#

OWASP Top 10 Vulnerabilities Monitoring

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-08-17	Draft document for documenting owasp top10 vulnerabilities	Dinesh Kumar	To be reviewed by CIP Security WG members
002	2021-08-30	Incorporated Yasin's (Siemens) feedback	Dinesh Kumar	Yasin

---

---

1. Objective

The primary objective of this document is to explain about how various OWASP. top 10 vulnerabilities are handled in CIP. This is to meet IEC-62443-4-2 CR6.2 security requirement.

This document is subject to revision either when OWASP document is revised or changes are made n CIP.

2. OWASP Top 10 Vulnerabilities

OWASP (Open Web Application Security Project) is a nonprofit organization focused on software security.

OWASP primarily recommends top 10 vulnerabilities to be monitored by web application developments. However, these receommendations are equaly important for any online systems.

Refer detail of these vulnerabilities at [[1]]

2.1 Injection

Injection flaws occur when insecure code is exploited to add special characters or insert any code which will help attackers to gain control of the application or system.

Examples of Injection flaws are

- SQL or NoSQL injections

- OS injections
- Command injections
- CRLF injections
- LDAP injections

All injection flaws affect or occur by exploiting application layers. Hence It should be taken care by CIP Users by running vulnerability scanner.

2.2 Broken Authentication

Broken Authentication can cause several type of vulnerabilities where attacker assumes role of a legitimate user and exploit systems.

Broadly, Broken Authentication refers to weaknesses in two areas: Session Management and Credential Management. Both are classified as broken authentication because attackers can use either avenue to masquerade as a user: hijacked session IDs or stolen login credentials.

Since Broken Authentication is mainly caused by poor implementation of session management or poor implementation of password policies. CIP supports several Debian packages to strengthen password management as well as session management.

CIP users are responsible to follow best practices and incorporate support in the end products.

1. Use 2 factors of authentication
2. Strengthen forgot password controls
3. Session timeout
4. Network encryption
5. Account lockout

2.3 Sensitive Data Exposure

Sensitive data exposure is one of the most widespread vulnerabilities on the OWASP list. It consists of compromising data that should have been protected.

Example of sensitive data are Credentials, Credit card numbers,Social Security Numbers, Medical information.

This requirement is not applicable to platforms like CIP hence CIP users should support it.

2.4 XML External Entities (XXE)

This vulnerability is specific to XML parsers and not applicable to CIP. CIP users need to investigate if this is relevant to their use cases.

2.5 Broken Access Control

If authentication and access control is not properly implemented, it's easy for attackers to exploit the system and steal confidential information.

CIP supports access control and authentication security packages which should be used by CIP users for their application and ensure access control is not broken.

This vulnerability can be easily detected by penetration testing. Following are some of the best practices to fix broken access control issues.

- Employ least privileged concepts – apply a role appropriate to the task and only for the amount of time necessary to complete said task and no more.
- Get rid of accounts you don't need or whose user no longer requires them.

- Audit your servers and websites – who is doing what, when, and why.
- If possible, apply multi-factor authentication to all your access points.
- Disable access points until they are needed in order to reduce your access windows.
- Remove unnecessary services off your server.
- Check applications that are externally accessible versus applications that are tied to your network.

Further refer OWASP 10 list of vulnerability for prevention of broken access control list.

2.6 Security Misconfiguration

Following definition from OWASP10 page

> Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

Following are the most common causes of this flaw.

- Unpatched flaws
- Default configurations
- Unused pages
- Unprotected files and directories
- Unnecessary services

CIP users should investigate further and take appropriate action to mitigate them.

2.7 Cross Site Scripting XSS

2.8 Insecure Deserialization

These specific kinds of vulnerabilities are not specificly expected in cip based products.

However we recommend to employ zero trust approaches to end systems designs so that

a) devices need to authenticate before beeing able to communicate with each other and

b) design interfaces whenever possible in a way so that even an authenticated attacker cannot execute code or introduce an illegal state to the system

2.9 Using Components with Known Vulnerabilities

CIP does regular CVE scanning for CIP Kernel as well as CIP application packages and keep sharing updates with CIP users.

However, CIP users shall further take preventive measures to mitigate the risk caused by this type of vulnerability.

2.10 Insufficient Logging & Monitoring

CIP includes security packages which should be used by CIP users for mitigating the risk cause by this vulnerability.

CIP offers syslog-ng package for logging and monitoring the system.

CIP features for system monitoring

This list will be updated to include all features provided by CIP for important system events related to security events.

CIP IEC layer has aide package installed which can be configured to monitor security events.

4. References

1. OWASP Top 10 Vulnerabilities
2. Broken Access Control