Unit IV

Web Applications Tools

---

1. Scanning for Web Vulnerabilities Tools

Web vulnerability scanning tools are used to find security weaknesses in websites and web applications before hackers can misuse them.

1.1 Nikto Tool

What is Nikto?

Nikto is a free and open-source web security scanning tool.

It is mainly used to check web servers for common security problems.

👉 Think of Nikto as a health check-up tool for a website.

How Nikto Works (in Simple Words)

1. Banner Grabbing
    - Nikto checks the information shown by the web server, such as:
        - Server name
        - Software version (Apache, PHP, etc.)
    - If the server is using old or unsafe software, Nikto reports it.
2. Checking Known Vulnerabilities
    - Nikto has a big list of already known security problems.
    - It checks if the website has issues like:
        - XSS (Cross-Site Scripting)
        - SQL Injection
        - Old or insecure software
3. Checking Wrong Settings (Misconfigurations)
    - Nikto checks if the server is not properly set up, such as:
        - Directory listing is ON
        - Default files are still present
    - These mistakes can help attackers enter the system easily.
4. Checking HTTP Methods
    - Nikto checks which actions (GET, POST, PUT, DELETE) are allowed.
    - Some actions are dangerous if not restricted.
5. Finding Other Security Issues
    - Nikto also looks for:
        - SSL/TLS problems
        - Information leaks
        - Session-related issues

Who Uses Nikto?

- Security Auditors – to check website security
- Penetration Testers – to find weak points
- Website Administrators – to keep websites safe
- Developers – to fix security issues during development

1.2 W3AF Tool (Web Application Attack and Audit Framework)

What is W3AF?

W3AF is an open-source tool used to scan web applications for security problems.

👉 If Nikto checks the server, W3AF mainly checks the web application itself.

How W3AF Works (in Simple Words)

1. Automatic Scanning
    - W3AF automatically scans the website without much manual effort.
    - It behaves like a real user and attacker.
2. Finding Common Vulnerabilities
    - It checks for serious problems such as:
        - SQL Injection
        - Cross-Site Scripting (XSS)
        - File Inclusion (LFI, RFI)
        - Command Injection
3. Crawling the Website
    - W3AF first moves through all web pages, links, and forms.
    - This helps it understand the structure of the website.
4. Exploiting Vulnerabilities (Safely)
    - W3AF can show how an attacker could misuse a weakness.
    - This helps in understanding the risk.
    - It can be controlled to avoid damage.
5. Detailed Report
    - After scanning, W3AF gives a report with:
        - Type of vulnerability
        - Severity (Low, Medium, High)
        - Suggestions to fix the issue

Who Uses W3AF?

- Security Auditors – for security assessment
- Penetration Testers – to simulate attacks
- Web Developers – to make applications secure
- Website Administrators – to protect live websites

Simple Difference Between Nikto and W3AF

Tool	Main Focus
Nikto	Web server security
W3AF	Web application security

Simple Conclusions

- Nikto checks *server-side weaknesses*
- W3AF checks *application-level weaknesses*
- Both tools help find problems before hackers do

---

2. HTTP Utilities

HTTP utilities are tools used to communicate with servers, test web services, and secure data transfer over networks.

2.1 Curl

Curl is a command-line utility used to transfer data between a client and a server using various internet protocols such as HTTP, HTTPS, FTP, etc.

How it Works:

- Curl sends requests to a server and receives responses.
- It allows direct interaction with websites and APIs without using a web browser.

Common Uses:

- API Testing: Send GET, POST, PUT, DELETE requests.
    - Example:
      `curl http://example.com`
- File Downloading: Download files from the internet.
    - Example:
      `curl -O https://example.com/file.zip`
- Custom Headers: Send headers for authentication.
    - Example:
      `curl -H "Authorization: Bearer token" https://api.example.com/data`

Advantages:

- Lightweight and fast
- Useful for debugging web services
- Widely used by developers and testers

2.2 OpenSSL

OpenSSL is an open-source software library that implements SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols for secure communication.

How it Works:

- Encrypts data exchanged between client and server.
- Helps generate cryptographic keys and digital certificates.
- Tests SSL/TLS security of servers.

Common Uses:

- Generate SSL Certificates:
  - Example:
    `openssl genpkey -algorithm RSA -out private_key.pem`
- Test SSL Connections:
  - Example:
    `openssl s_client -connect example.com:443`
- Encrypt/Decrypt Data:
  - Example:
    `openssl enc -aes-256-cbc -in file.txt -out file.enc`

Importance:

- Ensures confidentiality and integrity of data
- Essential for HTTPS and secure communications

2.3 Stunnel

Stunnel is a tool that creates a secure SSL/TLS tunnel to protect applications that do not support encryption by default.

How it Works:

- Acts as a proxy between client and server.
- Encrypts non-secure protocols using SSL/TLS.

