**Tools for Security Testing**

1. [Acunetix](https://httpslink.com/Visit-Acunetix-web-app-sec-page)

[Acunetix logo](https://httpslink.com/Visit-Acunetix-web-app-sec-page)

Acunetix online is a premium security testing tool worth trying. You can get the trial version for Acunetix here.

Acunetix Online includes a fully automated network vulnerability scanner that detects and reports on over 50,000 known network vulnerabilities and misconfigurations.

It discovers open ports and running services; assesses the security of routers, firewalls, switches, and load balancers; tests for weak passwords, DNS zone transfer, badly configured Proxy Servers, weak SNMP community strings, and TLS/SSL ciphers, among others.

It integrates with Acunetix Online to provide a comprehensive perimeter network security audit on top of the Acunetix web application audit.

1. **NetSparker**



NetSparker acts as a one-stop shop for all the web security needs. Available as both hosted as well as self-hosted solution, this platform can be easily integrated completely in any type of test and dev environment. NetSparker has a trade-marked Proof-Based-Scanning technology that uses automation to identify vulnerabilities and verify false positives, thus eliminating the need for unnecessary investment of huge man hours.

1. **ImmuniWeb**



ImmuniWeb is a next-gen platform that employs Artificial Intelligence to enable security testing. This AI-enabled penetration testing platform offers holistic benefits package for security teams, developers, CISOs, as well as CIOs. Having a one-click virtual patching system, this platform assists continuous complaince monitoring. It boasts a proprietary Multilayer Application Security Testing technology and checks a website for compliance, server hardening, and privacy.

1. **Vega**



It is a free, open-source vulnerability scanning and testing tool written in Java. Vega is GUI enabled and works with OS X, Linux and Windows platforms. It’s automated scanner powered by a website crawler that facilitates quick tests. The intercepting proxy aids tactical inspection by observing and monitoring client-server communication. Vega can detect web application vulnerabilities like blind SQL injection, shell injection, reflected and stored cross-site scripting, etc. Its detection modules are written in JavaScript and can be used to create new attack modules as and when required with APIs

1. **Google Nogotofail**



It is a network traffic security testing tool. It checks application for known TLS/SSL vulnerabilities and misconfigurations. Nogotofail provides a flexible and scalable way of scanning, identifying, and fixing weak SSL/TLS connections. It checks whether or not they are vulnerable to man-in-the-middle (MiTM) attacks. It can be set up as a router, VPN server or proxy server and works for Android, iOS, Linux, Windows, Chrome, OS, OSX, and any other device that is used to connect to the internet.