Vulnerability Assessment & Penetration Testing (VAPT) Report

1. Executive Summary

1.1 Purpose
This assessment was conducted to identify security vulnerabilities in a deliberately vulnerable system (Metasploitable 3) using open-source security tools.

1.2 Summary of Findings
- Multiple **High** and **Medium** risk vulnerabilities were identified.
- Several services were unnecessarily exposed.
- Weak configurations increased the risk of remote exploitation.

2. Objective & Scope

2.1 Objective
- Perform Vulnerability Assessment and basic Penetration Testing using open-source tools.
- Understand real-world VAPT workflow and reporting.

2.2 Scope
- **Target:** Metasploitable 3
- **Testing Type:**
  - Vulnerability Assessment
  - Limited Penetration Testing (non-destructive)

3. Testing Environment Setup

3.1 Virtual Environment
- **Virtualization:** VMware
- **Attacker Machine:** Kali Linux
- **Target Machine:** Metasploitable 3

3.2 Network Configuration
- NAT network

3.3 IP Identification

- **Command used:** *ip a*
- Kali Linux IP: 192.168.72.139

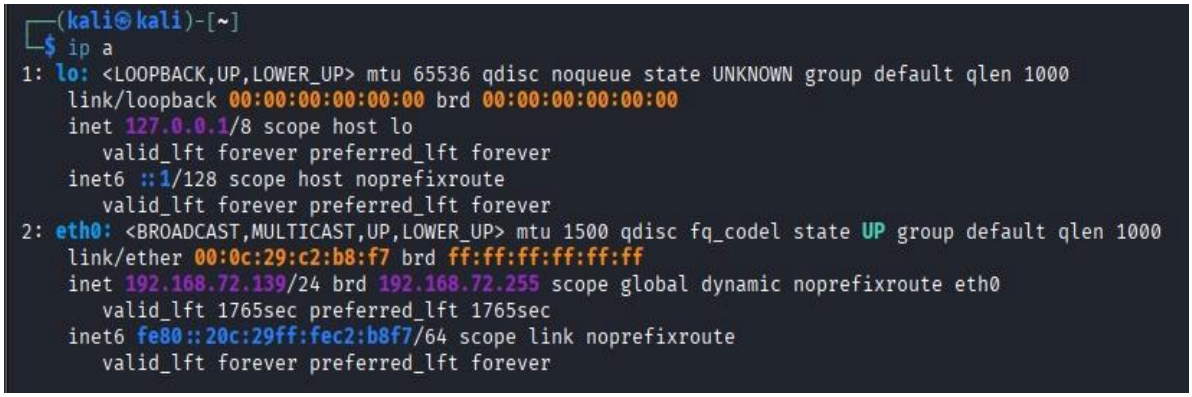

Fig-1

- Metasploitable IP: 192.168.72.140

Fig-2

4. VAPT Methodology Followed

4.1 Phases:

1. **Planning:** Defined scope and target IP
2. **Discovery:** Nmap and Nikto scans
3. **Assessment:** OpenVAS vulnerability scanning
4. **Reporting:** Findings documented using Dradis CE and spreadsheets

5. Tools Used

Tool	Purpose
Nmap	Port and service discovery
Nikto	Web vulnerability scanning
OpenVAS	Automated vulnerability assessment
Dradis CE	Centralized documentation & reporting
Spreadsheet	Risk tracking
VMware	Virtual lab
Metasploitable 3	Vulnerable target system

6. Vulnerability Assessment Results

6.1 Nmap

- Multiple open ports detected
- FTP, SSH, and HTTP services exposed
- **Command used:** *nmap -Pn 192.168.72.140*

Fig-3

6.2 Nikto

- Outdated web server
- Missing security headers
- Potential web vulnerabilities
- **Command used:** *nikto -h http://192.168.72.140*

Fig-4

6.3 OpenVAS

- High and Medium severity vulnerabilities identified
- CVE IDs and CVSS scores obtained
- OpenVAS was started using the **command:** ***sudo gvm-start***

6.3.1 Target Creation

- After launching the Greenbone interface, a **target** was created using the Metasploitable 3 IP address.

