

Penetration Testing on Web Server



**Model Institute of Engineering & Technology (Autonomous) Permanently
Affiliated to the University of Jammu Accredited by NAAC with “A” Grade
Jammu, India 2025**

Cybersecurity Assessment Process

Project Overview

Objective: Assess and harden the security of a company's web server.

- Scope: 1. Web server penetration testing
2. Employee social engineering protection
- Approach: 1. Footprinting and Reconnaissance
2. Vulnerability Scanning
3. Exploitation
4. Reporting and Remediation



Web Server Penetration Testing

Assessing web server security

Training employees against social engineering

Employee Social Engineering Protection



Footprinting and Reconnaissance

Gathering initial information

Identifying security weaknesses

Vulnerability Scanning



Exploitation

Testing identified vulnerabilities

Documenting findings and fixing issues

Reporting and Remediation



Footprinting and Reconnaissance

Footprinting is gathering information about a target system before launching an attack

- IP Address, Server Location, OS
- Web Server Version & Built-in Technologies
- WHOIS Data & Registrar Info
- Email IDs, LinkedIn & Social Profiles of Employees
- Company Address & Director Info

Footprinting Information

IP Address

Gathering IP address, server location, and operating system details.

Web Server

Identifying web server version and built-in technologies.

WHOIS Data

Collecting WHOIS data and registrar information.

Email IDs

Finding email IDs, LinkedIn, and social profiles of employees.

Company Address

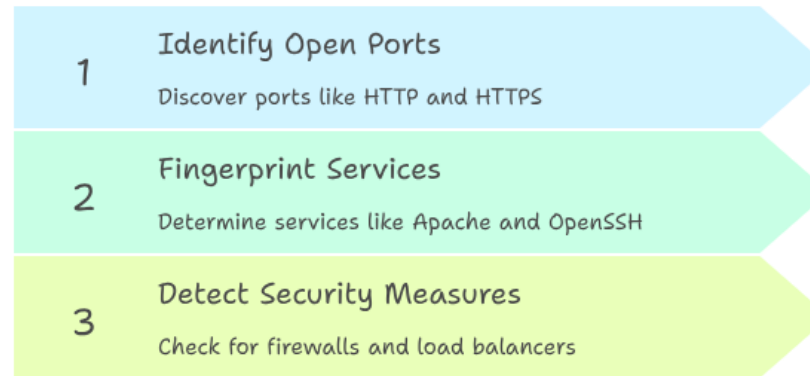
Obtaining company address and director information.

Port and Service Enumeration

Scanning is used to identify open ports and services running on the server.

- Open Ports Discovered: 80 (HTTP), 443 (HTTPS), etc.
- Service Fingerprinting (e.g., Apache 2.4.41, OpenSSH).
- Firewall/Load Balancer Presence.

