PEACH API SECURITY®
OVERVIEW

Peach API Security is an automated security testing solution that allows organizations to test their web APIs against the *OWASP Top-10* and *PCI Section 6.5*. Integrating Peach API Security into your existing continuous integration (CI) system ensures that your product development teams receive immediate feedback on the security of your latest release. Finding vulnerabilities earlier in the product development lifecycle saves you time, money, and reputation. Organizations use Peach API Security to reveal and correct vulnerabilities in their web APIs.

How It Works

Peach API Security performs a series of security checks against your web APIs based on requirements laid out in the OWASP Top-10. By leveraging the automated testing that your development team already performs (i.e. unit tests), Peach intelligently executes a series of fuzz and passive security tests. Once configured, interactions will primarily occur through your existing build-system interfaces. Coverage of REST, SOAP, and JSON RPC web APIs are all supported.

CI Integration

Peach was designed to seamlessly integrate into your existing CI systems. Implemented as a step in the build pipeline, Peach blocks deployment of builds that are not secure. The results of Peach's security tests are returned to the CI system, ensuring developers don't have to exit their current build tools.

Support for the following CI systems is included:

Jenkins

Travis

CircleCI*

TeamCity

Testing Profiles

Configurable testing profiles allow you to balance the depth of testing with the time available to test. Common profiles include:

Quick – Quick testing without fuzz testing, ideal for immediate results

Nightly – Quick testing with fuzz testing, ideal for nightly builds and quick results

Weekly – Complete testing, ideal for major product releases and complete test results

GENERATING TEST CASES

Peach API Security acts as a man-in-the-middle proxy, capturing traffic created by your existing automated testing. Once captured, this data is fuzzed by Peach and sent to the test target.

Integrations with popular automated testing frameworks make capturing traffic easy. In addition, custom traffic generators using REST API, Java, .NET, and Python are all supported.

JUnit

NUnit

Selenium

PyUnit

PyTest

Custom Generators

Why Choose Peach API Security

Automated testing finds vulnerabilities earlier in the product development lifecycle.

Test for OWASP Top-10 and PCI compliance with one tool.

Scalability is made easy by adding more Peach virtual appliances.

CI Integration enables bug findings in hours rather than days and ensures each build is secure.

Traffic Generated Automatically using common test suites.

Simple pass or fail reporting maps vulnerabilities to specific OWASP requirements.

SECURITY TESTING AND COMPLIANCE

Peach API Security is a comprehensive testing tool that tests against the OWASP Top-10 and PCI Section 6.5.

REPORTING

Comprehensive test results empower development teams to mitigate security weaknesses. Vulnerability data is automatically returned to your CI system. Faults are treated similarly to automation failures, blocking the release of a non-secure build. This enables developers to focus on fixing code, rather than making security decisions.

Each vulnerability includes actionable data including:

Fault Message Data – Used to efficiently find and mitigate vulnerabilities
OWASP Mapping – Identifies which OWASP Top-10 requirement failed
Exploitability Difficulty and Impact – Helping your team prioritize vulnerability fixed

OWASP Top-10 Coverage

A1 - Injection
A2 - Broken Authentication & Session Management
A3 - Cross-Site Scripting (XSS)
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
A10 - Unvalidated Redirects and Forwards

PCI Section 6.5 Coverage

6.5.1 - Injection Flaws
6.5.2 - Buffer Overflows
6.5.4 - Insecure Communication
6.5.5 - Improper Error Handling
6.5.7 - Cross-Site Scripting (XSS)
6.5.8 - Improper Access Control
6.5.9 - Cross-Site Request Forgery (CSRF)
6.5.10 - Broken Authentication

*Peach API Security currently supports commercial versions only.

All product names, logos, and brands are property of their respective owners. All company, product and service names used in this document are for identification purposes only. Use of these names, logos, and brands does not imply endorsement.