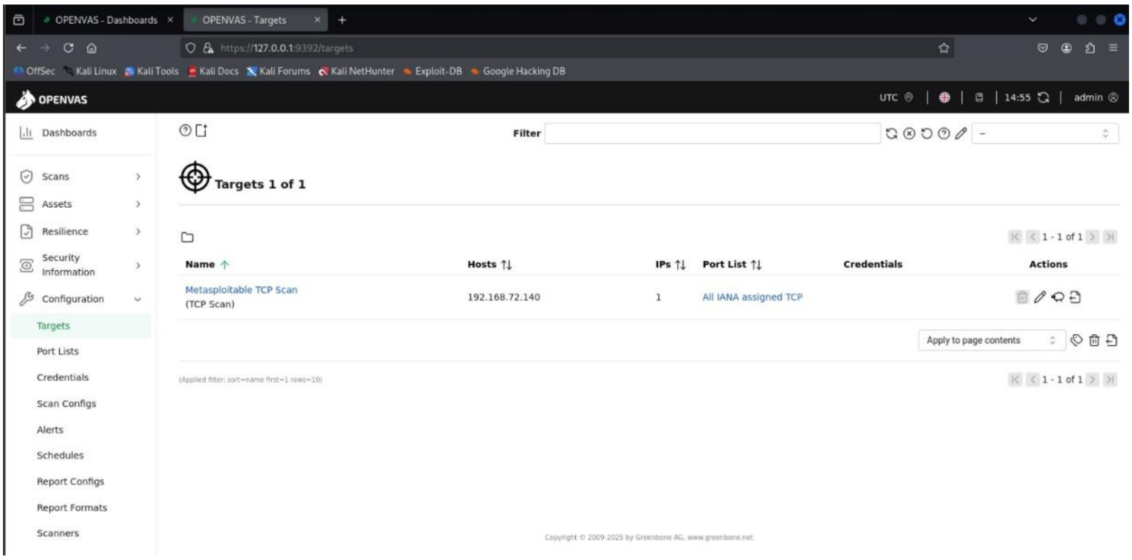

Fig-5

6.3.2 Feed Status

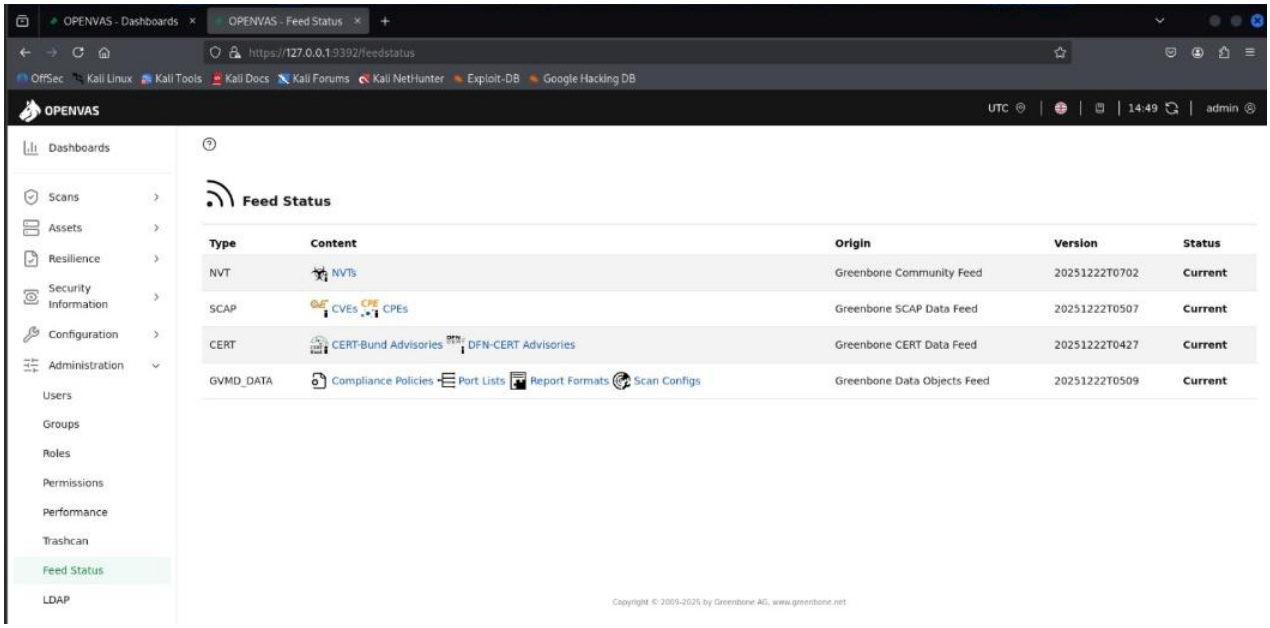

Fig-6

6.3.3 Task Creation & Execution

- A **scan task** was then created and executed using a Full and Fast scan profile.

