|  |  |  |
| --- | --- | --- |
| **S.no** | **Vulnerability Name** | **CWE - No** |
| **1**  **2**  **3**  **4**  **5** | Buffer Overflow Path Traversal  XML External Entity(XXE) Command Injection  Clickjacking | CWE-120 CWE-22 CWE-611 CWE-77 CWE-1021 |

**Stage – 1:**

**List of Vulnerability Table ➖**

**REPORT:-**

1. **Vulnerability Name:-** Buffer Overflow

**CWE : -** CWE-120

**OWASP/SANS Category:-** SANS Top 25: CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)

**Description:-** Buffer Overflow occurs when a program writes more data to a buffer than it can hold, causing adjacent memory locations to be overwritten. This can lead to crashes, data corruption, or execution of malicious code.

# Business Impact::-

* Can lead to unauthorized access to sensitive data.
* Potential for remote code execution, allowing attackers to control systems.
* System instability and crashes, affecting business operations

1. **Vulnerability Name:-** Path Traversal

**CWE : -** CWE-22

**OWASP/SANS Category:-** : OWASP Top 10 (A05:2021 – Security Misconfiguration)

**Description:-** Path Traversal (or Directory Traversal) allows attackers to access files and directories outside the intended scope by manipulating file paths. Attackers can access configuration files, credentials, or even system files

# Business Impact::-

* + Exposure of sensitive files (e.g., passwords, logs, source code).
  + Possible execution of unauthorized commands or scripts.
  + Loss of confidentiality and potential system compromise..

1. **Vulnerability Name:-** XML External Entity (XXE)

**CWE : -** CWE-611

**OWASP/SANS Category:-** OWASP Top 10 (A04:2021 – XML External Entities)

**Description:-** XXE vulnerabilities occur when applications improperly process XML input containing external entity references. This can lead to data exposure, file access, and even server-side request forgery (SSRF).

# Business Impact::-

* Leakage of sensitive internal files.
* Denial of Service (DoS) by consuming excessive system resources.
* Remote code execution in some cases.

1. **Vulnerability Name:-** Command Injection

**CWE : -** CWE-77

**OWASP/SANS Category:-** OWASP Top 10 (A03:2021 – Injection)

**Description:-** Command Injection occurs when an attacker injects arbitrary system commands into an application, which then executes them with the application's privileges.

# Business Impact::-

* + Full system compromise, allowing attackers to gain control.
  + Deletion or modification of business-critical data.
  + Launching further attacks (e.g., privilege escalation, lateral movement).

1. **Vulnerability Name:-** Clickjacking

**CWE : -** CWE-1021

**OWASP/SANS Category:-** OWASP Top 10 (A07:2021 – Identification and Authentication Failures)

**Description:-** Clickjacking is an attack where a user is tricked into clicking on something different from what they perceive, often embedding malicious content into an invisible frame.

# Business Impact::-

* + Unauthorized transactions or actions by users.
  + Potential account takeover or information theft.
  + Damage to brand reputation and user trust