Understanding App Penetration

An overview of the process:

Let’s say a test case has 3 actions, every action will have a list of rest calls.

1. Log In: www.myserivice.com/login
2. Purchase: www.myserivice.com/purchase
3. Log out: www.myserivice.com/logout

Below are the Actions:

1. Appvance IQ will invoke the logging URL and will collect session (cookies)
2. Appvance IQ will pass the logging URL and session to OWASP-Zap Active Scan and will collect vulnerabilities from it.
3. Once this URL is being processed by OWASP-Zap Active Scan, Appvance IQ will restart the script, when it reaches the next URL (purchase), will send the data to OWASP-Zap Active Scan and will again restart the process, until all URLs are being processed (Spider through). This is to ensure the session is not tainted by OWASP-Zap Active Scan actions.
4. Finally, Appvance will run a test without OWASP-Zap Active Scan interaction and will return results with all vulnerabilities founds, if none are found, it will display a message telling the below.
   "Alert Detail - The alert list is empty"

Last updated: October 15, 2026

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

Interpreting the workflow

The example separates login, purchase, and logout requests so the scanner can receive the authenticated session while the functional flow continues. Use test-only accounts and data, verify that session cookies are handled as intended, and compare the scan run with a clean functional run to distinguish scanner effects from application behavior.

Revision #8
Created 2026-07-31 15:09:41 UTC by Admin
Updated 2026-10-15 21:50:16 UTC by mmora