Security Testing Basics with OWASP PDF

Security testing looks for weaknesses that could expose data or let attackers misuse an application. Testers can use the OWASP Top 10 as a checklist: access control, injection, authentication, misconfiguration and more. Test only systems you are allowed to test, report findings responsibly and involve a security specialist for deeper work.

Key takeaways

- Only test applications you own or have written permission to test.
- The OWASP Top 10 lists common web application risk categories.
- Broken access control and injection are frequent and serious issues.
- Simple checks such as input validation and session handling are within a tester's reach.
- Security needs a team effort that includes developers, operations and specialists.

What is security testing basics?

Security testing is the practice of checking software for vulnerabilities and weak controls, so that data, accounts and services are protected against misuse, and OWASP provides widely used lists and guides for web application risks.

Why should testers learn security basics?

Functional tests ask whether features work. Security tests ask whether features can be abused. A form that accepts any input, a link that shows another user's data when an ID changes, or a session that never expires are all defects, even if the feature "works". Testers who know the basics catch many of these early and speak the same language as security teams.

What are the ground rules?

Test only your own systems, test environments or applications for which you hold written permission. Never run attack tools against live sites you do not own. Do not access real user data. Report issues privately to the right owner. If you find a serious weakness, stop and escalate instead of exploring further.

What is the OWASP Top 10?

OWASP, the Open Worldwide Application Security Project, publishes a list of the most critical web application risks. The list is updated from time to time, so read the current version. Categories

include broken access control, cryptographic failures, injection, insecure design, security misconfiguration, vulnerable components, authentication failures, integrity failures, logging gaps and server-side request forgery.

Which risks can a tester check by hand?

Risk	Simple check
Broken access control	Can user A open user B's record by changing an ID in the URL?
Injection	Does a field behave strangely with quotes or special characters?
Authentication	Are weak passwords accepted? Is there a lockout or delay after repeated failures?
Session handling	Does logout end the session? Does the session expire?
Sensitive data	Is data shown in URLs, logs or error messages?
Misconfiguration	Are default pages, debug output or directory listings visible?
Treat these as prompts for investigation, not a full audit.	

What is injection in simple words?

Injection happens when an application mixes user input into a command, such as a database query, without handling it safely. For testers, the sign is unusual errors or behaviour after entering special characters. The fix belongs to developers and uses safe query methods; the tester's job is to notice, record and report.

How does access control testing work?

Create two normal users and one admin in a test environment. Check that each can see only what they should. Try opening restricted pages directly, repeating requests after logout and changing identifiers. Verify that hidden buttons are also blocked on the server, since hiding a button in the interface does not protect the data behind it.

What tools can help?

Browser developer tools show requests, cookies and headers. Intercepting proxies and scanners can find common issues in a permitted test environment, and dependency scanners find vulnerable libraries. Tool results include false alarms, so confirm each finding by hand before reporting.

How do I report a security finding?

Give a clear title, the affected area, steps to reproduce, impact in plain words, evidence and a suggested severity. Avoid sharing sensitive details in open channels. Follow your company process for vulnerability reports and keep a record of fixes and retests.

How does security fit into the life cycle?

Shift security left: review designs for threats, add security cases to test plans, scan dependencies in the pipeline, run checks on every build and repeat tests before releases. Train developers and testers together.

What should I avoid?

Do not assume that a firewall solves everything, do not rely on one tool, do not test production without approval and do not ignore low-severity items that can combine into larger problems.

How do I practise security testing safely?

Use deliberately vulnerable practice applications that are meant to be attacked, run them on your own machine or in a lab, and follow their instructions. Work through one risk category at a time: read the OWASP description, find the matching exercise, note how the flaw looks from the outside and how a developer would fix it. Write a short report for each exercise using the template. This builds skills and vocabulary without legal risk, and it gives you something concrete to talk about in interviews.

What is the difference between security testing and penetration testing?

Security testing is a broad activity that includes reviews, scans and checks across the life cycle. Penetration testing is a focused exercise where specialists simulate an attack within an agreed scope and time. Testers on a product team normally do the first kind and request the second from specialists before major releases. Knowing the difference helps you plan and avoid promising more than a basic check can deliver.

Frequently asked questions

What is the OWASP Top 10?

It is a regularly updated list from OWASP of the most critical web application security risk categories, used as an awareness and testing guide.

Can a manual tester do security testing?

Yes, at a basic level. Testers can check access control, input handling and sessions, and escalate deeper issues to security specialists.

Is it legal to test any website for security?

No. Test only systems you own or have written permission to test, because unauthorised testing can be illegal and harmful.

What is broken access control?

It is when users can reach data or actions they should not, for example by changing an ID in a URL, and it is a common high-impact flaw.

Do scanners find everything?

No. Scanners miss logic flaws and also report false alarms, so combine them with manual checks and expert review.

Sources and further reading

- OWASP Top Ten
- OWASP Web Security Testing Guide

About this PDF

These PDFs are study material for learning and revision. They are not a certificate, a degree or a promise of a job, and technology changes, so check official documentation for the latest details. Spot an error? Write to info@uncodemy.com and the trainer team will review it.

More free resources and courses: uncodemy.com | info@uncodemy.com | +91 98183 66550