浙江大学

本科实验报告

课程名称：网络安全原理与实践

姓　　名：沈韵泓

学　　院：计算机科学与技术学院

系：计算机科学与技术系

专　　业：软件工程

学　　号：3200104392

指导教师：卜凯

2023 年 2 月 28 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

`http://10.15.111.100/game1/`

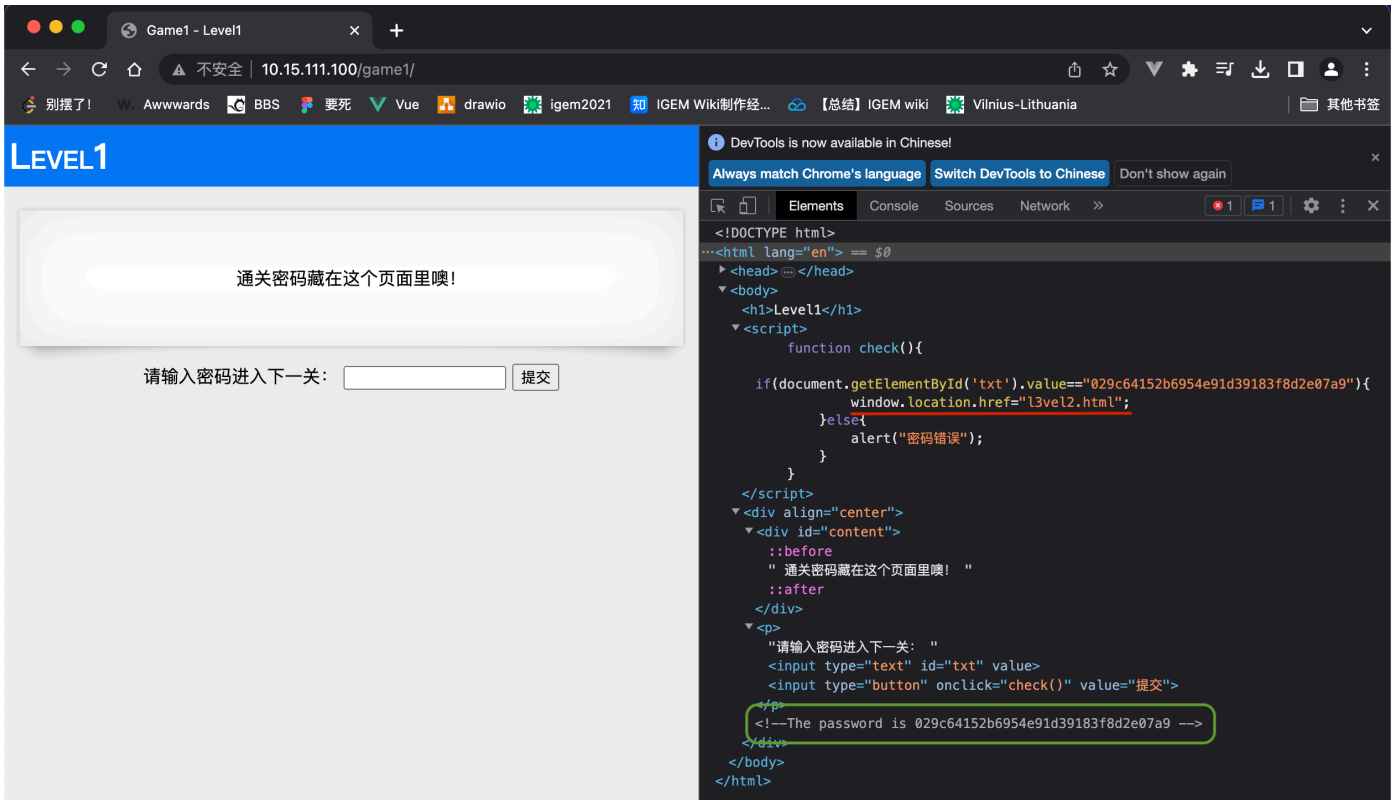
Step 1

> 1. View page source.

Using F12 to open DevTool, we can find that:

- The comment says that `The password is 029c64152b6954e91d39183f8d2e07a9`
- When we click the button `提交`, function `check()` would check whether the value equals to `029c64152b6954e91d39183f8d2e07a9`. If so, the page will redirect to `l3vel2.html`

Thus, we can infer that: the password of this step is `029c64152b6954e91d39183f8d2e07a9`.



