



# A Detailed Guide on Cewl



# Contenido

Introducción.....	3
Procedimiento predeterminado.....	5
Guarde esta lista de palabras en un archivo.....	6
Generar listas de palabras de cierta longitud.....	7
Recuperación de correos electrónicos del sitio web:.....	7
Para contar el número de palabras repetidas en el sitio web.....	8
Aumentar la profundidad de la araña .....	9
Modo detallado .....	10
Lista de palabras alfanuméricas .....	11
Cewl con autenticación implícita/básica.....	12
Poner en minúsculas todas las palabras analizadas .....	13
Soporte de proxy.....	14

## Introducción

CeWL: un generador de listas de palabras personalizado es un programa Ruby que rastrea una URL específica hasta una profundidad definida y devuelve una lista de palabras clave, que los descifradores de contraseñas como John the Ripper, Medusa y Wfuzz pueden usar para descifrar las contraseñas. Cewl también tiene una aplicación de línea de comandos asociada, FAB, que utiliza las mismas técnicas de extracción de metadatos para generar listas de autores/productores a partir de archivos ya descargados utilizando algoritmos de extracción de información como CeWL.

CeWL viene preinstalado con Kali Linux. Con esta herramienta, podemos recopilar fácilmente palabras y frases de la página de destino. Es un programa robusto que puede eliminar rápidamente el servidor web de cualquier sitio web.

Abra la terminal de Kali Linux y escriba "cewl -h" para ver las listas de todas las opciones que acepta, con una descripción completa.

Sintaxis: cewl <url> [opciones]

```

(root@kali)~[~/cewl]
# cewl --help
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Usage: cewl [OPTIONS] ... <url>

OPTIONS:
  -h, --help: Show help.
  -k, --keep: Keep the downloaded file.
  -d <x>, --depth <x>: Depth to spider to, default 2.
  -m, --min_word_length: Minimum word length, default 3.
  -o, --offsite: Let the spider visit other sites.
  --exclude: A file containing a list of paths to exclude
  --allowed: A regex pattern that path must match to be followed
  -w, --write: Write the output to the file.
  -u, --ua <agent>: User agent to send.
  -n, --no-words: Don't output the wordlist.
  -g <x>, --groups <x>: Return groups of words as well
  --lowercase: Lowercase all parsed words
  --with-numbers: Accept words with numbers in as well as just letters
  --convert-umlauts: Convert common ISO-8859-1 (Latin-1) umlauts (ä-ae, ö-oe, ü-ue,
  -a, --meta: include meta data.
  --meta_file file: Output file for meta data.
  -e, --email: Include email addresses.
  --email_file <file>: Output file for email addresses.
  --meta-temp-dir <dir>: The temporary directory used by exiftool when parsing file
  -c, --count: Show the count for each word found.
  -v, --verbose: Verbose.
  --debug: Extra debug information.

Authentication
  --auth_type: Digest or basic.
  --auth_user: Authentication username.
  --auth_pass: Authentication password.

Proxy Support
  --proxy_host: Proxy host.
  --proxy_port: Proxy port, default 8080.
  --proxy_username: Username for proxy, if required.
  --proxy_password: Password for proxy, if required.

Headers
  --header, -H: In format name:value - can pass multiple.

<url>: The site to spider.

```

Opciones generales :

-h, --ayuda:	Mostrar ayuda.
-k, --mantener:	Guarde el archivo descargado.
-d <x>, --profundidad <x>:	Profundidad a la que se desplaza la araña, por defecto 2.
-m, --min_longitud_palabra:	Longitud mínima de palabra, predeterminada 3.
-o, --fuera del sitio:	Deja que la araña visite otros sitios.
-w, --escribir:	Escriba la salida en el archivo.
-u, --ua <agente>:	Agente de usuario para enviar.

-n, -sin-palabras:	No genere la lista de palabras.
-con-números:	Acepte palabras con números y solo letras.
-a, -meta:	incluir metadatos.
-archivo meta_file:	Archivo de salida para metadatos.
-e, -correo electrónico:	Incluya direcciones de correo electrónico.
-archivo_correo electrónico <archivo>:	Archivo de salida para direcciones de correo electrónico.
-c, -cuenta:	Muestra el recuento de cada palabra encontrada.
-v, -detallado:	Verboso.
-depurar:	Información de depuración adicional
Autenticación	
-Tipo de autenticación:	Digerido o básico.
-auth_user:	Nombre de usuario de autenticación.
-auth_pass:	Contraseña de autenticación.
Soporte de proxy	
-proxy_host:	Host proxy.
-Puerto proxy:	Puerto proxy, predeterminado 8080.
-proxy_nombre de usuario:	Nombre de usuario para el proxy, si es necesario.
-contraseña_proxy:	Contraseña para proxy, si es necesario.

