Sri Lanka Institute of Information Technology

Cyber Security Assignment (2025)

Server Version Disclosure & Failed FTP Misconfiguration Attempt-Security Misconfiguration

Bug Bounty Report- 03

IT23363366

TABLE OF CONTENT

1. Title

Report Title: Server Version Disclosure & Failed FTP Misconfiguration Attempt
Reported By: Raahim Mahmooth
Tested On: https://www.worklenz.com/
Platform: *https://bugzero.io*

2. Scope and Objective

The objective of this security assessment was to evaluate the security posture of the web application hosted at uat.app.worklenz.com. The testing focused on identifying potential vulnerabilities such as server information leakage, FTP service misconfigurations, and web server misconfigurations without exploiting or damaging the target environment.

3. Enumeration and Reconnaissance

3.1. Tools Used

- **Nmap** – For network scanning and service enumeration.
- **Metasploit Framework** – For exploit testing
- **ZAP** - vulnerability detection.

3.2. Steps Taken

Initial Port Scanning:

- Conducted a port scan on the target IP address to identify open ports and services
  Result:

  Port 21 (FTP) open

  Port 80 (HTTP) open

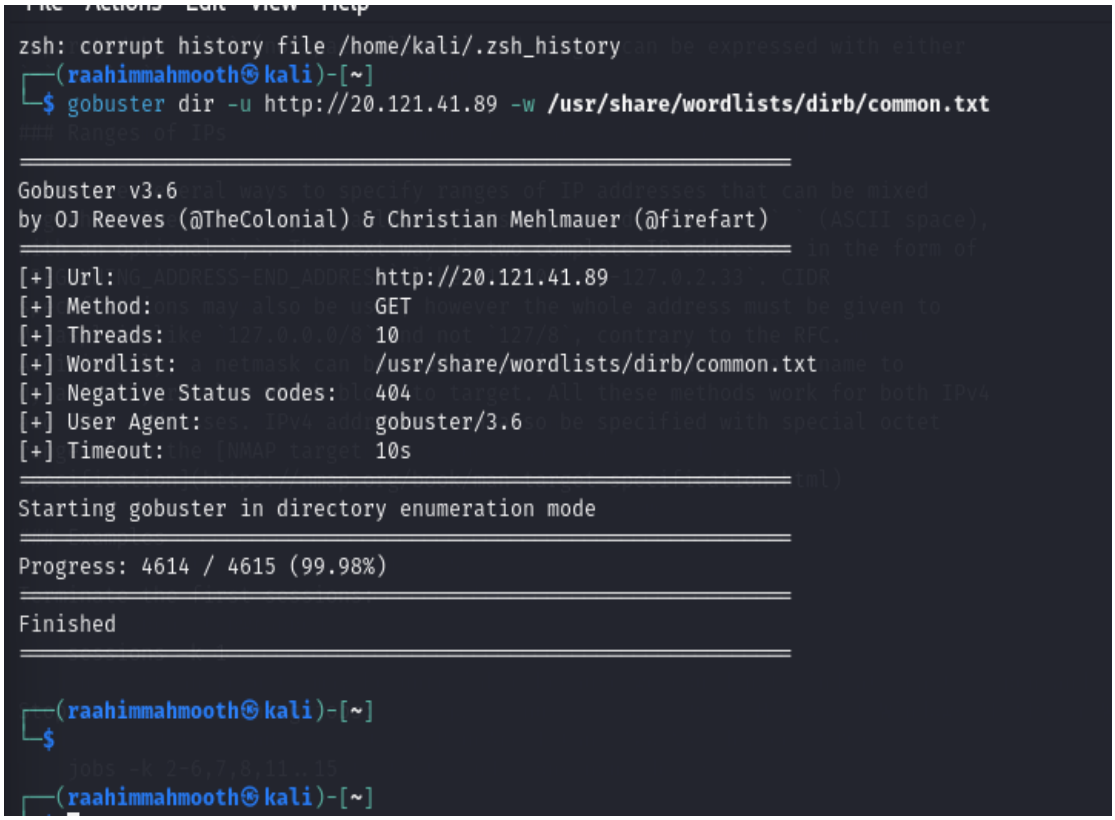
```
┌──(raahimmahmooth㉿kali)-[~/Desktop]
└─$ nmap -sS -A uat.app.worklenz.com -T 4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-25 19:02 EDT
Nmap scan report for uat.app.worklenz.com (20.121.41.89)
Host is up (0.0026s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp?
80/tcp   open  tcpwrapped
|_http-title: Did not follow redirect to https://uat.app.worklenz.com/
|_http-server-header: nginx/1.18.0 (Ubuntu)
443/tcp  open  tcpwrapped
|_ssl-date: TLS randomness does not represent time
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=uat.app.worklenz.com
| Subject Alternative Name: DNS:uat.app.worklenz.com
| Not valid before: 2025-04-11T10:35:48
|_Not valid after:  2025-07-10T10:35:47
|_http-server-header: nginx/1.18.0 (Ubuntu)
554/tcp  open  tcpwrapped
1723/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (96%), Microsoft Windows XP SP3 or Windows 7 or Windows Server
Linux 3.2 (92%), Linux 4.4 (92%), BlueArc Titan 2100 NAS device (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.53 ms 192.168.127.2
```

