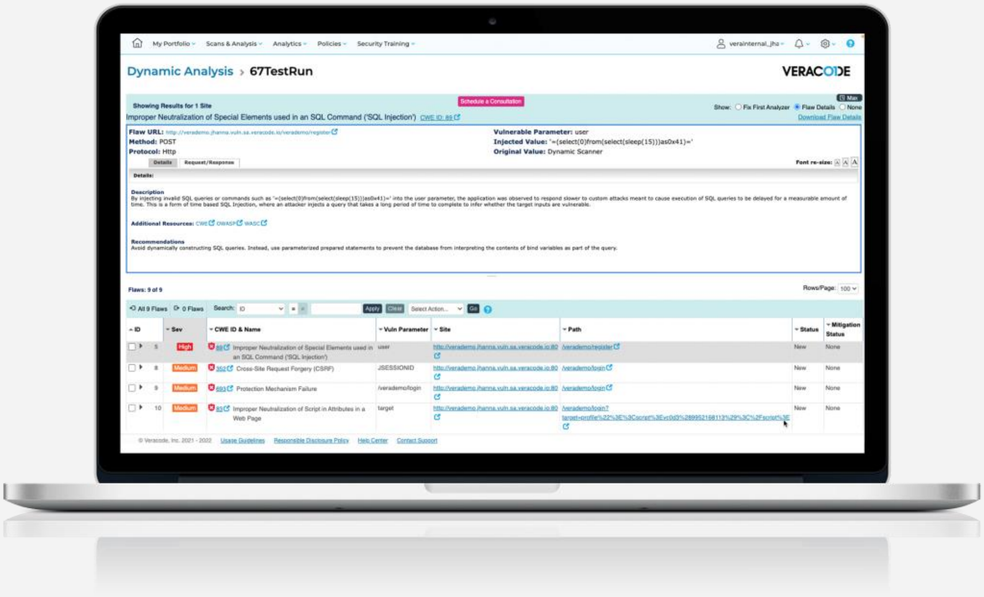
Veracode Dynamic Analysis:

Find and Fix Vulnerabilities at runtime

Leverage the power of real-world, simulated attacks to surface vulnerabilities before they become targets



Dynamic Analysis › 67TestRun

Showing Results for 1 Site

Show: ○ Fix First Analyzer ● Flaw Details ○ None

Download Flaw Details

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE ID: 89

Flaw URL: http://verademo.jhanna.vuln.sa.veracode.io/verademo/register
Method: POST
Protocol: Http

Vulnerable Parameter: user
Injected Value: '=(select(0)from(select(sleep(15)))as0x41)='
Original Value: Dynamic Scanner

Details:

Description
By injecting invalid SQL queries or commands such as '=(select(0)from(select(sleep(15)))as0x41)=' into the user parameter, the application was observed to respond slower to custom attacks meant to cause execution of SQL queries to be delayed for a measurable amount of time. This is a form of time based SQL Injection, where an attacker injects a query that takes a long period of time to complete to infer whether the target inputs are vulnerable.

Additional Resources: CWE OWASP WASC

Recommendations
Avoid dynamically constructing SQL queries. Instead, use parameterized prepared statements to prevent the database from interpreting the contents of bind variables as part of the query.

Flaws: 9 of 9

ID	Sev	CWE ID & Name	Vuln Parameter	Site	Path	Status	Mitigation Status
5	High	89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	user	http://verademo.jhanna.vuln.sa.veracode.io:80	/verademo/register	New	None
8	Medium	352 Cross-Site Request Forgery (CSRF)	JSESSIONID	http://verademo.jhanna.vuln.sa.veracode.io:80	/verademo/login	New	None
9	Medium	693 Protection Mechanism Failure	/verademo/login	http://verademo.jhanna.vuln.sa.veracode.io:80	/verademo/login	New	None
10	Medium	83 Improper Neutralization of Script in Attributes in a Web Page	target	http://verademo.jhanna.vuln.sa.veracode.io:80	/verademo/login?target=profile%22%3E%3Cscript%3Ev:0d3%28995216811 3%29%3C%2Fscript%3E	New	None

© Veracode, Inc. 2021 - 2022 Usage Guidelines Responsible Disclosure Policy Help Center Contact Support

Dynamic Analysis is part of the Veracode Continuous Software Security Platform that enables your security team to find vulnerabilities in runtime environments, define and manage policy, gain a comprehensive view of the security posture of your application and API portfolios, and leverage rich analytics and reporting to make informed plans, communicate performance metrics, and produce the evidence necessary to meet regulatory requirements.

Identify vulnerabilities in web apps and APIs

Identifying runtime vulnerabilities before an attacker does is critical. Point solutions throttle the number of dynamic scans for web apps and APIs, making it difficult to scale. Managed Service solutions can't keep pace with modern development cycles.

Veracode Dynamic Analysis allows security teams to simultaneously scan hundreds of web apps and APIs to find vulnerabilities quickly.

Focus on Fixing what Matters Most

False positive scan results overwhelm teams and make it difficult to understand what needs attention. Security and development teams lose clarity on what matters most.

With a <5% false positive rate, Veracode Dynamic Analysis allows teams to focus on remediating the vulnerabilities that have the greatest impact. Detailed, actionable remediation guidance means flaws are fixed faster.

.

Streamline Reporting and Automate Ticketing

Triaging disparate reports from point solutions and handing off PDF files to development teams to investigate is inefficient, time consuming and frustrating for everyone.

Veracode's Dynamic Scan results are easy to interpret and can be managed in a single platform. Integration into popular ticketing systems like JIRA, alleviate the manual remediation process. No more PDFs!

VERACODE

How it Works

Veracode Dynamic Analysis performs a comprehensive "black box" scan from the outside-in to identify critical web application and API vulnerabilities using both authenticated and non-authenticated access.

It looks for threat vectors that are easy to exploit from the OWASP Top 10 and CWE/SANS Top 25 including SQL Injection, cross-site scripting (SSX), insufficiently protected credentials, configuration errors and information leakage.

> In a production-safe mode, Dynamic Analysis probes the attack surface and deliberately supplies malicious data using the same techniques an attacker would.

Powerful Scan Engine

Thousands of scans and over a decade of scan experience gives the result set depth and breadth. Veracode Dynamic Analysis is cloud native, using its data to continually improve scan audit capabilities.

Individual control over scans

Granular scan management allows users to set scan parameters to meet their individual needs and gives practitioners more control.

Scan behind the firewall

Veracode's Internal Scan Management feature allows users to scan applications and APIs behind a firewall in staging or pre-production environments, without complex configuration.

Web app & API scanning in a single interface

Easily scan web apps or APIs. A purpose-built interface allows users to easily upload and scan popular API specifications and see the results alongside app scans. No tool switching!

Combined crawl and audit

A one-step scan with easy to configure parameters saves time and reduce errors. No need to launch clunky appliances or allow for lengthy set up.

Promote team unity

Unify security and development teams through a single platform that integrates dynamic scanning. See program progress and opportunities for improvement.

Get the details