**software security testing tools**

**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.

**2. 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.

**3. 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.

**4. Wapiti**

Wapiti is a command-line application that crawls through webpages to detect such scripts and forms where a data can be injected. It performs a blackbox scan and injects payloads in the detected scripts to check if it is vulnerable. With support for both GET and POSTHTTP attack methods, this tool generates vulnerability reports in various formats and features different levels of verbosity. It detects vulnerabilities like file disclosure, database injection, file inclusion, cross Site Scripting (XSS), weak .htaccess configuration etc. It is able to differentiate between permanent and reflected XSS vulnerabilities and raises warnings whenever an anomaly is found.

**5. 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.