Directory Bruteforcing (Web Enumeration)

- Used Go buster to brute-force hidden directories and pages on the web server.
- Command Used:

```
gobuster dir -u http://20.121.41.89 -w /usr/share/wordlists/dirb/common.txt.
```

- Tried finding on sensitive files like `/etc/passwd` through HTTP paths since the server version is directly not vulnerable but any misconfiguration can lead attackers to exploait(ex:RCE)
- Result: No sensitive or interesting directories discovered.



Banner Grabbing and Server Information Gathering:

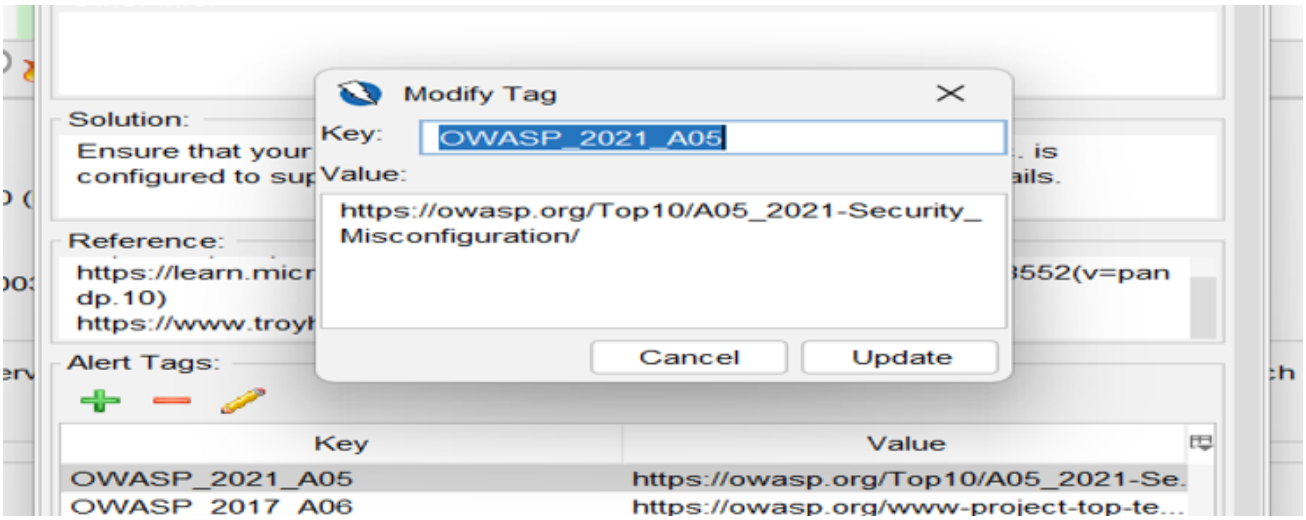
- Analyzed HTTP response headers using tools like OWASP ZAP and browser inspection.
- **Result:**
  - Server version disclosed in HTTP header: nginx/1.18.0 (Ubuntu)

Server Leaks Version Information via "Server" HTTP Response Header Field

URL: https://uat.app.worklenz.com/
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence: nginx/1.18.0 (Ubuntu)
CWE ID: 497
WASC ID: 13
Source: Passive (10036 - HTTP Server Response Header)
Input Vector:

Description:

