*Innovation & Entrepreneurship Hub for Educated Rural Youth (SURE Trust – IERY)*

# Vulnerability Assessment and Penetration Testing on IP addresses

The domain of the Project:

*Cybersecurity*

Under the guidance of

*Mr. Nishchay Gaba(OSCP Certified Penetration Tester)*

By

*Mr. Srujan Bandaru*

Period of the project

*September 2024 to March 2025*

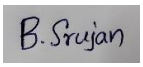
SURE TRUST

PUTTAPARTHI, ANDHRA PRADESH

# Declaration

The project titled "**VAPT on IP addresses"** has been mentored by **"Mr. Nishchay Gaba"**, organised by SURE Trust, from September 2024 to March 2025, for the benefit of the educated unemployed rural youth for gaining hands-on experience in working on industry relevant projects that would take them closer to the prospective employer.

I **"Mr. Srujan Bandaru"**, hereby declare that I have solely worked on this project under the guidance of my mentor. This project has significantly enhanced my practical knowledge and skills in the domain.

| **Name** | **Signature** |
|---|---|
| Mr. Srujan Bandaru |  |

| **Mentor** | **Signature** |
|---|---|
| Mr. Nishchay Gaba |  |

Prof. Radhakumari
Executive Director & Founder
SURE Trust

# Table of Contents

## 1.Confidentiality Statement

This Network Penetration Testing Report is confidential and intended solely for Sure Trust Organisation. It contains sensitive security findings and must not be shared, reproduced, or disclosed without prior written consent.

Unauthorized access or distribution is strictly prohibited. All findings and recommendations are for internal use only to enhance security. Handle this document with care to prevent exposure of vulnerabilities.

## 2. Disclaimer

This **Network Penetration Testing Report** was prepared as part of an internship project at **Sure Trust** and is based on the assessment of the provided IP addresses. The findings, analysis, and recommendations are derived from the testing conducted within the approved scope.

While all efforts have been made to identify vulnerabilities accurately, this report does not guarantee the complete security of the tested systems. The author and **Sure Trust** are not responsible for any misuse, unauthorized actions, or unintended consequences arising from this report.

Use this report responsibly and implement necessary security measures as appropriate.

## 3. Contact Information

### Client Details:

| Name | Title | Contact Information |
|---|---|---|
| Mr. Nishchay Gaba sir | OSCP Certified penetration tester | nishchaygaba1049@gmail.com |

### Pentesting done by :

| Name | Title | Contact Information |
|---|---|---|
| Srujan Bandaru | Network Pentesting Report | bandarusrujan@gmail.com |

# 4. Assessment Overview

As part of an internship project at Sure Trust, a Network Penetration Test was conducted on the IP addresses provided for security assessment. The objective was to identify vulnerabilities, evaluate potential risks, and provide recommendations for remediation.

The assessment followed industry-standard methodologies, including reconnaissance, scanning, exploitation, and post-exploitation analysis. The findings are categorized based on their severity—Critical, High, Medium, and Low—to help prioritize security improvements.

This report serves as a detailed record of the security posture of the tested systems as of January 1st, 2025, and includes actionable recommendations to enhance their security.

# 5. Methodology

Since exploitation was not permitted in this assessment, the testing focused on **passive and active security evaluation** without attempting to compromise systems. The following components were covered:

## 1. Scope Definition

- Assessment of the **provided IP addresses** within the approved boundaries.
- Defining testing constraints to ensure **non-intrusive** security evaluation.
- Exclusion of any activity that could disrupt services (**No Exploitation)**.

## 2. Reconnaissance

- Collecting **publicly available information** on the target systems.
- Identifying **exposed services, domain records, and subdomains**.

## 3. Scanning & Enumeration

- Identifying **open ports, running services, and system banners**.
- Checking for **misconfigurations, outdated software, and weak authentication mechanisms**.
- Tools Used: **Nmap, Nikto, SNMPWalk, Routersploit**.

## 4. Vulnerability Assessment

- Mapping identified services to known vulnerabilities.
- Analyzing **CVEs (Common Vulnerabilities and Exposures)** for potential risks.
- Tools Used: **TestSSL, SearchSploit**.

## 5. Risk Categorization & Impact Analysis

- Assigning severity levels (**Critical, High, Medium, Low**) based on **CVSS (Common Vulnerability Scoring System)**.
- Assessing the **likelihood of exploitation** and potential security impact.

## 6. Recommendations & Remediation

- Providing actionable security **hardening measures**.
- Suggesting **patches, secure configurations, and access restrictions**.
- Encouraging **continuous monitoring and periodic reassessments**.

This methodology ensures a **thorough, ethical, and risk-free evaluation** of the security posture of the assessed systems while adhering to professional and legal boundaries.

## 6. Finding Severity Ratings

| SEVERITY | CVSS 3.1 SCORE RANGE | DEFINITIONS |
|---|---|---|
| Critical | 9.0 – 10.0 | **Exploitation**:<br>• Exploitation is straightforward.<br>• Results in system-level compromise.<br>**Plan of Actions :**<br>• Patch Immediately |
| High | 7.0 – 8.9 | **Exploitation**:<br>• Exploitation is more difficult. Could cause elevated privileges.<br>• Potential to cause loss of data or downtime. .<br>**Plan of Actions :**<br>• Patch as soon as possible |
| Medium | 4.0 – 6.9 | **Exploitation**:<br>• Vulnerabilities exist but are not exploitable.<br>• Might require extra steps to make the vulnerability exploitable.<br>**Plan of Actions :**<br>• Patch after high-priority issues has been resolved. |
| Low | 0.1 – 3.9 | **Exploitation**:<br>• Vulnerabilities are non-exploitable.<br>• Mitigation would reduce an organization's attack surface.<br>**Plan of Actions :**<br>• Patch during the next maintenance window. |

# 7. Risk Factors

Risk is measured by two factors: Likelihood & Impact

## 7.1 Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

## 7.2 Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity and availability of client systems and/or data, reputational harm, and financial loss.

# 8. Scope

This **Network Penetration Testing Report** covers the assessment of **31 public IP addresses** provided for testing. The evaluation focused on identifying vulnerabilities through reconnaissance, scanning, and vulnerability assessment without performing exploitation.

# 9. Execution Summary

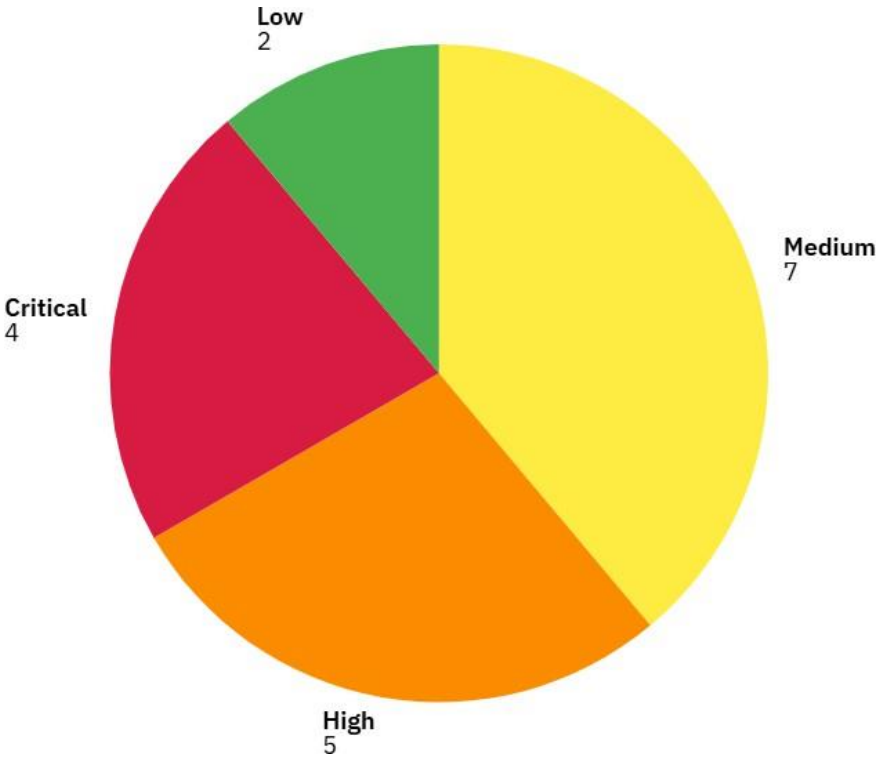
As part of an internship project, **Sure Trust** assigned a security assessment of **31 public IP addresses** to evaluate their security posture. The **network penetration testing** was conducted from **January 1st, 2025, to February 9th, 2025**.

## 9.1 Scope & Limitations

This **Network Penetration Testing Report** covers the assessment of **31 public IP addresses** provided for testing. The evaluation was conducted using reconnaissance, scanning, and vulnerability assessment techniques without performing any exploitation. **Denial-of-Service (DoS) attacks and active exploitation were strictly excluded.**

## 9.2 Technical Summary of Vulnerabilities

| Critical | High | Medium | Low | Total |
|---|---|---|---|---|
| 4 | 5 | 7 | 2 | 18 |


Low
2
Medium
7
Critical
4
High
5

# 10. Network Penetration Testing Findings

## 10.1 Critical

### 10.1.1 Critical OpenSSH Remote Code Execution via Agent Forwarding

**Description** :

The vulnerability resides in the PKCS#11 feature of ssh-agent. An insufficiently trustworthy search path allows for remote code execution if an agent is forwarded to an attacker-controlled system. This issue persists due to an incomplete fix for CVE-2016-10009.

