**Vulnerability Scan Report:**

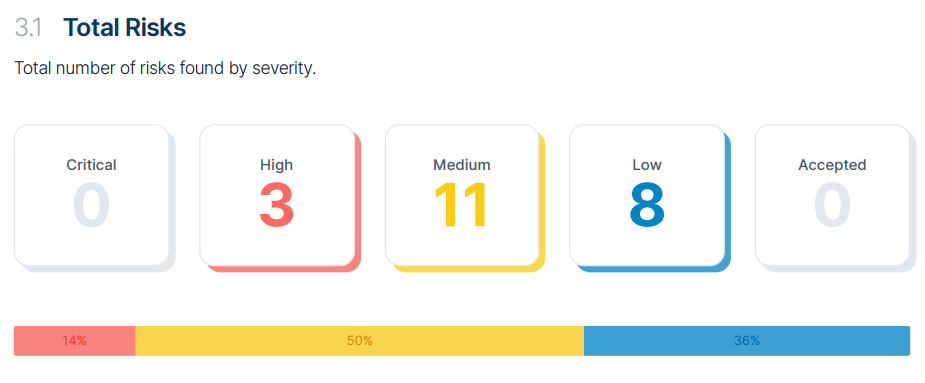
**Team Number:** Team 4.2

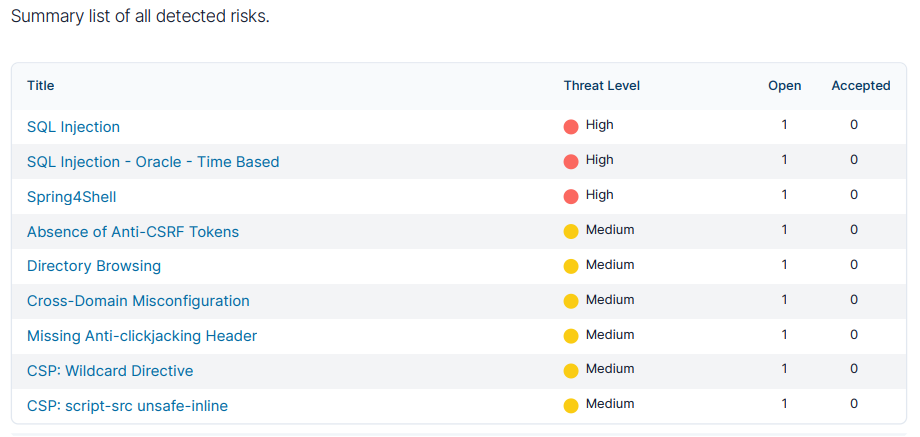
**Team Members:** Vishnu Veerapu  
 Mungali Chetan Sai Raju  
 Promodh Krishna  
 Charith Anil Kumar Nagar

**Project Name:** Network Anomaly detection

**Main website:** <https://www.staging.airtable.com/>

**Scanned Vulnerabilities are:**

****

****

****

**Some of the Vulnerabilities Description and Business Impacts are:**

Here is a classification of the vulnerabilities based on their description, OWASP category, CWE category, business impact, and solution:

