浙江大學

本科实验报告

课程名称：网络安全原理与实践

姓　　名：展翼飞

学　　院：计算机科学与技术学院

系：计算机科学与技术系

专　　业：计算机科学与技术

学　　号：3190102196

指导教师：林峰

2024 年 3 月 7 日

浙江大学实验报告

课程名称：网络安全原理与实践

实验名称：Lab 01

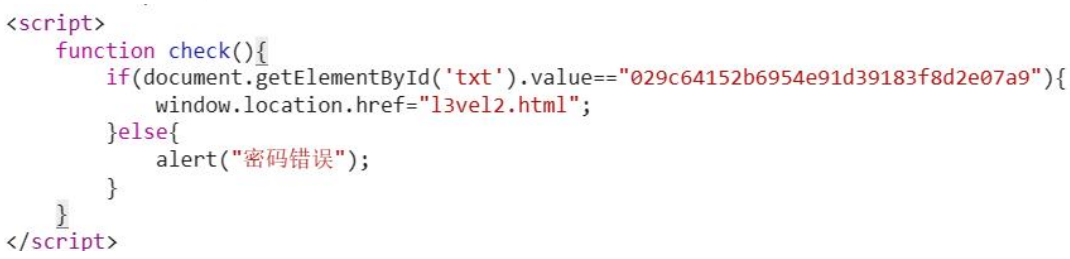
1. Lab Goal

Lab 01 aims to practice commonly used tools for packet sniffing, packet crafting, and port scanning.

2. Lab Steps

(1). http://10.15.111.100/game1

Step 1. view page source

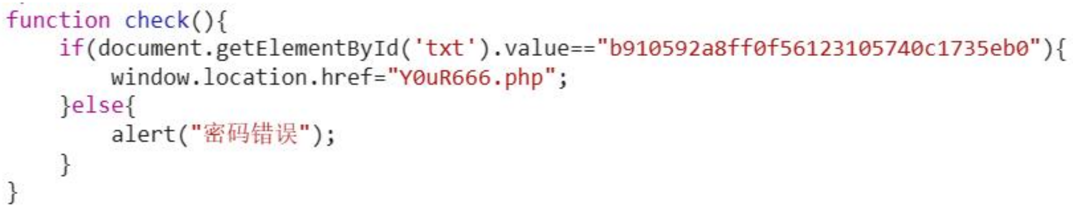


```
<script>
    function check(){
        if(document.getElementById('txt').value=="029c64152b6954e91d39183f8d2e07a9"){
            window.location.href="l3vel2.html";
        }else{
            alert("密码错误");
        }
    }
</script>
```

Open the browser's developer tools directly to view the HTML source code and find the hidden password in the check function.

The password is **029c64152b6954e91d39183f8d2e07a9**

Step 2. view page source

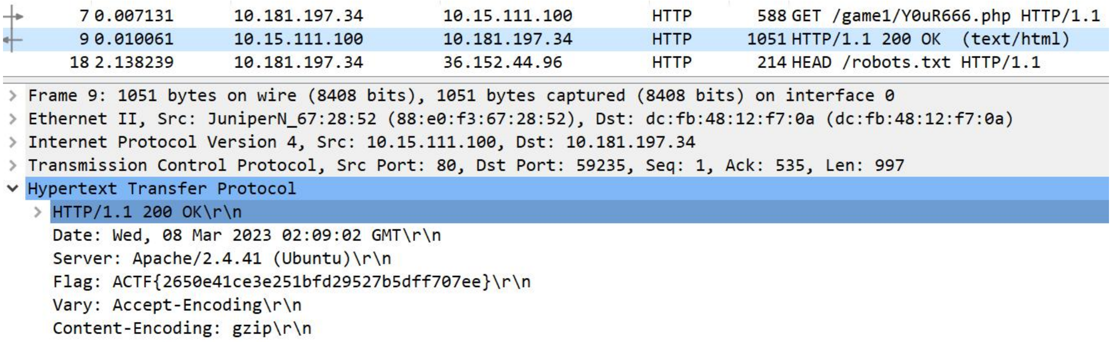


```
function check(){
    if(document.getElementById('txt').value=="b910592a8ff0f56123105740c1735eb0"){
        window.location.href="Y0uR666.php";
    }else{
        alert("密码错误");
    }
}
```

Enter the level 2 page and open the browser’s developer tools to view HTML source code and find the password is **b910592a8ff0f56123105740c1735eb0**

Step 3. capture RESONSE-packet header using WireShark

Enter next level and use WireShark to capture and view the Response header after the GET method.

