

## Veracode Results Review FAQs for Vendors

This document addresses many questions often asked upon results being made available to a vendor in an enterprise-vendor relationship.

### \*\*\*IMPORTANT NOTES\*\*\*

The most common point of confusion in 3<sup>rd</sup> party scans is around the mitigation and summary publication document. Please take the time to review the below process and send any questions you may have to [3rdPartySupport@Veracode.com](mailto:3rdPartySupport@Veracode.com).

Please note that mitigations can only be applied to the most current build of an application. Mitigations for flaws identified in previous builds can not be entered.

### \*\*\*IMPORTANT NOTES\*\*\*

#### Can you provide an overview of the results review process?

The results review process allows vendors to review all issues in a timely manner, address any that may have mitigating circumstances or false positives and provide the requesting enterprise with a summary report.

The typical process is as follows:

Step	Description	Owner
<b>Step 1: Results Published to Vendor</b>	Veracode publishes the analysis results to the vendor who is notified via an auto-generated email. The requesting enterprise receives a notification that results have been published to the vendor, but is not able to see any results.	Veracode
<b>Step 2: Vendor Reviews Results</b>	The vendor logs in to the Veracode platform and reviews the results within 3 days of publication. If needed, a readout call can be scheduled with your Veracode contact.	<b>Vendor</b>
<b>Step 3: Initial Report Published</b>	Once the vendor has reviewed the initial findings, a summary report can be published to the enterprise for initial review. <b>Note:</b> The vendor will still be able to work through the mitigation and false positive reduction processes at this time.	<b>Vendor</b>

<b>Step 4: Vendor Documents Mitigations/False Positives</b>	During the review process, the vendor may identify flaws that have mitigating circumstances requiring documentation, and less frequently may identify false positives. The vendor works with Veracode to document these flaws and gain approval from the enterprise (see below for more information)	<b>Vendor</b>
<b>Step 5: Approved Mitigations Entered in Platform</b>	Any mitigations receiving enterprise approval will be marked as such by the Enterprise via the Veracode platform and removed from the overall score.	Veracode
<b>Step 6: Enterprise Creates a New Build Upon Receiving Vendor Request</b>	After all mitigation activities are complete and the summary report published, the enterprise can create a new build for additional analysis upon receiving a request via from the vendor.	<b>Vendor and Enterprise</b>

### **I have flaws that have a mitigation or appear to be false positives. How do I handle these?**

Flaws identified by Veracode often fall in to one of three categories when reviewed by the development team:

1. **Valid Flaws Requiring Remediation** – Valid flaws that must be fixed and rescanned by Veracode to confirm proper remediation. These are the most common flaw category.
2. **False Positives** – Flaws errantly identified by Veracode analysis that should never be considered a flaw in any situation. The Veracode False Positive rate is very low (approximately 15%), but occasionally some do appear in final reports.
3. **Mitigated Flaws** – Flaws that are valid at their lowest level, but may have some kind of mitigating circumstance that should be considered. These mitigations often appear at one of three levels: mitigated by design, mitigated by OS environment and mitigated by network environment.

**To remove false positives:** Please note that the Veracode false positive rate is ~15% and many flaws belong in the “mitigated” category (see below) rather than false positive category. For flaws that appear to be false positives, document the reason why the flaw should be considered a false positive and provide it to your Veracode contact. Veracode will review the documentation and if it is deemed a false positive will remove it from the report as well as enter it into the queue for future analysis updates to help lower the false positive rate.

**To document mitigating circumstances:** Mitigating circumstances are to be documented by the development team via the Veracode platform. Once all documentation is complete, the vendor should contact the requesting enterprise for mitigation review and potential approval. If needed, the Veracode 3<sup>rd</sup> Party Support team ([3rdPartySupport@veracode.com](mailto:3rdPartySupport@veracode.com)) can be contacted for help in facilitating the process.

In some cases, vendors may choose to initially document mitigating circumstances in an Excel spreadsheet rather than directly in the Veracode flaw viewer. Vendors will still be required to enter the

mitigations directly in the flaw viewer for enterprise review, but this option may initially work better with their review and documentation process. The following table is often found useful by teams that elect for this method:

Flaw ID	CWE ID	Category	Mitigation Type (by design, by os environment, etc)	Proposal/roadmap
1	89	SQL Injection	mitigated by desgin	Mitigation details here
2	80	XSS	mitigated by design	Mitigation details here

Any mitigations that are approved by the requesting enterprise will be removed from the mitigated score recommendation. In the event that a vendor team elects to forgo the flaw viewer, additional support may be available from the Veracode 3<sup>rd</sup> Party Support team depending on the individual situation. The mitigations should be provided in the above table in an unfiltered format with only those flaws that need to be considered for mitigation approval. Please do not submit filtered, color-coded, or incomplete spreadsheets as they can lead to confusion and delays in the review process.

