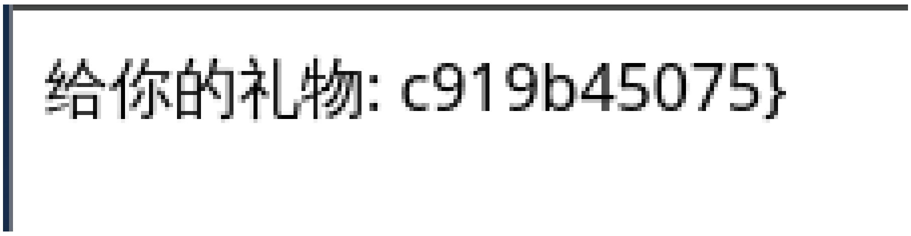
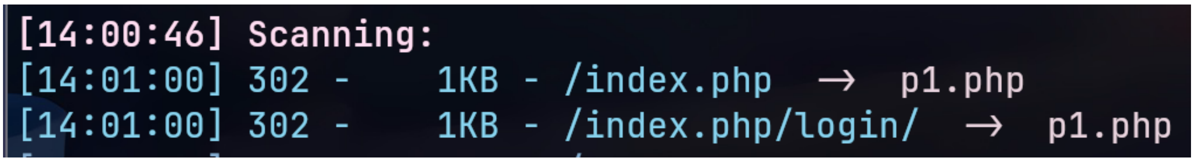


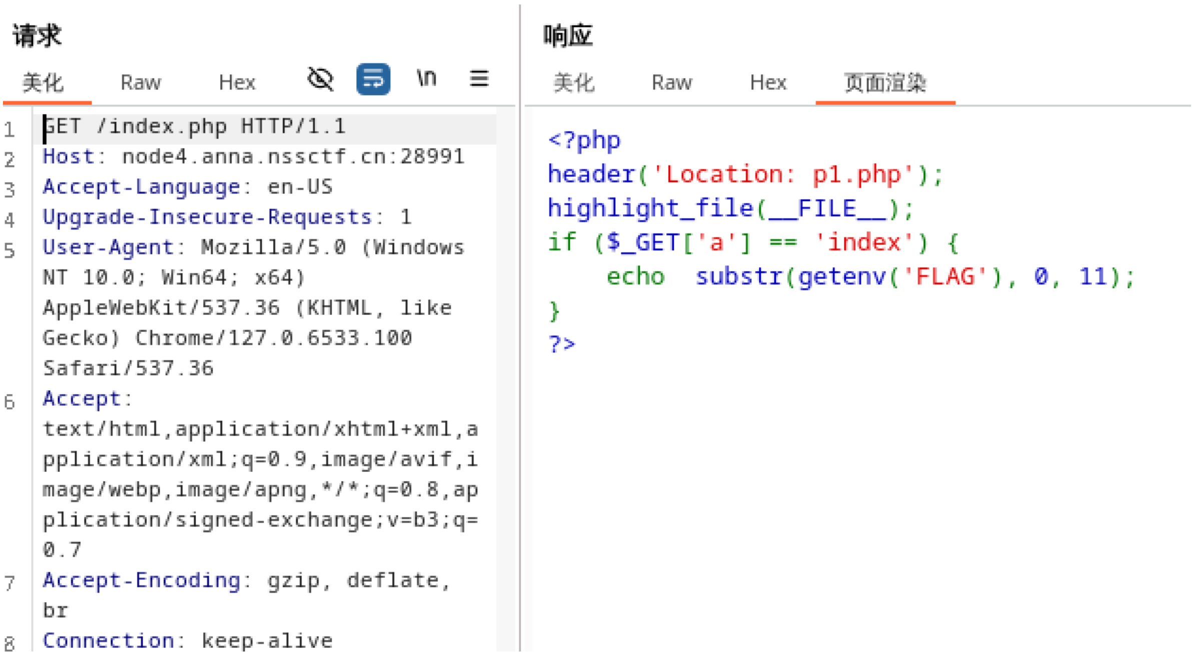
给你的礼物: c919b45075}

1.刚开始直接给了一部分flag，扫描目录看到主页index.php



```
[14:00:46] Scanning:
[14:01:00] 302 -    1KB - /index.php  →  p1.php
[14:01:00] 302 -    1KB - /index.php/login/  →  p1.php
```