### Procedimiento predeterminado

Use el siguiente comando para generar una lista de palabras que rastrearán la URL dada a una profundidad específica y podemos usarla como directorio para descifrar las contraseñas.

```
cewl http://www.vulnweb.com
```

```
(root@kali)-[~/cewl]
# cewl http://www.vulnweb.com
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Acunetix
learn
more
the
http
vulnweb
com
Review
scanner
topic
SQL
site
for
PHP
you
Web
Vulnerability
Scanner
websites
test
Apache
MySQL
```

#### Guarde esta lista de palabras en un archivo

Ahora, para guardar toda esta lista de palabras en un archivo para mantener registros, ser más eficiente y legible, usaremos la opción `-w` para guardar el resultado en un archivo de texto.

```
cewl http://www.vulnweb.com -w dict.txt
```

Aquí `dict.txt` es el nombre del archivo donde se almacenará la lista de palabras. Una vez creado el archivo, puede abrirlo para ver si el resultado está almacenado en el archivo.

```
(root@kali)-[~/cewl]
# cewl http://www.vulnweb.com -w dict.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

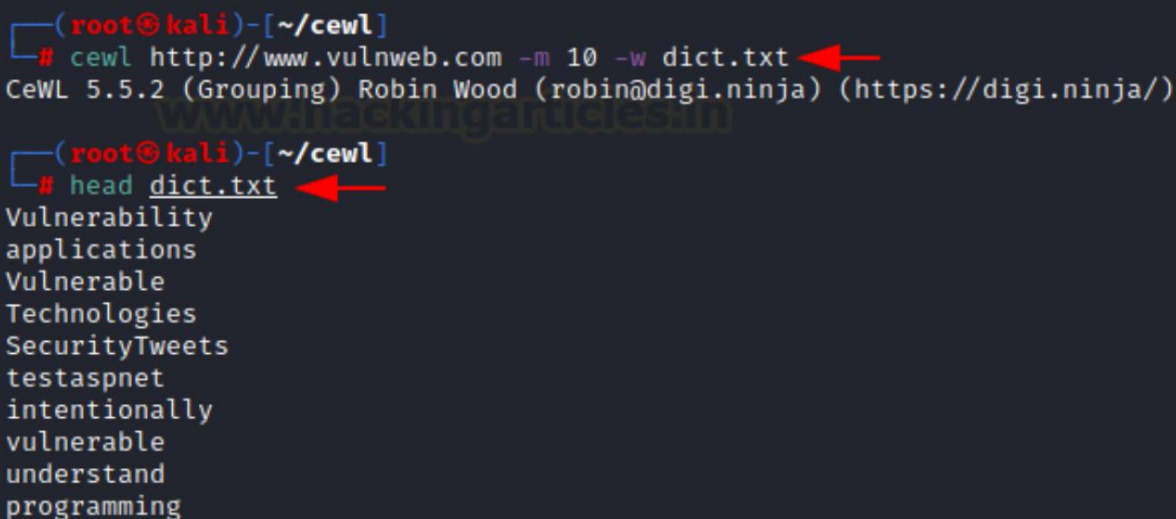
# head dict.txt
Acunetix
learn
more
the
http
vulnweb
com
Review
scanner
topic
```



### Generar listas de palabras de cierta longitud

Si desea crear una lista de palabras de una longitud específica, puede optar por utilizar la opción -m y proporcionar la longitud mínima para la palabra clave, por lo que se crearán listas de palabras de una longitud determinada.

```
cewl http://vulnweb.com / -m 10 -w dict.txt
```



```
(root@kali)-[~/cewl]
# cewl http://www.vulnweb.com -m 10 -w dict.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(root@kali)-[~/cewl]
# head dict.txt
Vulnerability
applications
Vulnerable
Technologies
SecurityTweets
testaspnet
intentionally
vulnerable
understand
programming
```

Básicamente, esto creará una lista de palabras en la que cada palabra tiene un mínimo de 10 letras y almacenará estas palabras clave en el archivo dict.txt. Se adjunta captura de pantalla para su referencia.