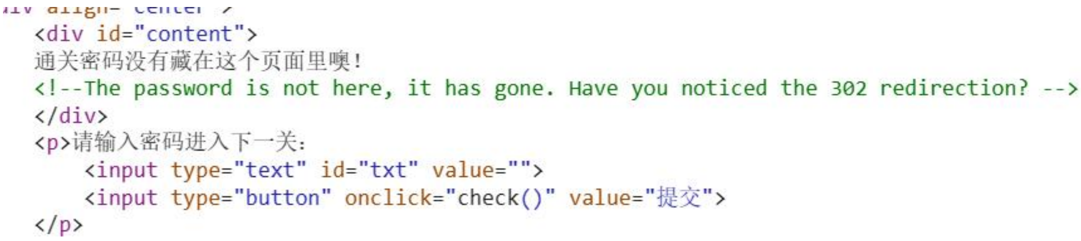


```
7 0.007131    10.181.197.34   10.15.111.100   HTTP    588 GET /game1/Y0uR666.php HTTP/1.1
9 0.010061    10.15.111.100   10.181.197.34   HTTP   1051 HTTP/1.1 200 OK  (text/html)
18 2.138239   10.181.197.34   36.152.44.96    HTTP    214 HEAD /robots.txt HTTP/1.1

> Frame 9: 1051 bytes on wire (8408 bits), 1051 bytes captured (8408 bits) on interface 0
> Ethernet II, Src: JuniperN_67:28:52 (88:e0:f3:67:28:52), Dst: dc:fb:48:12:f7:0a (dc:fb:48:12:f7:0a)
> Internet Protocol Version 4, Src: 10.15.111.100, Dst: 10.181.197.34
> Transmission Control Protocol, Src Port: 80, Dst Port: 59235, Seq: 1, Ack: 535, Len: 997
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 08 Mar 2023 02:09:02 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Flag: ACTF{2650e41ce3e251bfd29527b5dff707ee}\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
```

We can use the source address and the type of protocol to distinguish the response packet, and find the Flag is **ACTF{2650e41ce3e251bfd29527b5dff707ee}**

(2). http://10.15.111.100/game2

Step 1. view page source



```
iv align="center">
  <div id="content">
  通关密码没有藏在这个页面里噢！
  <!--The password is not here, it has gone. Have you noticed the 302 redirection? -->
  </div>
  <p>请输入密码进入下一关：
      <input type="text" id="txt" value="">
      <input type="button" onclick="check()" value="提交">
  </p>
```

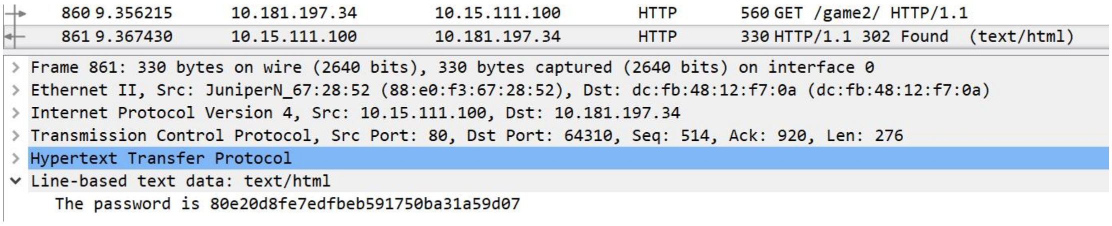
View the source code and find the prompt of 302 redirection.

Step 2. understand 302 redirection

A 302 is a status code in the HTTP protocol that can be interpreted to mean that the resource did exist, but has been temporarily redirected. For servers, the HTTP Location header is usually sent to the browser to redirect to the new location.

Step 3. locate redirected pages and find password

Check the GET request with status code 302 and find the password in the response body.