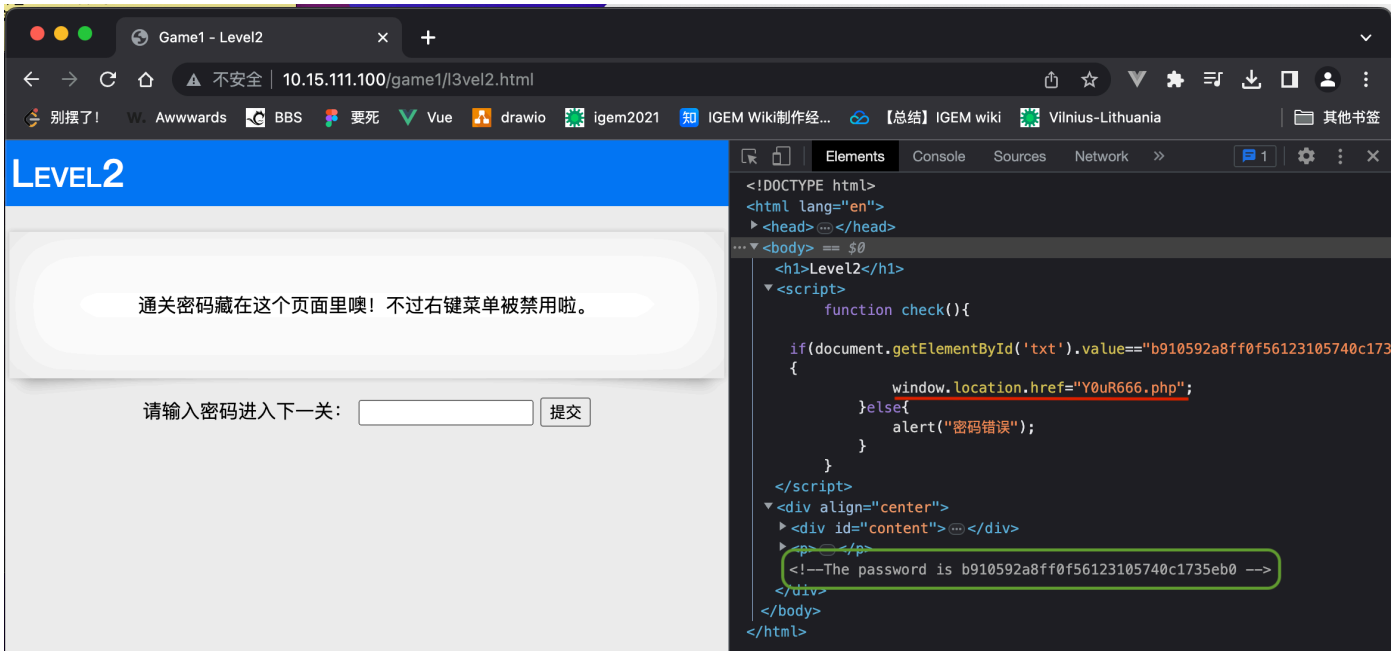
After entering the password, we then go to the next step.

> Actually, we can visit `http://10.15.111.100/game1/l3vel2.html` directly.

Step 2

> 2. View the source.

Since I use F12 to open the DevTool, blocking the right click doesn't bother me(?)

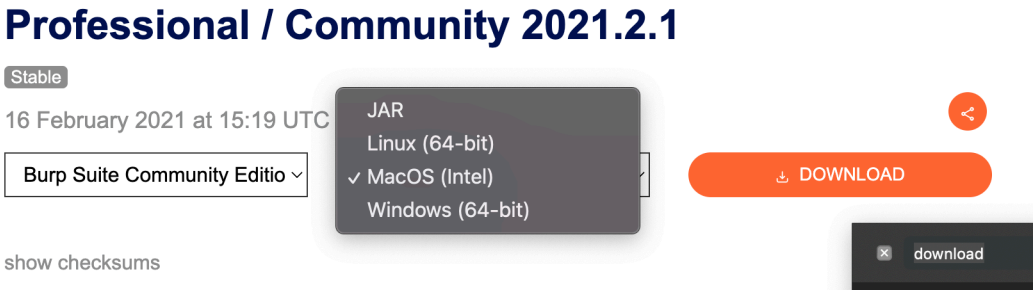


Just like what I have done in step 1: entering `b910592a8ff0f56123105740c1735eb0`, or visit `http://10.15.111.100/game1/Y0uR666.php` directly.

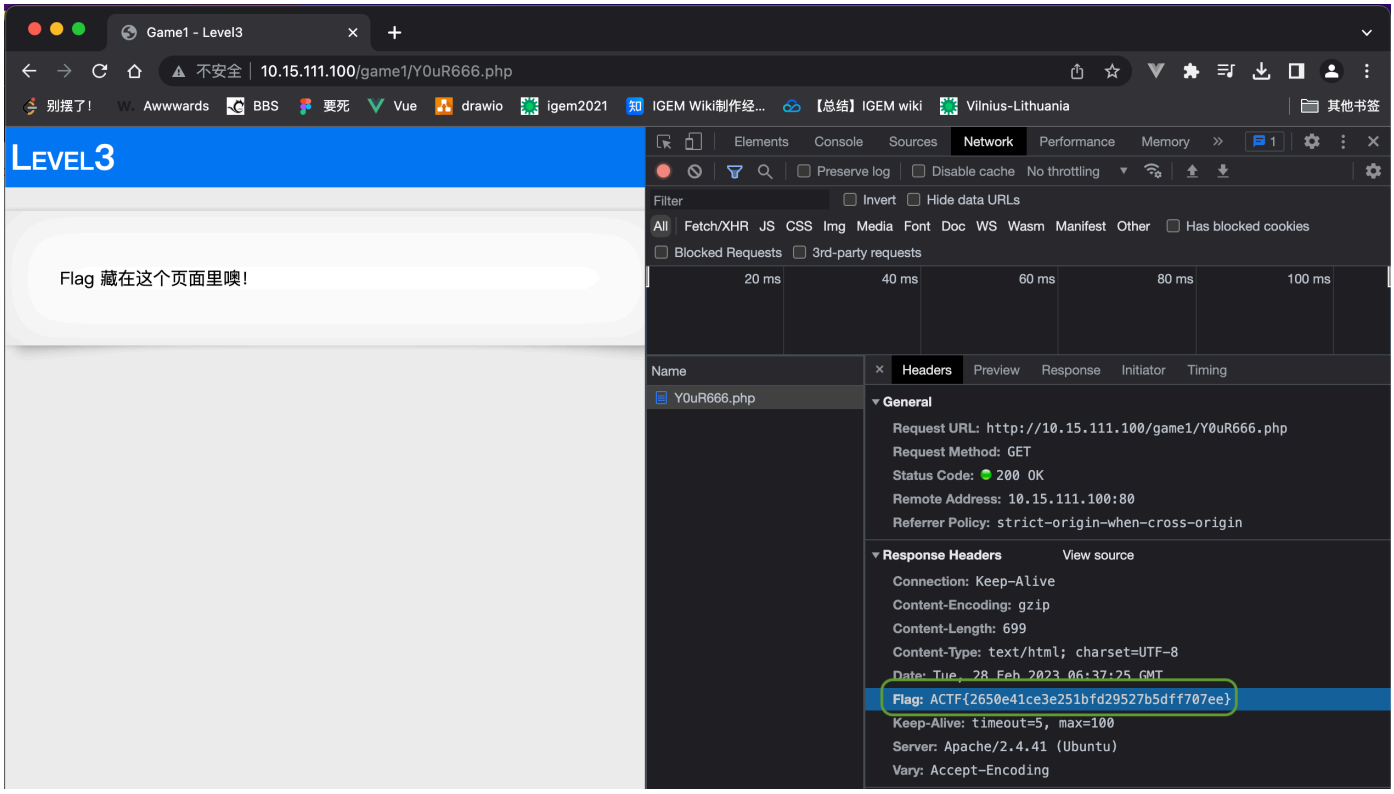
Step 3

> 3. Capture RESPONSE-packet header using Burp Suite.