The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.




```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 25 Apr 2025 23:09:25 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 25320
Connection: keep-alive
Vary: Accept-Encoding
```

```
<!DOCTYPE html><html lang="en" data-critters-container v="958"><head><meta charset="utf-8"><title>Worklenz</title><base href="/"><meta
name="viewport" content="width=device-width, initial-scale=1"><meta name="theme-color" content="#1976d2"><meta name="robots" content=
"noindex"><link rel="preconnect" href="https://fonts.googleapis.com"><link rel="preconnect" href="https://fonts.gstatic.com" crossorigi
=""><link rel="manifest" href="/manifest.webmanifest"><link rel="shortcut icon" href="/favicon.ico" type="image/x-icon"><style>
@font-face {
  font-family: 'Inter';
```

FTP Enumeration

- Checked if anonymous FTP login was allowed.
- Command Used:
  `nmap -p 21 --script ftp-anon 20.121.41.89`
- Result: Anonymous login **not allowed**.

```
ftp: Can't connect to `192.168.127.2:ftp'
ftp> exit

┌──(raahimmahmooth㉿kali)-[~/Desktop]
└─$ nmap -p 21 --script ftp-anon 20.121.41.89

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 02:46 EDT
Nmap scan report for 20.121.41.89
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 9.66 seconds

┌──(raahimmahmooth㉿kali)-[~/Desktop]
```

4. Vulnerability Description

FTP Misconfiguration Assessment (Low Risk)

- Port 21 (FTP) was found open during port scanning. Testing was conducted to check for anonymous login and potential misconfigurations.

Server Version Disclosure (Medium Risk)

- The HTTP response header leaks the server version: `nginx/1.18.0 (Ubuntu)`.
  This information may assist attackers in identifying specific exploits related to this Nginx version.

5. Affected Component

Web Server:

- Nginx 1.18.0 (Ubuntu) — leaking server version information via HTTP response headers.
- Misconfigured error handling leaking full server-side file paths.
- Potential exposure of sensitive files (/etc/passwd) through improper URL access controls.

FTP Server:

- FTP service running on Port 21.
- FTP service properly restricts anonymous login, but its exposure without additional security measures increases the attack surface.

Network Services:

- Ports 21 (FTP) and 80 (HTTP) are publicly accessible, which may allow enumeration and further exploitation attempts if other misconfigurations or vulnerabilities are present.

6. Impact Assessment

Information Disclosure:

- Leaking the Nginx version (**nginx/1.18.0 (Ubuntu**)) via HTTP response headers could allow attackers to research known vulnerabilities associated with this server version, aiding in targeted attacks.

Security Misconfiguration Risks:

- Misconfigured error handling and exposure of sensitive files like **/etc/passwd** could give attackers insights into the server environment, file structures, and potential user information, enabling more precise exploitation attempts such as Local File Inclusion (LFI) or privilege escalation attacks.

7. Proof of Concept

- *Description:*
  An exploitation attempt was made against the FTP server targeting the `vsftpd 2.3.4 backdoor` vulnerability using Metasploit. However, the exploit was unsuccessful.

- *Exploit Used:*
  `msf6 exploit(unix/ftp/vsftpd_234_backdoor)`

- *Command Used:*

  `set RHOSTS 20.121.42.89`
  `set RPORT 21`
  `run`

```
    set RHOSTS www.example.test/24
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 20.121.42.89
RHOSTS => 20.121.42.89
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 20.121.42.89:21 - Exploit failed: EOFError EOFError
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 1723
RPORT => 1723
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 20.121.42.89:1723 - Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

8. Proposed Mitigation

To strengthen the overall security posture, it is recommended to disable the disclosure of server version information by **setting server_tokens off**; in the Nginx configuration file. Additionally, review and harden all web server configurations to prevent sensitive files like **/etc/passwd** from being exposed through URL access. Proper error handling should be implemented to avoid leaking internal server paths in response messages. Although the FTP service currently does not allow anonymous logins, it is best practice to either disable FTP if not in use or migrate to a more secure protocol like SFTP. Regular vulnerability scans and server updates should also be part of the ongoing maintenance to reduce the risk of exploitation through misconfigurations or outdated software.

9. Conclusion

The assessment identified low to medium-risk issues such as server version leakage, Nginx misconfigurations, and an exposed FTP service. Although no critical exploit was successful, these misconfigurations could aid an attacker in future attacks. Securing the server headers, hardening file access permissions, and properly configuring services like FTP are essential. No immediate exploitation was possible during testing. However, addressing these issues promptly will reduce potential risks. Continuous monitoring and regular security assessments are recommended. This test aligns with **OWASP Top 10 - A05:2021**

10. References

- **OWASP Top 10 - A05:2021:**https://owasp.org/Top10/A05_2021-Security_Misconfiguration/