Day 19: Website Pentesting & DNS Tools

Website Pentesting Tools

- **Pentest Tools:** An online platform for finding website vulnerabilities automatically. It gives professional reports.
- **Web-Check.xyz:** A simple online tool to see what tech a website uses and find weak spots.

These tools help in the early stages of penetration testing (reconnaissance and scanning).

HTTP Status Codes Overview

These codes are how servers respond to requests. They help testers understand what the server is doing.

Code	Meaning
200	OK – Everything worked
301	Moved Permanently – Page moved
403	Forbidden – No access
404	Not Found – Page not there
500	Internal Server Error – Server problem

Knowing these codes helps find server issues or security flaws.

Python Virtual Environment

Used to keep Python project dependencies separate. This stops different versions of packages from clashing. Steps usually involve making a `.venv` folder and activating it.

DNS Lookup Tools

Understanding how DNS works is important for reconnaissance. These tools get DNS records (like A, MX, NS, TXT).

- **dig:** Gets detailed DNS records like name servers, IP addresses, and mail servers.
- **nslookup:** Another tool for getting domain records and checking DNS problems.

These tools show network structure for finding more attack points.

Key Learnings