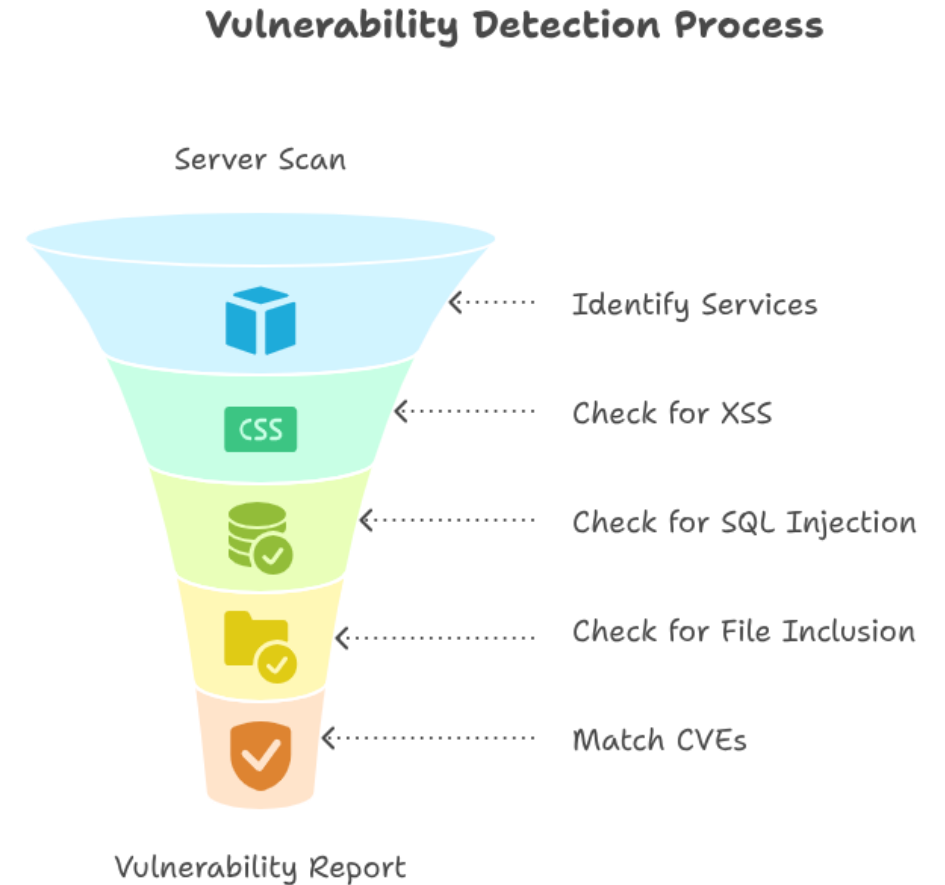
Server Security Assessment Funnel



Vulnerabilty Assessment

Scanning the server for known vulnerabilities in services & web apps.

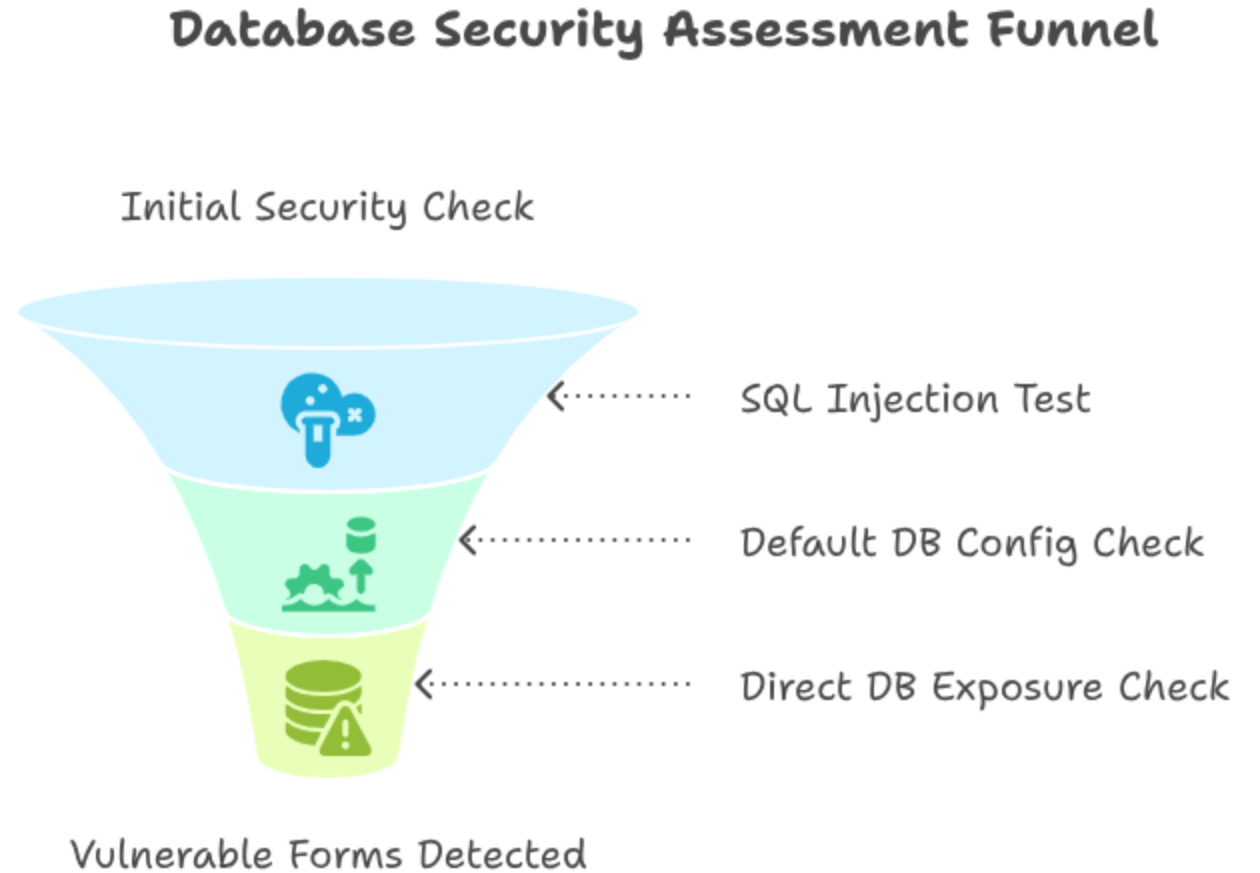
- Checked for XSS, SQL Injection, File Inclusion.
- CVEs matched using service version.



Database Exposure Testing

Checking for access to backend database or leaks.

- SQL Injection Test.
- Checked for default DB config.
- No direct DB exposed, but vulnerable forms detected.