Since there is no suitable version of Burp Suite for my PC(Mac with Apple Silicon), I tried to user DevTool to fix this problem(the jar file somehow can't work properly).



It's not hard to find the FLAG at the header of the RESPONSE-packet, which is `ACTF{2650e41ce3e251bfd29527b5dff707ee}`



Thus, the FLAG is ACTF{2650e41ce3e251bfd29527b5dff707ee}

2

`http://10.15.111.100/game2`

Step 1

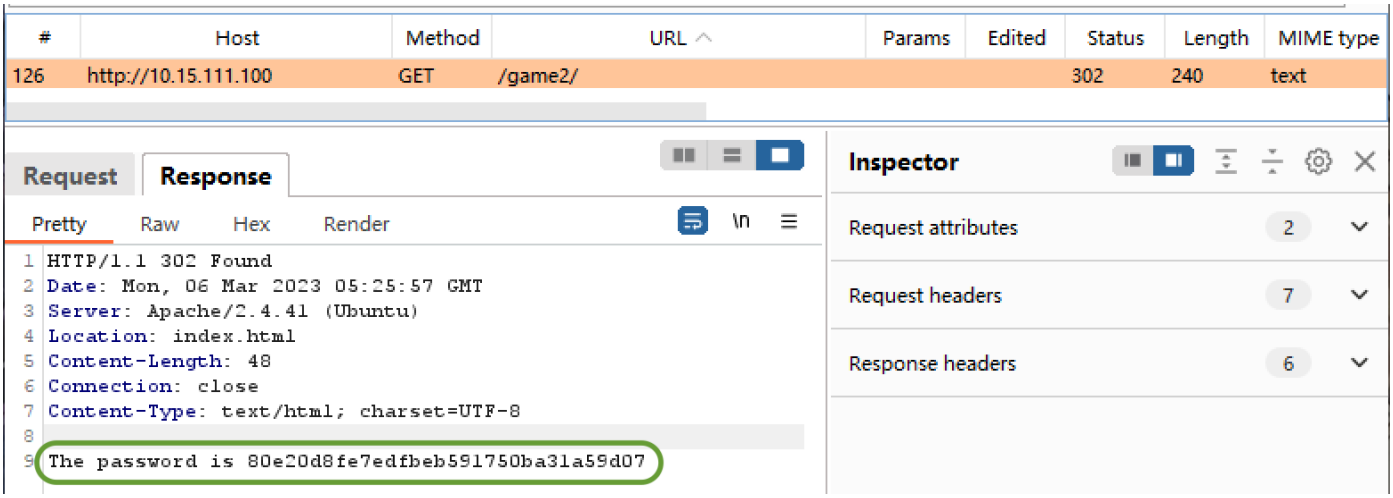
1. View page source.
2. Understand 302 redirection.

The comment told us to pay attention to the 302 redirection, which ndicates that the resource requested has been temporarily moved to the URL given by the `Location` header.

```
<!DOCTYPE html>
<html lang="en">
 ▶ <head> … </head>
 ▼ <body>
    <h1>Level1</h1>
   ▶ <script> … </script>
   ▼ <div align="center">
     ▼ <div id="content"> == $0
        ::before
        " 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? -->
        ::after
       </div>
     ▶ <p> … </p>
     </div>
   </body>
</html>
```

3. Locate redirected pages and find password.

By using Burp Suite, we can find the response with status 302, which told us that the password is `80e20d8fe7edfbeb591750ba31a59d07`.



