****

**Appian Vulnerability Submission Worksheet**

This worksheet was designed by Appian to help you submit vulnerabilities in alignment with our security team guidelines. Please review the guidelines [here](https://community.appian.com/support/w/kb/762/kb-1447-vulnerability-testing) and submit a completed version of this worksheet through a [Technical Support Case](https://forum.appian.com/suite/sites/myappian/page/support/).

# Important Note

Appian requires **verifiable evidence such as screenshots, payloads, or any other associated proof-of-concept material as well as manual reproduction steps in order to properly validate any reported vulnerability findings.**

**Our platform is unique and lends itself to a very high volume of false positives** **from automated scans**. This is because:

* Appian endpoints are dynamically created as a user navigates through the solution, which means the sitemaps generated by automated scanners are often incorrect.
* Due to our expression language - SAIL - solutions within our platform do not wait for user submission of state changing requests. For the sake of security and increased speed, data is posted back in memory as the user is interacting with the UI and validated either during that interaction or during submission. After entry of data into a given field, the application only returns object IDs and no actual values. This workflow is not conventional, and automated scanners cannot differentiate between vulnerable and non-vulnerable components.

We have yet to find a Dynamic Application Security Testing (DAST) tool that can adequately identify vulnerabilities within our platform and the solutions built on top of it. Therefore, we require evidence and manual reproduction steps for each reported vulnerability. We appreciate your help with ensuring a streamlined submission process!

# Requirements

Please copy and fill the table below for each vulnerability. All **DARK BLUE** fields are REQUIRED.

## **Vulnerability 1**

|  |  |
| --- | --- |
| **ID Number** | *The CVE or other ID number of the issue (if applicable).* |
| **Name** | ***REQUIRED***  *The name of the issue.* |
| **Severity Level** | ***REQUIRED***  *The severity level of the issue (L/M/H).* |
| **Description** | ***REQUIRED***  *A description of the risk to the system.* |
| **Evidence of Validation** | ***REQUIRED***  *Verifiable evidence such as screenshots, payloads, or other associated proof-of-concept material in order to properly validate any reported vulnerability findings that exploit the system. If there is not enough space to share in this box, feel free to include information immediately below this table.* |
| **Steps to Reproduce** | ***REQUIRED***  *Clear steps on how to reproduce the issue as well as guidance on how to reach the impacted endpoint(s). Please be as detailed as possible by including all relevant endpoints, filenames, and URLs where the vulnerability was discovered. This will help the Appian team attempt to reproduce the issue on their end.* |

## **Vulnerability 2**

|  |  |
| --- | --- |
| **ID Number** | *The CVE or other ID number of the issue (if applicable).* |
| **Name** | ***REQUIRED***  *The name of the issue.* |
| **Severity Level** | ***REQUIRED***  *The severity level of the issue (L/M/H).* |
| **Description** | ***REQUIRED***  *A description of the risk to the system.* |
| **Evidence of Validation** | ***REQUIRED***  *Verifiable evidence such as screenshots, payloads, or other associated proof-of-concept material in order to properly validate any reported vulnerability findings that exploit the system. If there is not enough space to share in this box, feel free to include information immediately below this table.* |
| **Steps to Reproduce** | ***REQUIRED***  *Clear steps on how to reproduce the issue as well as guidance on how to reach the impacted endpoint(s). Please be as detailed as possible by including all relevant endpoints, filenames, and URLs where the vulnerability was discovered. This will help the Appian team attempt to reproduce the issue on their end.* |