**CVSS Score : 9.8**

**Impact :**

Successful exploitation enables attackers to execute arbitrary code on the affected system, potentially leading to full system compromise and unauthorized access to sensitive information.

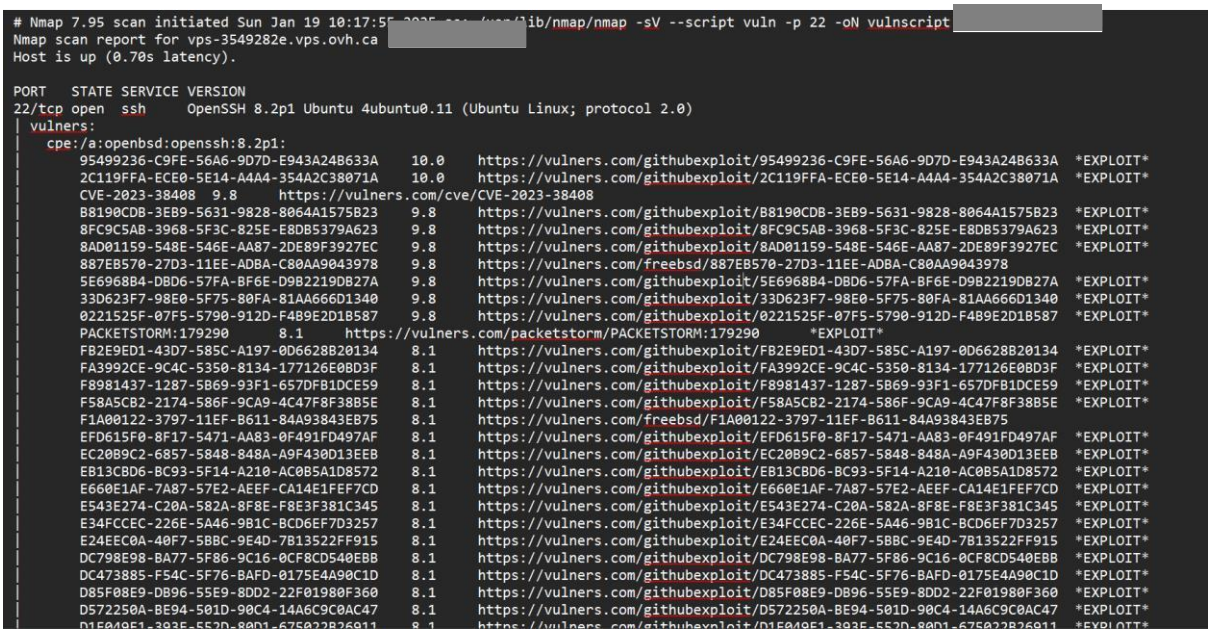
**Recommendations :**

- **Update OpenSSH :** Upgrade to OpenSSH version 9.3p2 or later to address this vulnerability.
- **Avoid Agent Forwarding :** Refrain from forwarding ssh-agent to untrusted systems.
- **Monitor and Audit :** Regularly review system logs and configurations to detect and prevent unauthorized access.

**References :**

- National Vulnerability Database : click here
- Ubuntu Security Notice : click here
- OpenSSH Release Notes : click here

## POC :



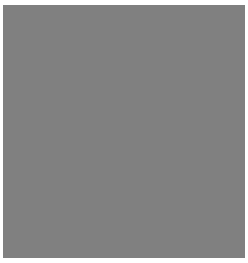
```
# Nmap 7.95 scan initiated Sun Jan 19 10:17:5[redacted] /usr/lib/nmap/nmap -sV --script vuln -p 22 -oN vulnscript [redacted]
Nmap scan report for vps-3549282e.vps.ovh.ca [redacted]
Host is up (0.70s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.2p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       887EB570-27D3-11EE-ADBA-C80AA9043978    9.8     https://vulners.com/freebsd/887EB570-27D3-11EE-ADBA-C80AA9043978
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340  *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134  *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F  *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59  *EXPLOIT*
|       F58A5CB2-2174-586F-9CA9-4C47F8F38B5E    8.1     https://vulners.com/githubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F38B5E  *EXPLOIT*
|       F1A00122-3797-11EF-B611-84A93843EB75    8.1     https://vulners.com/freebsd/F1A00122-3797-11EF-B611-84A93843EB75
|       EFD615F0-8F17-5471-AA83-0F491FD497AF    8.1     https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF  *EXPLOIT*
|       EC20B9C2-6857-5848-848A-A9F430D13EEB    8.1     https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D13EEB  *EXPLOIT*
|       EB13CBD6-BC93-5F14-A210-AC0B5A1D8572    8.1     https://vulners.com/githubexploit/EB13CBD6-BC93-5F14-A210-AC0B5A1D8572  *EXPLOIT*
|       E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD    8.1     https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD  *EXPLOIT*
|       E543E274-C20A-582A-8F8E-F8E3F381C345    8.1     https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345  *EXPLOIT*
|       E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257    8.1     https://vulners.com/githubexploit/E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257  *EXPLOIT*
|       E24EEC0A-40F7-5BBC-9E4D-7B13522FF915    8.1     https://vulners.com/githubexploit/E24EEC0A-40F7-5BBC-9E4D-7B13522FF915  *EXPLOIT*
|       DC798E98-BA77-5F86-9C16-0CF8CD540EBB    8.1     https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD540EBB  *EXPLOIT*
|       DC473885-F54C-5F76-BAFD-0175E4A90C1D    8.1     https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A90C1D  *EXPLOIT*
|       D85F08E9-DB96-55E9-8DD2-22F01980F360    8.1     https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8DD2-22F01980F360  *EXPLOIT*
|       D572250A-BE94-501D-90C4-14A6C9C0AC47    8.1     https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C0AC47  *EXPLOIT*
|       D1E049E1-393E-552D-80D1-675922B26911    8.1     https://vulners.com/githubexploit/D1E049E1-393E-552D-80D1-675922B26911  *EXPLOIT*
|       1FFDA397-F480-5C74-90F3-060E1FE11B2E    8.1     https://vulners.com/githubexploit/1FFDA397-F480-5C74-90F3-060E1FE11B2E  *EXPLOIT*
|       1F7A6000-9E6D-511C-B0F6-7CADB7200761    8.1     https://vulners.com/githubexploit/1F7A6000-9E6D-511C-B0F6-7CADB7200761  *EXPLOIT*
|       1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99    8.1     https://vulners.com/githubexploit/1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99  *EXPLOIT*
|       1AB9F1F4-9798-59A0-9213-1D907E81E7F6    8.1     https://vulners.com/githubexploit/1AB9F1F4-9798-59A0-9213-1D907E81E7F6  *EXPLOIT*
|       1A779279-F527-5C29-A64D-94AAA4ADD6FD    8.1     https://vulners.com/githubexploit/1A779279-F527-5C29-A64D-94AAA4ADD6FD  *EXPLOIT*
|       15C36683-070A-5CC1-B21F-5F0BF974D9D3    8.1     https://vulners.com/githubexploit/15C36683-070A-5CC1-B21F-5F0BF974D9D3  *EXPLOIT*
|       1337DAY-ID-39674        8.1     https://vulners.com/zdt/1337DAY-ID-39674        *EXPLOIT*
|       123C2683-74BE-5320-AA3A-C376C8E3A992    8.1     https://vulners.com/githubexploit/123C2683-74BE-5320-AA3A-C376C8E3A992  *EXPLOIT*
|       11F020AC-F907-5606-8805-0516E06160EE    8.1     https://vulners.com/githubexploit/11F020AC-F907-5606-8805-0516E06160EE  *EXPLOIT*
|       108E1D25-1F7E-534C-97CD-3F6045E32B98    8.1     https://vulners.com/githubexploit/108E1D25-1F7E-534C-97CD-3F6045E32B98  *EXPLOIT*
|       0FC4BE81-312B-51F4-9D9B-66D8B5C093CD    8.1     https://vulners.com/githubexploit/0FC4BE81-312B-51F4-9D9B-66D8B5C093CD  *EXPLOIT*
|       0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180    8.1     https://vulners.com/githubexploit/0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180  *EXPLOIT*
|       0E9294FD-6B44-503A-84C2-C6E76E53B0B7    8.1     https://vulners.com/githubexploit/0E9294FD-6B44-503A-84C2-C6E76E53B0B7  *EXPLOIT*
|       0A8CA57C-ED38-5301-A03A-C841BD3082EC    8.1     https://vulners.com/githubexploit/0A8CA57C-ED38-5301-A03A-C841BD3082EC  *EXPLOIT*
|       CVE-2020-15778  7.8     https://vulners.com/cve/CVE-2020-15778
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       CVE-2020-12062  7.5     https://vulners.com/cve/CVE-2020-12062
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       CVE-2021-28041  7.1     https://vulners.com/cve/CVE-2021-28041
|       76B5068C-8436-11EB-9469-080027F515EA    7.1     https://vulners.com/freebsd/76B5068C-8436-11EB-9469-080027F515EA
|       CVE-2021-41617  7.0     https://vulners.com/cve/CVE-2021-41617
|       2A1B931F-2B86-11EC-8ACD-C80AA9043978    7.0     https://vulners.com/freebsd/2A1B931F-2B86-11EC-8ACD-C80AA9043978
|       C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    6.8     https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3  *EXPLOIT*
|       10213DBE-F683-58BB-B6D3-353173626207    6.8     https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207  *EXPLOIT*
|       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2020-14145  5.9     https://vulners.com/cve/CVE-2020-14145
|       CVE-2016-20012  5.3     https://vulners.com/cve/CVE-2016-20012
|       CVE-2021-36368  3.7     https://vulners.com/cve/CVE-2021-36368
|_      PACKETSTORM:140261      0.0     https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jan 19 10:18:15 2025 -- 1 IP address (1 host up) scanned in 20.50 seconds
```

## Affected Ips :

1) [redacted]
2)
3)
4)

5)
6)
7)
8)
9)
10
11 

### 10.1.2 Critical Remote Code Execution Vulnerability in Remote Desktop Services (BlueKeep)

**Description** :

BlueKeep is a critical security vulnerability identified in Microsoft's Remote Desktop Services. It allows an unauthenticated attacker to connect to the target system using RDP and send specially crafted requests, leading to remote code execution. This vulnerability is pre-authentication and requires no user interaction.