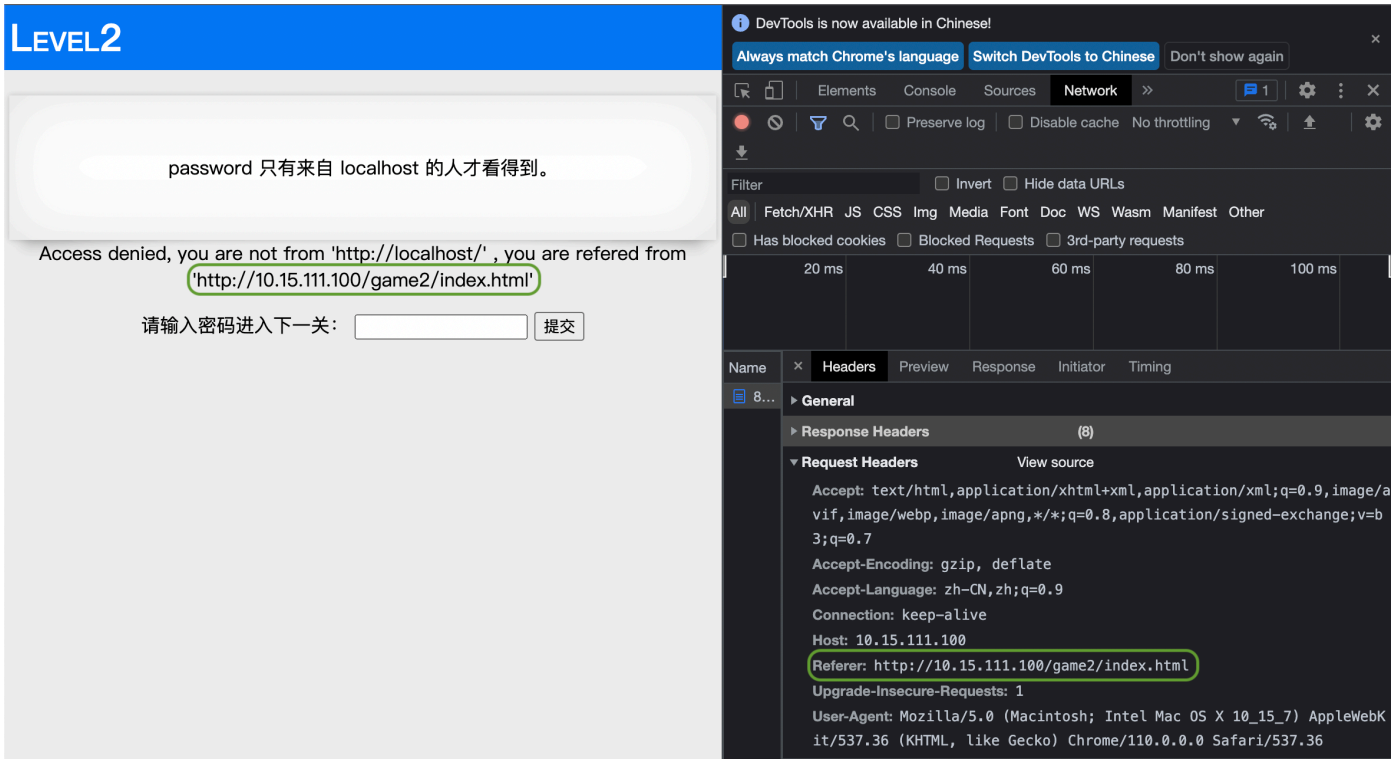
Enter the password, and we can move to the next step.

Step 2

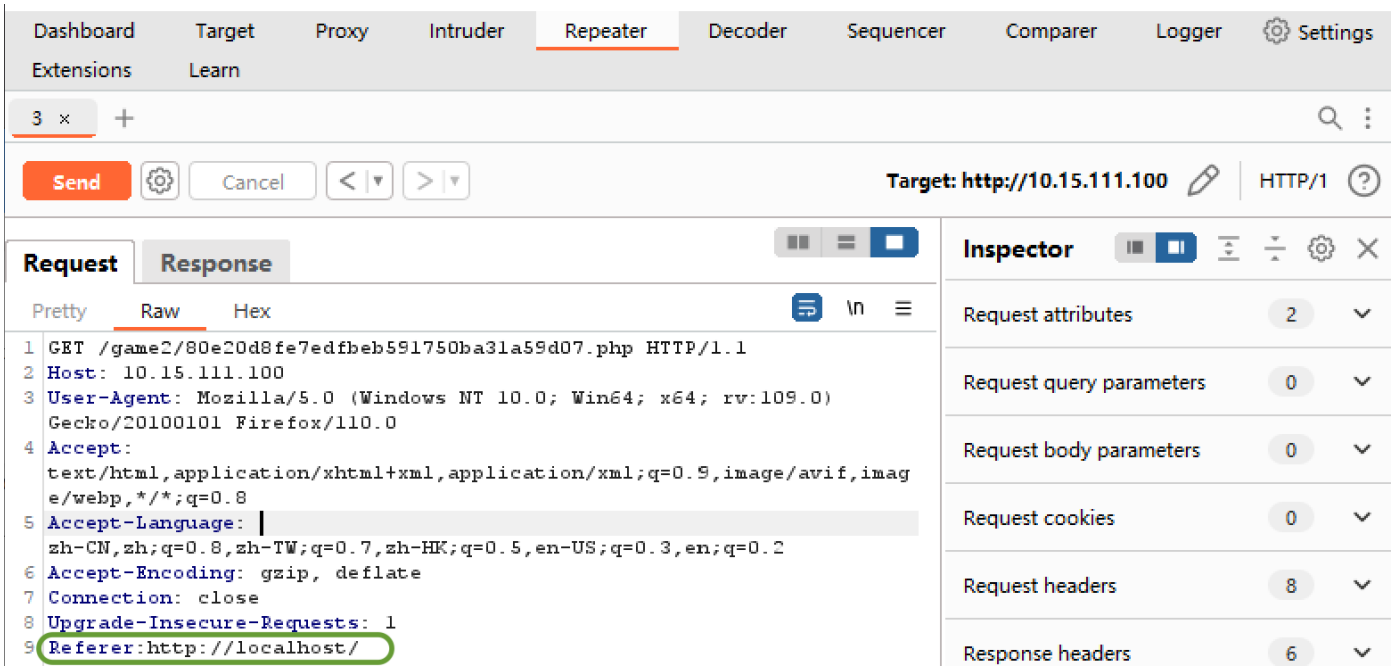
4. Understand HTTP Referer field.

The `Referer` HTTP request header contains the absolute or partial address from which a resource has been requested. It can prevent stealing link and blocking malicious requests.

