buuctf初学者学习记录--[ACTF2020 新生赛]Include

原创

pakho_C 已于 2022-02-08 14:31:41 修改 939 收藏

文章标签： php web安全

于 2022-01-15 21:59:41 首次发布

本文链接：https://blog.csdn.net/pakho_C/article/details/122515943

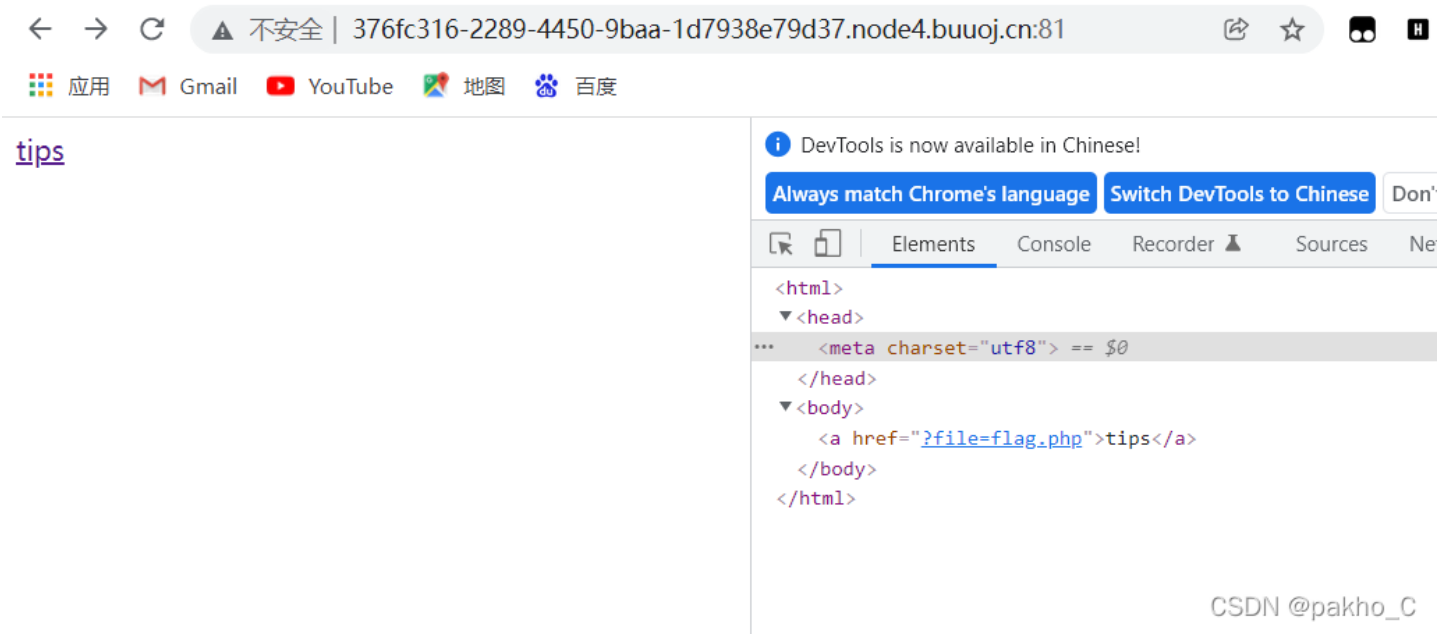
版权

web

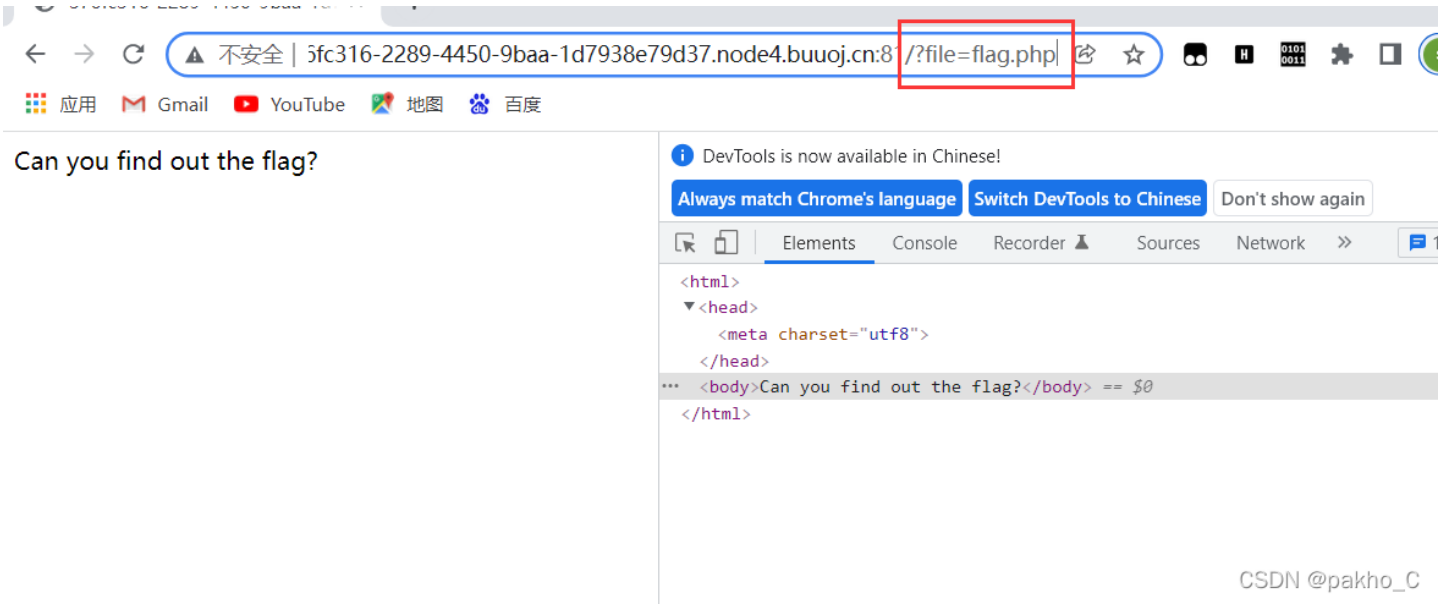
第八题

[ACTF2020 新生赛]Include

打开靶场



点击tips



通过url发现进行了文件读取，读取的文件为flag.php,结合题目思考这可能是一个文件包含的漏洞，并且flag就在flag.php中，此时需要进行读取文件内容

由于我是小白，对此类题没接触过（其实大多数都没接触过呜呜呜），经过一番搜索，只有wp解题了，就当知识积累
文件包含漏洞+PHP的伪协议

谈一谈php://filter的妙用

php://filter的理解：

php://filter简单理解：