**CVSS Score : 9.8**

**Impact :**

- Allows attackers to execute arbitrary code on the target system.
- Potential for the creation of wormable exploits, enabling rapid spread across vulnerable systems.
- Could lead to full system compromise, data theft, and disruption of services.

**Recommendations :**

- **Apply Patches :** Microsoft released patches for this vulnerability in May 2019. Ensure all affected systems are updated.

- **Disable RDP if Not Needed** : If Remote Desktop Services are not essential, disable them to reduce exposure.

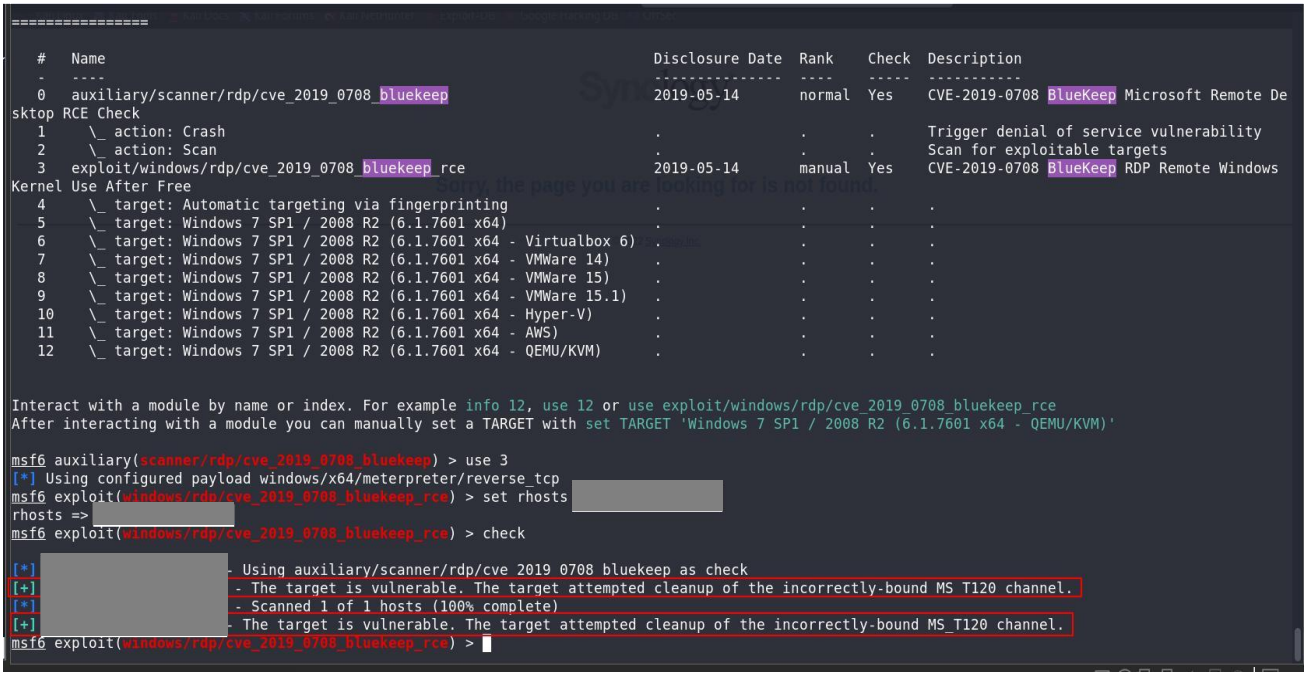
- **Enable Network Level Authentication (NLA) :** NLA adds an extra layer of authentication before establishing a session and can mitigate the risk.

- **Monitor RDP Access**: Regularly review and restrict RDP access through firewalls and employ intrusion detection systems to monitor unusual activities.

**References :**

- Microsoft Security Advisory on Bluekeep
- NVD entry for Bulekeep
- BlueKeep vulnerability details

**POC :**



```
==========

   #   Name                                                 Disclosure Date  Rank    Check  Description
   -   ----                                                 ---------------  ----    -----  -----------
   0   auxiliary/scanner/rdp/cve_2019_0708_bluekeep         2019-05-14       normal  Yes    CVE-2019-0708 BlueKeep Microsoft Remote De
sktop RCE Check
   1     \_ action: Crash                                   .                .       .      Trigger denial of service vulnerability
   2     \_ action: Scan                                    .                .       .      Scan for exploitable targets
   3   exploit/windows/rdp/cve_2019_0708_bluekeep_rce       2019-05-14       manual  Yes    CVE-2019-0708 BlueKeep RDP Remote Windows
Kernel Use After Free
   4     \_ target: Automatic targeting via fingerprinting  .                .       .      .
   5     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)  .                .       .      .
   6     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)   .                .       .      .
   7     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)      .                .       .      .
   8     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)      .                .       .      .
   9     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)    .                .       .      .
   10    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)        .                .       .      .
   11    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)            .                .       .      .
   12    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)       .                .       .      .


Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)'

msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > use 3
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts [redacted]
rhosts => [redacted]
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > check

[*] [redacted] - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] [redacted] - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] [redacted] - Scanned 1 of 1 hosts (100% complete)
[+] [redacted] - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

**Affected Ip :** [redacted]

### 10.1.3 Default Credentials Found on FTP and Telnet Services

**Description** :

During the penetration test, it was discovered that the FTP and Telnet services were accessible using default credentials. Default usernames and passwords are often well-known and publicly available, making them a common entry point for attackers. Unauthorized access to these services could allow an attacker to execute commands, exfiltrate data, or escalate privileges within the network.

**CVSS Score : 9.4**

## Impact :

- Unauthorized access to sensitive data stored on the FTP server.
- Potential for lateral movement within the network using Telnet access.
- Risk of data exfiltration, modification, or deletion.
- Excessive data uploads to FTP can fill up disk space, causing resource exhaustion.

## Recommendations :

- **Change Default Credentials Immediately:** Replace all default usernames and passwords with **strong, unique credentials**.
- **Disable Telnet and Use SSH**: Since Telnet transmits credentials in plaintext, it should be **disabled** in favor of **SSH**, which encrypts communications.
- **Use Secure FTP (SFTP/FTPS) Instead of FTP:** Standard FTP is insecure and should be replaced with **SFTP (Secure FTP) or FTPS (FTP over SSL/TLS)** to prevent credential interception.
- **Restrict Access to Trusted IPs**: Implement **firewall rules and access control lists (ACLs)** to limit service access to only authorized users and networks.
- **Enable Logging and Intrusion Detection :** Monitor login attempts and file modifications for suspicious activities.

## References :

- CVE-2022-47558 - NVD
- OWASP – Insecure Authentication
- CVE Databases

## POC :

```
21      ftp     root            root
21      ftp     root            solokey
21      ftp     root            system
21      ftp     root            svgodie
21      ftp     root            t0talc0ntr0l4!
21      ftp     root            taZz@01
21      ftp     root            tini
21      ftp     root            testpass123
21      ftp     root            toor
21      ftp     root            taZz@23495859
21      ftp     root            tslinux
21      ftp     root            tsgoingon
21      ftp     root            user
21      ftp     root            vmware
21      ftp     root            vizxv
21      ftp     root            wh00t!
21      ftp     root            xc3511
```

```
┌──(root㉿kali)-[/home/srujan]
└─# ftp
Connected to 207.148.103.159.
220 Welcome to the ftp service
Name (:                    ): root
12331 Password required for root.
Password:
230 User logged in, proceed
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd help
250 Requested File Action Completed OK
ftp> pwd
Remote directory: /help
ftp> mkdir g10
250 Requested File Action Completed OK
ftp> cd g10
250 Requested File Action Completed OK
ftp> pwd
Remote directory: /help/g10
ftp>
```