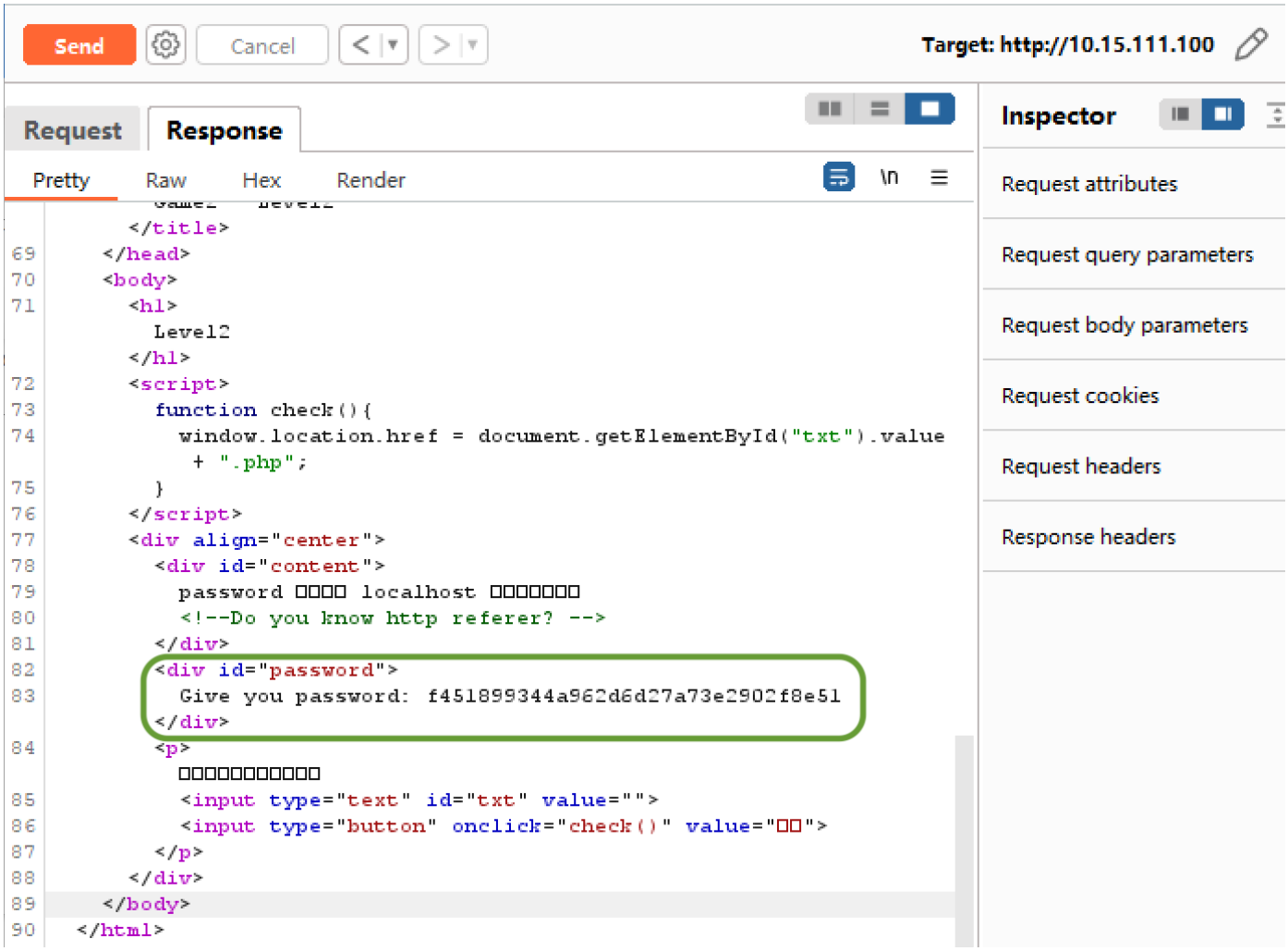
5. Capture GET-packet and rewrite Referer filed using Burp Suite.



Since the website denied our access because of we are not from `http://localhost/` we can use the Repeater of Burp Suite to rewrite Referer field accordingly:



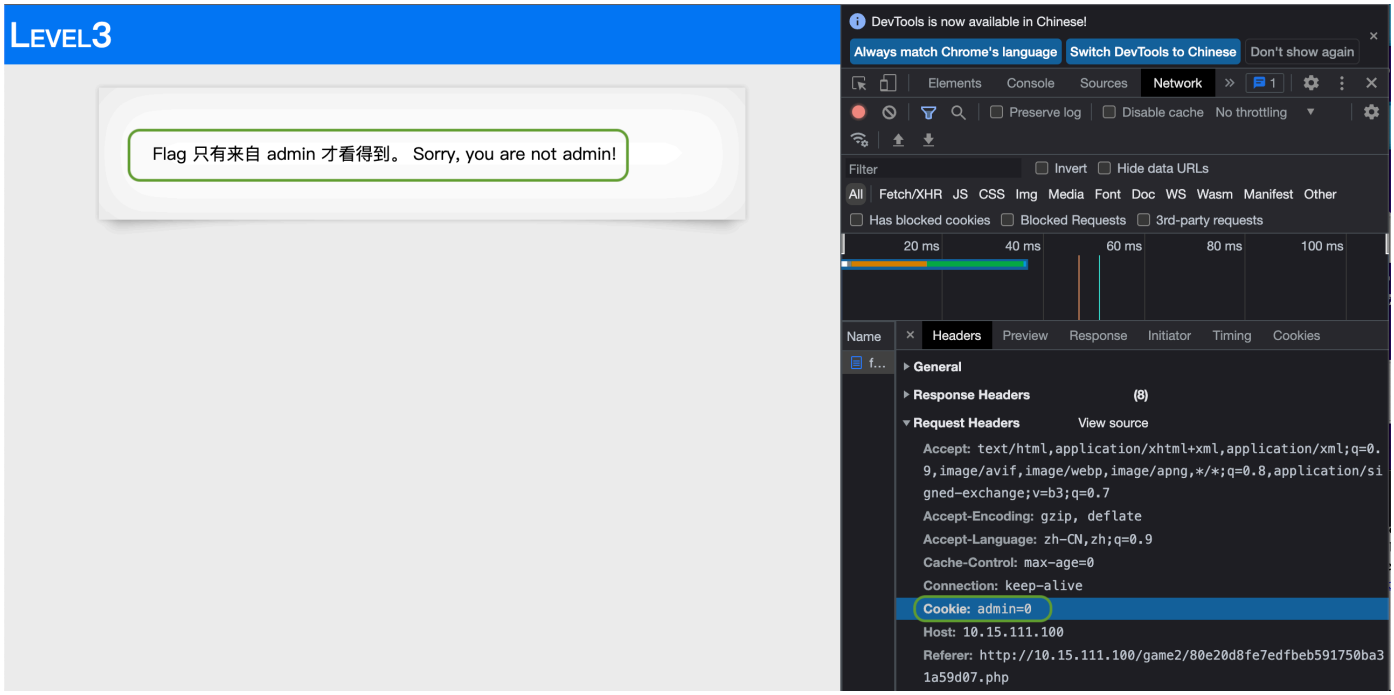
Then, we can get the password in the RESPONSE-packet:



Step 3

> 6. Capture GET-packet and rewrite Cookie field with admin privilege using Burp Suite.