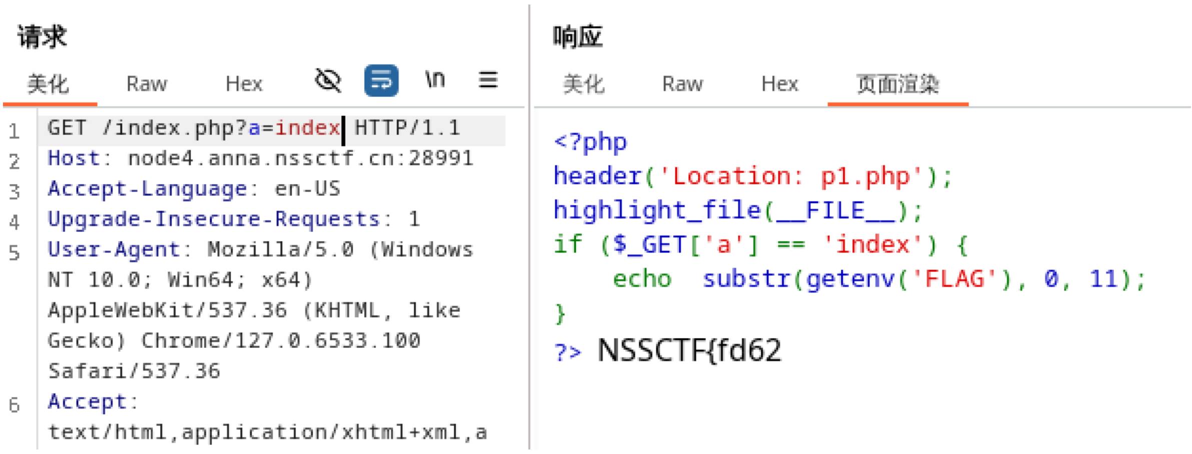
2.直接访问主页用burpsuit抓包，Chrl+R发送到重发器->发送，看到index.php内容



```
GET /index.php HTTP/1.1
Host: node4.anna.nssctf.cn:28991
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,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
<?php
header('Location: p1.php');
highlight_file(__FILE__);
if ($_GET['a'] == 'index') {
    echo  substr(getenv('FLAG'), 0, 11);
}
?>
```

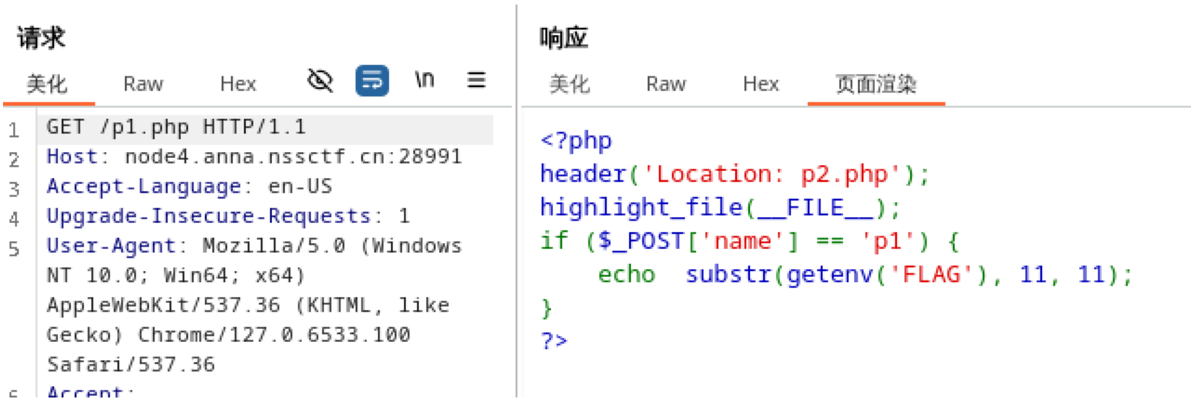
3.改请求包，get传参a=index->发送得到flag第一部分



```
GET /index.php?a=index HTTP/1.1
Host: node4.anna.nssctf.cn:28991
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,a
```

```
<?php
header('Location: p1.php');
highlight_file(__FILE__);
if ($_GET['a'] == 'index') {
    echo  substr(getenv('FLAG'), 0, 11);
}
?> NSSCTF{fd62
```