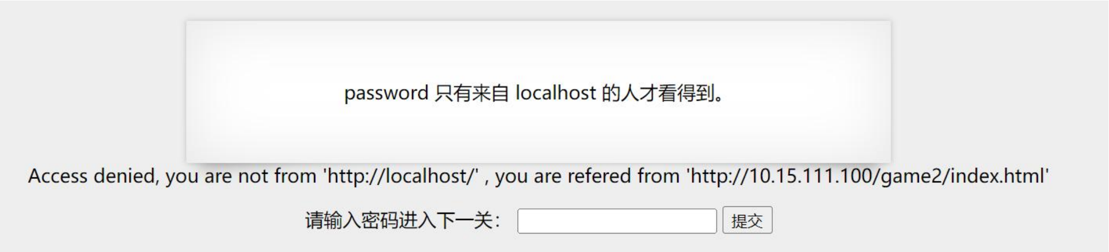
```
860 9.356215   10.181.197.34   10.15.111.100   HTTP   560 GET /game2/ HTTP/1.1
861 9.367430   10.15.111.100   10.181.197.34   HTTP   330 HTTP/1.1 302 Found  (text/html)

> Frame 861: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface 0
> Ethernet II, Src: JuniperN_67:28:52 (88:e0:f3:67:28:52), Dst: dc:fb:48:12:f7:0a (dc:fb:48:12:f7:0a)
> Internet Protocol Version 4, Src: 10.15.111.100, Dst: 10.181.197.34
> Transmission Control Protocol, Src Port: 80, Dst Port: 64310, Seq: 514, Ack: 920, Len: 276
> Hypertext Transfer Protocol
v Line-based text data: text/html
    The password is 80e20d8fe7edfbeb591750ba31a59d07
```

The password is **80e20d8fe7edfbeb591750ba31a59d07**

Step 4. understand HTTP Referer field

Referer is a common field in the header of HTTP requests that provides information about the source of the access. The client sends the request with or without this field at its own discretion. Servers generally use the referer to identify the source of a visit, which may be used for statistical analysis, logging, and cache optimization.

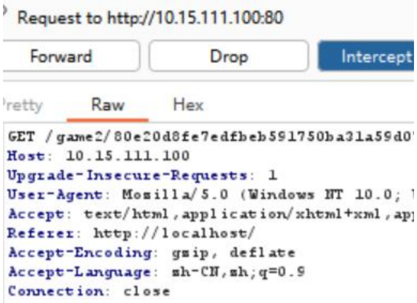
Step 5. capture GET-packet and rewrite Referer field using Burp Suite



password 只有来自 localhost 的人才看得到。

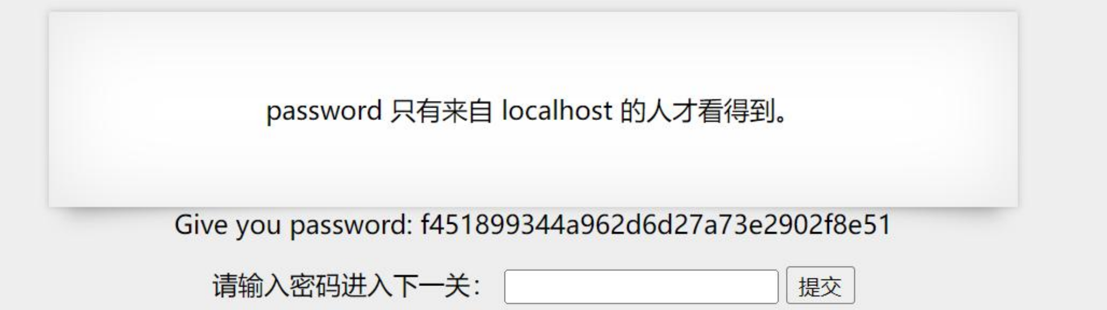
Access denied, you are not from 'http://localhost/' , you are refered from 'http://10.15.111.100/game2/index.html'

