

Using Lucent Sky AVM to overcome the limitations of SAST

A brief look at how organizations can move past analysis to secure application layer vulnerabilities with Lucent Sky AVM.



SUMMARY

Application layer security and secure code walk hand in hand. However, many organizations treat static analyzer results like white noise that can be ignored and dealt with later in the Secure Software Development Lifecycle (SSDLC). This is because teams understand traditional SAST tools to be analysis oriented, rather than functional additions to their security practice. Analysis alone does not secure code.

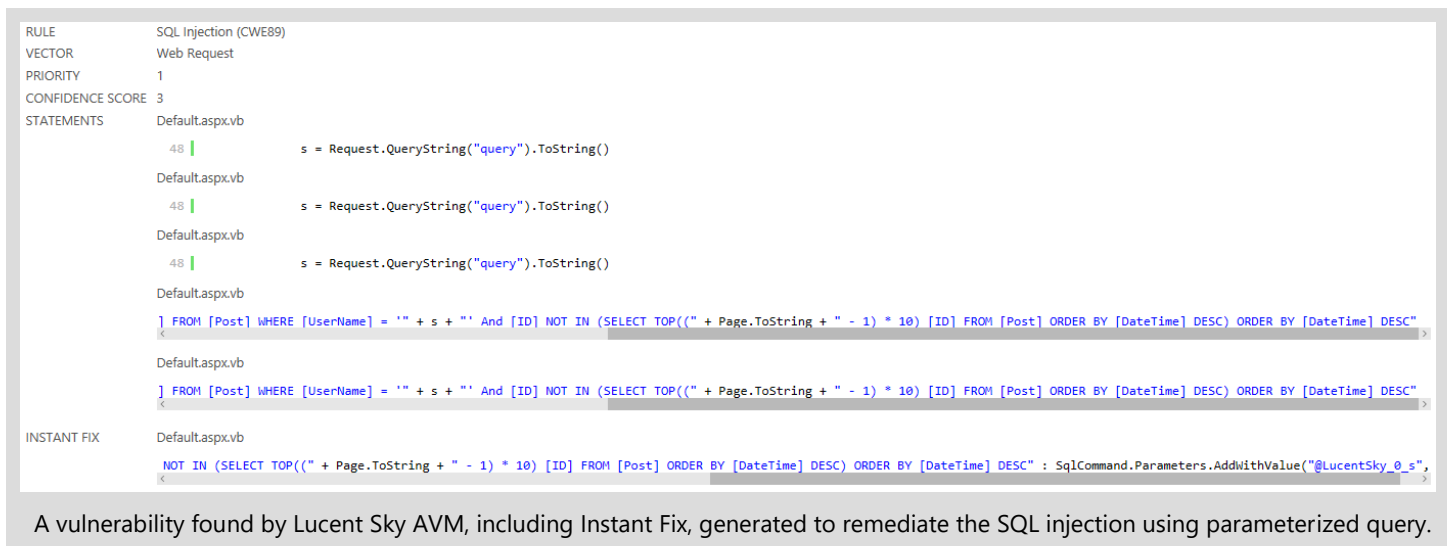
Analysis doesn't fix any vulnerabilities

We could say humans do, but all research shows that companies struggle to remediate known vulnerabilities at the rate they're introduced. For most companies this isn't a process problem: many have the reports to identify where the vulnerabilities are. However, few teams have the time to reallocate toward their remediation during and between build cycles.

This means that traditional SAST vendors are providing little more than a report and a checkbox as part of a security process. The challenge, then, for SAST reports is to either give more insight into code quality, or to do anything action in addition to analysis. Code quality and security have to move hand-in-hand to keep up with the pace of the SSDLC. Lucent Sky AVM fills the gap between a traditional SAST tool and accelerated development lifecycles that don't leave time for manual remediation.

To make sure security cannot be ignored, security tools need to functionally do security, not just reporting. Lucent Sky AVM does more than a traditional SAST tool by providing code-based Instant Fixes for identified vulnerabilities. Lucent Sky AVM can automatically remediate up to 90% of found vulnerabilities in one scan, reducing the bulk number of vulnerabilities and eliminating the introduction of new vulnerabilities as code is built.

The result of analysis should be a more secure code base, not a fancy report. Do more with Lucent Sky AVM.



The screenshot displays a security report for a SQL Injection (CWE89) vulnerability. It includes the following details:

- RULE:** SQL Injection (CWE89)
- VECTOR:** Web Request
- PRIORITY:** 1
- CONFIDENCE SCORE:** 3
- STATEMENTS:** Three instances of `s = Request.QueryString("query").ToString()` in `Default.aspx.vb`.
- Instant Fix:** A code snippet showing the replacement of the vulnerable query with a parameterized query: `NOT IN (SELECT TOP((" + Page.ToString + " - 1) * 10) [ID] FROM [Post] ORDER BY [DateTime] DESC) : SqlCommand.Parameters.AddWithValue("@LucentSky_0_s",`

A vulnerability found by Lucent Sky AVM, including Instant Fix, generated to remediate the SQL injection using parameterized query.

By doing more, Lucent Sky AVM reports can say more: it reports both the number of found and **fixed** vulnerabilities. It summarizes work done, not work an engineer needs to then do.

Reducing reporting noise, enhancing security

Lucent Sky AVM delivers the same integration, oversight and reporting capabilities as traditional SAST without the reliance on designated security experts.

Whereas SAST tools are designed for use by security consultants, they often generate as many results as possible even if there are few actual vulnerabilities. The triage of results and follow up tasks require time and expertise to weed out things like false positives. This reliance on security expertise and manual review time means their reports are not digestible or functional for most development teams.

Lucent Sky AVM is built with the developer's needs in mind. It offers an ease of integration with any development methodology (eg. waterfall, agile) and is designed to streamline tasks and reduce noise.

Enterprise quality mitigation and sophisticated deployment

Turning SAST reports into remediated, secure code could be a full-time job. So, it doesn't get done. Lucent Sky AVM is rules-based and centralized, meaning that a team or developers have full control of when vulnerabilities are removed from code.

- Review and approve Instant Fixes.
- Deploy as fits best into the SSDLC - within the build script, via API calls or using a web interface.
- Centralize remediation: developers and managers have full oversight of if and when Instant Fixes are placed and which security libraries are used, allowing them to solve vulnerabilities systematically and at scale. This also allows libraries to be approved for use within any applicable compliance regimes.

CONCLUSION

Lucent Sky AVM is a targeted remediation product that does the work of many developers in one scan. Analysis alone does not secure code: SAST reports are limited by not providing actionable remediation. By integrating with the SSDLC in a centralized, rules-based manner, Lucent Sky AVM advances application security outcomes by removing vulnerabilities at the source.

ABOUT LUCENT SKY

Lucent Sky has developed a new application security technology that enables application layer vulnerabilities to be removed from the source code in a centralized and automated manner.

Existing applications can rapidly increase their security posture in one scan by removing vulnerabilities en masse, enabling legacy applications to be compliant with new security standards. For new applications, Lucent Sky AVM allows developers to secure code as its developed, preventing a security backlog by removing common vulnerabilities within their code.

Fast and expedient, Lucent Sky AVM fits within the SSDLC and works at the pace of development.