- **Finding:** Tomcat vulnerable to RCE via weak/default credentials and outdated version.
- **Remediation:** Upgrade Tomcat to the latest version. Remove/disable Manager application. Use strong credentials.

Escalation Email (100 words)

Subject: Urgent Critical Vulnerabilities Found on 192.168.56.104

Dear Team,
During a vulnerability assessment, I identified several critical issues on the Metasploitable2 host (192.168.56.104). Specifically, vsftpd 2.3.4 contains a backdoor (CVSS 10.0) that allows remote code execution, and Samba 3.x is vulnerable to RCE (CVSS 9.3). These flaws are exploitable with public PoCs, posing severe risks to system integrity. Immediate remediation is required: disable vsftpd, patch Samba, and upgrade Apache. Failure to act leaves the system exposed to attackers. PoC: Metasploit module exploit/unix/ftp/vsftpd_234_backdoor confirms remote shell access.

Regards,

Hilary H. Joachim

ii. Nikto Scan (nikto – h http://192.168.56.104)

Scan ID	Vulnerability / Issue	CVSS Score	Priority	CVE ID / Ref	Host
N001	Apache 2.2.8 outdated (EOL, multiple vulns)	7.5	High	CVE-2007-6750, CVE-2011-3192	192.168.56.104
N002	Missing X-Frame-Options header (Clickjacking)	6.5	Medium	CWE-1021	192.168.56.104
N003	Missing X-Content-Type-Options header	6.0	Medium	CWE-16	192.168.56.104
N004	Apache mod_negotiation allows brute-forcing	5.0	Medium	N/A	192.168.56.104

Scan ID	Vulnerability / Issue	CVSS Score	Priority	CVE ID / Ref	Host
N005	TRACE method enabled (XST attack)	6.8	Medium	CWE-693	192.168.56.104
N006	phpinfo.php exposed (info disclosure)	7.0	High	CWE-552	192.168.56.104
N007	/doc/ directory indexing enabled	5.5	Medium	CWE-548	192.168.56.104
N008	PHP script info disclosure (/usr/doc)	7.5	High	CVE-1999-0678	192.168.56.104
N009	/phpMyAdmin exposed (default interface)	9.0	Critical	CWE-287	192.168.56.104
N010	phpMyAdmin changelog reveals version info	5.3	Medium	CVE-2003-1418	192.168.56.104
N011	/test/ directory exposed (potential code/files)	6.0	Medium	N/A	192.168.56.104
N012	/icons/ directory indexing enabled	5.0	Medium	CWE-548	192.168.56.104
N013	Apache default file /icons/README found	4.5	Low	N/A	192.168.56.104
N014	/wp-config.php# backup file exposed (creds leak)	9.5	Critical	CWE-200	192.168.56.104

Vulnerability Findings and Remediation:

1. Apache 2.2.8 Outdated (EOL, Multiple Vulnerabilities)

- **Finding:** The server is running Apache 2.2.8, which is end-of-life and contains multiple publicly known vulnerabilities (e.g., CVE-2007-6750, CVE-2011-3192).

- **Remediation:** Upgrade to a supported version (Apache 2.4.x or later) and apply the latest security patches.

2. Missing X-Frame-Options Header (Clickjacking)

- **Finding:** The site does not implement the X-Frame-Options header, leaving it vulnerable to clickjacking attacks.
- **Remediation:** Configure the web server to add X-Frame-Options: SAMEORIGIN or Content-Security-Policy: frame-ancestors.

3. Missing X-Content-Type-Options Header

- **Finding:** The X-Content-Type-Options header is not set, allowing browsers to MIME-sniff content and potentially execute malicious code.
- **Remediation:** Add X-Content-Type-Options: nosniff to the web server configuration.

4. Apache mod_negotiation Allows Brute Forcing

- **Finding:** The Apache mod_negotiation feature is enabled, which may allow attackers to brute-force file names and discover hidden resources.
- **Remediation:** Disable mod_negotiation unless explicitly required, or restrict access using .htaccess or server configuration.

5. TRACE Method Enabled (Cross-Site Tracing, XST)

- **Finding:** The server accepts HTTP TRACE requests, which can be abused for cross-site tracing attacks and information disclosure.
- **Remediation:** Disable TRACE by setting TraceEnable off in the Apache configuration.

6. phpinfo.php Exposed (Information Disclosure)

- **Finding:** The phpinfo.php script is publicly accessible, exposing detailed PHP configuration and system information.
- **Remediation:** Remove or restrict access to phpinfo.php. Only allow access in controlled test environments.

7. /doc/ Directory Indexing Enabled

- **Finding:** Directory browsing is enabled on /doc/, exposing internal documentation and files.