

2.12 - Application Penetration

Application Penetration — Appvance IQ documentation.

- [Application Penetration](#)
- [Understanding App Penetration](#)
- [Create an Application Penetration Scenario in Scenario Editor](#)
- [OWASP Top Ten](#)
- [ZAP Alert Details](#)
- [Application Penetration Testing FAQ for AIQ](#)

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](#)

Last updated: June 01, 2023

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

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.

- a. Log In: www.myserivice.com/login
- b. Purchase: www.myserivice.com/purchase
- c. 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: June 02, 2023

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

Create an Application Penetration Scenario in Scenario Editor

Recommended guidance

Create application penetration scenarios only in approved test environments and with explicit customer authorization. Use Scenario Editor terminology for current AIQ workflows; keep “Designer Script” only when maintaining older assets or historical file names.

Before creating the scenario

- Confirm written scope, target application, environment, accounts, data, and allowed test windows.
- Define which checks are safe to automate and which require manual security review.
- Use dedicated test accounts and non-production data.
- Coordinate with monitoring, security, and application owners to prevent false incidents.

Scenario guidance

1. Start with a controlled login and navigation path.
2. Add assertions that prove expected application behavior and safe failure handling.
3. Record evidence without exposing secrets, personal data, or exploit details beyond the approved audience.
4. Review results with security stakeholders before sharing externally.

Last updated: October 6, 2026

OWASP Top Ten

AppvanceIQ performs vulnerability testing according to the OWASP Top Ten. For more information see [OWASP Top Ten](#).

"The OWASP Top Ten is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications."
- The OWASP Foundation

Last updated: June 02, 2023

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

ZAP Alert Details

AIQ has support for ZAP (Zed Attack Proxy), which is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.

For a complete list of alerts that can be detected by the ZAP proxy see: [ZAP Alert Details](#)

Last updated: June 02, 2023

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

Application Penetration Testing FAQ for AIQ

Recommended guidance

Application penetration testing content must stay within approved scope and customer authorization. Use AIQ and Scenario Editor terminology for current workflows, and avoid documenting steps that could be interpreted as bypassing security controls outside an approved test.

Common questions

- **Can AIQ automate security checks?** Yes, when the checks are approved, repeatable, and safe for the target environment.
- **Can production systems be tested?** Only with explicit written authorization, controls, and an agreed test window.
- **Can real credentials or customer data be used?** Avoid them; use dedicated test accounts and masked/non-production data.
- **What evidence should be captured?** Capture results, logs, screenshots, and timestamps without exposing secrets.

Escalation checklist

1. Confirm scope, owner, target, environment, and allowed techniques.
2. Coordinate with security monitoring teams before execution.
3. Review findings with approved stakeholders only.
4. Document risks, remediation, and retest expectations.

Last updated: October 6, 2026