Since the website said that 'only the admin can see the Flag', and the Cookie field fo the GET-packet equals to `admin=0`. We can guess that `admin=1` means the request is from the admin.

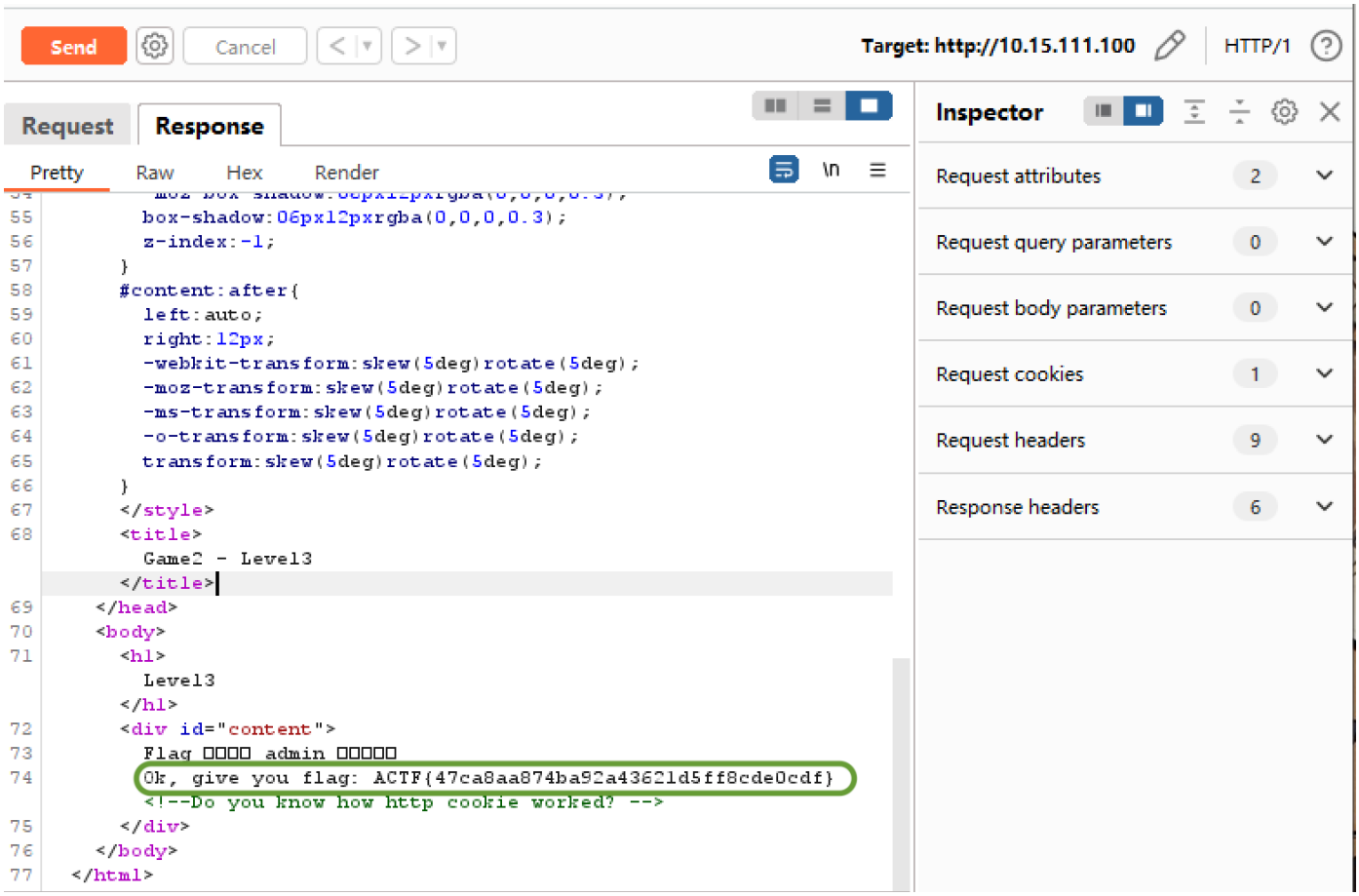


We can rewrite the packet accordingly then:

Pretty Raw Hex \n

```
1  GET /game2/f451899344a962d6d27a73e2902f8e51.php HTTP/1.1
2  Host: 10.15.111.100
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/110.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
   e/webp,*/*;q=0.8
5  Accept-Language:
   zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6  Accept-Encoding: gzip, deflate
7  Referer:
   http://10.15.111.100/game2/80e20d8fe7edfbeb591750ba31a59d07.php
8  Connection: close
9  Cookie: admin=1
10 Upgrade-Insecure-Requests: 1
```

The RESPONSE-packet show the Flag this time:



Thus, the FLAG is ACTF{47ca8aa874ba92a4362ld5ffBedededfl}

3

`http://10.214.160.13:10000`

Step 1

> 1. View page source.

Using F12 to open DevTool and then unfold `<body>` tag, we can discover that `删除1.php.bak` has been commented.

