Searchsploit

→ O searchsploit é uma ferramenta que armazena exploits do exploit-db
→ Para manter ele sempre atualizado

```
searchsploit -u
```

→ Para ver o exploits relacionados ao webmin por exemplo, basta

```
searchsploit webmin
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# searchsploit webmin
```

Exploit Title	Path
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal	cgi/webapps/23535.txt
phpMyWebmin 1.0 - 'target' Remote File Inclusion	php/webapps/2462.txt
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion	php/webapps/2451.txt
Webmin - Brute Force / Command Execution	multiple/remote/705.pl
webmin 0.91 - Directory Traversal	cgi/remote/21183.txt
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing	linux/remote/22275.pl
Webmin 0.x - 'RPC' Privilege Escalation	linux/remote/21765.pl
Webmin 0.x - Code Input Validation	linux/local/21348.txt
Webmin 1.5 - Brute Force / Command Execution	multiple/remote/746.pl
Webmin 1.5 - Web Brute Force (CGI)	multiple/remote/745.pl
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)	unix/remote/21851.rb
Webmin 1.850 - Multiple Vulnerabilities	cgi/webapps/42989.txt
Webmin 1.900 - Remote Command Execution (Metasploit)	cgi/remote/46201.rb
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)	linux/remote/46984.rb
Webmin 1.920 - Remote Code Execution	linux/webapps/47293.sh
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)	linux/remote/47230.rb
Webmin 1.962 - 'Package Updates' Escape Bypass RCE (Metasploit)	linux/webapps/49318.rb
Webmin 1.973 - 'run.cgi' Cross-Site Request Forgery (CSRF)	linux/webapps/50144.py
Webmin 1.973 - 'save_user.cgi' Cross-Site Request Forgery (CSRF)	linux/webapps/50126.py
Webmin 1.984 - Remote Code Execution (Authenticated)	linux/webapps/50809.py
Webmin 1.996 - Remote Code Execution (RCE) (Authenticated)	linux/webapps/50998.py
Webmin 1.x - HTML Email Command Execution	cgi/webapps/24574.txt
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	multiple/remote/1997.php
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	multiple/remote/2017.pl
Webmin < 1.920 - 'rpc.cgi' Remote Code Execution (Metasploit)	linux/webapps/47330.rb

Shellcodes: No Results

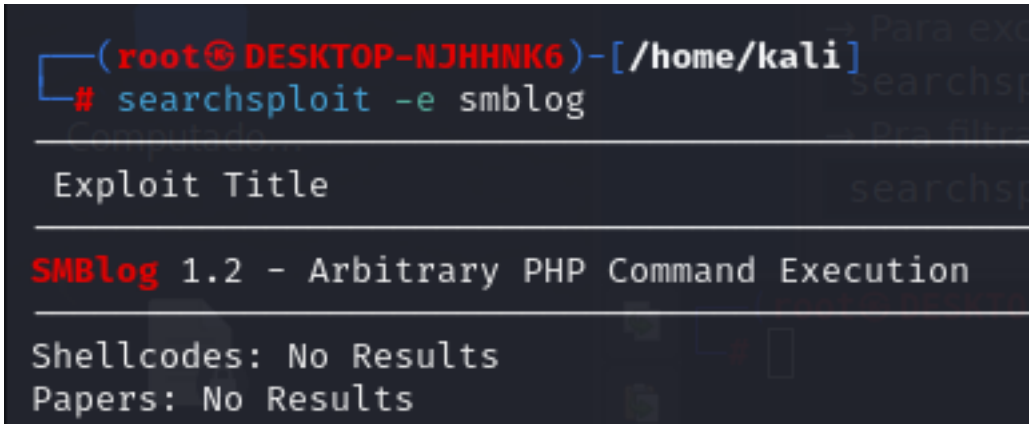
Paper Title	Path
WebMin - (XSS BUG) Remote Arbitrary File Disclosure	docs/english/13117-webmin——(xss

→ Para excluir essas saídas do DansGuardian e do phpMy, basta

```
searchsploit webmin --exclude="phpMy|Dans"
```

→ Pra filtrar e fazer uma busca exata, basta adicionar um -e

```
searchsploit -e smblog
```



```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# searchsploit -e smblog
```

Exploit Title
SMBlog 1.2 - Arbitrary PHP Command Execution

Shellcodes: No Results
Papers: No Results

→ Para ver só o ID:

```
searchsploit ipfire --id
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# searchsploit ipfire --id
------------------------------------------------------------------------------------------ ---------
 Exploit Title                                                                            |  EDB-ID
------------------------------------------------------------------------------------------ ---------
IPFire - 'proxy.cgi' Remote Code Execution (Metasploit)                                   | 39917
IPFire - 'Shellshock' Bash Environment Variable Command Injection (Metasploit)           | 39918
IPFire - CGI Web Interface (Authenticated) Bash Environment Variable Code Injection      | 34839
IPFire 2.19 - Remote Code Execution                                                       | 42149
IPFire 2.21 - Cross-Site Scripting                                                        | 46344
IPFire 2.25 - Remote Code Execution (Authenticated)                                       | 49869
IPFire < 2.19 Core Update 101 - Remote Command Execution                                  | 39765
IPFire < 2.19 Update Core 110 - Remote Code Execution (Metasploit)                        | 42369
------------------------------------------------------------------------------------------ ---------
Shellcodes: No Results
Papers: No Results
```

→ Para fazer uma cópia:

```
searchsploit ipfire --id -m 42149
```