Enter next level and record the required referer ‘http://localhost/’, then go back to last level and intercept the GET-packet.



```
GET /game2/80e20d8fe7edfbeb591750ba31a59d0
Host: 10.15.111.100
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Accept: text/html,application/xhtml+xml,ap
Referer: http://localhost/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Rewrite the GET-packet and then forward it.

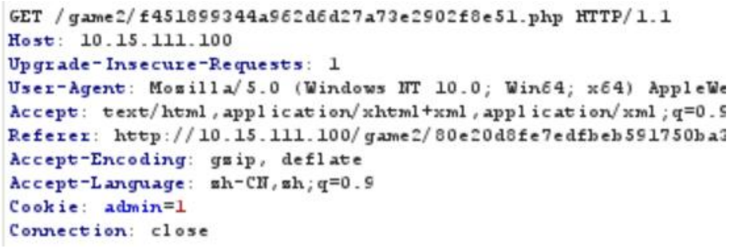


password 只有来自 localhost 的人才看得到。

Give you password: f451899344a962d6d27a73e2902f8e51

Now we can get the password : **f451899344a962d6d27a73e2902f8e51**

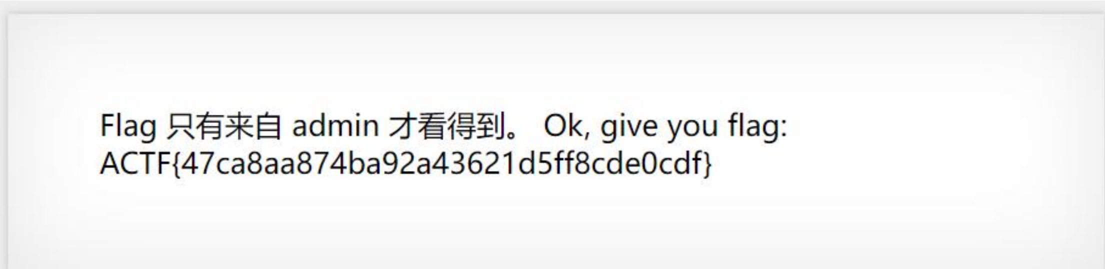
Step 6. capture GET-packet and rewrite Cookie field with admin privilege using Burp Suite



```
GET /game2/f451899344a962d6d27a73e2902f8e51.php HTTP/1.1
Host: 10.15.111.100
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
Referer: http://10.15.111.100/game2/80e20d8fe7edfbeb591750ba
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin=1
Connection: close
```

Before we go to next level, we intercept the Get-packet and set Cookie field with

admin = 1

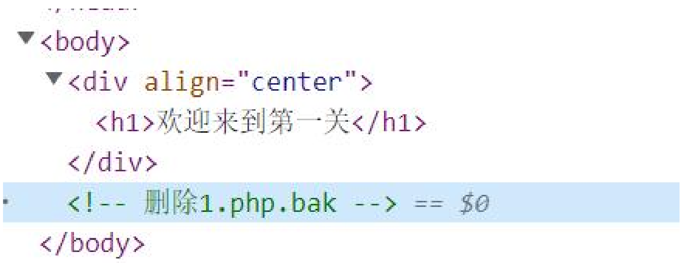


Flag 只有来自 admin 才看得到。 Ok, give you flag:
ACTF{47ca8aa874ba92a43621d5ff8cde0cdf}

Forward the packet and we can get the Flag : **ACTF{47ca8aa874ba92a43621d5ff8cde0cdf}**

(3)http://10.214.160.13:10000/

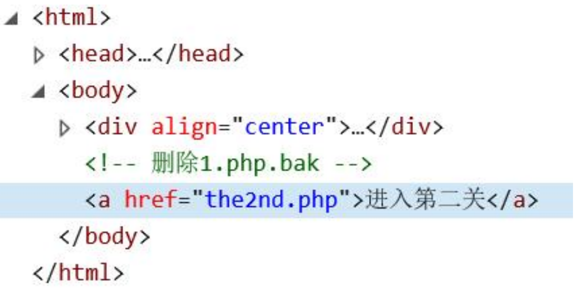
Step 1. view page source



```
▼<body>
  ▼<div align="center">
     <h1>欢迎来到第一关</h1>
   </div>
   <!-- 删除1.php.bak --> == $0
 </body>
```

Step 2. get link from .bak file

Change the URL to get the 1.php.bak file and open it in browser with developer tool

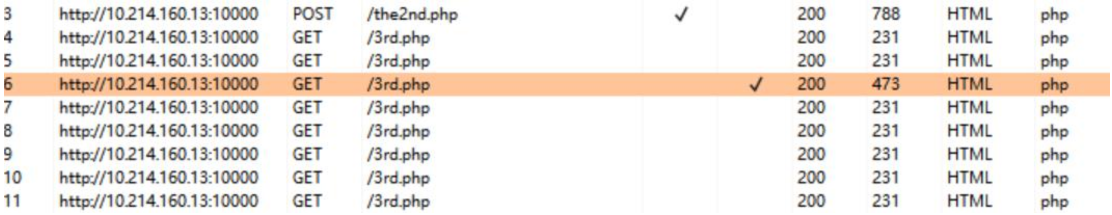