然后跟随重定向,看到p1内容

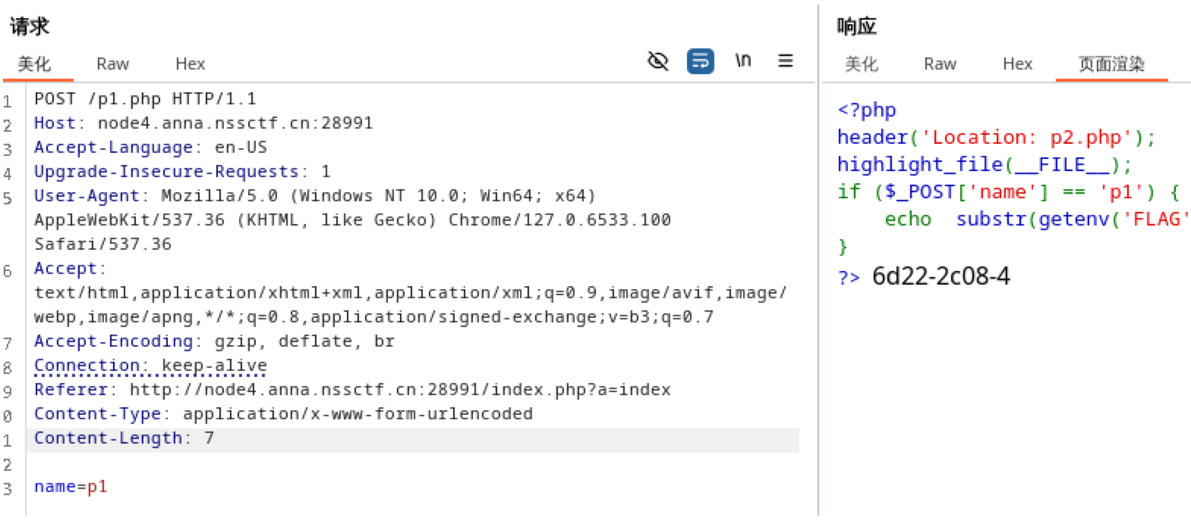


```
GET /p1.php HTTP/1.1
Host: node4.anna.nssctf.cn:28991
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
```

```
<?php
header('Location: p2.php');
highlight_file(__FILE__);
if ($_POST['name'] == 'p1') {
    echo  substr(getenv('FLAG'), 11, 11);
}
?>
```

4.将请求方式改成POST，加入请求头Content-Type: application/x-www-form-urlencoded，post传参name=p1

发送得到flag第二部分

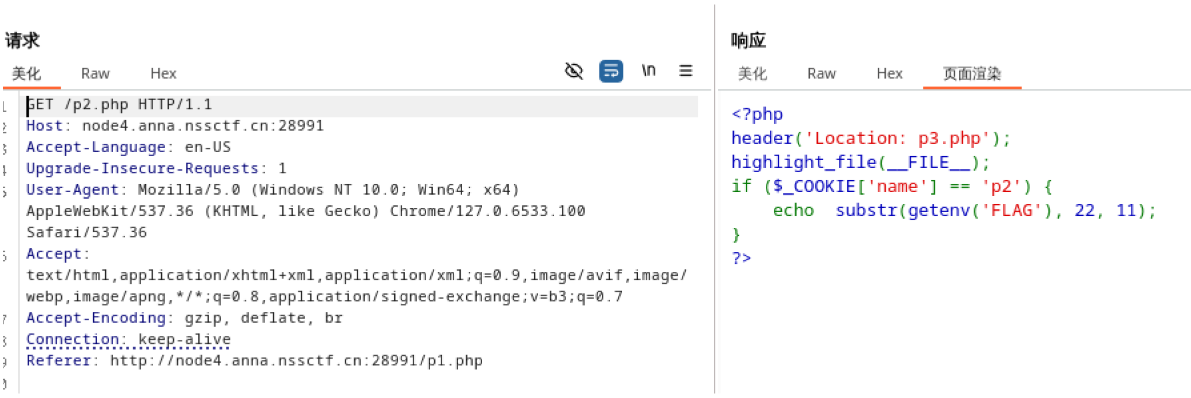


```
POST /p1.php HTTP/1.1
Host: node4.anna.nssctf.cn:28991
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://node4.anna.nssctf.cn:28991/index.php?a=index
Content-Type: application/x-www-form-urlencoded
Content-Length: 7

name=p1
```

```
<?php
header('Location: p2.php');
highlight_file(__FILE__);
if ($_POST['name'] == 'p1') {
    echo  substr(getenv('FLAG'
}
?> 6d22-2c08-4
```