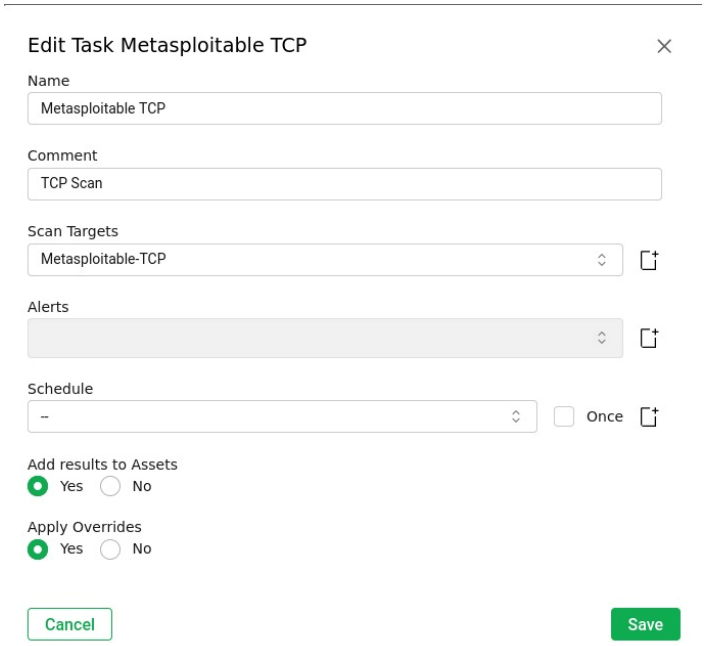

Fig-7

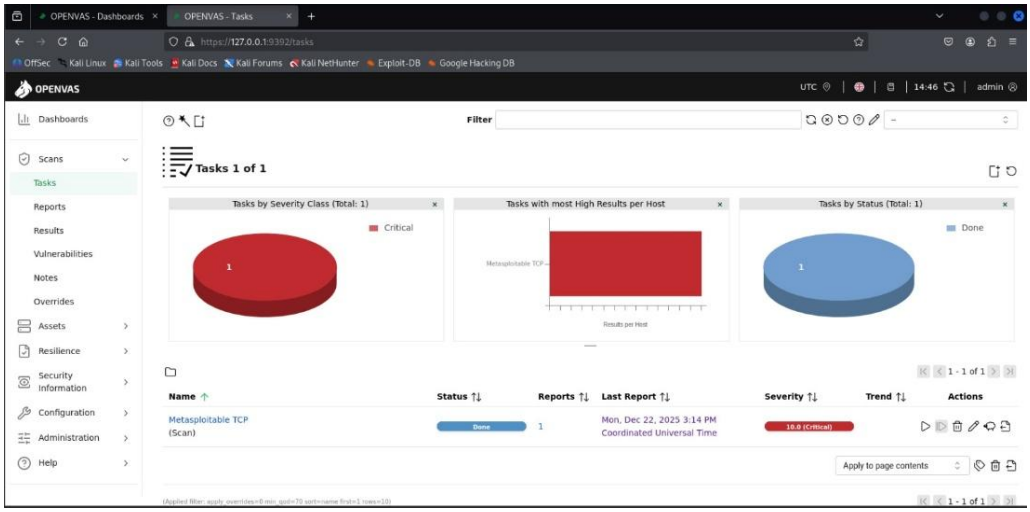

Fig-8

6.3.4 Scan Result

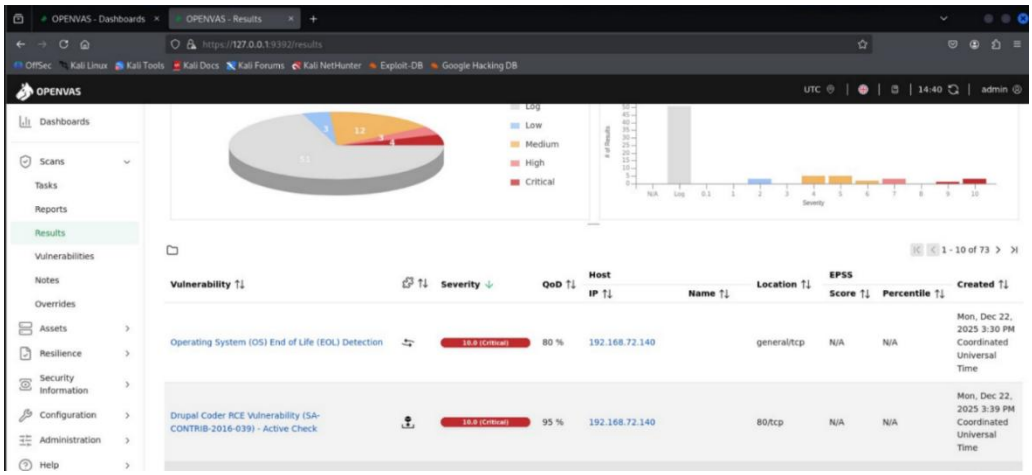

Fig-9

7. Risk Assessment

- CVSS scores were calculated from CVSS calculator.