1. **SQL Injection**
   * Description: This is a high-level vulnerability that allows attackers to manipulate a web application's database through malicious SQL queries.
   * OWASP Category: A1 - Injection
   * CWE Category: CWE-89 - SQL Injection
   * Business Impact: Data theft, data manipulation, and potentially unauthorized access to the database.
   * Solution: Use prepared statements or parameterized queries to prevent SQL injection. Validate and sanitize user inputs.
2. **SQL Injection - Oracle - Time Based**
   * Description: Similar to standard SQL injection, but specifically targeting Oracle databases and exploiting time-based vulnerabilities.
   * OWASP Category: A1 - Injection
   * CWE Category: CWE-89 - SQL Injection
   * Business Impact: Same as SQL Injection - data theft, data manipulation, and unauthorized database access.
   * Solution: Follow the same mitigation measures as standard SQL injection, with extra consideration for Oracle-specific SQL.
3. **Spring4Shell**
   * Description: A high-level vulnerability that targets the Spring Framework, allowing remote code execution.
   * OWASP Category: A1 - Injection
   * CWE Category: CWE-94 - Code Injection
   * Business Impact: Remote code execution can lead to complete compromise of the application and server.
   * Solution: Update Spring Framework to the latest version and patch the vulnerability.
4. **Absence of Anti-CSRF Tokens**
   * Description: A medium-level vulnerability where Cross-Site Request Forgery (CSRF) protection tokens are missing.
   * OWASP Category: A8 - Insecure Deserialization
   * CWE Category: CWE-352 - Cross-Site Request Forgery (CSRF)
   * Business Impact: Allows attackers to perform actions on behalf of the victim user.
   * Solution: Implement anti-CSRF tokens in your application to verify the authenticity of incoming requests.
5. **Directory Browsing**
   * Description: A medium-level vulnerability that allows attackers to list the contents of directories on the web server.
   * OWASP Category: A4 - XML External Entities (XXE)
   * CWE Category: CWE-548 - Information Exposure Through Directory Listing
   * Business Impact: Disclosure of sensitive information and directory structure.
   * Solution: Disable directory listing in the web server configuration.
6. **Cross-Domain Misconfiguration**
   * Description: A medium-level vulnerability involving improper configuration of cross-origin resource sharing.
   * OWASP Category: A6 - Security Misconfiguration
   * CWE Category: CWE-942 - Application-Level Configuration
   * Business Impact: Can lead to unauthorized data access or data leakage between domains.
   * Solution: Properly configure Cross-Origin Resource Sharing (CORS) policies.
7. **Missing Anti-clickjacking Header**
   * Description: A medium-level vulnerability where the X-Frame-Options header is not set, making the application susceptible to clickjacking attacks.
   * OWASP Category: A7 - Missing Function Level Access Control
   * CWE Category: CWE-693 - Protection Mechanism Failure
   * Business Impact: Potential data theft or unauthorized actions on behalf of the user.
   * Solution: Set the X-Frame-Options header to deny framing or limit framing to trusted domains.
8. **CSP: Wildcard Directive**
   * Description: A medium-level vulnerability where Content Security Policy (CSP) allows wildcard directives, making the application less secure.
   * OWASP Category: A5 - Broken Access Control
   * CWE Category: CWE-16 - Configuration
   * Business Impact: Weakened security, allowing for potential script execution from untrusted sources.
   * Solution: Restrict CSP directives to trusted sources and avoid using wildcards.
9. **CSP: script-src unsafe-inline**
   * Description: A medium-level CSP vulnerability that allows unsafe inline script execution.
   * OWASP Category: A5 - Broken Access Control
   * CWE Category: CWE-16 - Configuration
   * Business Impact: Increased risk of XSS attacks.
   * Solution: Remove unsafe-inline from the script-src directive in the CSP header.
10. **CSP: style-src unsafe-inline**
    * Description: A medium-level CSP vulnerability that allows unsafe inline style execution.
    * OWASP Category: A5 - Broken Access Control
    * CWE Category: CWE-16 - Configuration
    * Business Impact: Increased risk of style-based attacks.
    * Solution: Remove unsafe-inline from the style-src directive in the CSP header.
11. **XSLT Injection**
    * Description: A medium-level vulnerability involving the injection of malicious XSLT code into an application.
    * OWASP Category: A1 - Injection
    * CWE Category: CWE-91 - XML Injection
    * Business Impact: Can lead to data manipulation and unauthorized access.
    * Solution: Validate and sanitize XML inputs, and use a safe XML processing library.
12. **CSP: script-src unsafe-eval**
    * Description: A medium-level CSP vulnerability that allows unsafe script evaluation through eval() or similar functions.
    * OWASP Category: A5 - Broken Access Control
    * CWE Category: CWE-16 - Configuration
    * Business Impact: Increased risk of script-based attacks.
    * Solution: Remove unsafe-eval from the script-src directive in the CSP header.
13. **Content Security Policy (CSP) Header Not Set**
    * Description: A medium-level vulnerability where no CSP header is set, exposing the application to various security risks.
    * OWASP Category: A5 - Broken Access Control
    * CWE Category: CWE-16 - Configuration
    * Business Impact: Increased risk of XSS attacks and other security threats.
    * Solution: Implement a proper CSP header to restrict content sources and protect against various attacks.
14. **Vulnerable JS Library**
    * Description: A medium-level vulnerability related to the use of outdated or vulnerable JavaScript libraries.
    * OWASP Category: A9 - Using Components with Known Vulnerabilities
    * CWE Category: CWE-937 - OWASP Top Ten 2017 Category
    * Business Impact: Increased risk of exploitation through known library vulnerabilities.
    * Solution: Regularly update and patch JavaScript libraries to address known vulnerabilities.
15. **Cloud Metadata Potentially Exposed**

* Description: This vulnerability indicates that cloud metadata, which often contains sensitive information about the cloud instance and its configuration, may be exposed to unauthorized users.
* OWASP Category: Not directly categorized by OWASP, but it falls under A6 - Security Misconfiguration or A5 - Broken Access Control depending on the context.
* CWE Category: CWE-200 - Information Exposure
* Business Impact: Unauthorized access to cloud metadata can lead to sensitive data exposure, potential security misconfigurations, and exploitation of cloud resources.
* Solution: To mitigate this vulnerability, ensure that access controls are properly configured to restrict access to cloud metadata. Review and update cloud security policies and configurations to prevent unauthorized access. Regularly audit and monitor cloud infrastructure for security vulnerabilities. Implement strong authentication mechanisms and encryption for sensitive metadata. Additionally, follow cloud service provider's best practices and security guidelines to secure cloud resources effectively.

The complete report of the scan can be accessed using the following link:

<https://drive.google.com/file/d/1kiZqPBJLw8_ELe1tPOetQQ181ZOvg3C0/view?usp=sharing>