

**Dynamic Vulnerability Assessment**

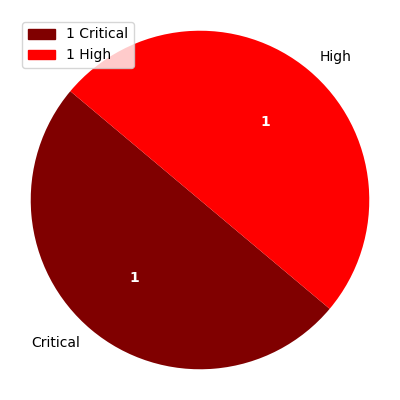
**dfhdfh**

**Requested by:** dfhdfh

## Version Information

|  |  |  |
| --- | --- | --- |
| Date | Application Version | Reviewer |
| 30-May-2025 | Initial Draft | dfhdfh |
| 30-May-2025 | Peer Review |  |
| 30-May-2025 | Approved |  |

**Vulnerability Severity Distribution**



## Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No. | Security Observation | Risk Rating | Page No. |
| **Critical Severity** | | | |
| 1 | Security Misconfiguration | Critical | 4 |
| **High Severity** | | | |
| 2 | API key exposes PII Information | High | 5 |

## URLs and Scope

URLs: dfxhdfh

Scope: dfhdfh

## Vulnerability Details

### 1. API key exposes PII Information

**Severity: High**

CVSS Score: 8.5

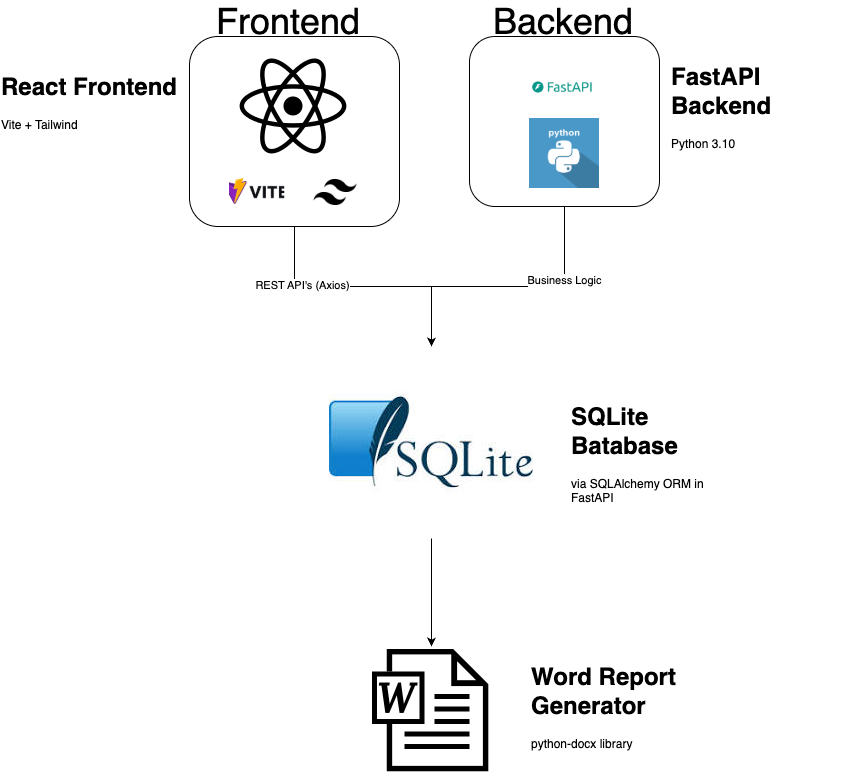
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

#### Description

Information leakage issues arise when applications reveal information that could be useful to a malicious actor in gaining a better knowledge of the application or underlying infrastructure. This can occur in several places and may include (but is not limited to):   
  
Sensitive information such as credentials, API keys and endpoints.   
  
Accessing default application installation/configuration pages that disclose the underlying software.   
  
Comments that are viewable in HTML source code.

#### Evidence

Step 1: test



Step 2: tersdhf



#### Recommendation

Please ensure that sensitive files are not served through the web server. Such files need to be blocked through server config rules or must be made accessible only to the server backend code

#### Reference

https://owasp.org/www-project-top-ten/OWASP\_Top\_Ten\_2017/Top\_10-2017\_A3-Sensitive\_Data\_Exposure

### 2. Security Misconfiguration

**Severity: Critical**

CVSS Score: 9.4

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

#### Description

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date. It is observed Credit Scoring tool is vulnerable to Information disclosure via a direct request. Perceive the below evidence that the PEGA platform does not enforce strict access control, which divulged the information of PegaRules Build, System Properties, Environment, Java Virtual Machine, PegaDatabase.

#### Evidence

#### Recommendation

It is suggested to enforce strong access controls to avoid security misconfiguration vulnerabilities, disable direct request to sensitive information and verify directories permissions.

#### Reference

https://portswigger.net/web-security/information-disclosure