Penetration Testing on Web Server

By Raghunandan Sharma
Roll number: 2023A7R020
Branch: CSE-Cybersecurity

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

Project Overview

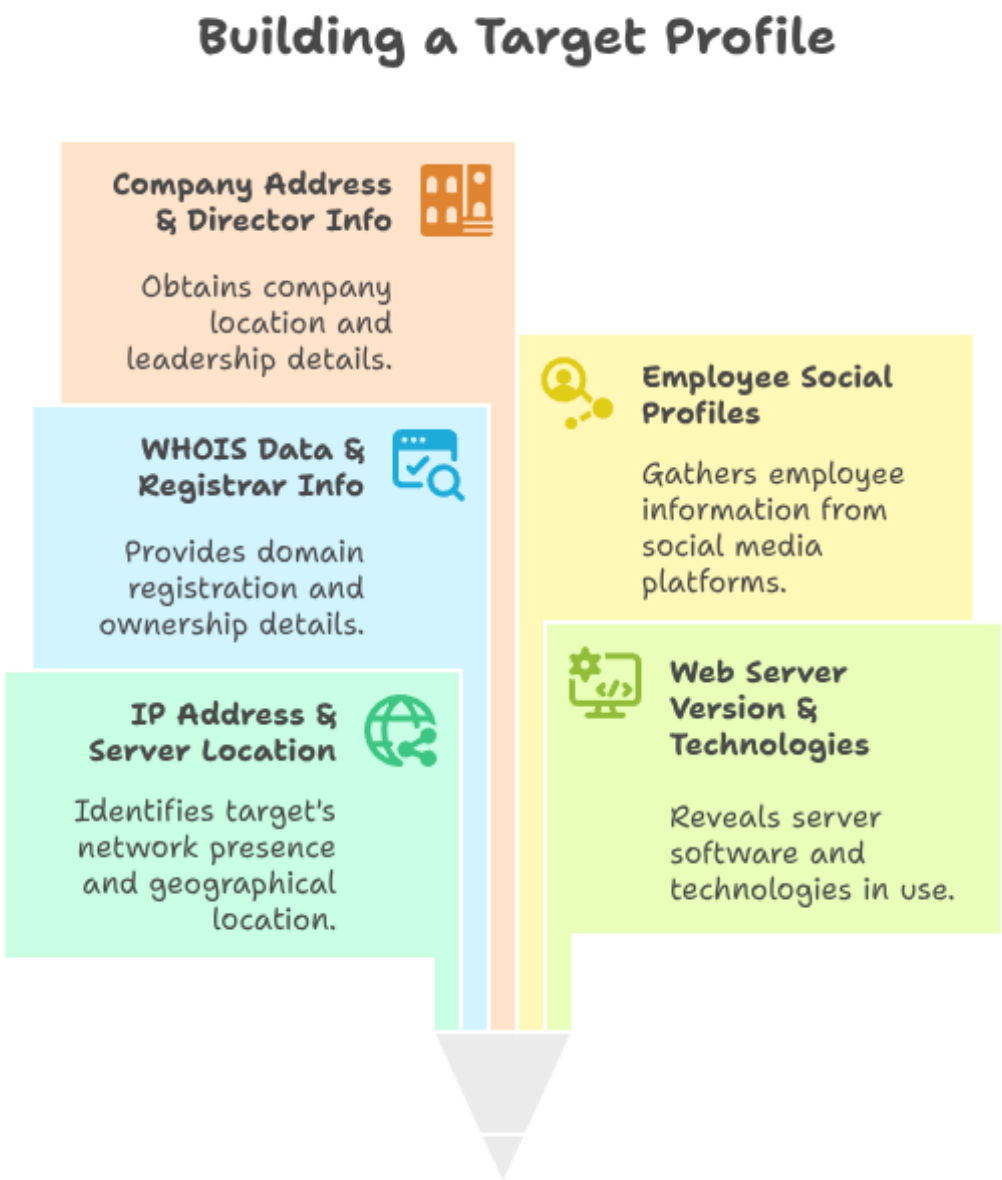
Objective: Assess and harden the security of a company's web server.