5.再跟随重定向，看到p2.php内容

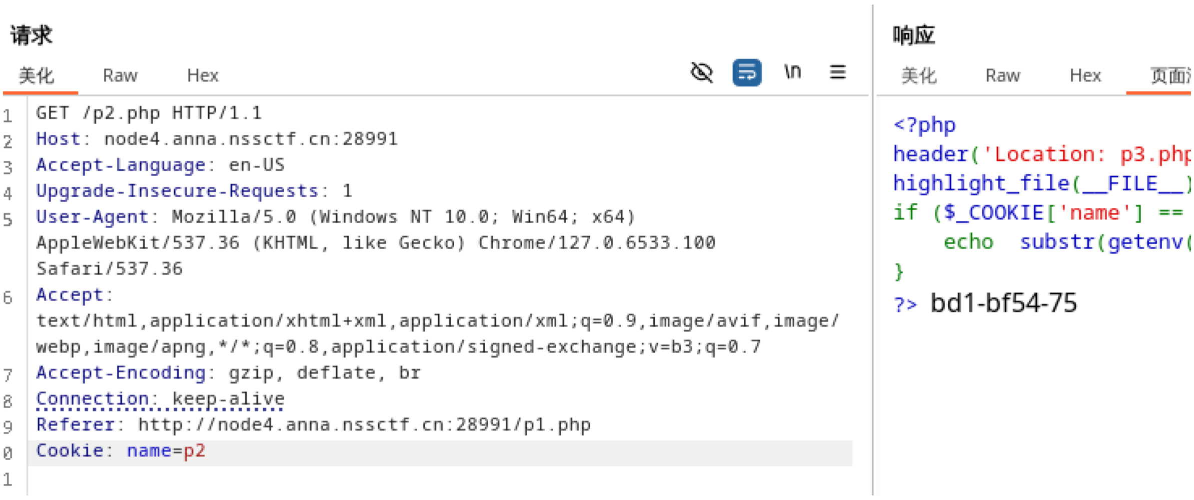


```
GET /p2.php HTTP/1.1
Host: node4.anna.nssctf.cn:28991
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://node4.anna.nssctf.cn:28991/p1.php
```

```
<?php
header('Location: p3.php');
highlight_file(__FILE__);
if ($_COOKIE['name'] == 'p2') {
    echo  substr(getenv('FLAG'), 22, 11);
}
?>
```

6.加入请求头Cookie: name=p2->发送，得到flag第三部分

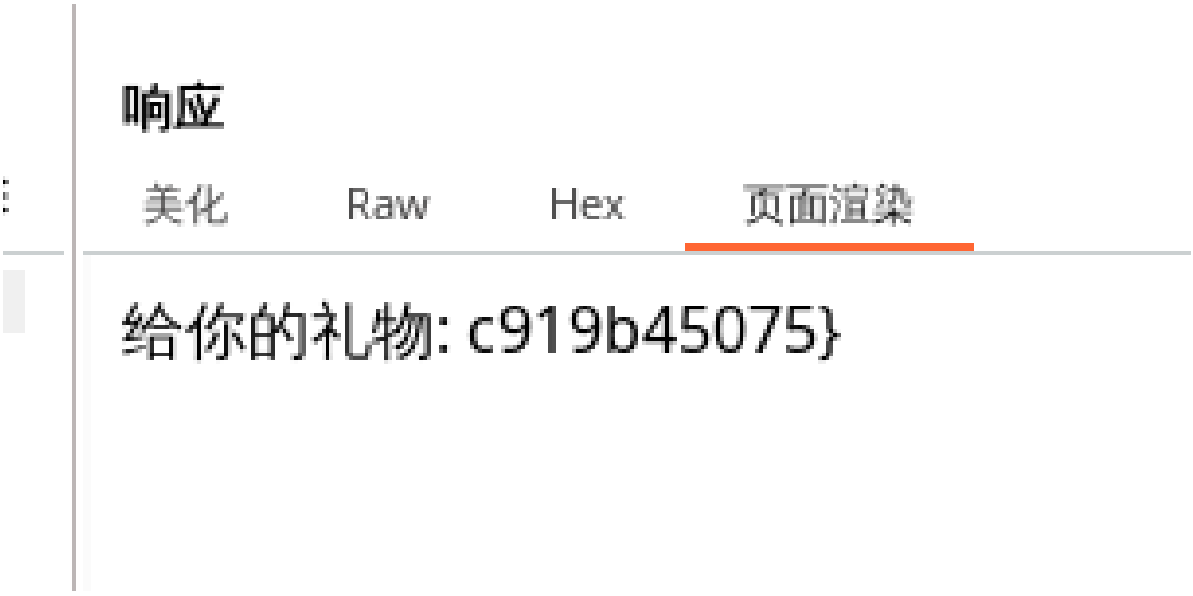
注意：下面要保持两行空行



```
GET /p2.php HTTP/1.1
Host: node4.anna.nssctf.cn:28991
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,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://node4.anna.nssctf.cn:28991/p1.php
Cookie: name=p2
```

```
<?php
header('Location: p3.php
highlight_file(__FILE__)
if ($_COOKIE['name'] ==
    echo  substr(getenv(
}
?> bd1-bf54-75
```

7.继续跟随重定向得到最后一部分



给你的礼物: c919b45075}