Practice 2

CWE - Common Weakness Enumeration

Name: Madizhan Islambek

Email: p42isdam@uco.es

Professor: Juan Antonio Romero Castillo

Exercises

1. General Overview of the CWE Project

CWE is a project maintained by MITRE Corporation and endorsed by organizations like NIST and the Department of Homeland Security. It is a globally recognized framework that helps classify and understand software vulnerabilities.

- **Sponsors and Support:** MITRE, NIST, DHS, and leading tech companies like Microsoft and Oracle.
- **Global Recognition:** Integrated into ISO/IEC standards and widely used in compliance and vulnerability management tools.
- **Purpose:** To provide a structured taxonomy for software weaknesses to improve security practices.

2. Main Chapters or Sub-Projects of CWE

1. **CWE Top 25 Most Dangerous Software Weaknesses**

   A prioritized list of critical vulnerabilities helps organizations address the most impactful vulnerabilities. These vulnerabilities are easy to find or use, so it's very important for testers and developers to address them because the users' or companies' data might be stolen.

2. **CWE-IDs (Identifiers)**

   Unique identifiers for software weaknesses that facilitates consistent tracking and reporting of vulnerabilities.

3. **CWE Compatibility Program**

   Ensures that tools and solutions align with CWE standards. It has 6 requirements to be CWE Compatible. To be CWE effective 4 of them is used.

4. **CWE Taxonomy**

   A hierarchical organization of vulnerabilities based on common traits. It Simplifies the analysis of vulnerability patterns for root cause identification.

3. Analysis of CWE Top 25 List

The **CWE Top 25 Most Dangerous Software Weaknesses** ranks vulnerabilities based on their severity, exploitability, and impact.

- **Weakness ID and Rank:** Every weakness is assigned a unique CWE ID (e.g., CWE-79) and a Rank based on its priority in addressing risks.
- **KEV (Known Exploited Vulnerabilities):** Highlights vulnerabilities with active exploits, urging immediate attention for mitigation.

4. Categorization of Top 25 Errors

Proposed Categories for CWE Top 25 Errors:

1. **Improper neutralization:**
    - Examples: CWE-79 (Cross-Site Scripting), CWE-89 (SQL Injection), CWE-78(OS Command Injection)
2. **Access Control Flaws:**
    - Examples: CWE-285 (Improper Authorization), CWE-862 (Missing Authorization).
3. **Memory Management Issues:**
    - Examples: CWE-125 (Out-of-Bounds Read), CWE-787 (Out-of-Bounds Write).

5. Example Vulnerability

Chosen Vulnerability: CWE-79 (Cross-Site Scripting - XSS)

- **Description:** Occurs when user input is improperly sanitized, allowing malicious scripts to execute in users' browsers.
- **Affected Software:** Common in web applications like WordPress and Facebook.
- **Case Studies:** Facebook faced XSS issues that compromised user sessions.
- **Countermeasures:**
    - Input validation and sanitization.
    - Implementing Content Security Policies (CSP).
    - Rigorous user input testing.

6. CWE Compatibility Project

The CWE Compatibility Program ensures that products and tools meet CWE standards, fostering consistency in vulnerability identification and remediation.

Requirements for CWE Compatibility:

1. Use CWE Identifiers in reports.
2. Align tools with CWE Taxonomy.
3. Declare compatibility and demonstrate adherence to CWE standards.

7. Significance of International Efforts in IT Security

International collaborations like CWE are crucial for addressing global cybersecurity challenges. They:

- Standardize vulnerability identification and mitigation practices.
- Foster collaboration among industry leaders.
- Enable resource sharing to combat emerging threats effectively.

8. Similar Communities and Initiatives

1. **OWASP (Open Web Application Security Project):** Focused on web security; known for its "Top 10" project.
2. **MITRE ATT&CK:** A comprehensive repository of adversarial tactics and techniques.
3. **FIRST CVSS:** Provides a system for scoring and assessing the severity of vulnerabilities.

Bibliography

1. CWE Official Website: https://cwe.mitre.org
2. MITRE ATT&CK: https://attack.mitre.org
3. FIRST CVSS: https://www.first.org/cvss
4. OWASP: https://owasp.org