php文件包含漏洞（input与filter）

转载

a173262565 于 2018-03-06 22:52:00 发布 857 收藏 1
文章标签： php
原文链接：http://www.cnblogs.com/Ragd0ll/p/8519690.html

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

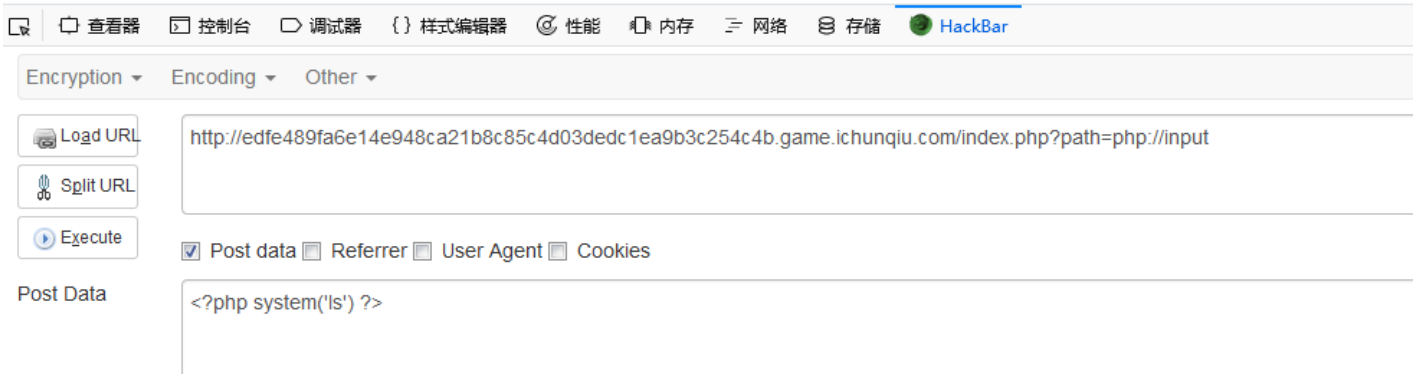
以i春秋上一道文件包含的CTF题为例：（来自rgrgrgrgrggrgrg大佬的Writeup）

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

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

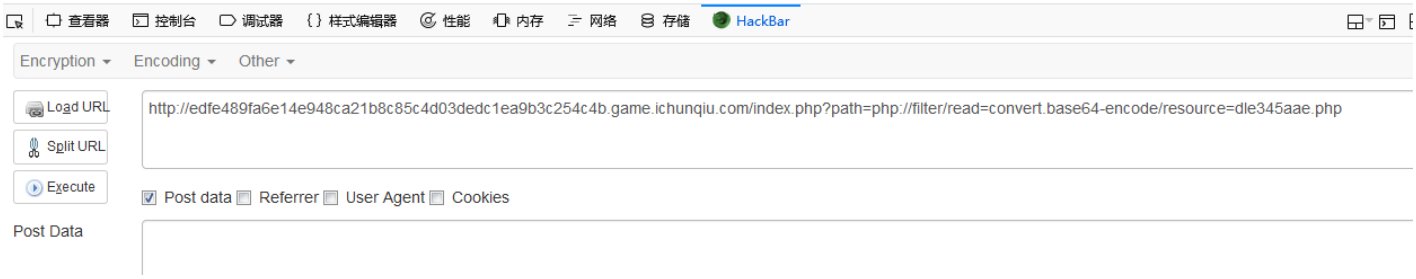
dle345aae.php index.php phpinfo.php



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

PD9waHAgCiRmbGFnPSJmbGFnezU1YThhN2YxLTAzMzQtNGVlMS1hZWNkLThiM2JhOTUzOTY0OX0iOwo=



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