Name: Priyanka Salvi

Batch: 7670

SECURITY TESTING TOOLS

1) Zap (Zed Attack Proxy): Multi-platform, open-source online application security testing tool developed by OWASP (Open Web Application Security Project).

   Zap utilized by both newcomers and experts its user-friendly interface.

   It will perform web application scanning automatically.

   ZAP is a Java application.

   ZAP may also be used to intercept a proxy and test a webpage manually.

   - Application error disclosure
   - Cookie not HttpOnly flag
   - SQL injection
   - Application error disclosure
   - XSS injection
   - Missing anti-CSRF tokens and security headers
   - Private IP disclosure
   - Cookie not HttpOnly flag
   - Session ID in URL rewrite

2) Netsparker: It is used to detect the web application's vulnerabilities in a unique way, as well as to verify whether the application's weaknesses are correct or erroneous.
   Netsparker is an automated online application security scanner that allows you to scan websites, web applications, and web services for security issues while remaining fully customizable.

3) Iron Wasp: Iron Wasp is a strong open-source scanning tool that can detect over 25 different types of web application flaws. It can also distinguish between false positives and false negatives. Iron Wasp aids in the discovery of a wide range of flaws, including:

- Broken authentication
- Cross-site scripting
- CSRF
- Hidden parameters
- Privilege escalation

4) Wfuzz: Wfuzz is a tool for brute-forcing Web applications. It can be used to find non-linked directories, servlets, scripts, and other resources, as well as brute-force, GET and POST parameters for checking various types of injections (SQL, XSS, LDAP, and so on), brute-force Forms parameters (User/Password), and fuzzing. Wfuzz is a popular tool for brute-forcing web applications that were created in Python. The open-source security testing tool has no GUI interface and is usable only via the command line. Vulnerabilities exposed by Wfuzz are:
    - LDAP injection
    - SQL injection
    - XSS injection

5) Grabber: The Grabber is a simple web application scanner that can be used to search forums and personal websites. The Python-based lightweight security testing tool has no graphical user interface. Grabber discovered the following vulnerabilities:
    - Backup files verification
    - Cross-site scripting
    - File inclusion
    - Hidden parameters
    - Privilege escalation
    - Simple AJAX verification
    - SQL injection