```
┌──(root㉿kali)-[/home/sruian/project/ip23]
└─# telnet
Trying
Connect
Escape character is '^]'.
login: ubnt
Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

ubnt@server:~$ id
uid=1001(ubnt) gid=1001(ubnt) groups=1001(ubnt)
ubnt@server:~$ ls
richard
ubnt@server:~$ cd richard
ubnt@server:~/richard$ ls
ubnt@server:~/richard$ cd ..
ubnt@server:~$
```

## Affected Ips :

- [redacted]
- [redacted]

### 10.1.4 Anonymous FTP Login with File Traversal, Write, and Folder Deletion Permissions

## Description :

The FTP server allows unauthenticated (anonymous) users to:

Traverse directories (potential information disclosure)
Upload files (possible malware/phishing kits)
Create new folders (for persistent access or attack staging)
Delete folders (potential denial-of-service)

## CVSS Score : 9.1

## Impact :

- **Data Exfiltration:** Attackers can upload and later download stolen data.
- **Malware Hosting:** Public anonymous FTP can serve as a **malware distribution point**.
- **Evasion & Persistence:** Attackers can hide files inside subdirectories.
- **DoS (Denial of Service):** By deleting folders, attackers can break applications relying on directory structures.
- **Phishing Campaigns:** Attackers can upload HTML-based phishing kits and dynamically delete evidence.

## Recommendations :

- **Disable Anonymous FTP Access:**
  - Edit the FTP configuration file : sudo nano /etc/vsftpd.conf
  - Change the following line : anonymous_enable=NO
  - Restart the FTP service : sudo systemctl restart vsftpd

- **Restrict Write Permissions**:

- Disable anonymous write access :
  write_enable=NO
  anon_upload_enable=NO
  anon_mkdir_write_enable=NO
  anon_other_write_enable=NO
- Restart the FTP service : sudo systemctl restart vsftpd

- **Implement Firewall Rules:**
  - Block FTP from external access : sudo ufw deny 21

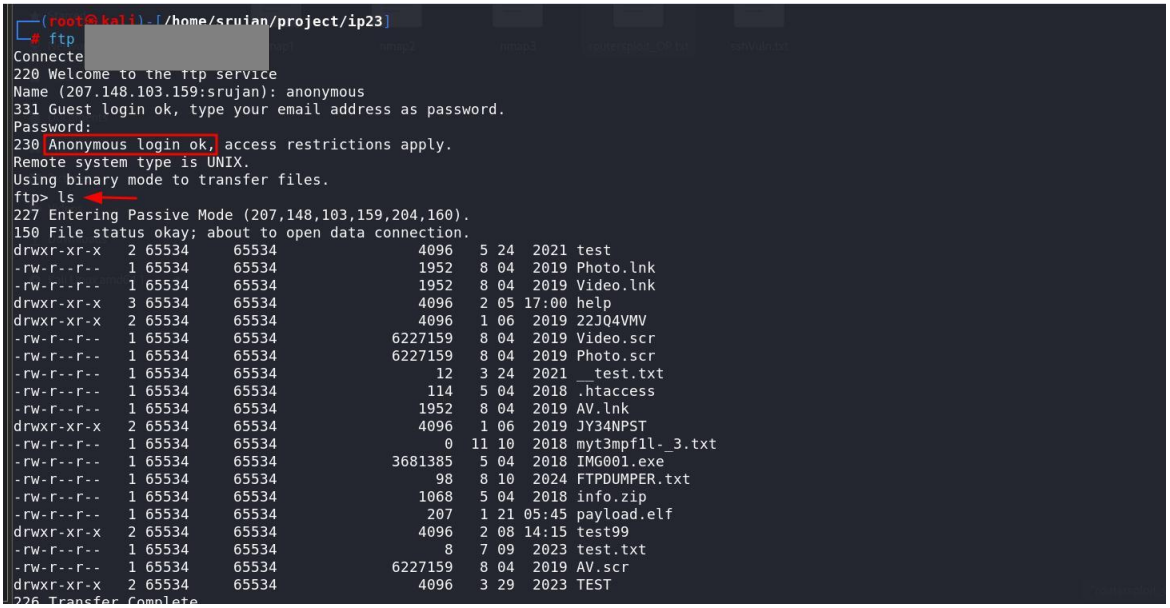
- **Enable Authentication:**

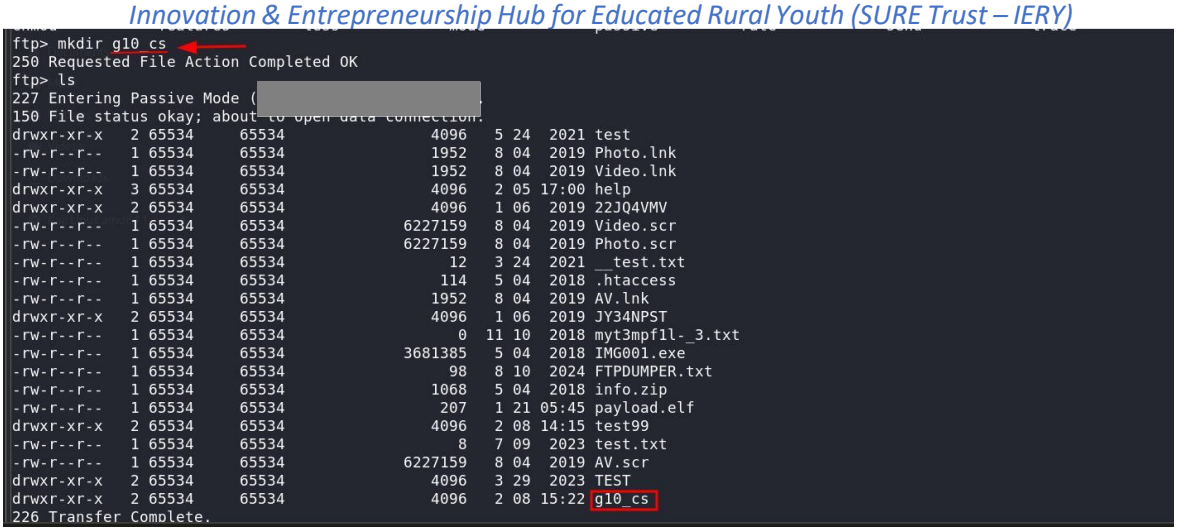
  - Require user credentials before accessing FTP: local_enable=YES
  - Restart the FTP service : sudo systemctl restart vsftpd

## References :

- [OWASP Unrestricted File Upload]

## POC :






- **Affected Ip :** [redacted]

## 10.2 High

### 10.2.1 Exposed and Insecure Admin Login Page

**Description** :

The admin login page for a Sangfor system is publicly accessible over an unsecured HTTP connection, making it vulnerable to various attacks. Additionally, the login form reveals the username "admin" by default, which increases the risk of brute-force and credential-stuffing attacks.

**Identified Security Issues:**

1. **Unencrypted Login (HTTP Instead of HTTPS)**
   - The page is served over HTTP instead of HTTPS, meaning credentials can be intercepted via MITM attacks.
2. **Publicly Exposed Admin Panel**
   - The login page is accessible from the internet, making it a potential target for brute-force attacks.
3. **Username Enumeration**
   - The prefilled "admin" username provides attackers with a known valid username for brute-force attempts.
4. **Outdated UI & ActiveX Requirement**
   - The system indicates support only for Internet Explorer and ActiveX, suggesting obsolete security measures and possible exploitation via ActiveX vulnerabilities.

**CVSS Score : 8.2**

**Impact :**

- **MITM Attack:** Credentials can be intercepted if a user logs in over an insecure network.
- **Brute Force Attacks:** The prefilled "admin" username makes it easier to attempt password guessing.
- **Remote Exploitation:** If the system uses outdated cryptographic methods, attackers could exploit known vulnerabilities.
- **Privilege Escalation:** If weak or default credentials are in use, an attacker could gain full administrative access.

**Recommendations :**

- **Enfoce HTTPS :**

- Implement SSL/TLS encryption to secure login credentials.
- Redirect all **HTTP requests to HTTPS**.

- **Restrict Access:**
  - Limit access to the admin panel via **IP whitelisting or VPN**.
  - Block internet-facing login portals unless absolutely necessary.

- **Remove Username Autofill:**
  - Prevent the admin username from being displayed by default.
  - Implement **generic login failure messages** (e.g., "Invalid credentials" instead of "Invalid password").
- **Implement MFA:**
  - Enforce **multi-factor authentication (MFA)** to prevent unauthorized access.

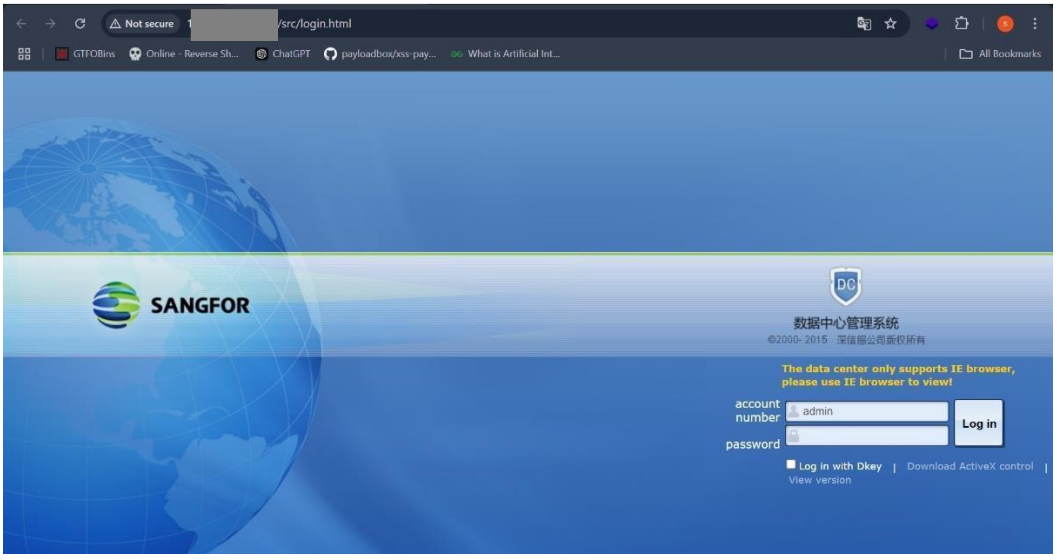
- **Upgrade the System:**
  - Since the system recommends **Internet Explorer & ActiveX**, it may be outdated and vulnerable.
  - Update to a modern, **actively maintained system**.

- **Enable Rate Limiting & Lockout Policies:**
  - Restrict login attempts per IP..
  - Implement progressive delays for repeated failed login attempts.

## References :

- OWASP Transport Layer Security Cheat Sheet
- CWE-523: Unprotected Transport of Credentials

## POC :



**Affected Ip :** [redacted]

### 10.2.2 SNMP Agent Default Community Name (public)

**Description** :

**Simple Network Management Protocol (SNMP) v1** is an outdated network management protocol that uses **plaintext community strings** (such as "public" or "private") for authentication. SNMP v1 lacks encryption and strong authentication mechanisms, making it highly vulnerable to **Man-in-the-Middle (MitM) attacks**, **credential sniffing**, and **unauthorized access to network devices**.

**CVSS Score : 7.5**

**Impact :**

- **Network Enumeration:** Attackers can discover active hosts, interfaces, and device information.
- **Exposure of Credentials & Configurations:** SNMP responses may contain password hashes, IP addresses, and sensitive device details.
- **Configuration Manipulation:** If **SNMP write access** is enabled, attackers can **alter device configurations**, disrupt routing, or disable security settings.

**Recommendations :**

- **Disable SNMP v1 & Upgrade to SNMP v3 :** SNMP v3 supports **encryption (AES/DES)** and **strong authentication**.
- **Restrict SNMP Access:** Use **firewall rules** to allow SNMP queries **only from trusted Ips.** Disable SNMP if not required on a system**.**

- **Change Default Community Strings:** Avoid "public", "private", or "admin". Use long, complex SNMP community strings.

- **Regularly Audit & Patch Devices**: Ensure all network devices (switches, routers, firewalls) are **updated** and **patched** for SNMP vulnerabilities.

**References :**

- Tenable

**POC :**