Common Uses:

- Securing Non-SSL Applications: (FTP, SMTP, POP3)
- Email Security: Encrypts email communication.
- VPN-like Secure Tunnels: Provides encrypted communication without a full VPN.

Advantages:

- Adds encryption without modifying applications
- Simple and effective security solution

Summary of HTTP Utilities

Tool	Purpose
Curl	Data transfer and API testing
OpenSSL	Encryption, certificates, SSL/TLS security
Stunnel	Securing non-SSL applications

---

3. Application Inspection Tools

These tools are used to identify vulnerabilities in web applications.

3.1 Zed Attack Proxy (ZAP)

ZAP is an open-source web application security testing tool.

How it Works:

- Acts as a man-in-the-middle between browser and web application.
- Scans for security flaws.

Uses:

- Detects vulnerabilities like authentication issues and data leaks
- Used by penetration testers and developers
- Helps improve application security during development

3.2 SQLMap

SQLMap is an automated tool for detecting and exploiting SQL injection vulnerabilities.

How it Works:

- Injects SQL queries into web inputs to test database security.

Uses:

- Identifies database vulnerabilities
- Helps retrieve sensitive data during ethical hacking tests
- Used by security professionals for penetration testing

3.3 DVWA (Damn Vulnerable Web Application)

DVWA is an intentionally vulnerable web application designed for security training.

How it Works:

- Contains built-in vulnerabilities for practice.

Uses:

- Learning and practising ethical hacking
- Understanding vulnerabilities like SQL Injection and XSS
- Safe environment for beginners

3.4 WebGoat

WebGoat is a deliberately insecure web application used for learning web security concepts.

How it Works:

- Provides lessons along with vulnerabilities.

Uses:

- Educational training in web security
- Practice CSRF, XSS, authentication flaws
- Widely used in academic environments

Summary of Application Inspection Tools

Tool	Purpose
ZAP	Web vulnerability scanning
SQLMap	SQL injection testing
DVWA	Hands-on vulnerability practice
WebGoat	Learning web security concepts

Note:

All these tools are legal and ethical when used only for authorised testing and educational purposes. They are widely used by cyber security professionals to protect systems from cyberattacks.

4. Password Cracking and Brute-Force Tools

1. John the Ripper

What it is:

John the Ripper is a widely used password-cracking tool designed to recover passwords from encrypted data, such as password hashes.

How it works:

It attempts to guess passwords by trying different combinations of letters, numbers, and symbols. It uses methods such as:

- Dictionary attacks: Using a list of common or leaked passwords.
- Brute-force attacks: Trying all possible combinations until the correct one is found.

Uses:

- Used by security professionals to test whether user passwords are strong or weak.
- Commonly used in penetration testing (ethical hacking).
- Supports many types of password hashes, making it useful for different systems.

---

2. L0htcrack

What it is:

L0htcrack is a password-cracking tool mainly used for cracking Windows password hashes.

How it works:

It works in a similar way to John the Ripper by trying multiple password combinations. It also supports:

- Dictionary attacks
- Brute-force attacks

Uses:

- Used to test the strength of passwords on Windows systems.
- Used by system administrators and security professionals to assess network security.
- Helpful in penetration testing to identify weak Windows passwords.

---

3. Pwdump

What it is:

Pwdump is a tool used to extract (dump) password hashes from Windows systems. These hashes can later be cracked using tools like John the Ripper or L0htcrack.

How it works:

Pwdump collects password hashes stored in Windows system files. This allows security testers to perform offline password cracking, which is safer and faster than attacking a live system.

Uses:

- Used to obtain password hashes for offline cracking.
- Helps in penetration testing to evaluate password storage security.
- Assists in gathering password data for further security testing.

---

4. THC-Hydra (often called Hydra)

What it is:

THC-Hydra is a fast and flexible password-cracking tool that supports many network services such as SSH, FTP, HTTP, Telnet, and more.

How it works:

It performs:

- Brute-force attacks
- Dictionary attacks

  to guess passwords for network login services. It can target multiple protocols, making it highly versatile.

Uses:

- Used by penetration testers to test network services like SSH and FTP.
- Helps security professionals identify weak passwords and vulnerable services.
- Used to simulate real-world password attacks on network logins.

Summary of Purpose and Uses

- John the Ripper:

  Cracks password hashes to test password strength across many systems.
- L0htcrack:

  Focuses on cracking Windows password hashes to detect weak passwords.
- Pwdump:

  Extracts password hashes from Windows systems for offline cracking.

- THC-Hydra:

  Cracks passwords for network services such as SSH, FTP, and HTTP.

Overall Importance

All these tools are used in security testing (penetration testing) to identify weak passwords that attackers could exploit. They help organisations improve password policies and strengthen security systems by simulating real password-cracking attempts.