Sheikh Iyad | CodeAlpha | 18th January ‘25

Secure Coding Review Report

The "Hackathon Starter" project was scanned for security vulnerabilities using the `“npm audit”` tool. This scan has identified several high-severity vulnerabilities like cross-site request forgery (CSRF), denial of service (DoS), and uncontrolled resource consumption. This report provides a overview of urgent fixes of five vulnerabilities.

Detailed Vulnerabilities

1. Axios Cross-Site Request Forgery (CSRF) [< v0.27.2]

- **Severity:** High
- **Info:** CSRF is a web security vulnerability that tricks a web browser into executing an unwanted action on a trusted site
- **Fix:** Update `axios` to version `0.27.2` or later by running the following command:

  ```
  npm audit fix
  ```

2. body-parser Denial of Service (DoS) `[< v1.20.3]`

- **Severity:** High
- Info: DoS floods the server and prevents user from connecting to it.
- **Fix:** Upgrade to `body-parser` version `1.20.3` or later:

  ```
  npm install body-parser@latest
  ```

3. Uncontrolled Resource Consumption in Braces [< v3.0.3]

- **Dependency:** `braces`
- **Severity:** High
- **Info:** An attacker can cause the application to allocate excessive memory and potentially crash by sending imbalanced braces as input.

Vulnerability 4: Cookie Vulnerability [< v0.7.0]

- **Dependency:** `cookie`
- **Severity:** High
- **Info:** A cookie vulnerability is a weakness in a cookie that can allow an attacker to access sensitive user data.

5. Regular Expression Denial of Service (ReDoS) [< v7.0.4]

- **Dependency:** `cross-spawn`
- **Severity:** High
- **Info:** A **Regular Expression Denial of Service (ReDoS)** attack occurs when an attacker crafts an input that exploits the way a regular expression is processed, leading to excessive resource consumption (CPU and memory) on the target system.