# bugku web21 WriteUp

原创

Casuall 于 2021-01-09 16:30:44 发布 314 收藏 1

分类专栏： ctf 文章标签： bugku bugku web21 作者：御结冰城 ctf

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/Casuall/article/details/112393548

版权

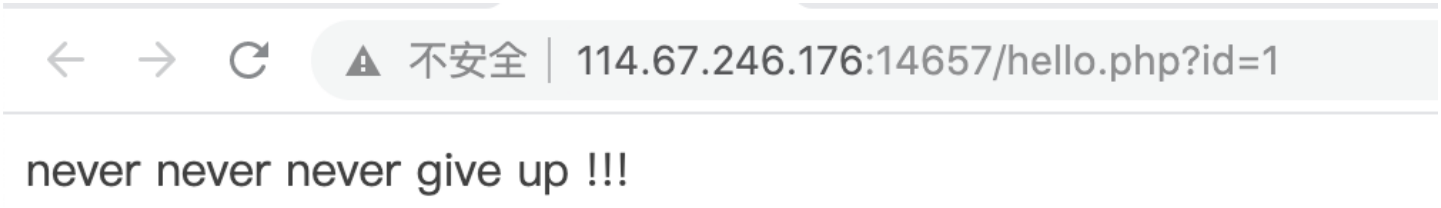
ctf 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

bugku平台更新后的web21，作者：御结冰城

点开链接发现进行了跳转




查看源代码，发现注释中有一个 1p.html 页面，尝试打开发现自动跳转到了bugku首页，用**burpsuite抓包**或者用**view-source**查看源码。

```
<HTML>
<HEAD>
<SCRIPT LANGUAGE="Javascript">
<!--
var Words ="%3Cscript%3Ewindow.location.href%3D'http%3A%2F%2Fwww.bugku.com'%3B%3C%2Fscript%3E%20%0A%3C!--JTIyJTNCaWYoISUyNF9HRVQlNUlnaWQnJTVEKSUwQSU3QiUwQSUwOWhlYWRlcignTG9jYXRpb24lM0ElMjBoZWxsby5waHAlM0ZpZCUzRDEnKSUzQiUwQSUwOWV4aXQoKSUzQiUwQSU3RCUwQSUyNGlkJTNEJTI0X0dFVCU1QidpZCclNUQlM0llMEElMjRhJTNEJTI0X0dFVCU1QidhJyU1RCUzQiUwQSUyNGllM0QlMjRfR0VUJTVCJ2lnJTVEJTNCJTBBaWYoc3RyaXBvcyglMjRhJTJDJy4nKSklMEElN0llMEElMDllY2hvJTIwJ25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJyUzQiUwQSUwOXJldHVybiUyMCUzQiUwQSU3RCUwQSUyNGRhdGElMjAlM0QlMjAlNDBmaWxlX2dldF9jb250ZW50cygl
MjRhJTJDJ3InKSUzRiUwQWlmKCUyNGRhdGElM0QlM0QlMjJidWdrdSUyMGlzJTIwYSUyMG5pY2UlMjBwbGF0ZWZvcm0hJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuKCUyNGlpJTNFNSUyMGFuZCUyMGVyZWdpKCUyMjExMSUyMi5zdWJzdHIoJTI0YiUyQzAlMkMxKSUyQyUyMjExMTQlMjIpJTIwYW5kJTIwc3Vic3RyKCUyNGIlMkMwJTJDMSkhJTNENCklMEElN0llMEElMDklMjRmbGFnJTIwJTNEJTIwJTIyZmxhZyU3QioqKioqKioqJTdEJTIyJTBBJTdEJTBBZWxzZSUwQSU3QiUwQSUwOXByaW50JTIwJTIybmV2ZXIlMjBuZXZlciUyMG5ldmVyJTIwZ2l2ZSUyMHVwJTIwSEhJTIyJTNCJTBBJTdEJTBBJTBBJTBBJTNGJTNF--%3E"
function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();
// -->
</SCRIPT>
</HEAD>
<BODY>
</BODY>
</HTML>
```

