




# Web Application Security

## Overview table penetration tests




 <b>SPOT CHECK LEVEL 1</b>	 <b>REGULAR PENTEST LEVEL 3</b>	 <b>ADVANCED PENTEST LEVEL 3</b>
<b>Initial assessment</b> Initial assessment of the security level in the context of a sample.	<b>For most applications</b> Deep investigation to identify the most common risks or vulnerabilities for web applications.	<b>High level of security</b> Extended, deeper investigation with more test cases, e.g. for applications that process business-critical operations and sensitive data.

### GENERAL

<b>Attacker level</b>	Simulation of an attacker using simple techniques to identify easy-to-find/exploitable vulnerabilities (low-hanging fruits).	Simulation of a resolute attacker, who uses current attack techniques from the hacker scene.	Simulation of a resolute and skilled attacker using current attack techniques from the hacking scene and targeting the web application.
<b>Test methods</b>	Random automated tests & manual penetration tests	Automated tests & manual penetration tests, which are usually not found by automated tools.	Automated tests & deeper manual penetration tests, which are usually not found by automated tools.
<b>Test cases</b>	Sample examination	Test cases that take into account the OWASP Top 10 vulnerabilities and thus contain the most frequently exploited security risks for web applications.	Test cases that consider the OWASP Top 10 vulnerabilities (see Regular Pentest) & additional, selected test cases/requirements from the OWASP Application Security Verification Standard (ASVS)

### TEST CONTENT

<b>Portscans (web server)</b>	<b>Basic portscan</b> (Top 100 TCP)	<b>Advanced portscan</b> (Top 1000 TCP/Top 10 UDP)	<b>Complete portscan</b> (all 65535 TCP/Top 10 UDP)
<b>Vulnerability scan (web server)</b>		<b>Basic</b> vulnerability scan	<b>Complete</b> vulnerability scan
<b>SSL/TLS verification/scans (web server)</b>	✓	✓	✓

	 SPOT CHECK LEVEL 1	 REGULAR PENTEST LEVEL 3	 ADVANCED PENTEST LEVEL 3
Provision of technical attachments, e.g. the raw results of the port & vulnerability scans			✓
<b>REPORT</b>			
Overview of all test cases in the report, also positive ones			Optionally orderable
<b>OTHER AND TEST PERIODS</b>			
Re-testing of the findings after remediation	Not included	Up to 5 (within 3 months)	Unlimited (within 3 months)
Test time frame	≤ 3 days	≥ 5 days	≥ 10 days