## Title: Chained Exploit on Web Server

Author: Ishan Chowdhury  
Date: 13-10-2025  
Scope: Authorized lab assessment — Target: 192.168.132.135 (Metasploitable2)

## Executive Summary

During an authorized lab assessment of 192.168.132.135, multiple chained vulnerabilities were identified that could lead from client-side input to remote code execution (RCE) and potential local privilege escalation. The key finding demonstrates how an input reflection and insecure file handling can be combined to achieve system compromise. Immediate remediation actions are required to reduce risk.

## Findings

**Finding 1** — **CVE-2021-22205 (example / image-processing RCE)** — Host: 192.168.132.135. Chaining of reflected input with insecure upload/processing can lead to RCE. Evidence: ~/lab/evidence/msf2/exploit-session-YYYYMMDD.txt, ~/lab/pcaps/msf2-traffic-YYYYMMDD.pcap.

**Finding 2** — **Reflected XSS (DVWA)** — Host: 192.168.132.135 — /dvwa/vulnerabilities/xss\_r/?name= reflected input (Hello TEST observed). Evidence: ~/lab/scans/dvwa-xss-check.html.

## Technical Details

Recon: Nmap service/version scan saved at ~/lab/scans/msf2-services.txt. Web apps discovered: DVWA, Mutillidae, phpMyAdmin, phpMyAdmin instance observed in Burp captures.

Exploit chain conceptual flow: Reflected XSS → Session theft (or admin tricking) → Upload abuse / image processing → RCE → Local enumeration & privilege escalation.

## Remediation

Sanitize and validate all user inputs (server-side). Use output encoding/escaping for all reflected content.

Harden file upload handling: validate MIME types and file headers, restrict extensions, store uploads outside webroot, scan uploads, use content-type checks and file-size limits.

Review and restrict privileged functionality (suid binaries, sudoers). Implement least privilege on web service accounts.

Implement logging, monitoring, and file integrity checks.

## Evidence & Artifacts

Terminal transcript: ~/lab/evidence/msf2/exploit-session-YYYYMMDD.txt

PoC log: ~/lab/poctesting/poc\_log.txt

PCAP: ~/lab/pcaps/msf2-traffic-YYYYMMDD.pcap

Hash list: ~/lab/evidence/msf2/hashlist.txt

## Appendix: Findings Table

| **Finding ID** | **Vulnerability** | **CVE (if known)** | **Target IP** | **CVSS (est)** | **Remediation** |
| --- | --- | --- | --- | --- | --- |
| F002 | Reflected XSS (search/name param) | N/A | 192.168.132.135 | 6.1 | Output-encode reflected input; input validation |