1. OS End of Life (EOL) Detection

Fig-10

2. Drupal Coder RCE (CVE-2016-5385)

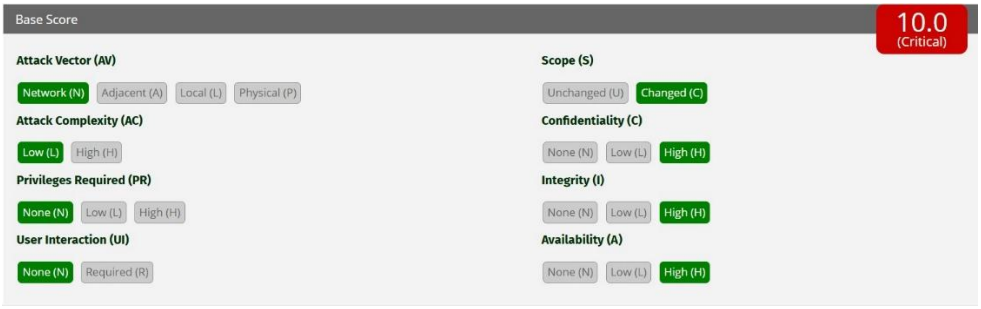

Fig-11

3. ProFTPD mod_copy (CVE-2015-3306)

Fig-12

4. SSH Default Credentials

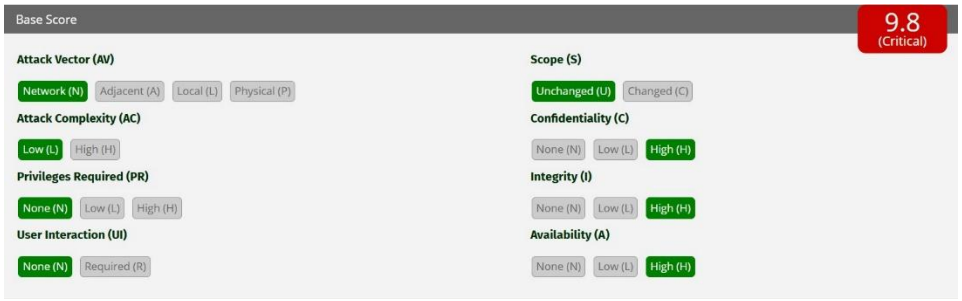

Fig-13

5. Drupal Core SQL Injection (CVE-2014-005)

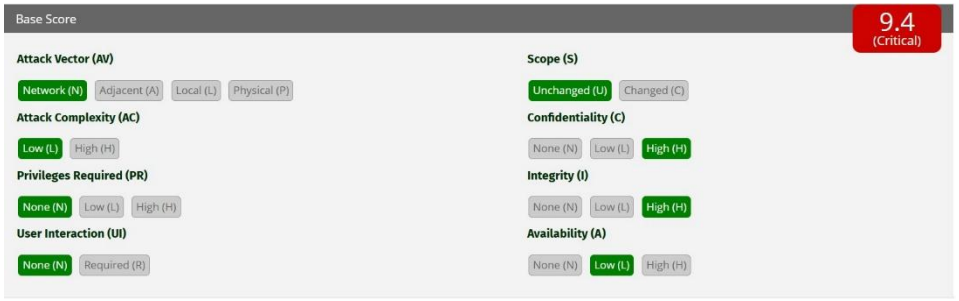

Fig-14

6. HTTP Dangerous Methods

Fig-15

7. FTP Default Credentials

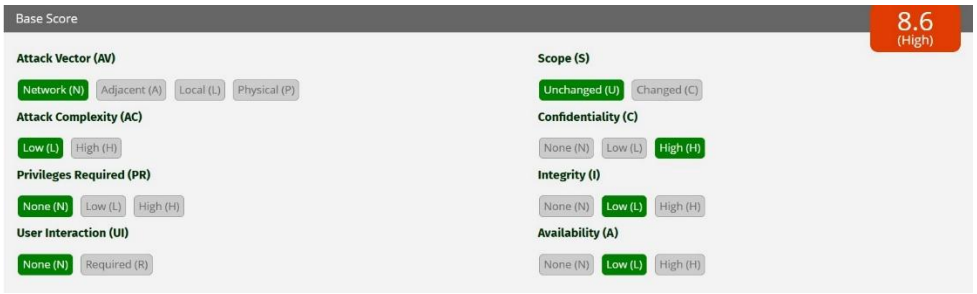

Fig-16

8. jQuery < 1.9.0 XSS

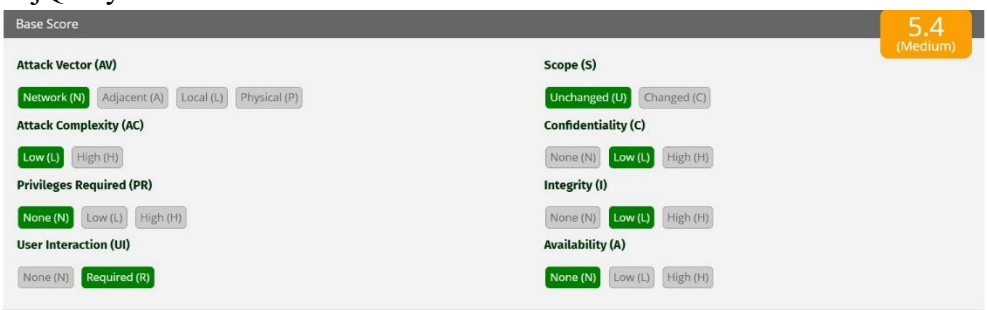

Fig-17

9. Weak SSH Host Key Algorithm

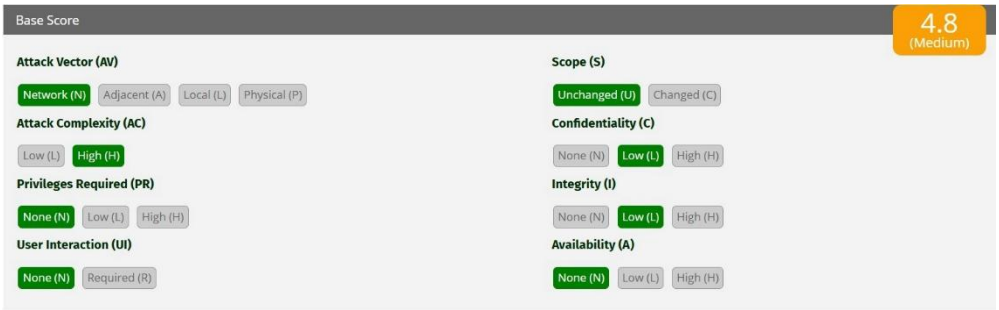

Fig-18

8. Vulnerability Spreadsheet

- Used Excel Sheet

Vulnerabilities									
Host IP	**Vulnerability Name**	**CVE ID**	**Port / Service**	**CVSS**	**Likelihood**	**Impact**	**Risk Level**	**Recommendation**	**Status**
192.168.72.140	OS End of Life Detection	N/A	General	10	High	High	**Critical**	Upgrade OS to supported version	Open
192.168.72.140	Drupal Coder RCE	CVE-2016-5385	80/tcp	10	High	High	**Critical**	Apply Drupal security updates	Open
