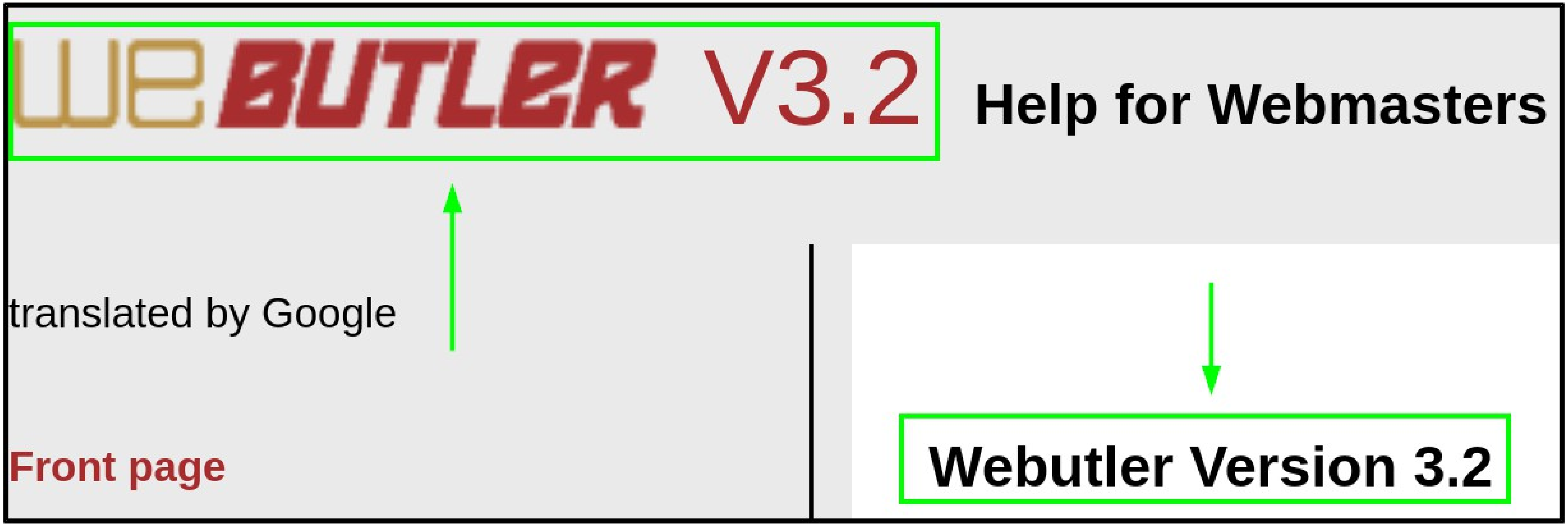
Butler – Vulnerable CMS Version



weBUTLER V3.2

Help for Webmasters

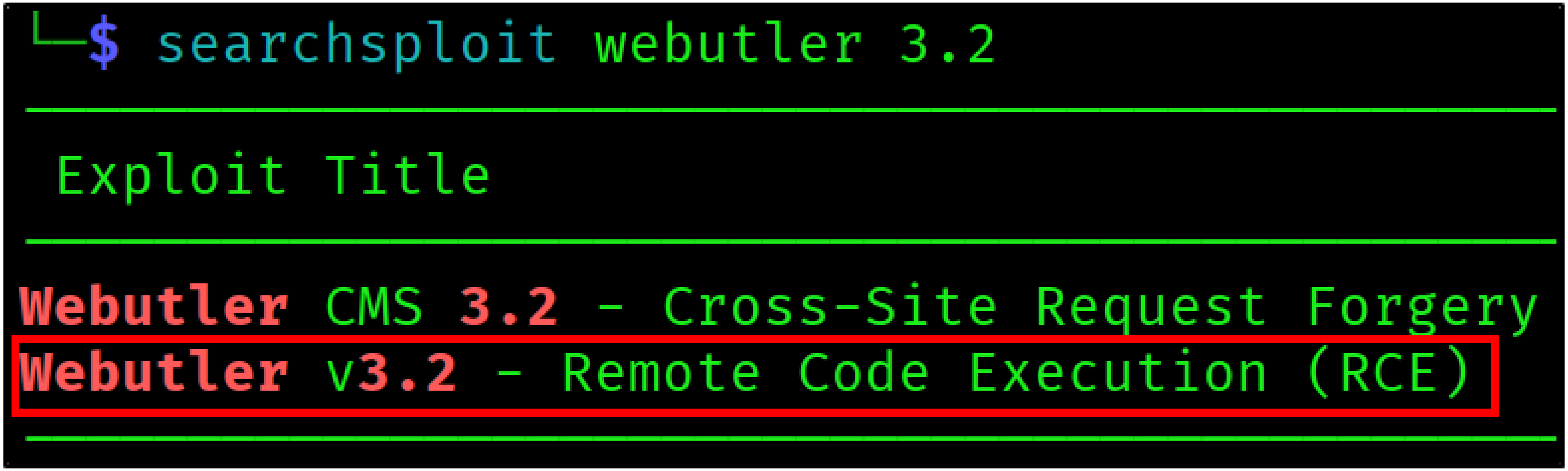
translated by Google

Front page

Webutler Version 3.2

In this challenge we discover a CMS web app with a specific version mentioned

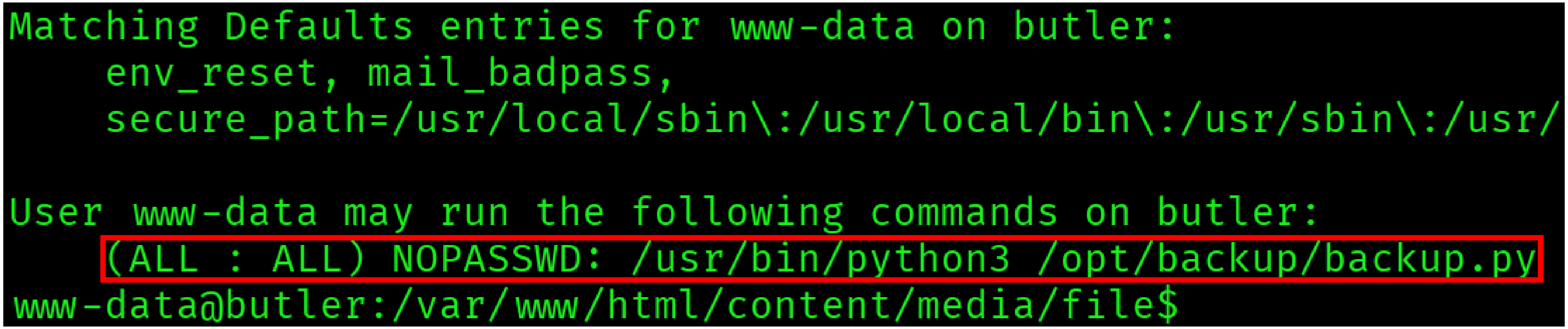
Butler – Vulnerable CMS Version



```
└─$ searchsploit webutler 3.2
-----------------------------------------------------------------
 Exploit Title
-----------------------------------------------------------------
Webutler CMS 3.2 - Cross-Site Request Forgery
Webutler v3.2 - Remote Code Execution (RCE)
-----------------------------------------------------------------
```

There is a known attack for this version of the CMS

Privilege Escalation
