***3.1 List of Vulnerabilities Table***

|  |  |  |
| --- | --- | --- |
| S.no | Vulnerability Name | CWE -No. |
| 1. | SSL Certificate can’t be trusted | 195 |
| 2. | NodeJs version related many issues. | 1104 |
| 3. | Open-jdk 8<=8u432/11.0.25/17.0.0<=17.0.<=21.0.5/23.0.1 vulnerability( 2025-01-21) | 21502 |
| 4. | Apache http server site enumeration. | 200 |
| 5. | Node.js18.x<18.20.1/20.x<20.12.1/<21.7.2 multiple vulnerabilities | 400, 352 |

***3.2 Solution Requirements***

**Vulnerability Assessment Report**

**1. SSL Certificate Cannot Be Trusted**

* **Impact**:
  + Risk of man-in-the-middle (MITM) attacks.
  + Users may be unable to verify the authenticity of your server.
* **Fix**:
  + Obtain a valid SSL/TLS certificate from a trusted certificate authority (CA).
  + Verify proper installation and expiration dates.

**2. Node.js Version-Related Multiple Issues**

* **Affected Versions**:
  + Node.js 18.x < 18.20.1
  + Node.js 20.x < 20.12.1
  + Node.js < 21.7.2
* **Common Weakness Enumerations (CWEs)**:
  + **CWE-295**: Improper certificate validation.
  + **CWE-1104**: Use of untrusted libraries or dependencies.
  + **CWE-21502**: Security misconfigurations leading to exposure.
  + **CWE-200**: Information exposure.
  + **CWE-400**: Uncontrolled resource consumption (DoS risk).
  + **CWE-352**: Cross-Site Request Forgery (CSRF) vulnerabilities.
* **Impact**:
  + Unauthorized access.
  + Risk of data leakage.
  + DoS attacks due to resource exhaustion.
* **Fix**:
  + Upgrade Node.js to the latest stable version (21.7.2 or higher).
  + Use LTS versions for production.
  + Regularly audit dependencies with npm audit.

**3. OpenJDK Vulnerabilities (2025-01-21)**

* **Affected Versions**:
  + OpenJDK 8 ≤ 8u432
  + OpenJDK 11 ≤ 11.0.25
  + OpenJDK 17 ≤ 17.0.21
  + OpenJDK 23 ≤ 23.0.1
* **Impact**:
  + Remote code execution (RCE).
  + Cryptographic vulnerabilities.
  + Unauthorized privilege escalation.
* **Fix**:
  + Upgrade to the latest OpenJDK version.
  + Regularly check vendor security patches.

**4. Apache HTTP Server Site Enumeration**

* **Impact**:
  + Attackers can list directories, misconfigured virtual hosts, and available services.
* **Fix**:
  + Disable directory listing in Apache configuration (Options -Indexes).
  + Configure proper permissions for httpd.conf.
  + Use security modules like mod\_security.

**Conclusion**

All these vulnerabilities pose security risks that need immediate remediation. It is crucial to apply updates, patch systems, and follow best security practices.

***3.3 Technology Stack***

 **SSL Certificate & HTTPS**

* Let's Encrypt / OpenSSL / Certbot
* Apache / NGINX with TLS 1.2+

 **Node.js Security**

* NVM for version management
* npm audit / Snyk for dependency scanning
* Helmet.js / CSRF protection / Rate limiting

 **OpenJDK Security**

* SDKMAN! for JDK version control
* OWASP Dependency-Check for vulnerability scanning

 **Apache HTTP Server Hardening**

* ModSecurity (WAF)
* Disable directory listing, use .htaccess
* Fail2Ban for brute-force attack prevention

 **Continuous Security Monitoring**

* SIEM: Splunk / ELK Stack / Wazuh
* Automated Scanners: OWASP ZAP / Nmap / Qualys SSL Labs