



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	2
0.2	Pergunta P1.2	2
0.3	Pergunta P1.3	3

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

CWE-7: J2EE Misconfiguration: Missing Custom Error Page

Weakness ID: 7

Abstraction: Variant

Structure: Simple

Status: Incomplete

Presentation Filter: Basic

Description

The default error page of a web application should not display sensitive information about the software system.

Extended Description

A Web application must define a default error page for 4xx errors (e.g. 404), 5xx (e.g. 500) errors and catch java.lang.Throwable exceptions to prevent attackers from mining information from the application container's built-in error response.

When an attacker explores a web site looking for vulnerabilities, the amount of information that the site provides is crucial to the eventual success or failure of any attempted attacks.

Figura 3: Vulnerabilidade de Projeto.

CWE-7: J2EE Misconfiguration: Missing Custom Error Page

Weakness ID: 7

Abstraction: Variant

Structure: Simple

Presentation Filter: Basic

Description

The default error page of a web application should not display sensitive information about the software system.

Extended Description

A Web application must define a default error page for 4xx errors (e.g. 404), 5xx (e.g. 500) errors and catch java.lang.Throwable exceptions to prevent attackers from mining information from the application container's built-in error response.

When an attacker explores a web site looking for vulnerabilities, the amount of information that the site provides is crucial to the eventual success or failure of any attempted attacks.

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

CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption

Weakness ID: 5

Abstraction: Variant

Structure: Simple

Status: Draft

Presentation Filter: Basic

Description

Information sent over a network can be compromised while in transit. An attacker may be able to read or modify the contents if the data are sent in plaintext or are weakly encrypted.

Relationships

The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

Relevant to the view "Research Concepts" (CWE-1000)

Relevant to the view "Development Concepts" (CWE-699)

Figura 5: Vulnerabilidade de Codificação.

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.

Figura 6: Vulnerabilidade de Codificação.

CWE-7: J2EE Misconfiguration: Missing Custom Error Page

Weakness ID: 7

Abstraction: Variant

Structure: Simple

Presentation Filter: Basic

Description

The default error page of a web application should not display sensitive information about the software system.

Extended Description

A Web application must define a default error page for 4xx errors (e.g. 404), 5xx (e.g. 500) errors and catch java.lang.Throwable exceptions to prevent attackers from mining information from the application container's built-in error response.

When an attacker explores a web site looking for vulnerabilities, the amount of information that the site provides is crucial to the eventual success or failure of any attempted attacks.

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

4

CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption

Weakness ID: 5

Abstraction: Grant

Structure: Simple

Status: Draft

Presentation Filter: Basic

Description

Information sent over a network can be compromised while in transit. An attacker may be able to read or modify the contents if the data are sent in plaintext or are weakly encrypted.

Relationships

The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

- Relevant to the view "Research Concepts" (CWE-1000)
- Relevant to the view "Development Concepts" (CWE-699)

Figura 8: Vulnerabilidade Operacional.

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.

Figura 9: Vulnerabilidade Operacional.