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

Footprinting and Reconnaissance

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

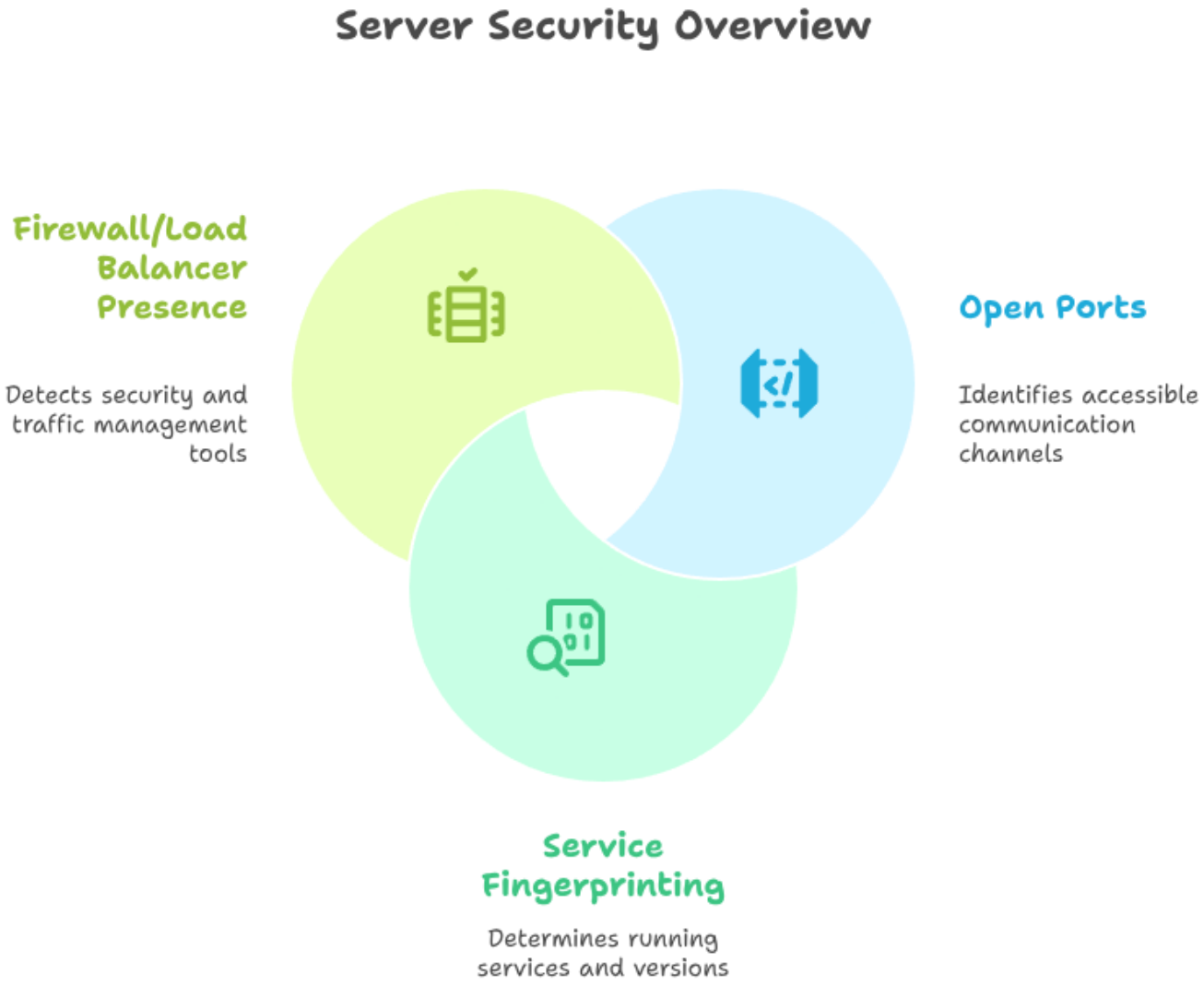
- IP Address, Server Location, OS
- Web Server Version & Built-in Technologies
- WHOIS Data & Registrar Info
- Email IDs, LinkedIn & Social Profiles of Employees
- Company Address & Director Info



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.



Vulnerabilty Assessment

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

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

Vulnerability Scanning Results

Check Type	Services	Web Apps
XSS	Yes	Yes
SQL Injection	Yes	Yes
File Inclusion	Yes	Yes
CVE Matching	Yes	Yes

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.