### Recuperación de correos electrónicos del sitio web:

Para recuperar correos electrónicos del sitio web, podemos usar la opción -e, mientras que la opción -n ocultará las listas creadas mientras rastreamos el sitio web proporcionado. Como puede ver en la captura de pantalla adjunta, se encontró 1 ID de correo electrónico del sitio web.

```
cewl https://digi.ninja/contact.php -e -n
```

```
(root@kali)-[~/cewl]
# cewl https://digi.ninja/contact.php -e -n
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

Email addresses found

Rick@Havu.us
chrisbruhin@gmail.com
gog1873@hotmail.com
jason_215@hotmail.com
logic@steelcon.info
robin@digi.ninja
robin@test.com
stuart@moabretreat.com
tutug60@hotmail.com
unni79@gmail.com
xraychen73@gmail.com
yashinl@discovery.co.za
ziggy1962@sympatico.ca
zuzujar@msn.com
```

## Para contar el número de palabras repetidas en el sitio web.

Si desea contar la cantidad de veces que se repite una palabra en un sitio web, utilice la opción -c que habilitará el parámetro de recuento.

```
cewl http://www.vulnweb.com -c
```

Para su referencia, se agrega una captura de pantalla a continuación que imprime el recuento de cada palabra clave repetida en el sitio web.



```
(root@kali)-[~/cewl]
# cewl http://www.vulnweb.com -c
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Acunetix, 9
learn, 6
more, 6
the, 6
http, 5
vulnweb, 5
com, 5
Review, 5
scanner, 5
topic, 5
SQL, 4
site, 4
for, 3
PHP, 3
you, 3
Web, 2
Vulnerability, 2
Scanner, 2
websites, 2
```

#### Aumentar la profundidad de Spider

Puede usar la opción -d con el número de profundidad para activar el parámetro de profundidad para un rastreo más rápido e intenso de modo que se cree una gran lista de palabras. El nivel de profundidad está establecido en 2 de forma predeterminada.

```
cewl http://vulnweb.com -d 3
```

```
(root@kali)-[~/cewl]
# cewl http://www.vulnweb.com -d 3
CeWL 5.5.2 (Grouping) Robin Wood (robin@digini.ninja) (https://digini.ninja/)
Acunetix
learn
more
the
http
vulnweb
com
Review
scanner
topic
SQL
site
for
PHP
you
Web
Vulnerability
Scanner
websites
test
Apache
MySQL
```

## Modo detallado

Tenemos una opción `-v` para el modo detallado para ampliar el resultado del rastreo del sitio web y recuperar detalles completos del sitio web.

```
cewl http://vulnweb.com -v
```

Entonces, esto mostrará resultados extendidos de rastreo de sitios web. A continuación adjuntamos una captura de pantalla para que tengas una idea clara.

```
(root@kali)-[~/cewl]
# cewl http://www.vulnweb.com -v
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Starting at http://www.vulnweb.com
Visiting: http://www.vulnweb.com, got response code 200
Attribute text found:
Acunetix website security

Offsite link, not following: https://www.acunetix.com/
Offsite link, not following: https://www.acunetix.com/vulnerability-scanner/
Offsite link, not following: http://testhtml5.vulnweb.com/
Offsite link, not following: https://www.acunetix.com/vulnerability-scanner/html5-website-sec
Offsite link, not following: https://www.acunetix.com/vulnerability-scanner/crawling-html5-ja
Offsite link, not following: http://testphp.vulnweb.com/
Offsite link, not following: https://www.acunetix.com/vulnerability-scanner/php-security-scan
Offsite link, not following: https://www.acunetix.com/blog/articles/prevent-sql-injection-vul
Offsite link, not following: http://testasp.vulnweb.com/
Offsite link, not following: https://www.acunetix.com/vulnerability-scanner/sql-injection/
Offsite link, not following: https://www.acunetix.com/websitesecurity/sql-injection/
Offsite link, not following: http://testaspnet.vulnweb.com/
Offsite link, not following: https://www.acunetix.com/vulnerability-scanner/network-vulnerabi
Offsite link, not following: https://www.acunetix.com/blog/articles/network-vulnerability-ass
Offsite link, not following: http://rest.vulnweb.com/
Offsite link, not following: https://www.acunetix.com/blog/articles/rest-api-security-testing
Offsite link, not following: https://www.acunetix.com/blog/articles/rest-api-security-testing
Words found
Acunetix
learn
more
the
http
vulnweb
com
Review
scanner
topic
```