```
┌──(root㉿kali)-[/home/srujan/project/ip7]
└─# nmap -sV -sU [redacted] -p 161 -Pn -oN snmp
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 20:49 IST
Nmap scan report for fk.dist.uns.ac.id ([redacted])
Host is up (0.87s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; MikroTik SNMPv3 server (public)
Service Info: Host: [CHR] Dist. Public

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.10 seconds
```

```
File  Edit  View  Search  Terminal  Tabs  Help
root@kali: /home/srujan/project/ip19 | root@kali: /home/srujan/project | root@kali: /home/srujan/project/ip7 | root@kali: /home/srujan

                                                    (Accepted: none, user, user&realm)
   PASSWORD                                  no     The password to test
   PASS_FILE          /usr/share/metasploit-framework/  no  File containing communities, one per line
                      data/wordlists/snmp_default_pass
                      .txt
   PROTOCOL           udp                    yes    The SNMP protocol to use (Accepted: udp, tcp)
   RHOSTS                                    yes    The target host(s), see https://docs.metasploit.com/docs
                                                    /using-metasploit/basics/using-metasploit.html
   RPORT              161                    yes    The target port
   STOP_ON_SUCCESS    false                  yes    Stop guessing when a credential works for a host
   THREADS            1                      yes    The number of concurrent threads (max one per host)
   USER_AS_PASS       false                  no     Try the username as the password for all users
   VERBOSE            true                   yes    Whether to print output for all attempts
   VERSION            1                      yes    The SNMP version to scan (Accepted: 1, 2c, all)

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

msf6 auxiliary(scanner/snmp/snmp_login) > set rhosts [redacted]
rhosts => [redacted]
msf6 auxiliary(scanner/snmp/snmp_login) > set threads 30
threads => 30
msf6 auxiliary(scanner/snmp/snmp_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 1[redacted]61 - Login Successful: public (Access level: read-only); Proof (sysDescr.0): RouterOS CHR
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/snmp/snmp_login) >
```

**Affected Ip :** [redacted]

### 10.2.3 Apache Byte-Range Filter Denial of Service (DoS) Attack

**Description** :

The Apache Byte-Range Filter DoS vulnerability (CVE-2011-3192) affects Apache HTTP Server 2.2.x when processing malicious Range or Request-Range headers. Attackers can exploit this by sending specially crafted HTTP requests with multiple overlapping byte ranges. This causes excessive memory and CPU consumption, leading to server crashes or resource exhaustion. Since the attack requires no authentication and can be executed remotely, it poses a **serious risk** to publicly accessible Apache servers.

## CVSS Score : 7.5

## Impact :

- **Denial of Service (DoS):** Attackers **crash the Apache server** by overloading memory with multiple overlapping byte-range requests.
- **High Resource Utilization:** The vulnerability forces the server to allocate **large memory buffers**, slowing down or crashing services.
- **Affects Shared Hosting Environments:** Servers hosting multiple websites are more vulnerable as a single attack can impact all hosted services.

## Recommendations :

- **Update Apache HTTP Serverv3 :** Upgrade to **Apache 2.2.20 or later**, where this issue is fixed.
- **Disable Byte-Range Requests (Temporary Mitigation):** Modify **httpd.conf or .htaccess** to disable the filter.
- **Rate-Limit Requests:** Use mod_ratelimit to limit the number of requests per IP.
- **Monitor & Log Suspicious Requests**: Regularly check Apache logs for excessive Range requests.

## References :

- Apache security advisory
- CVE-2011-3192 - NIST NVD

## POC :

```
443/tcp  open  https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.tenable.com/plugins/nessus/55976
|       https://www.securityfocus.com/bid/49303
|       https://seclists.org/fulldisclosure/2011/Aug/175
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
5000/tcp open  upnp
5001/tcp open  commplex-link

Nmap done: 1 IP address (1 host up) scanned in 811.87 seconds
```

**Affected Ip :** [redacted]

### 10.2.4 IRZ Mobile Router Information Disclosure Due to Unauthenticated Access

**Description** :
A publicly accessible **IRZ Mobile Router** was discovered, exposing **device configuration details**, including **MAC addresses, routing tables, and other sensitive network information**. This occurs due to **misconfigured access control**, allowing unauthenticated users to retrieve device data by directly accessing the router's web interface using its IP address.

Such exposure poses a **significant security risk**, as attackers can use leaked **MAC addresses** for network spoofing, analyze **routing tables** to map network topology, and exploit **device firmware vulnerabilities** for further attacks.

**CVSS Score : 7.5**

**Impact :**

- **Network Reconnaissance:** Attackers can analyze routing tables and MAC addresses, allowing them to map network infrastructure.
- **Spoofing & MITM Attacks:** Exposed **MAC addresses** enable **MAC spoofing**, potentially allowing unauthorized network access.

- **Exploitation of Router Vulnerabilities:** Attackers can search for **known vulnerabilities** in the router model and exploit them for remote code execution or configuration changes.

**Recommendations :**

- **Restrict Web Interface Access:**
  - Configure firewall rules to allow access only from trusted IPs.
  - Disable external access if remote management is not required

- **Implement Authentication Controls:**
  - Enable **password protection** for the router's web interface.
  - If supported, enable **multi-factor authentication (MFA)**.

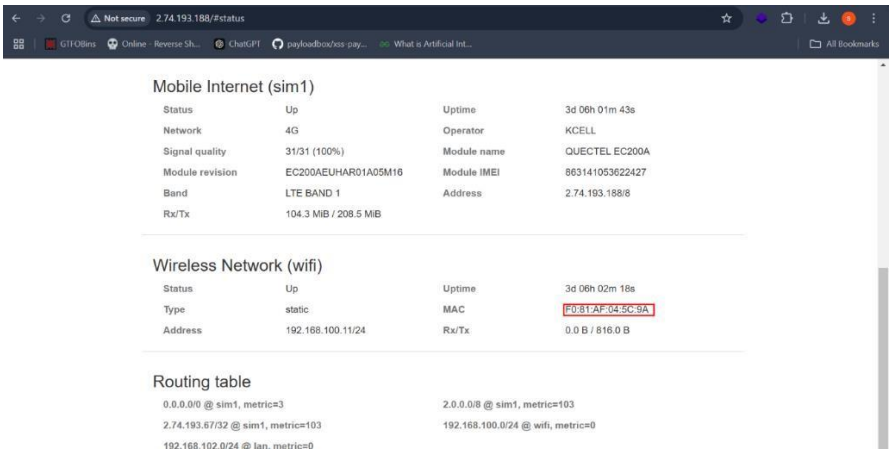
- **Disable Unnecessary Service:**
  - Check the router settings and **disable any unnecessary protocols** that might expose sensitive information.
  - Ensure **SNMP is properly secured or disabled** if not in use.
- **Firmware Updates & Security Patches**:
  - Regularly **update the router firmware** to fix security vulnerabilities.

Subscribe to vendor security alerts to stay updated on potential threats.

## References :

- IRZ Services
- CVE-2021-20090 - Exposed Router Configuration

## POC :




## Affected Ip : [redacted]

### 10.2.5 Exim libspf2 Integer Underflow Remote Code Execution Vulnerability

## Description :

This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Exim's libspf2. The issue arises during the parsing of SPF macros, where the process fails to properly validate user-supplied data, leading to an integer underflow before writing to memory. An attacker can exploit this flaw to execute code in the context of the service account.

## CVSS Score : 7.5

## Impact :

Successful exploitation of this vulnerability allows an attacker to execute arbitrary code within the context of the affected service account. This can lead to unauthorized access, data manipulation, and potential disruption of services.

## Recommendations :

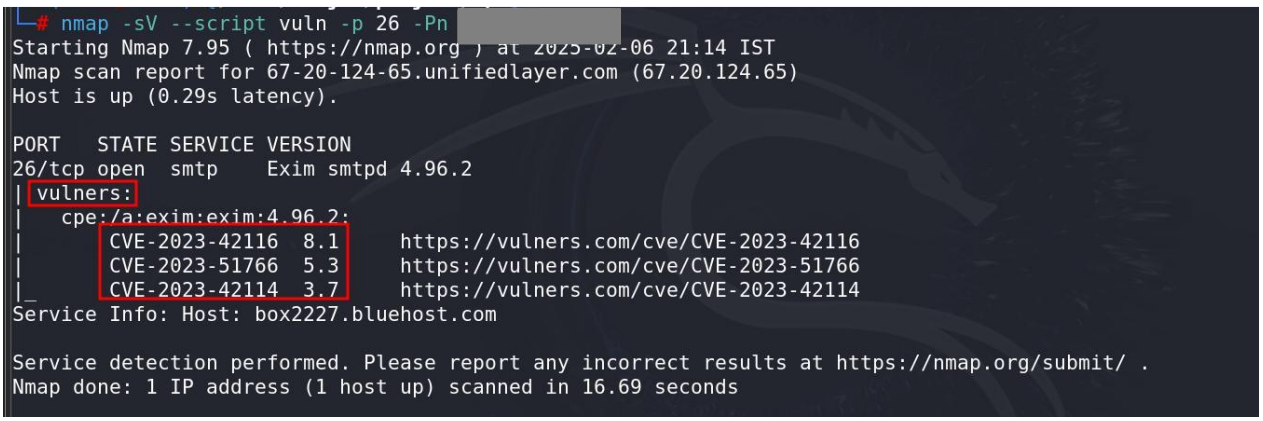
- **Mitigation:** Avoid using the spf condition in your Access Control Lists (ACLs) until a patched version of libspf2 is available.

- **Patch Application:** Monitor for updates from the libspf2 maintainers and apply patches once they are released to address this vulnerability.

## References :

- Zero day initiative
- National Vulnerability Database Entry
- Pentest tools

## POC :



**Affected Ips :**

- [redacted]
- [redacted]

## 10.3 Medium

### 10.3.1 Overly Permissive Cross-Domain and Client Access Policy Leading to Unauthorized Access

**Description** :

A cross-domain policy file (crossdomain.xml) is used by web applications to specify which external domains can access resources on the server. In this case, the policy is overly permissive, allowing all domains (<allow-access-from domain="*"/>), which poses a significant security risk.

**CVSS Score : 6.5**

**Impact :**

- **Sensitive Data Exposure:** Attackers can access restricted APIs or fetch user data.
- **Unauthorized Actions via CSRF:** Attackers can force users to perform actions without consent.
- **Integration with XSS Attacks:** If XSS is present, attackers can steal cookies, credentials, or tokens.
- **Phishing & Social Engineering Risks:** Attackers can embed server content in fraudulent sites.

**Recommendations :**

- **Restrict Cross-Domain Access:** Modify crossdomain.xml to allow only trusted domains:

