NetSPI™

Do you have your own web application penetration testing checklist?

5 Tips to get you started

1. Agree on the scope and application information

Having a scoping call with your penetration testing partner is critical to ensure that all parties follow the penetration test rules of engagement. This step also helps build out your web application checklist as it will identify areas that may be out of scope, additional technologies that are in use, functional elements that deserve a higher degree of focus, or specific manual test cases that the client has identified based on their business threat model.

2. Create testing categories

Grouping tests into logical categories can make it easier to build and maintain checklists over time. Use the **OWASP Top 10** for guidance, but tailor the categories specific to your environment.

Common categories that NetSPI recommends:

- Authentication bypass
- Injections issues
- Sensitive data exposure
- Application functionality and business logic checks
- 3rd party components checks
- Session management
- Weak application configuration checks
- Weak server configuration checks
- Weak platform configuration checks

3. Create test baselines

No checklist will cover every scenario for all applications but creating tests that cover core technologies and processes used during most web application penetration tests will save you time and ensure that you and your organization are covering the most common vulnerabilities.

Online resources to get you started:

- **OWASP Testing Guide**
- **Web Application Hackers Handbook**

Project-specific information:
A checklist serves as a place to store required procedures for engagements. It can also be a valuable place to store information discovered before, during, and after a test. A dynamic checklist creates a single source of information related to the test.

Common categories that NetSPI recommends:

- Connection information
- Application overviews notes
- Application contacts
- Application-specific testing requirements
- Why certain procedures were skipped/modified
- Relevant notes for future testers

4. Link to external content

Trying to fit every verbose testing procedure into your checklist may not be plausible but including links to relevant information can help you. NetSPI recommends limiting procedures to the most common scenarios and linking tothe outliners. Including a small summary with resources and any troubleshooting that occurred during the first use can greatly increase the speed with which they can be used.

5. Choose a testing platform

Choosing the right platform for web application penetration testing can help free up time for digging into vulnerabilities and issues not covered in your baseline checklist process. Several checklist platforms exist online that can be leveraged to create and maintain a list of common tasks. We recommend using one that can tie the tests to the findings that will turn into the report or ticket for the business owner. This helps reduce redundant tasks and increases the speed at which your team can get results to the people who need them.

6. Track and remediate

The whole point of testing for web application vulnerabilities is to fix them before someone else can take advantage of them. Having an established process for delivering identified vulnerabilities to the right people should be your first step at the end of your test.

- **Bug bounty hunters**
  Make sure to follow the affected vendor's channel — or work through a broker like HackerOne and Bugcrowd.
- **Internal penetration testers**
  Work with internal business units to ensure the vulnerability is reported and remediated in accordance with the company's policy. We recommend having a checklist and a reporting process that integrates into ticketing systems. For example, The NetSPI Platform seamlessly integrates with your existing technology stack to streamline workflows and save countless hours of manual labor.
- **Third-party proactive security solutions**
  76% of companies have experienced some type of cyberattack in which the attack itself started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset.[1] Partnering with a third-party provider who can advise on security measures to aid a proactive approach is an important step toward maturing programs.

Learn more about The NetSPI Platform by visiting www.netspi.com.

[1]ESG by TechTarget: Research Report: Security Hygiene and Posture Management Remains Decentralized and Complex: https://research.esg-global.com/reportaction/515201639/Marketing

You deserve The NetSPI Advantage

250+ In-house security experts

Intelligent process

Advanced technology

Your proactive security partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), Attack Surface Management (ASM), and Breach and Attack Simulation (BAS).