Multi-Stage WordPress Exploit Chain

Target: Mr. Robot VulnHub VM
Primary Vector: WordPress Plugin RCE

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

Custom PoC (Python Buffer Overflow)

I modified an Exploit-DB PoC to adjust **offset and shellcode** for compatibility.

50-word summary:
I adapted a buffer overflow PoC in Python, customizing the offset length and inserting a reverse shell payload for Linux. The exploit successfully triggered a segmentation fault, redirected execution flow to shellcode, and provided attacker control. This modification validated exploit development and adaptation skills for real-world environments.

Bypass (ROP for ASLR)

I crafted a **ROP chain** to disable ASLR protections in a vulnerable binary.
50-word summary:
Using Ghidra and ROPgadget, I constructed a return-oriented programming (ROP) chain to bypass ASLR in a target binary. The chain manipulated system calls to execute

/bin/sh regardless of randomized memory addresses. This bypass demonstrated advanced binary exploitation techniques to achieve reliable code execution under modern defense mechanisms.

Google Doc Report Outline

Title: Critical WordPress Exploit Chain
Findings: CVE-2023-12345 – Exploitable WordPress Plugin, Host: 192.168.1.100
Remediation:

- Update vulnerable plugins
- Enable Web Application Firewall (WAF)
- Enforce least privilege for web services