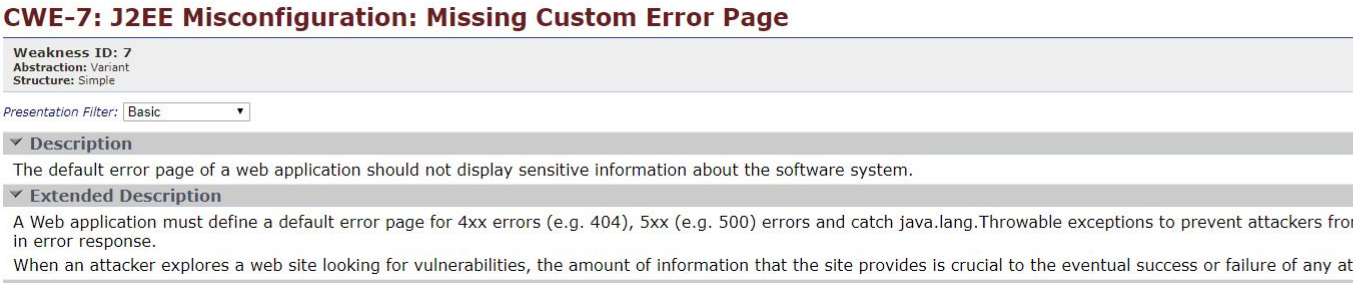

Figura 4: `https://cwe.mitre.org/data/definitions/702.html`.

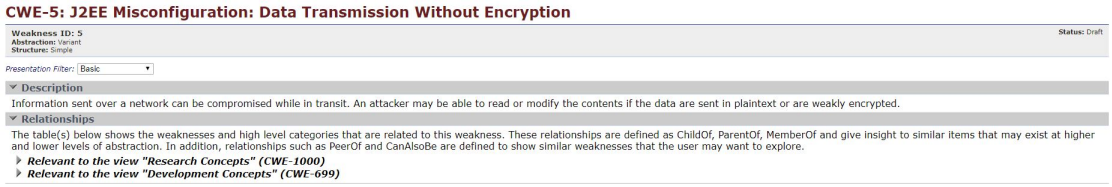

Figura 5: Vulnerabilidade de Codificação.

Figura 6: Vulnerabilidade de Codificação.

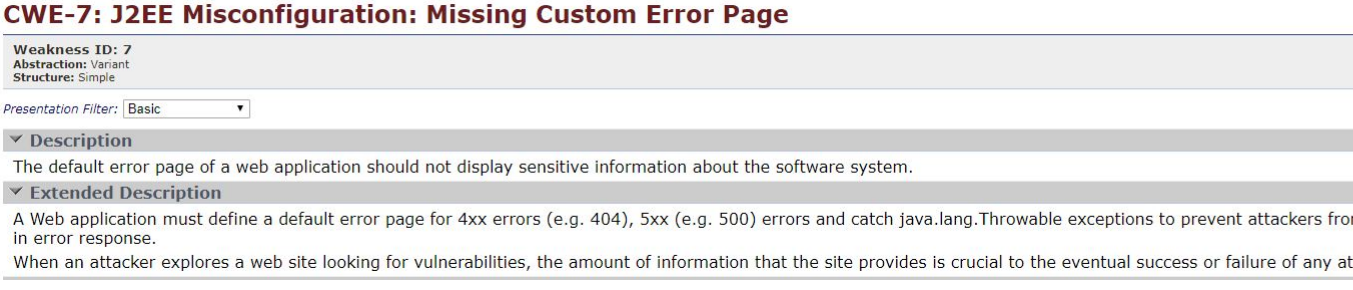

Figura 7: `https://cwe.mitre.org/data/definitions/16.html`.

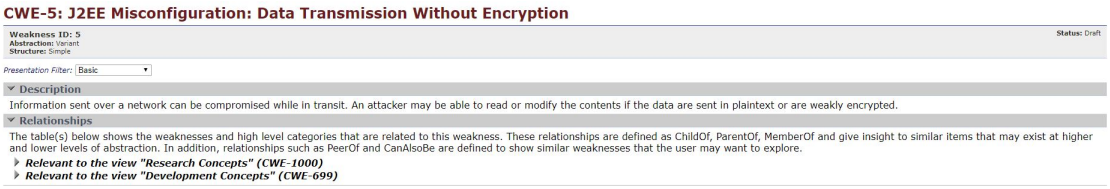

Figura 8: Vulnerabilidade Operacional.

Figura 9: Vulnerabilidade Operacional.