192.168.72.140	ProFTPD mod_copy File Copy	CVE-2015-3306	21/tcp	9.4	High	High	**Critical**	Disable mod_copy / update ProFTPD	Open
192.168.72.140	SSH Default Credentials	N/A	22/tcp	9.8	High	High	**Critical**	Enforce strong credentials	Open
192.168.72.140	Drupal Core SQL Injection	CVE-2014-005	80/tcp	9.4	High	Medium	**Critical**	Patch Drupal core	Open
192.168.72.140	FTP Default Credentials	N/A	21/tcp	8.6	High	Medium	**High**	Change FTP credentials	Open
192.168.72.140	HTTP Dangerous Methods	N/A	80/tcp	7.3	Medium	Medium	**Medium**	Disable unused methods	Open
192.168.72.140	jQuery < 1.9.0 XSS	N/A	80/tcp	5.4	Medium	Medium	**Medium**	Upgrade jQuery	Open
192.168.72.140	Weak SSH Host Key Algorithm	N/A	22/tcp	4.8	Low	Medium	**Low**	Use stronger SSH algorithms	Open

Fig-19

9. 3×3 Risk Matrix & Risk Mapping

- Used Excel Sheet

9.1 3x3 Risk Matrix

1. Likelihood

- Low – Hard to exploit
- Medium – Needs effort
- High – Easily exploitable

2. Impact

- Low – Minimal effect
- Medium – Service disruption
- High – Full compromise

Risk Matrix Table			
Impact ↓ / Likelihood →	**Low**	**Medium**	**High**
High	Medium	High	**Critical**
Medium	Low	Medium	High
Low	Low	Low	Medium

Fig-20

9.2 Risk Mapping

Risk Mapping			
Vulnerability Name	**Likelihood**	**Impact**	**Final Risk**
OS End of Life Detection	High	High	**Critical**
Drupal Coder RCE	High	High	**Critical**
ProFTPD mod_copy File Copy	High	High	**Critical**
SSH Default Credentials	High	High	**Critical**
Drupal Core SQL Injection	High	Medium	**High**
FTP Default Credentials	High	Medium	**High**
HTTP Dangerous Methods	Medium	Medium	**Medium**
jQuery < 1.9.0 XSS	Medium	Medium	**Medium**
Weak SSH Host Key Algorithm	Low	Medium	**Low**

Fig-21

10. Documentation & Reporting

Dradis Community Edition (CE) was used as a centralized platform to document and organize vulnerability findings.
In Dradis, the following structure was maintained:

- **Node:** Target host
- **Issue:** Identified vulnerability
- **Evidence:** Scan output & vulnerability details