Thus, I try to visit `http://10.214.160.13:10000/1.php.bat`, the content of `1.php.bat` is as follows:

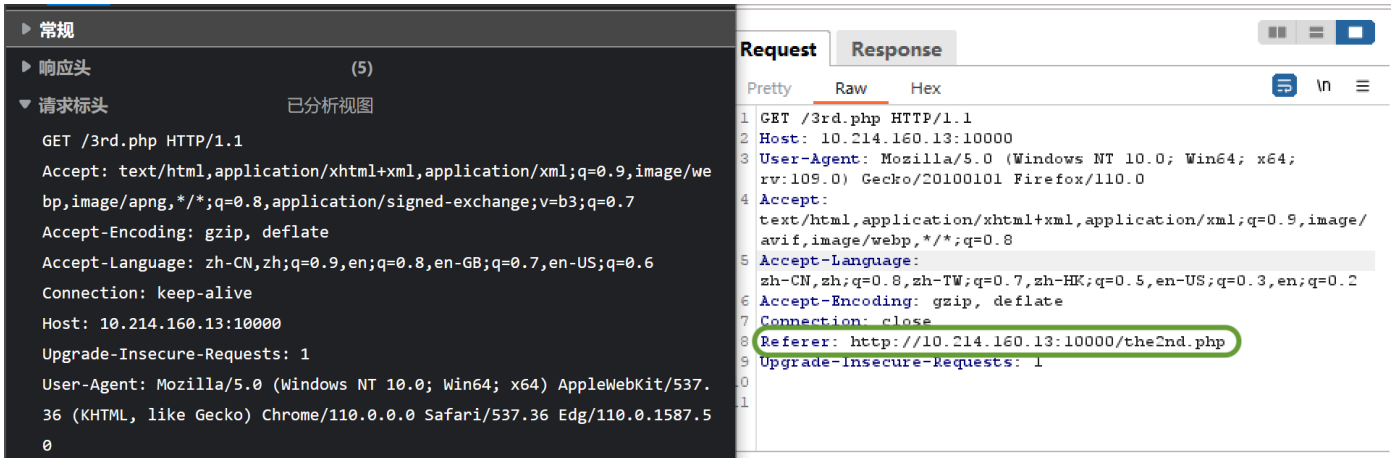
> 2. Get link from `.bak` file.

It seems that the `<a>` tag aiming to redirect us to `http://10.214.160.13:10000/the2nd.php`

Step 2

> 3. Capture GET-packet and null Referer filed using Burp Suite.

In this step, my Firefox browser redirect me to the next step directly, while Chrome show me the alert '你从哪里来？'. Contrasting the difference of two GET-packet, we can guess that the null-referee field might be the cause.



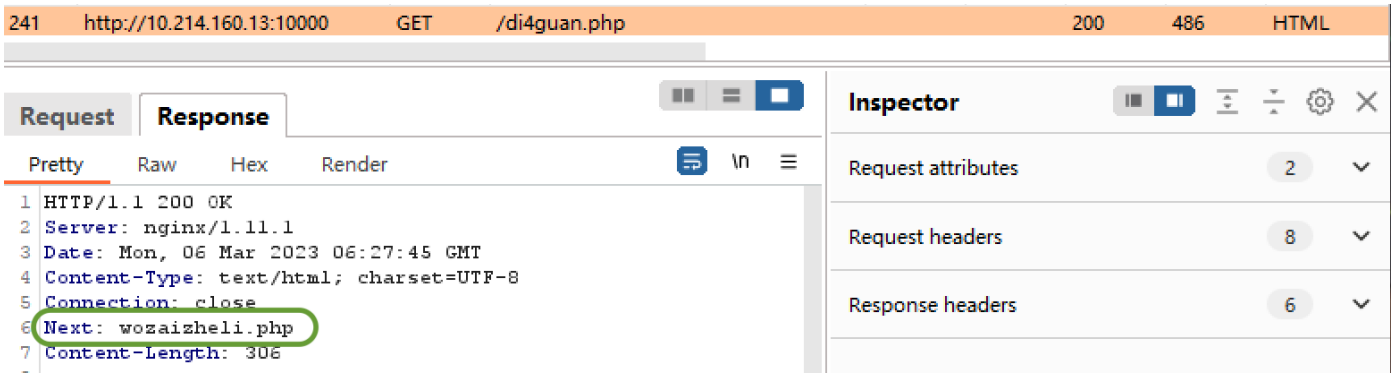
Add correct Referee field to the packet, it leads us to the next step.

Step 3

> 4. Capture RESONSE-packet header with next link included using Burp Suite.

Click the button in `3rd.php`, it direct us to `http://10.214.160.13:10000/di4guan.php` then.

According to the hint, we can view the RESPONSE-packet of `di4guan.php` :