```
◢ <html>
  ▷ <head>…</head>
  ◢ <body>
    ▷ <div align="center">…</div>
      <!-- 删除1.php.bak -->
      <a href="the2nd.php">进入第二关</a>
    </body>
  </html>
```

We can get the url to the next level

Step 3. capture GET-packet and null Referer field using Burp Suite

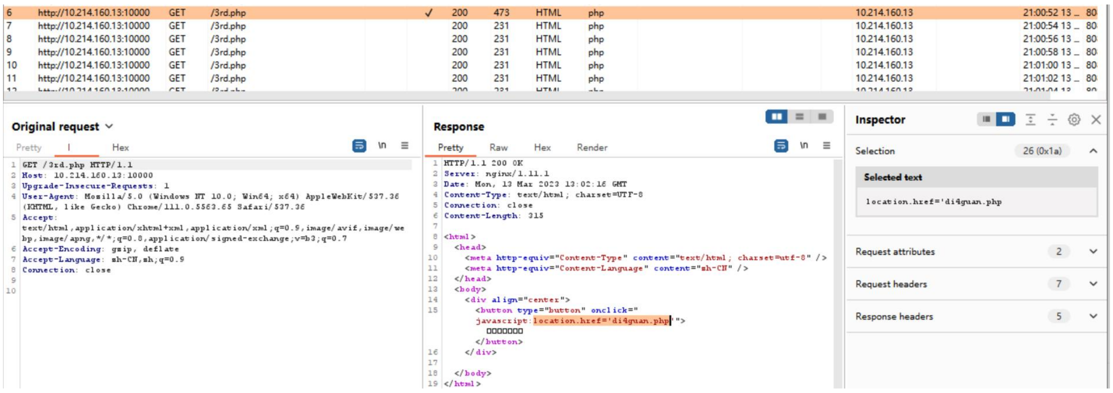
Click the go to the next level button, then there will be a Post request and a lot of Get request without Referer field.



3	http://10.214.160.13:10000	POST	/the2nd.php	✓		200	788	HTML	php
4	http://10.214.160.13:10000	GET	/3rd.php			200	231	HTML	php
5	http://10.214.160.13:10000	GET	/3rd.php			200	231	HTML	php
6	http://10.214.160.13:10000	GET	/3rd.php		✓	200	473	HTML	php
7	http://10.214.160.13:10000	GET	/3rd.php			200	231	HTML	php
8	http://10.214.160.13:10000	GET	/3rd.php			200	231	HTML	php
9	http://10.214.160.13:10000	GET	/3rd.php			200	231	HTML	php
10	http://10.214.160.13:10000	GET	/3rd.php			200	231	HTML	php
11	http://10.214.160.13:10000	GET	/3rd.php			200	231	HTML	php

Select a GET request, and add the Referer field with value ‘null’ and then forward it using Burp Suite, then we can get the Response

Step 4. capture RESONSE-packet header with next link included using Burp Suite



6	http://10.214.160.13:10000	GET	/3rd.php	✓	200	473	HTML	php	10.214.160.13	21:00:52 13 ...	80
7	http://10.214.160.13:10000	GET	/3rd.php		200	231	HTML	php	10.214.160.13	21:00:54 13 ...	80
8	http://10.214.160.13:10000	GET	/3rd.php		200	231	HTML	php	10.214.160.13	21:00:56 13 ...	80
9	http://10.214.160.13:10000	GET	/3rd.php		200	231	HTML	php	10.214.160.13	21:00:58 13 ...	80
10	http://10.214.160.13:10000	GET	/3rd.php		200	231	HTML	php	10.214.160.13	21:01:00 13 ...	80
11	http://10.214.160.13:10000	GET	/3rd.php		200	231	HTML	php	10.214.160.13	21:01:02 13 ...	80

```
GET /3rd.php HTTP/1.1
Host: 10.214.160.13:10000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,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
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.11.1
Date: Mon, 13 Mar 2023 13:02:16 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 315

<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta http-equiv="Content-Language" content="zh-CN" />
  </head>
  <body>
    <div align="center">
      <button type="button" onclick="
      javascript:location.href='di4guan.php'">
        □□□□□□□
      </button>
    </div>