Tools and Their Purpose

Summary of key tools used:

- nmap – Network scanning and service detection
- whois, nslookup, dig – Domain and IP info
- nikto – Web app vulnerabilities
- sqlmap – Password & DB attacks
- BuiltWith – Tech stack discovery

Security Tools

Nmap

Network scanning and service detection.

Whois,
nslookup, dig

Domain and IP information retrieval.

Nikto

Web application vulnerability scanning.

Sqlmap

Password and database attack tool.

BuiltWith

Technology stack discovery and analysis.

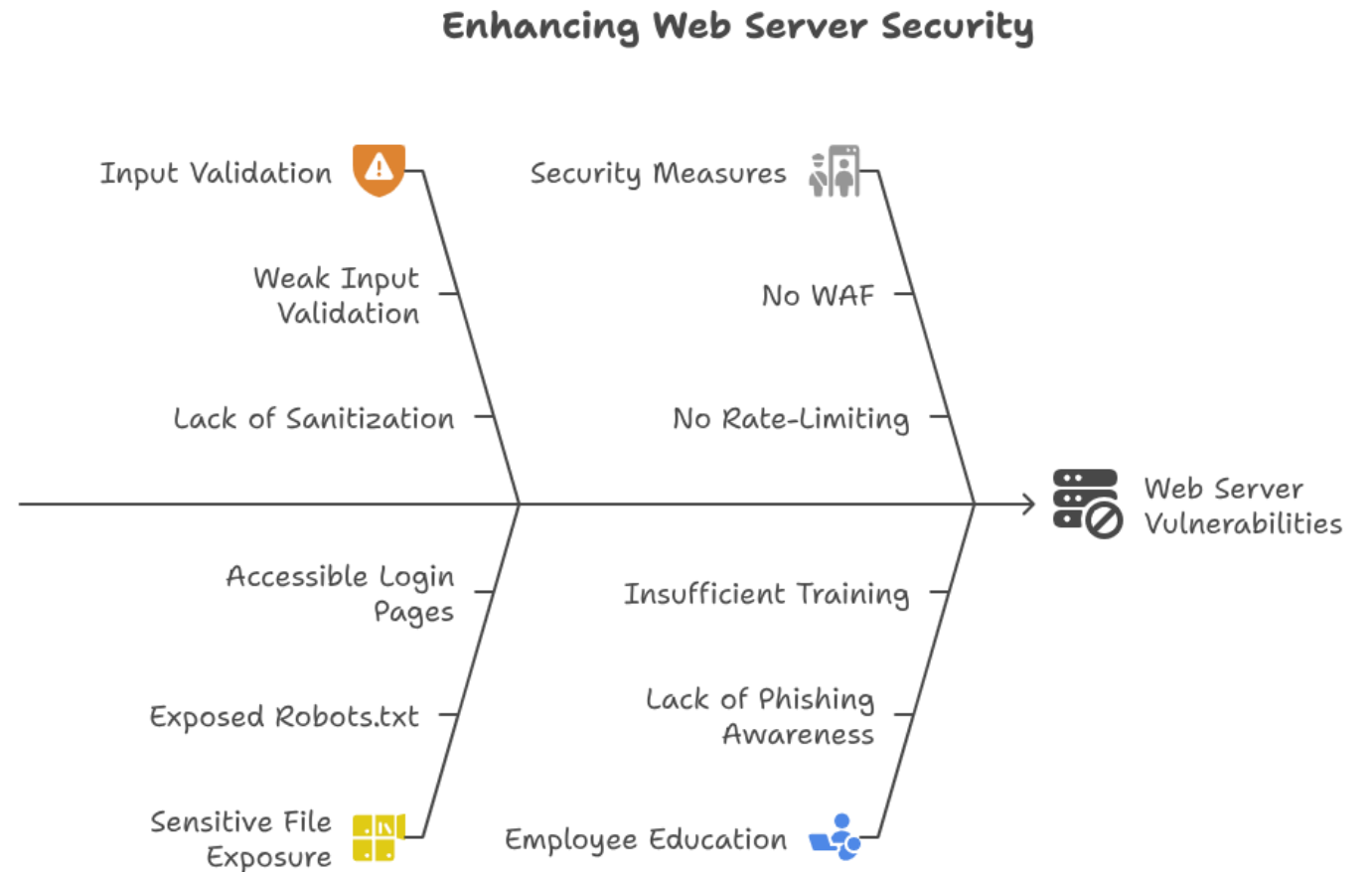
Final Conclusion and Remediation

Findings:

- Web server has weak input validation.
- Sensitive files exposed (robots.txt, login pages)
- No WAF or rate-limiting found

Recommendations:

- Input validation & sanitization
- Enable WAF & IDS
- Disable directory listing
- Educate employees about phishing



References and Additional Content

- Detailed command outputs and screenshots are available in the PDF attached/submitted separately.
- [Commands and Output Link](#)