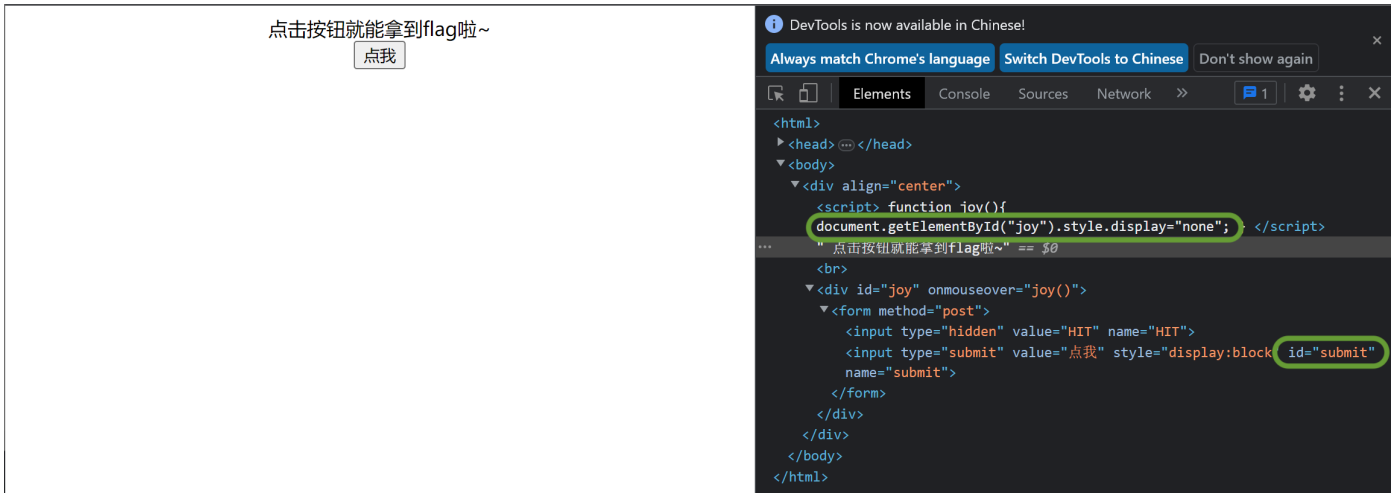
The Next field in the header seems to be the URL of the next step.

Visit `http://10.214.160.13:10000/wozaizheli.php` directly, we can then go to the next step.

Step 4

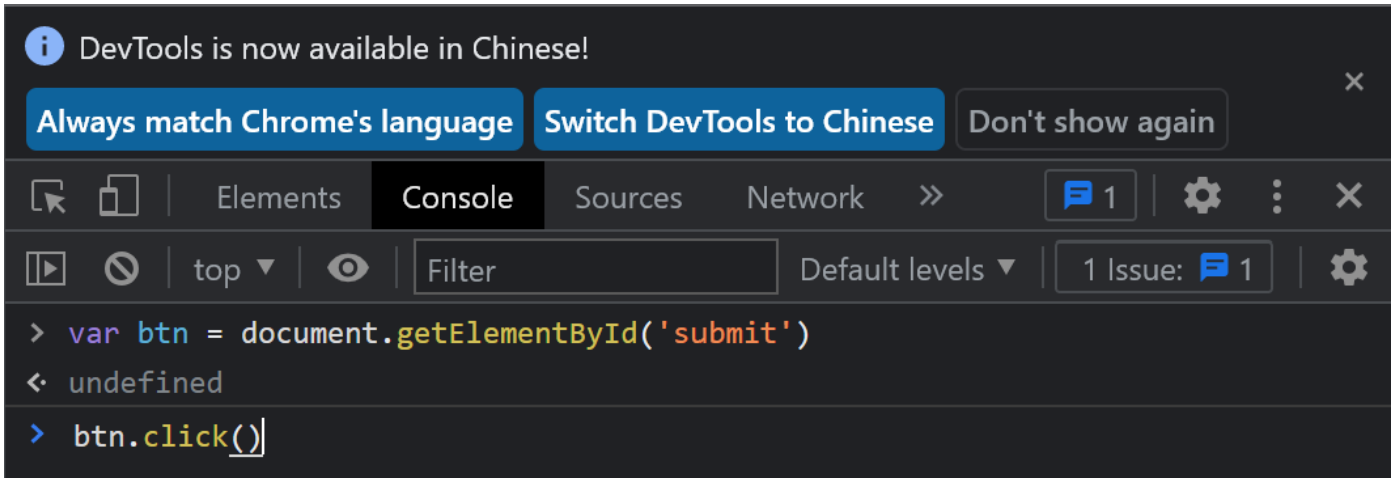
> 5. View page source and try to click the button or craft packet with button click effect.

Function `joy()` add style `display:none` to `#joy` when the mouse is over this element.

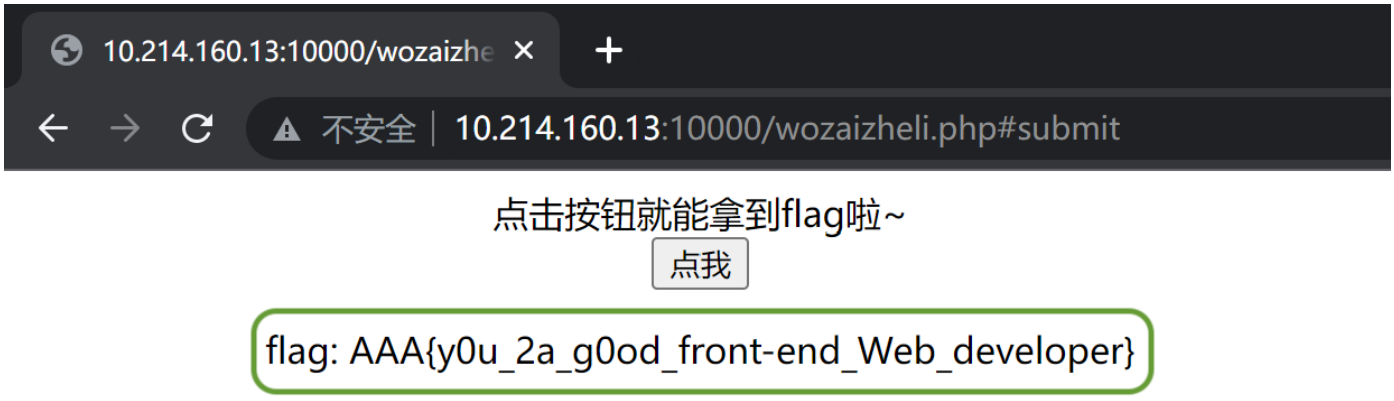


Since modifying the JS in DevTool wouldn't work this time, I try to trigger the click event in the console this time:

1. Get the submit button by its Id.
2. Trigger the click event of the button.



We can finally get the Flag from the website:



Thus, the FLAG is AAA{yOu 2a gOod front-end Web developer}