### Lista de palabras alfanuméricas

A veces puede suceder que necesite una lista de palabras alfanuméricas que pueda usar: la opción con números para obtener una lista de palabras alfanuméricas.

```
cewl http://testphp.vulnweb.com/artists.php --con-números
```

```
(root@kali)-[~/cewl]
# cewl http://testphp.vulnweb.com/artists.php --with-numbers
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
and
Acunetix
site
your
InstanceBeginEditable
name
rgn
InstanceEndEditable
end
```

```

Storage
Link
DNS
313
enclosure
SATA
Price359
Camera
A4Tech
335E
Price10
Laser
Color
Printer
LaserJet
M551dn
Price812
Example
check
Original
article
Posters
Paintings
user
press
submit
button
will
transferred
asecured
connection
Retype
Name
Credit
card
Mail
Phone
Address

```

## Cewl con autenticación implícita/básica

A veces puede suceder que algunas aplicaciones web tengan una página de autenticación para iniciar sesión y, por eso, el comando básico anterior no dará los resultados deseados. Entonces, para eso, debe omitir la página de autenticación usando el comando que se proporciona a continuación.

```
cewl http://testphp.vulnweb.com/login.php --auth_type Digest --auth_user prueba --auth_pass prueba -v
```

En este comando hemos utilizado las siguientes opciones:

-Tipo de autenticación:

Resumen / Básico

--auth\_user:

Nombre de usuario de autenticación

Contraseña de autenticación

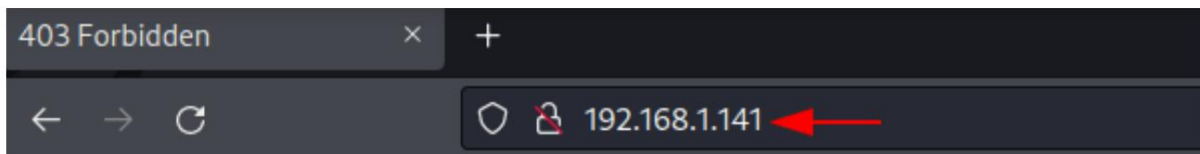
Poner en minúsculas todas las palabras analizadas

Página 13 de 15

```
(root@kali)-[~]
# cewl http://www.vulnweb.com --lowercase
CeWL 5.5.2 (Grouping) Robin Wood (robin@diginiinja) (https://diginiinja/)
acunetix
scanner
learn
more
the
http
vulnweb
com
review
topic
sql
site
you
web
test
for
```

## Soporte de proxy

Este comando predeterminado para cewl no funcionará correctamente si ha conectado un servidor proxy. Intentamos acceder a la aplicación a través de la dirección IP pero el servidor proxy está conectado, por lo que nos mostró una página de Error prohibido.



# Forbidden

You don't have permission to access this resource.

*Apache/2.4.41 (Ubuntu) Server at 192.168.1.141 Port 80*

Y aquí, si aplicamos el comando cewl predeterminado, generará la lista de palabras de la página de error. Por lo tanto, para obtener la lista de palabras adecuada de la aplicación web, hemos utilizado comandos como:

```
cewl http://192.168.1.141 --proxy_host 192.168.1.141 --proxy_port 3128
```

En este comando hemos utilizado las siguientes opciones:

--proxy_host:	Tu anfitrión
-Puerto proxy:	Número de puerto de su proxy



```
(root@kali)~[~]
# cewl http://192.168.1.141
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Forbidden
You
don
have
permission
access
this
resource
Apache
Ubuntu
Server
Port

(root@kali)~[~]
# cewl http://192.168.1.141 --proxy_host 192.168.1.141 --proxy_port 3128
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
the
Ubuntu
configuration
apache
this
conf
Apache
server
for
web
default
and
enabled
from
files
site
file
The
page
can
var
www
html
your
with
not
Debian
bugs
```

# ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

