# FINDINGS

This section presents the vulnerabilities identified during the penetration test, along with their potential impact and evidence collected. The findings are categorized by severity to assist in prioritizing remediation efforts.

## CRITICAL VULNERABILITIES

This section describes critical vulnerabilities discovered during this assessment.
USE THIS TEMPLATE TO DESCRIBE EACH VULNERABILITY YOU WERE ABLE TO CONFIRM. DUPLICATE THE TABLE TEMPLATE IF YOU VERIFIED MORE THAN ONE VULNERABILITY.

| **Vulnerability** | **Outdated WordPress Core Version** |
|---|---|
| CVE | CVE-2019-9978 - (PoC) RCE in Social WarFare Plugin (<=3.5.2) |
| Severity | High (10) |
| OWASP Top 10 | A01 (Broken Access Control) |
| Risk | Publicly available exploits exist for this vulnerability. |
| Steps to exploit | 1. Created a payload file with a system command to read sensitive data.<br>2. Hosted the payload on an accessible web server.<br>3. Configured Metasploit to listen for incoming reverse shell connections.<br>4. Sent a crafted URL to the target site to trigger the vulnerability.<br>5. Verified the command output confirmed successful code execution.<br>6. Established a reverse shell session with the target system.<br>7. Upgraded the shell to Meterpreter for enhanced control. |
| Evidence | Retrieved `/etc/passwd` file via remote code execution.<br><br>Metasploit session logs showing reverse shell connection established and upgraded to Meterpreter.<br><br>Target system confirmed as Debian 10.2 running WordPress with vulnerable Social Warfare plugin. |

# EXPLOITATION AND POST-EXPLOITATION

The exploitation phase involved leveraging identified vulnerabilities to compromise the target systems, followed by post-exploitation activities to assess the potential impact. This section provides a detailed account of the actions taken.

## EXPLOITATION PHASE

- Remote Code Execution (RCE) in Social Warfare WordPress plugin
- Retrieval of sensitive system file `/etc/passwd`
- Established reverse shell access via Metasploit
- Verified plugin version and vulnerability presence with targeted requests
- Exploited plugin's debug parameter to inject malicious payload
- Bypassed authentication by leveraging unauthenticated plugin endpoint

## POST-EXPLOITATION PHASE

- Gathered system information (OS version, architecture, current user)
- Upgraded shell to Meterpreter for better control
- Verified access permissions without further privilege escalation
- Enumerated running processes and network connections
- Captured environment variables for further analysis
- Maintained session stability for ongoing testing without system disruption