发现执行了一个函数，**url解码**(可以用浏览器自带的控制台直接把语句执行一遍，也可以用burpsuite自带的decoder）查看函数内容。

```
"<script>window.location.href='http://www.bugku.com';</script>
<!--JTIyJTNCaWYoISUyNF9HRVQlNUlnaWQnJTVEKSUwQSU3QiUwQSUwOWhlYWRlcignTG9jYXRpb24lM0ElMjBoZWxsby5waHAlM0ZpZCUzRDEnKSUzQiUwQSUwOWV4aXQoKSUzQiUwQSU3RCUwQSUyNGlkJTNEJTI0X0dFVCU1QidpZCclNUQlM0llMEElMjRhJTNEJTI0X0dFVCU1QidhJyU1RCUzQiUwQSUyNGllM0QlMjRfR0VUJTVCJ2lnJTVEJTNCJTBBaWYoc3RyaXBvcyglMjRhJTJDJy4nKSklMEElN0llMEElMDllY2hvJTIwJ25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJyUzQiUwQSUwOXJldHVybiUyMCUzQiUwQSU3RCUwQSUyNGRhdGElMjAlM0QlMjAlNDBmaWxlX2dldF9jb250ZW50cygl
MjRhJTJDJ3InKSUzRiUwQWlmKCUyNGRhdGElM0QlM0QlMjJidWdrdSUyMGlzJTIwYSUyMG5pY2UlMjBwbGF0ZWZvcm0hJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuKCUyNGlpJTNFNSUyMGFuZCUyMGVyZWdpKCUyMjExMSUyMi5zdWJzdHIoJTI0YiUyQzAlMkMxKSUyQyUyMjExMTQlMjIpJTIwYW5kJTIwc3Vic3RyKCUyNGIlMkMwJTJDMSkhJTNENCklMEElN0llMEElMDklMjRmbGFnJTIwJTNEJTIwJTIyZmxhZyU3QioqKioqKioqJTdEJTIyJTBBJTdEJTBBZWxzZSUwQSU3QiUwQSUwOXByaW50JTIwJTIybmV2ZXIlMjBuZXZlciUyMG5ldmVyJTIwZ2l2ZSUyMHVwJTIwSEhJTIyJTNCJTBBJTdEJTBBJTBBJTBBJTNGJTNF-->"
```

里面有个注释，base64解码后再通过url解码，得到源码

```
";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($b,0,1),"1114") and substr($b,0,1)!=4)
{
 $flag = "flag{**********}"
}
else
{
 print "never never never give up !!!";
}
?>
```

根据源码我们得到以下几个条件：

`!$_GET['id']` 应该为 `true`，否则会跳转到 `hello.php?id=1` 这个页面

`$a` 中不能含有" . "

将 `$a` 文件通过 `file_get_contents` 读入到 `$data`，并且 `$a` 文件到内容为"bugku is a nice plateform!"

`$id==0`，这似乎与第一点相矛盾

`$b` 的长度大于5

将 `$b` 的第一个字符提取出来，与"111"进行拼接后，满足正则匹配

`$b` 的第一个字符不能是4

首先来看**第1点**和**第4点**，这个是对 `$id` 进行限制，`$id` 如果为 `0` 的话第1个条件就不满足了，但是注意在比较$id的时候用的是而不是=

`==` 在比较的时候，会将两个变量**转换为相同的类型**，再比较

`===` 在进行比较的时候，会**先判断**两种字符串的**类型是否相等**，再比较

这里可以让 `$id` 可以为 `0e123` (会当成科学计数法进行转换)，可以为 `0abc`，或者就直接为 `abc`，可以自行百度一下**php弱类型**。

**第2**和**第3点**条件是针对于 `$a` 的, 读取的文件名中不能包含".", 并且 `$a` 表示的文件中的内容为"bugku is a nice plateform!"。我们可以看到该题目是通过 `file_get_contents` 函数进行读取的文件内容，这个函数可以通过php伪协议( `php://input` )去绕过。

`php://input` 是个可以访问请求的原始数据的只读流.CTF中经常使用 `file_get_contents` 获取 `php://input` 内容(通过POST数据)，需要开启 `allow_url_include`，并且当 `enctype="multipart/form-data"` 的时候 `php://input` 是无效的。
我们令 `$a=php://input`，然后将"bugku is a nice plateform!"通过**POST方法**进行传递。

接下来看**最后三点约束**，首先`$b`的长度大于`5`，然后通过`eregi`函数进行正则匹配，这个函数作用是：不区分大小写的正则表达式匹配。此函数在PHP 5.3.0中已弃用，在PHP 7.0.0中已删除。

函数原型为`eregi ( string $pattern , string $string , array &$regs = ? ) : int`。第一个参数是匹配模式，根据**第7点**条件，`$b`的第一个字符不能是**4**，但是还得满足`eregi`的正则匹配，所以这里用一个通配符来绕过，可以让`$b`为`.12345`(“111”.substr(*b*,0,1)拼接后为”111.”，”.”表示任意单个字符，匹配成功)，或者‘* 12345‘（”111”.*substr(* b,0,1)拼接后为”111*”

最后的payload为`?id=0e123&a=php://input&b=.12345`， 并将"bugku is a nice plateform!"通过POST方法传递。