```
<cross-domain-policy>
<allow-access-from domain="trusted-site.com"/>
</cross-domain-policy>
```

Remove crossdomain.xml if not needed to eliminate this risk entirely.

- **Enable Strong Authentication:**

  - Implement **OAuth 2.0, JWT tokens, or API keys** to prevent unauthorized access.Cloud services like AWS, Cloudflare, and Azure offer **managed SSL certificates** that auto-renew.

## References :

- Acunetix
- Adobe
- OWASP Cheat Sheet

## POC :


## Affected Ip :

### 10.3.2 Jetty 9.4.z-SNAPSHOT Denial of Service (DoS) and DDoS Vulnerability Report

## Description :

Improper parsing of the Accept header with numerous quality factor (q) values leads to high CPU utilization. Attackers can craft requests that result in excessive processing, leading to a Denial of Service (DoS) condition.

## CVSS Score : 6.5

## Impact :

- Attackers can craft malicious HTTP/2 requests to overload system resources.

- Unpatched versions of Jetty 9.4.z-SNAPSHOT are susceptible to DoS attacks without rate-limiting protections.
- An attacker with a botnet could leverage DDoS tactics to amplify the impact of these vulnerabilities.

## Recommendations :

- **Upgrade Jetty** to the latest stable version that includes security patches.
- **Disable HTTP/2** if not required, or apply rate-limiting configurations.
- **Implement Web Application Firewalls (WAFs)** to detect and block malicious traffic.
- **Monitor network traffic** for unusual patterns that could indicate ongoing attacks.
- **Enable TLS protections** and configure appropriate timeout settings to prevent resource exhaustion

## POC :

```
┌──(root㉿kali)-[/home/srujan/project/ip17]
└─# cat nmap2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 15:56 IST
Nmap scan report for vps-3549282e.vps.ovh.ca (
Host is up (0.52s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d0:8e:17:64:a9:4e:6e:51:a6:58:b8:e4:15:9c:82:0d (RSA)
|   256 56:9c:e9:14:fe:a5:7f:6f:77:04:62:d1:c6:25:a6:0c (ECDSA)
|_  256 4f:b5:14:3c:b2:2d:17:40:c7:bc:12:e0:77:0c:5f:8e (ED25519)
80/tcp   closed http
443/tcp  closed https
4444/tcp open   http       Jetty 9.4.z-SNAPSHOT
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
5900/tcp open   vnc        VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|_    VNC Authentication (2)
8080/tcp closed http-proxy
8081/tcp open   http       Python BaseHTTPServer http.server 2 or 3.0 - 3.1
|_http-title: Site doesn't have a title (text/html).
```

## Affected Ip :

- [redacted]

### 10.3.3 Expired HTTPS Certificate- Loss of Encryption & Trust

## Description :

An **expired HTTPS certificate** means that a website's **SSL/TLS certificate is no longer valid**, causing browsers and security tools to **flag the site as insecure**. HTTPS certificates ensure **encrypted communication** between users and servers, preventing **Man-in-the-Middle (MitM) attacks, data interception, and phishing risks**.

When a certificate expires, users will see browser warnings (e.g., "Your connection is not private"), which may lead to:

- **Loss of customer trust** and website reputation.
- **Insecure communications**, making **user credentials, payment details, and sensitive data vulnerable** to eavesdropping.
- **Blocking by browsers, firewalls, or security policies**, preventing access to the website.

## CVSS Score : 6.4

## Impact :

- **Data Interception & Man-in-the-Middle Attacks:** Attackers can impersonate the website (e.g., via **SSL stripping**) and intercept login credentials, payment details, or personal data.
- **Loss of Trust & Reputation:** Users encountering HTTPS warnings may **abandon the site**, leading to **business loss**.
- **Website Downtime & SEO Penalties:** Major browsers (Chrome, Firefox, Edge) **block sites with expired certificates**, reducing traffic and SEO ranking.

## Recommendations :

- **Renew SSL/TLS Certificates Before Expiry:** Set up **automated certificate renewal** using tools like **Let's Encrypt (Eg :** certbot renew --quiet**). Monitor certificate expiration using scripts or security monitoring tools.**
- **Monitor HTTPS Traffic & Alerts :** Set up monitoring systems to detect expired certificates (e.g., Zabbix, Nagios, or SSL monitoring tools).
- **Use Long-Term & Auto-Renewing Certificates:**
- Consider **multi-year SSL certificates** (e.g., 1-2 years) and automated renewal mechanisms.
- Cloud services like AWS, Cloudflare, and Azure offer **managed SSL certificates** that auto-renew.

**References :**

- Mozilla SSL configuration guide
- Transport layer security guide
- SSL lab test for certificate expiry

**POC :**


**Affected Ip :** [redacted]

### 10.3.4 Weak Diffie-Hellman Key Exchange- Insufficient Group Strength (Logjam Attack)

**Description** :

The system is using **Diffie-Hellman (DH) key exchange** with a **1024-bit group**, which is vulnerable to precomputed discrete logarithm attacks (**Logjam**). This allows attackers to intercept encrypted traffic by forcing a downgrade to weak cryptographic parameters.

If an attacker has access to significant computing power, they can **decrypt TLS communications**, compromising confidentiality and security. The **modulus source is RFC2409/Oakley Group 2**, which is widely known and vulnerable to precomputed attacks.

**CVSS Score : 5.9**

**Impact :**

- **Man-in-the-Middle (MitM) Attack:** Attackers can intercept TLS traffic by forcing the use of weak 1024-bit DH keys.
- **SSL/TLS Downgrade Attack:** Clients and servers may be forced to use weak encryption, making them susceptible to decryption.

- **VPNs and SSH Affected: IPSec VPNs and SSH key exchanges** relying on weak DH groups are also vulnerable.

## Recommendations :

- **Disable 1024-bit Diffie-Hellman Groups:** Ensure all **DH groups use at least 2048-bit keys**.
- **Use Elliptic Curve Diffie-Hellman (ECDH):** Prefer **ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)** over traditional **DHE**.
- **Perform Security Scanning & Compliance Checks :** Scan for weak DH parameters (**nmap** --script ssl-enum-ciphers -p 443 <target>)

## References :

- Weak DH Attack (Logjam)
- CVE-2015-4000 - Logjam

## POC :

