ICS ACTIVE LEARNING REPORT

List and state briefly security testing tools.

**Presented By:**

**PC-44 Tejas Redkar**

**PC-49 Gayatrini Neogi**

**PC-50 Atharva Chaher**

**PC-63 Jinal Gulhane**

Introduction:

From mini eateries to big-box retailers, from small organizations to federal bodies, cyber attackers are eyeing every small opportunity to steal valuable data on Personality Identifiable Information (PII).

Whether it’s Facebook or Equifax, a single vulnerability, a tiny flaw in the security system, has caused them to lose both revenues and reputation.

If security incidents like these have taught us anything, it is that web security cannot be taken lightly, and even the best of us are not safe from it.

Web security testing tools are useful in proactively detecting application vulnerabilities and safeguarding websites against malicious attacks.

Some of the security testing tools are:

1. NetSparker:

Automatic, accurate and easy-to-use web application security scanner .

NetSparker acts as a one-stop shop for all the web security needs.

Available as both a hosted as well as self-hosted solution.

NetSparker has a trademarked Proof-Based-Scanning technology that uses automation to identify vulnerabilities and verify false positives.

1. Google Nogotofail:

It is a network traffic security testing tool.

Nogotofail provides a flexible and scalable way of scanning, identifying, and fixing weak SSL/TLS connections.

It checks whether they are vulnerable to man-in-the-middle (MiTM) attacks.

It can be set up as a router, VPN server, or proxy server.

3.ImmuniWeb:

ImmuniWeb is a next-gen platform that employs Artificial Intelligence to enable security testing.

This AI-enabled penetration testing platform offers a holistic benefits package for security teams, developers, CISOs, as well as CIOs.

Having a one-click virtual patching system, this platform assists in continuous compliance 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 an 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. Wapiti:
2. Wapiti:

Wapiti is a command-line application that crawls through webpages to detect such scripts and forms where data can be injected.

It performs a black box scan and injects payloads in the detected scripts to check for vulnerability.

With support for both GET and POST HTTP attack methods, this tool generates vulnerability reports in various formats and features different verbosity levels.

It detects vulnerabilities like file disclosure, database injection, file inclusion, cross-site scripting (XSS), weak .htaccess configuration, etc.

It can differentiate between permanent and reflected XSS vulnerabilities and raises warnings whenever an anomaly is found.

1. Acunetix:

Acunetix, with its vulnerability scanner, pioneered automated web application security testing.

The Acunetix Vulnerability Scanner features innovative black-box scanning and SPA crawling techniques in the form of AcuSensor and DeepScan.

The multi-threaded, DeepScan crawler has the capability to run an uninterrupted scan of WordPress installation for over a thousand vulnerabilities.

A Login Sequence Recorder enables the tool to scan password-protected fields, whereas an in-built vulnerability management system helps generate various technical and compliance reports.

CONCLUSION:

Therefore, we have seen several tools that are used to test a website for various errors and security breaches. These security testing tools helps us in making sure that we have a strong website which would stand attacks from hackers.