Application Penetration

Contents

- Understanding App Penetration
- Creating a new App Penetration Scenario with Designer Script
- OWASP Top Ten
- ZAP Alert Details
- App Penetration Common Questions

This section explains Appvance IQ App penetration web application security testing methodology and explains how to test for evidence of vulnerabilities within the application due to deficiencies with identified security controls.

- This Simulates dynamic attacks on software applications using the OWASP-Zap Active Scan to surface security vulnerabilities. Operates by re-using scripts/use-cases developed for other Appvance tests.
- A security test is a method of evaluating the security of a computer system or network by methodically validating and verifying the effectiveness of application security controls. A web application security test focuses only on evaluating the security of a web application. The process involves an active analysis of the application for any weaknesses, technical flaws, or vulnerabilities. Any security issues that are found will be presented as a PDF report on the result analysis page, together with an assessment of the impact, a proposal for mitigation, or a technical solution.
- A vulnerability is a flaw or weakness in a system's design, implementation, operation, or management that could be exploited to compromise the system's security objectives.
- A threat is anything (a malicious external attacker, an internal user, a system instability, etc) that may harm the assets owned by an application (resources of value, such as the data in a database or in the file system) by exploiting a vulnerability.
- App Penetration allows the user to run security tests on your app at a whole new level. While standard penetration level is to do with unregistered users. New Threads come from users which are registered. An example could be a user which registered to a sales site, is trying to purchase without entering their credit card information.
- Appvance IQ Security App Penetration system allows you to run security tests with users which are already logged in and run an actual functional test.

Related Topics

- Understanding App Penetration
- Creating a new App Penetration Scenario with Designer Script
- OWASP Top Ten
- ZAP Alert Details
- App Penetration Common Questions

Scope and safety

Run active scanning only against an approved test environment and written scope. Reuse an existing AIQ use case only when its accounts, data, and side effects are safe for security testing. Review the generated findings with the application owner before remediation; a scanner result is evidence for investigation, not proof of exploitability.

Last updated: October 15, 2026

If you have any feedback on this topic, please contact us at documentation@appvance.ai

---

Revision #5
Created 2026-07-31 15:09:41 UTC by Admin
Updated 2026-10-15 18:20:13 UTC by mmora