Web Server Security Assessment Report (Port 80)

1. Executive Summary

This report documents a hands-on **Web Server Security Assessment** conducted on a web server running **Apache HTTP Server**.
The primary objective of this assessment was to identify security misconfigurations, exposed services, and potential risks through enumeration and analysis.

All activities were performed in a **controlled virtual lab environment** for educational purposes only.

---

2. Scope and Environment

Target Information:

- Target IP: 192.168.56.103
- Service: HTTP
- Port: 80
- Web Server: Apache HTTP Server 2.2.8

Environment:

- Virtual Lab (Metasploitable)
- Assessment conducted for learning and demonstration purposes only

---

3. Methodology

The assessment followed a structured penetration testing approach focusing on enumeration and analysis:

1. Service discovery and version detection
2. Web vulnerability scanning
3. Directory and file enumeration
4. Manual verification of findings
5. Risk analysis and security recommendations

4. Tools Used

The following tools were used during this assessment:

- **Nmap** – Service discovery and version detection
- **Nikto** – Web server vulnerability scanning
- **Dirb** – Directory and file enumeration

---

5. Findings

5.1 Outdated Apache Version

The web server was identified as running **Apache HTTP Server 2.2.8**, which is an outdated version and no longer supported.

Risk:

- Increased exposure to known vulnerabilities
- Lack of security patches

5.2 Insecure WebDAV Configuration

The server supports **WebDAV**, and the /dav/ directory was found to be publicly accessible without authentication.

Risk:

- Unauthorized access to server directories
- Potential file upload or modification

5.3 Directory Listing Enabled

Multiple directories were found to have **directory listing enabled**, exposing internal structure and files.

Examples:

- /dav/
- /test/
- /phpMyAdmin/
- /twiki/

Risk:

- Information disclosure
- Increased attack surface

5.4 Exposed Administrative Paths

Sensitive administrative paths such as **phpMyAdmin** were publicly accessible.

Risk:

- Brute-force or credential-based attacks
- Database exposure if misconfigured

---

6. Evidence

Screenshots were collected during the assessment to demonstrate key findings, including:

- Nmap service and version detection
- Nikto vulnerability scan results
- Dirb directory enumeration output
- WebDAV directory exposure

(See Screenshots folder in the repository)

---

7. Risk Assessment

Based on the findings, the overall risk level of the web server is considered **High**, mainly due to:

- Outdated software
- Insecure configurations
- Publicly exposed directories and services

---

8. Recommendations

To mitigate the identified risks, the following actions are recommended:

1. Upgrade Apache HTTP Server to a supported version
2. Disable WebDAV if not required
3. Restrict access to sensitive directories
4. Disable directory listing
5. Apply proper authentication and authorization
6. Perform regular security assessments

---

9. Conclusion

This project demonstrates how basic enumeration techniques can uncover critical security weaknesses in web servers.
It highlights the importance of secure configurations, patch management, and continuous security monitoring.

This assessment strengthened practical skills in **Web Security**, **Enumeration**, and **Risk Analysis**.

---

10. Disclaimer

This assessment was conducted in a controlled lab environment for educational purposes only.
No real-world systems were targeted.