```
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| sslv2-drown:
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
990/tcp  open  ftps
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 553.61 seconds
```

## Affected Ip :

- [redacted]

## 10.3.5 SSL POODLE Vulnerability (CVE-2014-3566)- Padding Oracle On Downgraded Legacy Encryption

### Description :

The POODLE (Padding Oracle On Downgraded Legacy Encryption) attack, identified as CVE-2014-3566, exploits a vulnerability in the SSL 3.0 protocol that allows attackers to perform padding oracle attacks and decrypt sensitive data. SSL 3.0 uses block ciphers with CBC mode, which are vulnerable to padding-related weaknesses when improperly handled.

### CVSS Score : 5.4

### Impact :

- **Sensitive Data Exposure:** Attackers can decrypt session cookies, passwords, or authentication tokens if the website relies on SSL 3.0.
- **Session Hijacking:** By decrypting session cookies, attackers can impersonate users and gain unauthorized access to accounts
- **Downgrade Attack:** Attackers can **force browsers or applications to fall back to SSL 3.0**, making them susceptible to the POODLE exploit.

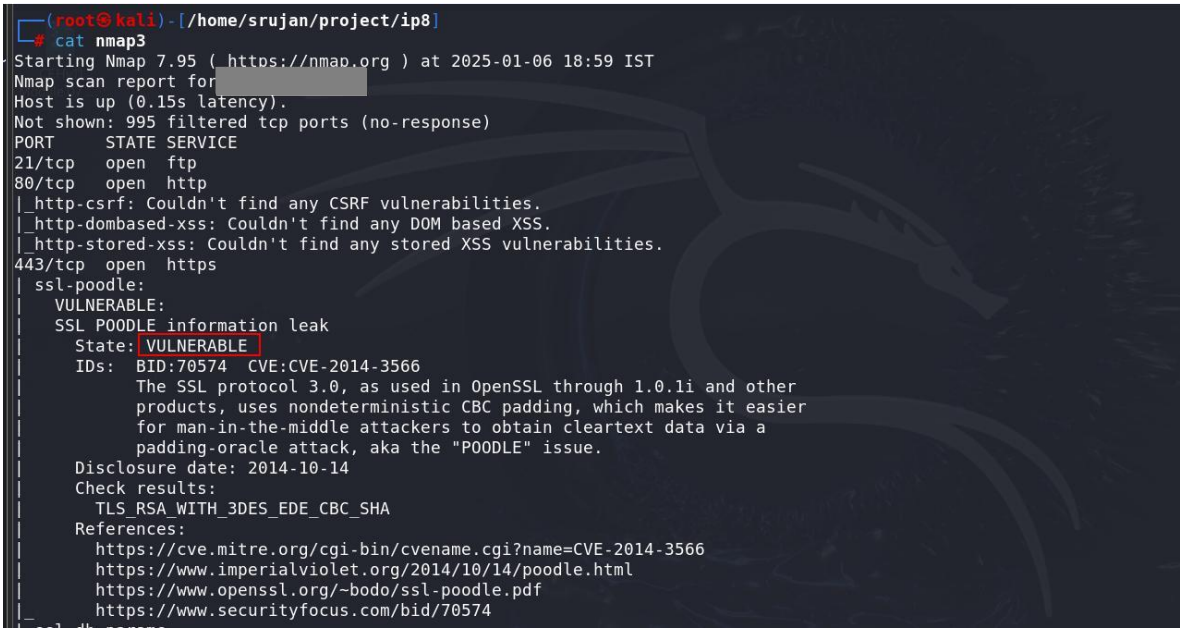
### Recommendations :

- **Disable SSL 3.0 on Servers and Clients:** Configure servers to support only **TLS 1.2 or TLS 1.3**.
- **Use Secure Ciphers:** Disable weak **CBC-mode ciphers** and prefer strong ciphers such as **AES-GCM**.

### References :

- NIST NVD CVE-2014-3566

**POC :**




**Affected Ip :**

### 10.3.6 Remote Desktop Protocol (RDP) Exposure to the Internet

**Description** :

Remote Desktop Protocol (RDP) allows remote access to Windows systems. If exposed to the internet without proper security measures, it can become a prime target for **brute-force attacks**, **credential stuffing**, **RDP exploits**. Attackers can exploit weak passwords or vulnerabilities in the RDP service to gain unauthorized access, execute arbitrary code, or spread malicious payloads.

**CVSS Score : 5.5 – 6.0**

**Impact :**

- Attackers may gain full access to the system if RDP is exposed to the internet without proper authentication or security controls.
- Sensitive data may be exposed if the attacker has sufficient privileges.
- Attackers could compromise the system and deploy ransomware to lock the system or encrypt files for extortion.

## Recommendations :

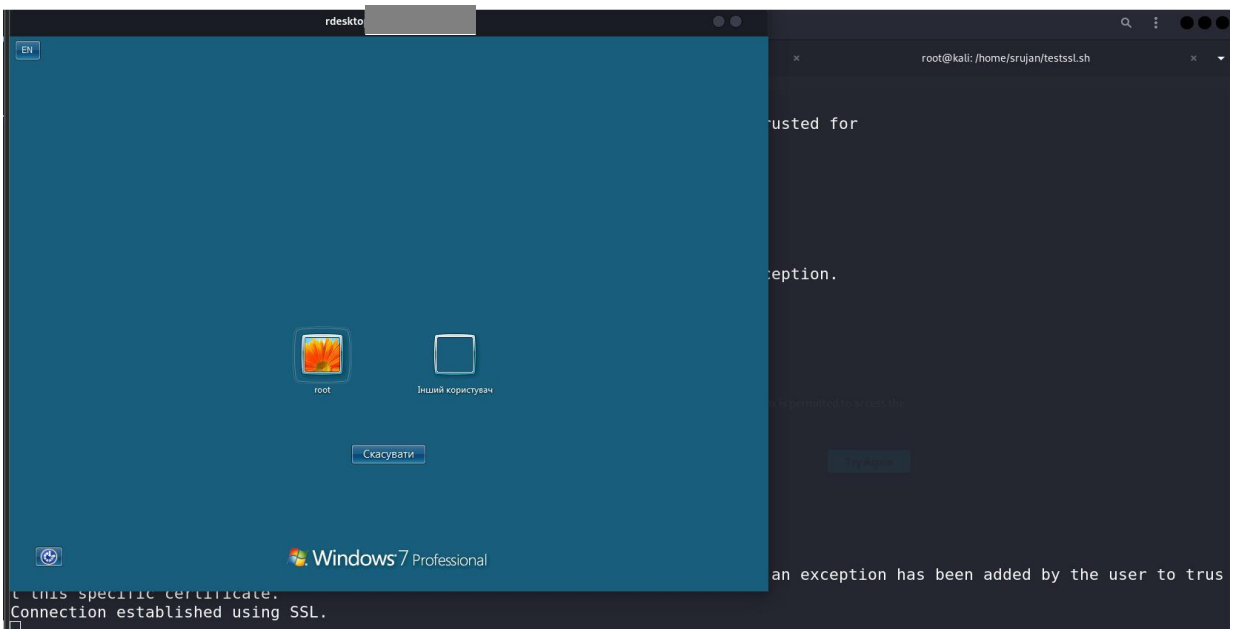
- **Limit RDP Exposure:**
  - Do not expose RDP to the internet unless absolutely necessary.
  - Use **firewall rules** to limit access to trusted IPs only.

- **Disable RDP if Not Needed** : If Remote Desktop Services are not essential, disable them to reduce exposure.

- **Enable Network Level Authentication (NLA) :** NLA adds an extra layer of authentication before establishing a session and can mitigate the risk.

- **Use Strong Authentication**: Enforce **strong password policies** (complex and lengthy passwords) for all accounts with RDP access.

## POC :




## Affected Ip :

- 
- 
- 

### 10.3.7 Unsecured HTTP Login Pages- Sensitive Information Exposure

**Description** :

Unsecured HTTP login pages (i.e., those served over HTTP instead of HTTPS) expose sensitive user credentials (such as usernames and passwords) to potential attackers. When a login page is not encrypted, login credentials are transmitted in plaintext over the network, which can be intercepted by attackers using Man-in-the-Middle (MitM) attacks or packet sniffing tools. This vulnerability is especially dangerous on untrusted or public networks, where attackers can easily intercept data.

**CVSS Score : 6.5**

**Impact :**

- **Sensitive Data Exposure:** Login credentials are transmitted in plaintext, making them vulnerable to interception.
- **Man-in-the-Middle (MitM) Attacks:** An attacker can intercept communications between the user and the server, compromising confidentiality.
- **Session Hijacking:** Attackers can steal session cookies and potentially gain unauthorized access to user accounts.

**Recommendations :**

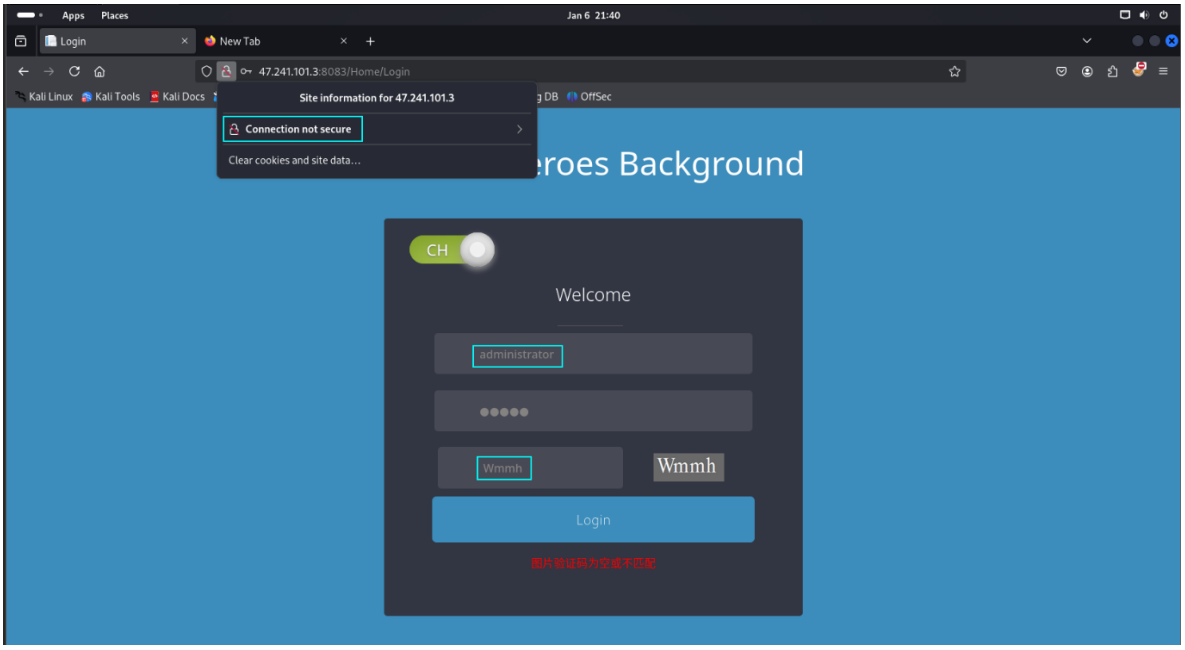
- **Force HTTPS for All Login Pages:**
  - Ensure that the login page is served over **HTTPS**, which uses encryption (SSL/TLS) to protect data in transit.
  - Obtain an **SSL/TLS certificate** for your website and configure your server to use **strong encryption algorithms**
- **Use Strong Authentication Mechanisms:** Consider implementing **multi-factor authentication (MFA)** to provide an additional layer of security.

- **Implement Secure Session Management:** Ensure that session cookies are marked as **Secure** and **HttpOnly** to prevent interception via **JavaScript** or **cross-site scripting (XSS)** attacks.

## References :

- OWASP Security Authentication cheat sheet
- OWASP Top 10

## POC :



