Security Testing Cheat Sheet

Know what you're asking for and what to expect!

Vulnerability Scan

What is it?

The scan uses automated tools to identify known security issues through matching conditions with known vulnerabilities.

What do you get?

Reported risk level is set automatically by the tool with no manual verification or interpretation of the results prior to issue. Great for identifying technical vulnerabilities at a low financial cost. However, generates high level of false positives while missing certain types of issues, which limits the overall level of assurance gained.

Vulnerability Assessment

What is it?

Using security tester's knowledge to drive appropriate use of automated tools and test scripts.

What do you get?

Report manually created to place the findings into the context of the environment under test. An example would be removing common false positives from the report and deciding risk levels that should be applied to each report finding to improve business understanding and overall context of a finding. Great for increasing the level of assurance gained through automated testing.

Security Assessment

What is it?

Building upon Vulnerability Assessment by adding manual verification to confirm exposure, but does not include the use of exploitation code to gain further access to systems.

What do you get?

A Security Assessment is looking to gain a broad coverage of the systems under test but not the depth of exposure that a specific vulnerability could lead to. False positives should be excluded through analysis of results. Great for exposing business logic flaws and identifying security vulnerabilities that automated tools are unable to identify. Therefore leading to a higher level of assurance. However, time and effort required to complete are higher than vulnerability scanning and assessments and requires a higher level of technical skill to deliver.

Penetration Test

What is it?

Penetration testing simulates an attack by a malicious party by using tools and manual investigation to identify weaknesses. Testing involves exploitation of found vulnerabilities to gain further access. Using this approach will result in an understanding of the ability of an attacker to gain access to confidential information, affect data integrity or availability of a service and the respective impact.

What do you get?

This approach looks at the depth and impact of attack as compared to the Security Assessment approach that looks at the broader coverage. Great for understanding the depth of exposure from a vulnerability but can result in a narrow focus and potentially miss vulnerabilities that would have been identified through a security assessment. Level of assurance gained is directly associated with the ability of the tester, the scope of engagement and the time and effort allocated.