Title: Critical Web Vulnerabilities

Findings:

- [CVE-2011-2523], [Service: FTP (vsftpd 2.3.4)], [CVSS: 10.0], [Host: 192.168.132.129]

- [CVE-2021-41773], [Service: Apache HTTP Server], [CVSS: 9.8], [Host: 192.168.132.129]

- [Default Credentials], [Service: Apache Tomcat Manager], [CVSS: 9.0], [Host: 192.168.132.129]

- [Weak Credentials], [Service: MySQL], [CVSS: 8.8], [Host: 192.168.132.129]

- [Remote Code Execution], [Service: Java RMI], [CVSS: 9.8], [Host: 192.168.132.129]

Remediation:

- Patch Apache HTTP Server to the latest secure version.

- Remove or disable vulnerable FTP services.

- Change default credentials on Tomcat and restrict access.

- Enforce strong authentication for database services.

- Disable unused services and close unnecessary ports.