Database Security Assessment

Test	Result
Backend Access/Leaks	No direct DB exposed, but vulnerable forms detected
SQL Injection	Vulnerable forms detected
Default DB Configuration	Checked

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

Key Tools Summary

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

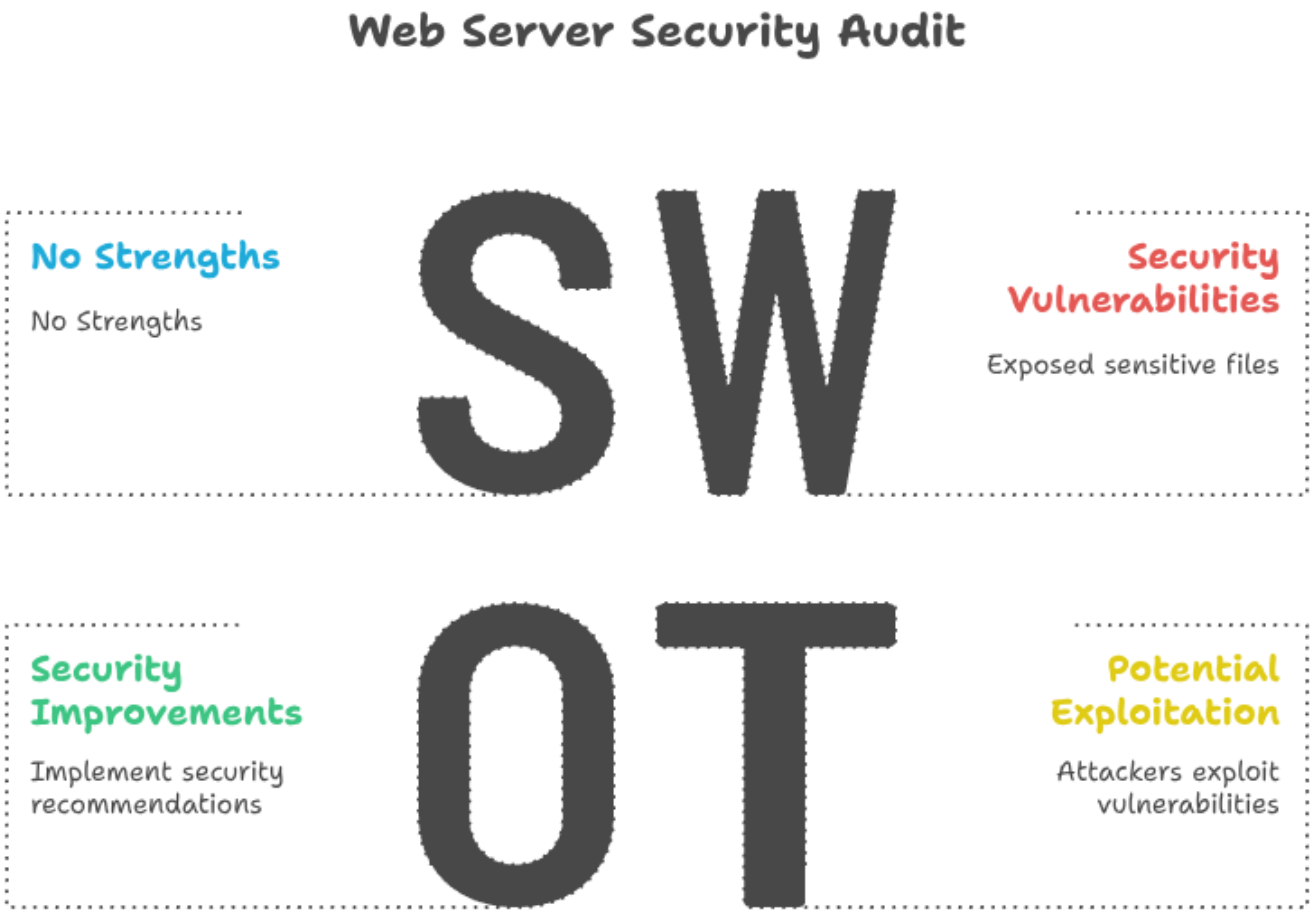
Final Conclusion and Remediation

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:

https://drive.google.com/file/d/1BL7XUAs2aOMA1VZDhJBmHw-f3tn-w4vM/view?usp=sharing