```
POST /api/Login/Login HTTP/1.1
Host: 47.241.101.3:8083
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 61
Origin: http://47.241.101.3:8083
Connection: keep-alive
Referer: http://47.241.101.3:8083/Home/Login
Priority: u=0

{"userName":"administrator","password":"12345","code":"Wmmh"}HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
Set-Cookie: token=; expires=Thu, 01 Jan 1970 00:00:00 GMT; path=/
X-Powered-By: ASP.NET
Date: Mon, 06 Jan 2025 16:03:29 GMT

57
{"data":null,"isSuccess":false,"result":".............................","code":906}
0
```

The data is not encrypted

**Affected Ip :**

- [redacted]

## 10.4 Low :

### 10.4.1 – FTP Anonymous Login (Limited Access)

**Description** :

The **FTP Anonymous Login** vulnerability occurs when an FTP server allows unauthorized users to authenticate using the username anonymous without requiring a password or with a generic password (e.g., "anonymous" or an email address). While you were able to log in successfully, the lack of access to data reduces the immediate impact. However, even limited access could still expose system metadata, directory structures, or misconfigurations.

**CVSS Score : 3.9**

## Impact :

- Unauthorized users can log in to the FTP server.
- Even without data access, attackers can enumerate directories, system information, or exploit further misconfigurations
- May lead to **brute-force attempts** or **credential stuffing attacks** if weak permissions exist.

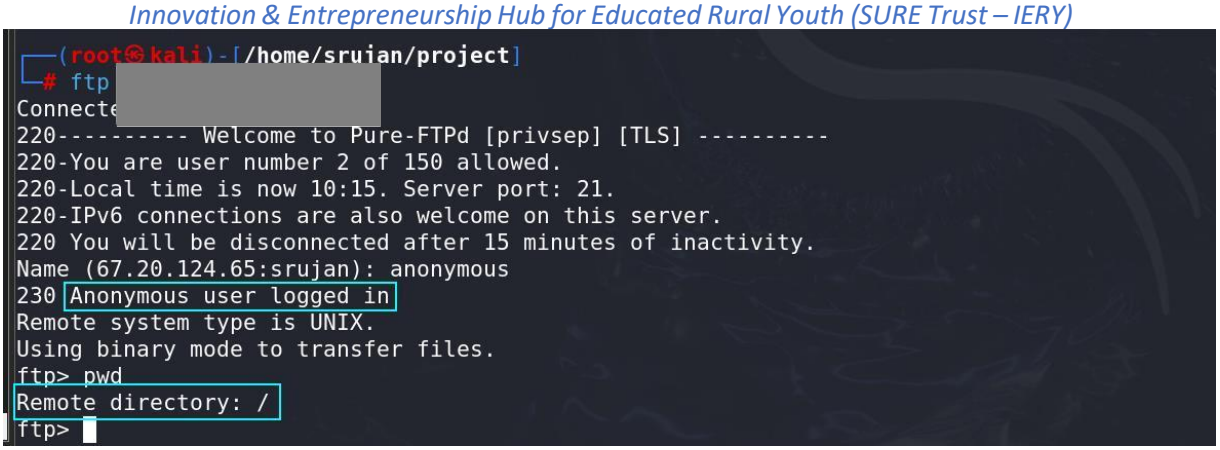
## Recommendations :

- Set **Disable Anonymous FTP Login** unless explicitly required..
- **Restrict Access Permissions** for anonymous users to prevent directory enumeration.
- **Use Strong Authentication** (e.g., username/password authentication or FTPS/SFTP).
- **Monitor FTP Logs** for unusual login attempts or brute-force activity.
- **Firewall & IP Restrictions** to limit access to trusted users/networks.

## References :

- RFC 959 - File Transfer Protocol

## POC :




**Affected Ip :** [redacted]

### 10.4.2 – Public Exposure of Technology Versions May Lead to Future Exploits

**Description** :

During the penetration test, **Wappalyzer** detected and disclosed the versions of various technologies used on the target websites, including **CMS platforms, JavaScript libraries, web frameworks, and server software**. While these versions may not currently have known vulnerabilities, exposing them publicly **increases the risk of future attacks** as new exploits are discovered. Attackers can use this information for **fingerprinting, reconnaissance, and automated attacks** when security flaws in these versions are identified

**CVSS Score : 3.0 – 4.0**

**Impact :**

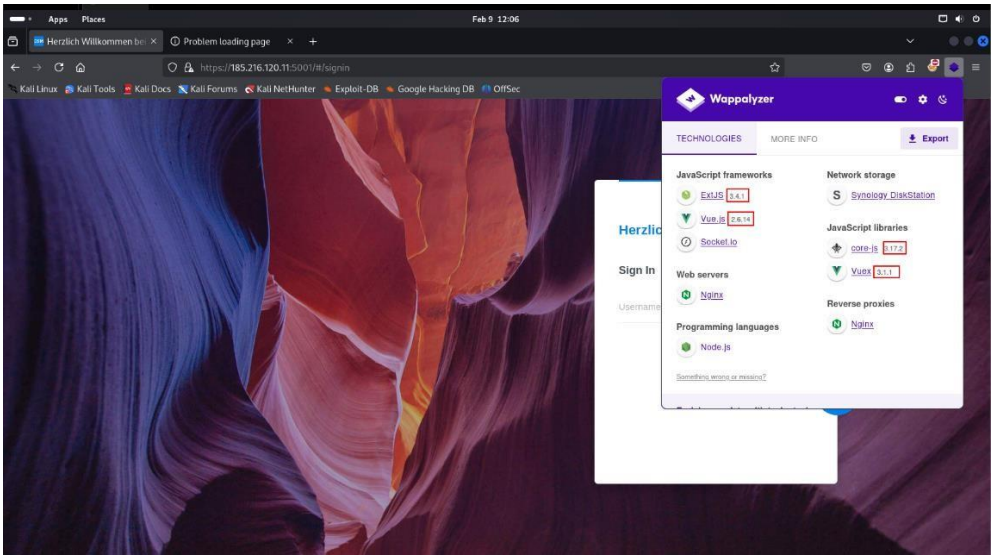
- **Reconnaissance & Targeting:** Attackers can use the disclosed versions to **identify weaknesses** and plan future attacks.
- **Automated Scanning:** Bots and threat actors **track exposed versions** and exploit them when new vulnerabilities arise.
- **Potential for Future Exploits:** If the disclosed versions become vulnerable, attackers can **quickly take advantage** of unpatched systems.

**Recommendations :**

- **Remove technology version details** from HTTP headers, meta tags, and error messages.
- **Disable banner grabbing** on web servers (Apache, Nginx, IIS) to hide version details.
- **Regularly update software** to prevent exploits if vulnerabilities are discovered.

- **Implement security headers** like ServerTokens Prod (Apache) and server_tokens off; (Nginx).
- **Monitor security databases (CVE, NVD, CISA)** for vulnerabilities affecting disclosed technologies.

**POC :**




**Affected Ip :**

- [redacted]

## 11. Conclusion

- **Summary of Findings:** The network has critical vulnerabilities that could lead to unauthorized access and data breaches.
- **Overall Risk Level:** High
- **Next Steps:** Implement the recommended remediation steps and schedule a retest.

## 12. Recommendations

- **Patch Management:** Regularly update all software and systems.
- **Firewall Configuration:** Restrict access to unnecessary ports and services.
- **Employee Training:** Conduct security awareness training for employees.
- **Regular Audits:** Perform periodic vulnerability assessments and penetration tests.