Sudo Python / Writable Script

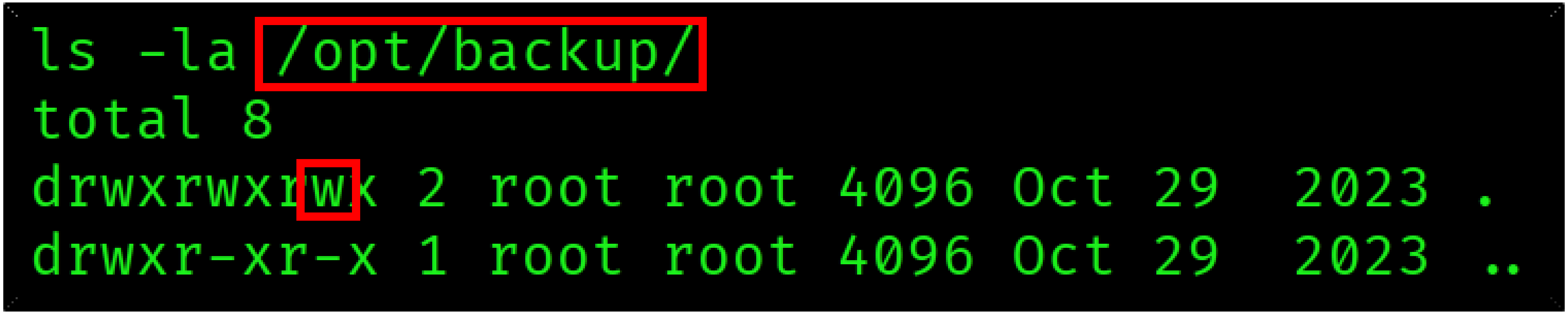


```
Matching Defaults entries for www-data on butler:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/

User www-data may run the following commands on butler:
    (ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/backup/backup.py
www-data@butler:/var/www/html/content/media/file$
```

Our user has sudo access to the Python binary, but only with a specific script

Privilege Escalation
Sudo Python / Writable Script



```
ls -la /opt/backup/
total 8
drwxrwxrwx 2 root root 4096 Oct 29  2023 .
drwxr-xr-x 1 root root 4096 Oct 29  2023 ..
```

On this system, the backup.py script is missing, and the directory where it is supposed to be is writable, so we can create our own backup.py script with whatever contents we want