  </body>
</html>
```

Selection 26 (0x1a)

Selected text

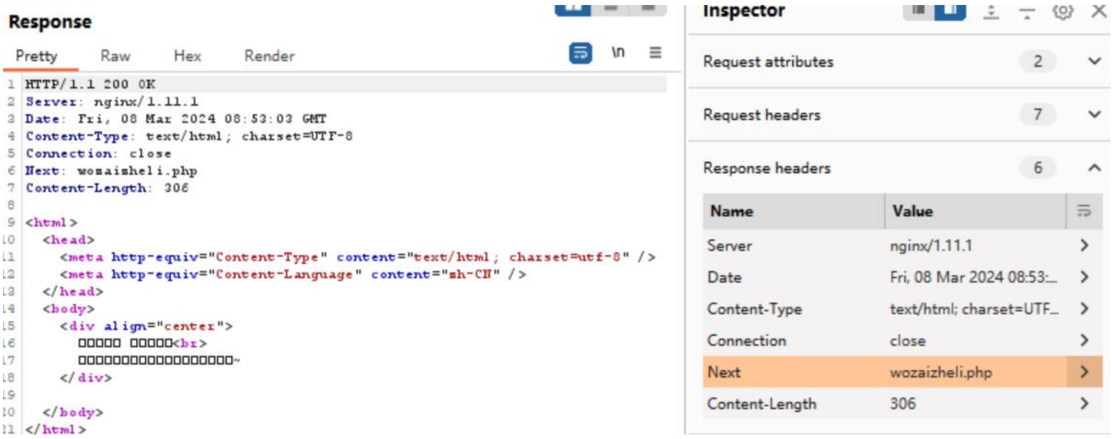
```
location.href='di4guan.php
```

Request attributes	2
Request headers	7
Response headers	5

The url of the next level is **di4guan.php**

Step 5. view page source and try to click the button or craft packet with button click effect

The response packet of Get Method of url di4guan.php give us next level’s url : wozaizheli.php



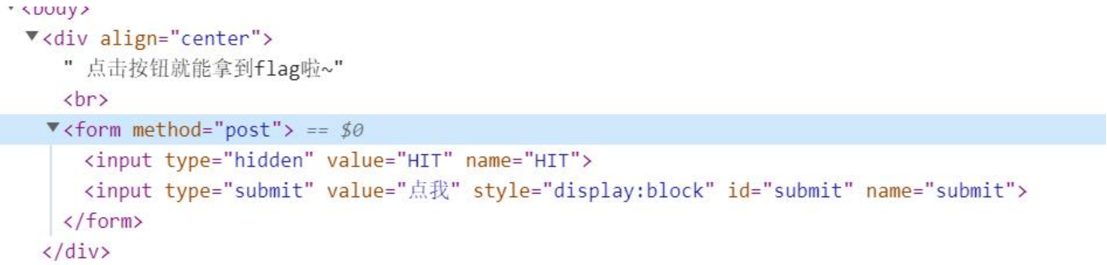
```
HTTP/1.1 200 OK
Server: nginx/1.11.1
Date: Fri, 08 Mar 2024 08:53:03 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Next: wozaizheli.php
Content-Length: 306

<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta http-equiv="Content-Language" content="zh-CN" />
  </head>
  <body>
    <div align="center">
      □□□□□ □□□□□<br>
      □□□□□□□□□□□□□□□□□□~
    </div>

  </body>
</html>
```

Request attributes	2
Request headers	7
Response headers	6

Name	Value
Server	nginx/1.11.1
Date	Fri, 08 Mar 2024 08:53:...
Content-Type	text/html; charset=UTF...
Connection	close
Next	wozaizheli.php
Content-Length	306

Enter wozaizheli.php then we find hint to click the button but the button disappear quickly.

We can modify the page source and delete the script which hide the button, then we can click the button.



```
▾ <body>
  ▼<div align="center">
     " 点击按钮就能拿到flag啦~"
     <br>
    ▼<form method="post"> == $0
       <input type="hidden" value="HIT" name="HIT">
       <input type="submit" value="点我" style="display:block" id="submit" name="submit">
     </form>
   </div>
```

Then we can get the flag

flag: AAA{y0u_2a_g0od_front-end_Web_developer}