# Critical Web Vulnerabilities on Metasploitable2 — 192.168.132.135

## Executive Summary

An assessment of 192.168.132.135 (Metasploitable2) identified multiple critical and high-severity issues: remote code execution/backdoor in vsftpd 2.3.4, PHP source disclosure via vulnerable PHP/Apache, exposed backup/configuration files, and an active bindshell. These findings enable full compromise of the host and disclosure/exfiltration of sensitive files.

## Findings

### vsftpd 2.3.4 backdoor (CVE-2011-2523)

**Host:** 192.168.132.135:21  
**Severity:** CVSS: 10.0  
**Details:** Remote root shell possible via backdoor in vsftpd 2.3.4. Evidence: nmap detected vsftpd 2.3.4.

### PHP source disclosure / Apache 2.2.8 (PHP 5.2.4)

**Host:** 192.168.132.135:80  
**Severity:** CVSS: 9.1  
**Details:** Nikto: /dvwa/login.php?-s returns PHP source; x-powered-by header reveals PHP/5.2.4.

### Exposed backup/config files (.tar/.pem/.jks/.war)

**Host:** 192.168.132.135:80  
**Severity:** CVSS: 7.5  
**Details:** Nikto discovered many backup and cert filenames accessible via HTTP; may contain credentials/keys.

### Bindshell service (port 1524)

**Host:** 192.168.132.135:1524  
**Severity:** CVSS: 10.0  
**Details:** Intentional Metasploitable bindshell present; unauthenticated root shell available.

### SIPS v0.2.2 user-info disclosure (EDB-22381)

**Host:** 192.168.132.135:80  
**Severity:** CVSS: 8.6  
**Details:** Nikto: SIPS endpoint allows retrieval of user info, including possible passwords.

### Missing security headers / Insecure cookies / TRACE method

**Host:** 192.168.132.135:80  
**Severity:** CVSS range: 4.3–6.1  
**Details:** Missing X-Frame-Options and X-Content-Type-Options; cookies missing HttpOnly; TRACE enabled (XST risk).

## Impact

Successful exploitation of the high/critical findings (vsftpd backdoor, bindshell, PHP source disclosure) could lead to full host compromise, credential disclosure, and lateral movement within the network.

## Remediation (Immediate Actions)

- Isolate the host from production and untrusted networks.

- Remove or upgrade vulnerable software: replace vsftpd 2.3.4, upgrade PHP to a supported version, and update Apache.

- Remove, relocate, or protect backup and certificate files; restrict HTTP access to sensitive files.

- Disable or firewall off the bind shell (port 1524) and any unnecessary legacy services.

- Disable HTTP TRACE method and add security headers: X-Frame-Options, X-Content-Type-Options. Set HttpOnly on cookies.

- Harden Samba, restrict anonymous/null sessions, and restrict RMI and database services to trusted hosts.

- After remediation, re-scan with Nmap/OpenVAS and re-run Nikto to validate fixes.

## Evidence & Attachments

Include with this report when submitting to developers/ops:  
- nmap scans (nmap\_cyart\_basic.txt, nmap\_cyart\_allport.txt)  
- nikto\_192-168-132-135.txt  
- scan CSV summary (scans\_192-168-132-135.csv)

## Notes

This assessment was performed against an intentionally vulnerable Metasploitable2 VM for training and lab purposes. All findings are reproducible in the local lab environment. Ensure any testing in production follows an approved engagement plan and change control.