10.1 Node Created

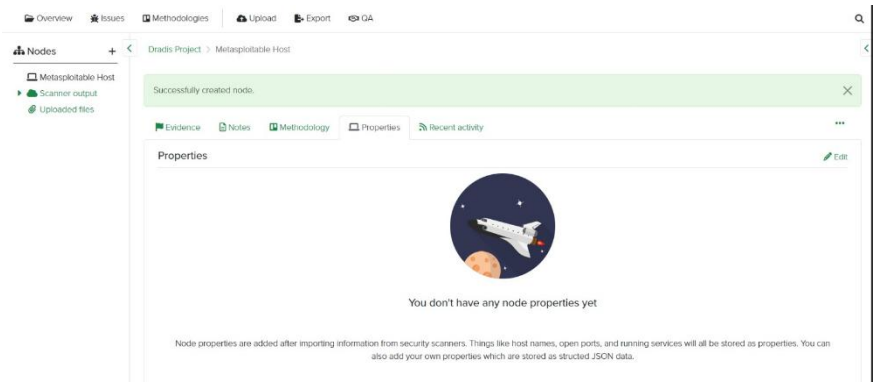

Fig-22

10.2 Issue Created

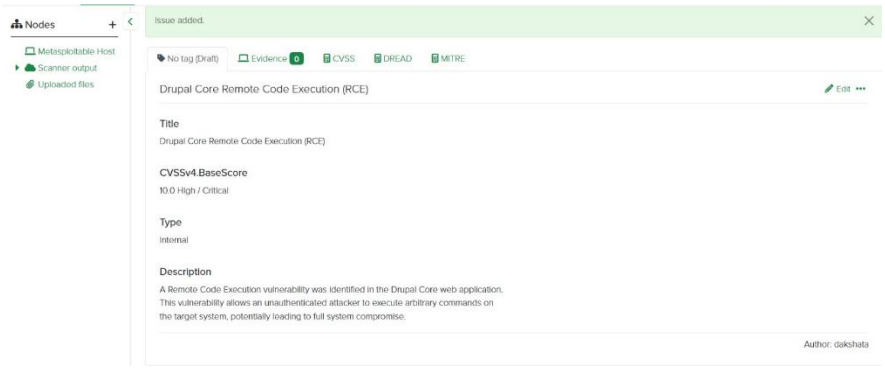

Fig-23

10.3 Evidence

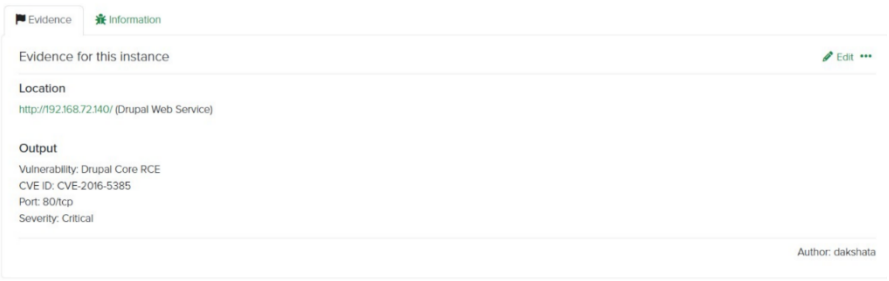

Fig-24

11. Challenges Faced

Challenge: Missing Scan Configuration (Feed Sync Failure)

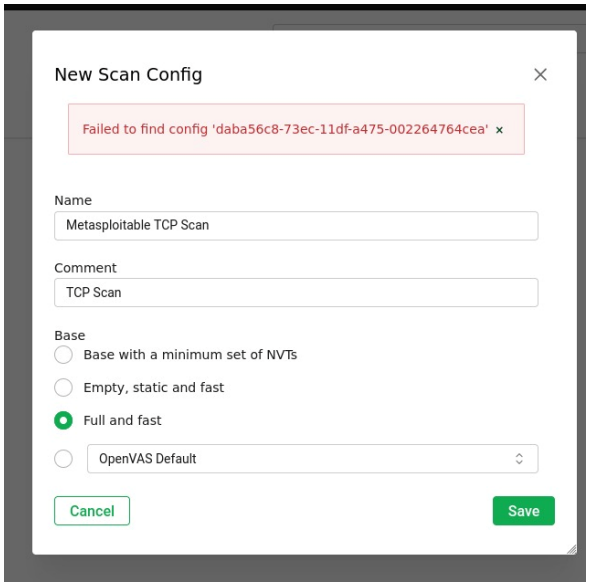

Fig-25

- **Issue:** Creating a scan using the default *Full and Fast* profile failed with the error: ***Failed to find config daba56c8-73ec-11df-a475-002264764cea***.
- **Impact:** Scan tasks could not be created due to the absence of a valid scan configuration.
- **Root Cause:** The gvmd database was incomplete because the Greenbone Community Feed had not been synchronized after installation, resulting in missing NVTs and scan profiles.

12. Conclusion

This VAPT task provided practical exposure to vulnerability assessment, risk prioritization, and security documentation using open-source tools. The assessment highlights the importance of proactive security testing to identify and remediate vulnerabilities before exploitation.