Web_php_include

点开是这样的界面


```
<?php
show_source(__FILE__);
echo  $_GET['hello'];
$page=$_GET['page'];
while  (strstr($page,  "php://"))  {
        $page=str_replace("php://",  "",  $page);
}
include($page);
?>
```

get hello会有回显，于是尝试一下


```
<?php
show_source(__FILE__);
echo  $_GET['hello'];
$page=$_GET['page'];
while  (strstr($page,  "php://"))  {
        $page=str_replace("php://",  "",  $page);
}
include($page);
?>
1
```

看了一下核心的部分是用strstr函数，过滤php://协议

查一下strstr函数，内容如下

php strstr()函数怎么用?

strstr() 函数搜索字符串在另一字符串中是否存在，如果是，返回该字符串及剩余部分，否则返回 FALSE。

注：该函数是二进制安全的；该函数区分大小写。

语法

```
strstr(string,search,before_search)
```

该函数大小写敏感，所以可以用大写绕过strstr函数，然后执行php://协议

使用Burpsuite构造这样的payload，然后cat flag文件就可以了

方法二：data://协议绕过

因为会对php://协议过滤，所以使用data://协议进行绕过

data://伪协议
php5.2.0起，数据流封装器开始有效，主要用于数据流的读取。如果传入的数据是PHP代码，就会执行代码
使用方法:data://text/plain;base64,xxxx(base64编码后的数据)

方法三：利用hello回显

输入hello有回显，因此尝试构造

/?page=http://127.0.0.1/?hello=

/?page=http://127.0.0.1/?hello=

就可以拿到flag