

**Dynamic Vulnerability Assessment**

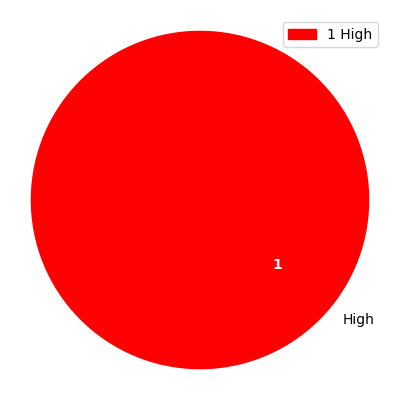
**test**

**Requested by:** test

## Version Information

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

**Vulnerability Severity Distribution**



## Summary Table

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

## URLs and Scope

URLs: test

Scope: test

## Vulnerability Details

### 1. API key exposes PII Information

**Severity: High**

CVSS Score: 7.1

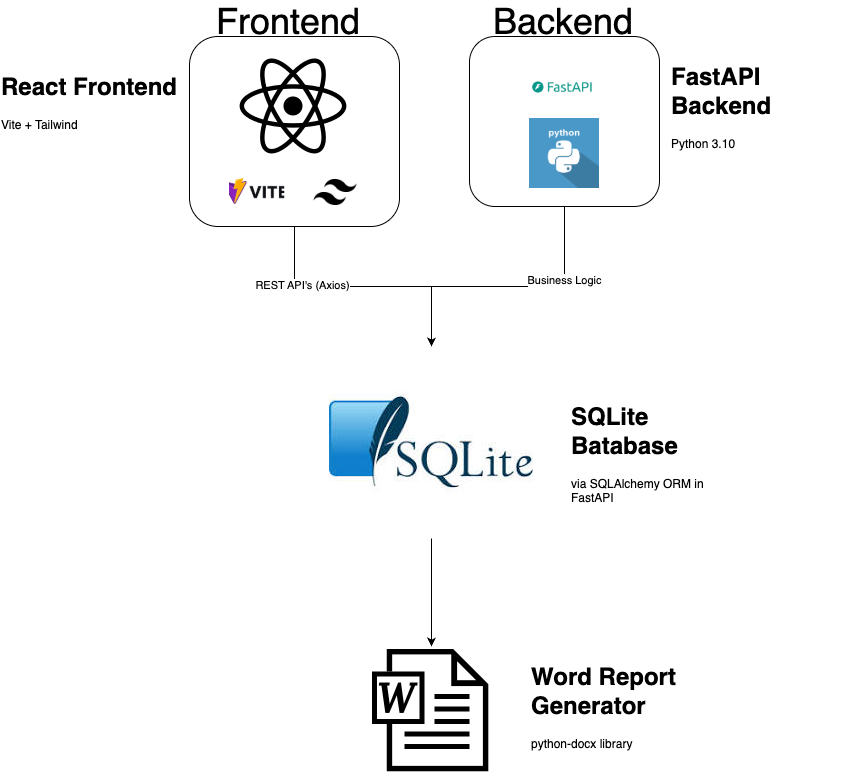
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:H

#### 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: eeeeee



#### 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