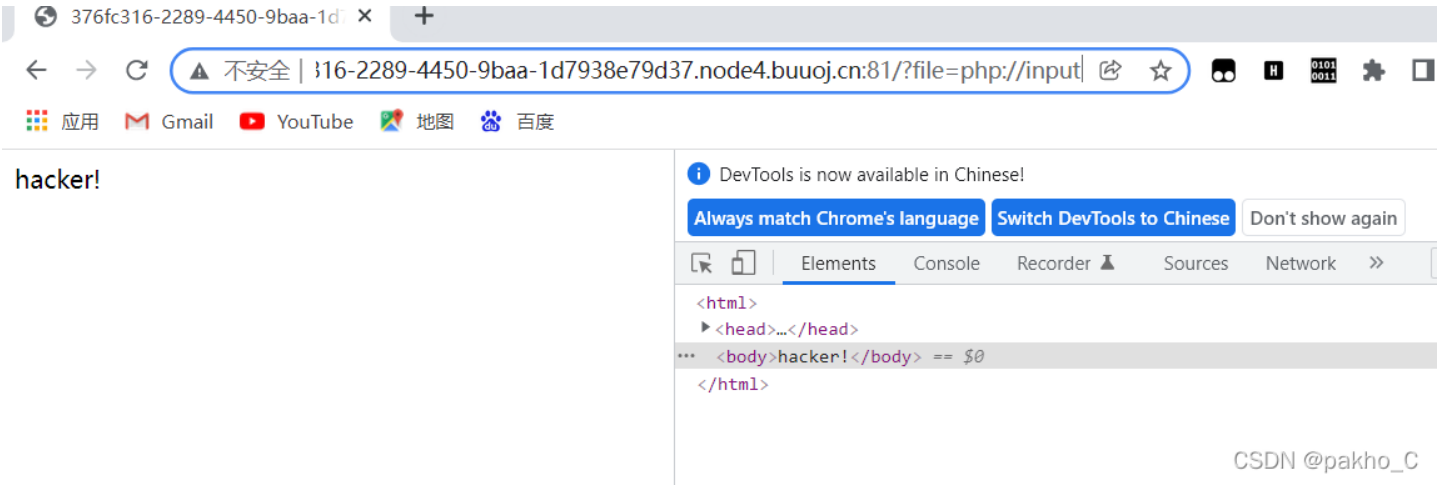
php://filter 是php中独有的一个协议，可以作为一个中间流来处理其他流，可以进行任意文件的读取；根据名字，filter，可以很容易想到这个协议可以用来过滤一些东西；

使用不同的参数可以达到不同的目的和效果：

名称	描述	备注
resource=<要过滤的数据流>	指定了你要筛选过滤的数据流。	必选
read=<读链的筛选列表>	可以设定一个或多个过滤器名称，以管道符 (|) 分隔。	可选
write=<写链的筛选列表>	可以设定一个或多个过滤器名称，以管道符 (|) 分隔。	可选
<; 两个链的筛选列表>	任何没有以 read= 或 write= 作前缀 的筛选器列表会视情况应用于读或写链。	

引用于 php://filter 的使用

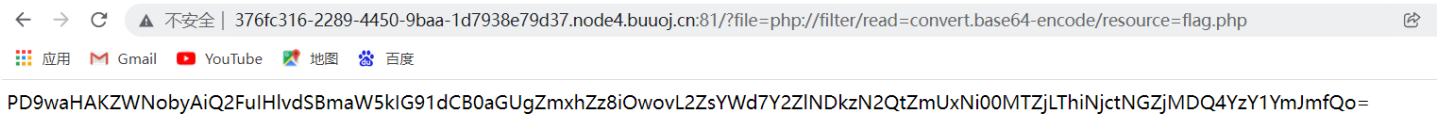
首先使用输入流进行测试



那么猜测可能是被过滤

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

意思是将flag.php进行base64编码后然后读取



将其进行base64解码得到flag