Cybersecurity Daily Dairy

Day 19: Website Pentesting & DNS Tools

Date: July 9, 2025

Website Pentesting Tools

Online Pentest Platforms:

1. **Pentest Tools**

A web-based platform that helps identify vulnerabilities on websites. It automates common security tests and provides professional-grade vulnerability reports.

2. **Web-Check.xyz**

A lightweight online tool used to detect the underlying technologies of a target website and highlight potential weak points in the setup.

These tools assist during the reconnaissance and scanning phases of penetration testing.

HTTP Status Codes Overview

HTTP status codes are server responses to client requests, helping testers interpret how the server handles different scenarios.

Common codes:

Code	Meaning
200	OK – Successful response
301	Moved Permanently – Redirection
403	Forbidden – Access denied
404	Not Found – Resource missing
500	Internal Server Error – Server-side problem

Understanding these codes helps in analyzing web server behavior and identifying misconfigurations or security issues.

Python Virtual Environment

Virtual environments are used to isolate Python project dependencies. This helps in managing different package versions for different tools or scripts without conflicts.

Steps generally include creating a .venv directory and activating the environment for package installation.

DNS Lookup Tools

Understanding DNS infrastructure is a key part of reconnaissance. These tools help extract DNS records, such as A, MX, NS, and TXT.

1. **dig**

A DNS lookup tool that retrieves detailed DNS records of a domain, including name servers, IP addresses, and mail servers.

2. **nslookup**

Another DNS query tool used to obtain domain-related records and test DNS resolution issues.

These tools reveal network structure and infrastructure that can be used for further attack surface mapping.

Key Learnings

- Web-based penetration testing tools simplify and automate vulnerability detection.
- HTTP status codes provide critical insights into how servers respond to different requests.
- DNS analysis using tools like dig and nslookup supports infrastructure reconnaissance.
- Python virtual environments are essential for managing tool dependencies in a clean and isolated way.