#### What are the mitigation options and some examples of mitigating circumstances?

There are three types of mitigations that can be documented – “Mitigated by Design”, “Mitigated by Network Environment” and “Mitigated by OS Environment”. Below are guidelines and examples of each:

- **Mitigated by Design** - These are findings that are technically valid but have mitigating circumstances in the design of the application, such as custom validation routines or use case scenarios that do not put the application at risk.
- **Mitigated by Network Environment** - These are findings that are technically valid but have mitigating circumstances at the network level, such as intrusion detection, web application firewalls, etc.
- **Mitigated by OS Environment** - These are findings that are technically valid, but have a mitigating circumstances at the OS level, such as restricted user access (admins) or limited file access.

Additionally, in some cases a flaw may be identified by the development team as a false positive (FP). False positives are findings that should never be returned to a Veracode customer and are technically incorrect. The Veracode false positive rate is approximately 15% across all applications.

#### Can mitigations be retroactively applied?

The mitigation process is designed to ensure that all flaws are reviewed and addressed before a new build of the application is created. Because of this, all mitigation activity must occur before a new build is requested by the vendor. Once the new build is created, mitigations cannot be retroactively applied.

### **Will I have to re-document mitigations in future scans?**

Part of Veracode's standard service is to match flaws against previous scan results with as high a degree of accuracy as possible. This helps to properly identify which flaws are new and which are old. Additionally, any matched flaws that have a mitigation proposed or approved will have the mitigation carried over between builds.

### **How can I import my results into an Excel Spreadsheet?**

Veracode has created an Excel template that can be used to easily import the downloadable XML report directly into a spreadsheet for review and mitigation activities. This template is available at <https://analysiscenter.veracode.com/auth/helpCenter/api/samples/VeracodeResultsExport.xlsx> and includes import instructions in the first tab. Valid user credentials are required to access this template.

### **How will I know when results are available?**

The Veracode platform will send an auto-generated email to the original submitter of the application for analysis. In some cases these will get stuck in spam filters, so adding [support@veracode.com](mailto:support@veracode.com) and [3rdPartySupport@Veracode.com](mailto:3rdPartySupport@Veracode.com) to your safe senders list is recommended.

Additionally, the current analysis status is always available by logging in to the Veracode platform.

### **What level of details will be available to my team for the flaws identified?**

Veracode provides multiple levels of details based on analysis results ranging from high level executive summaries to a detailed triage flaws view that allows users to view results at a source code level. More details on understanding scan results is available at [https://analysiscenter.veracode.com/auth/helpCenter/review/review\\_master.html](https://analysiscenter.veracode.com/auth/helpCenter/review/review_master.html)

### **I've made fixes to identified flaws. How can I get a rescan?**

Once fixes are made, the vendor can request the enterprise to create a new build of the application. This requires that all mitigation activities first be completed and a summary report be published to the enterprise by the vendor.

**There is a high level of detail in my results. Will the enterprise see all of these?**

No. The enterprise only receives a very high level summary report that reports the types and number of issues, but no other significant data.

**How can the summary results be released to the requesting enterprise?**

The summary results can be released to the requesting enterprise by clicking the “Publish to Enterprise” button on the application profile page in the Veracode platform.

**Are false positives included in my score?**

If you identify false positives that are confirmed by Veracode they will be removed completely from your score and report.

**Are approved mitigated flaws included in my score?**

Any mitigations approved by the enterprise will not be counted towards your overall mitigated grade which is used to determine if enterprise requirements are met. The mitigated status and comments will be included in the reports.

**How can vendors document mitigations on the platform?**

Vendor users can log in, review the findings, and singly/bulk mitigate flaws through the triage flaw viewer. Upon completion of the mitigation proposals, the Vendor must “Publish to enterprise” to allow the enterprise to review/accept/reject the mitigations. Further details on this functionality are available through the Veracode help center at

[https://analysiscenter.veracode.com/auth/helpCenter/review/improve\\_mitigation.html](https://analysiscenter.veracode.com/auth/helpCenter/review/improve_mitigation.html)

**How can enterprises approve/reject proposed vendor mitigations?**

Beginning with the Veracode 2011.4 release (August 2011), enterprise users with “Mitigation Approver” permissions can log in, review high level details of proposed mitigations and directly accept or reject the mitigations. Further details on this functionality are available through the Veracode help center at

[https://analysiscenter.veracode.com/auth/helpCenter/review/improve\\_mitigation.html#accept](https://analysiscenter.veracode.com/auth/helpCenter/review/improve_mitigation.html#accept)