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:

学　　院: 计算机科学与技术学院

系: 计算机科学与技术系

专　　业:

学　　号:

指导教师: 卜凯

2021 年 3 月 21 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. Requirements

Find the flag hidden in the pages.

2. Environments

Browser: Chrome version 89.0.4389.90

System: MacOS Catalina

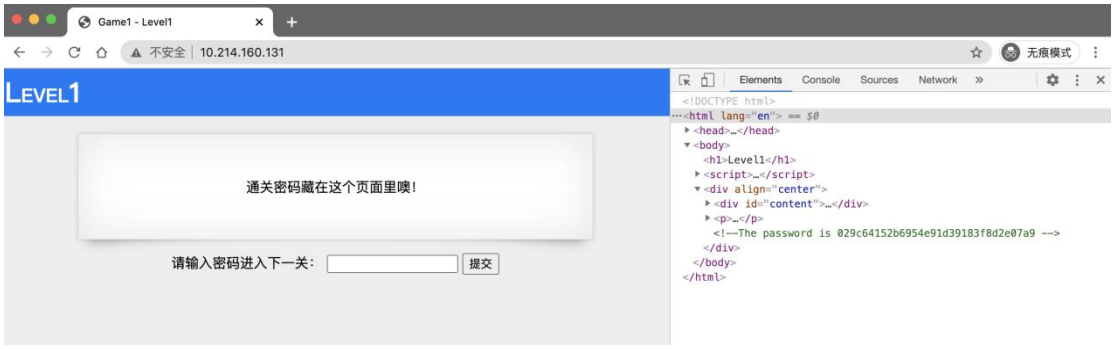
3. Processes

3.1 Part 1

Click the link and jump to a new page:

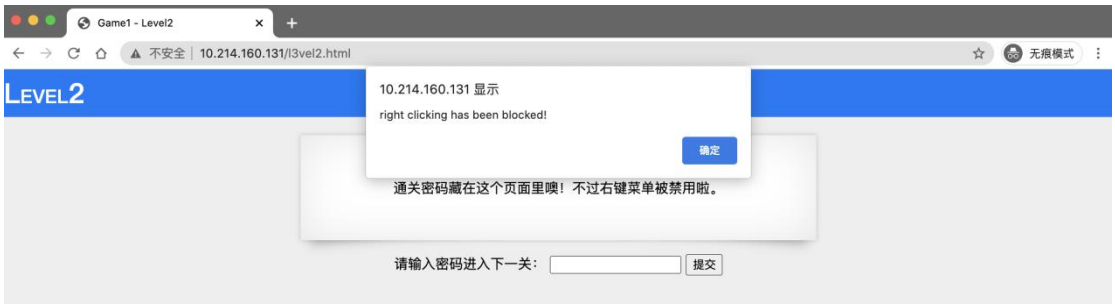
Chrome has supplied us a useful tool to know more information about pages.

Open the right click menu and select “check” to open the developer tools:

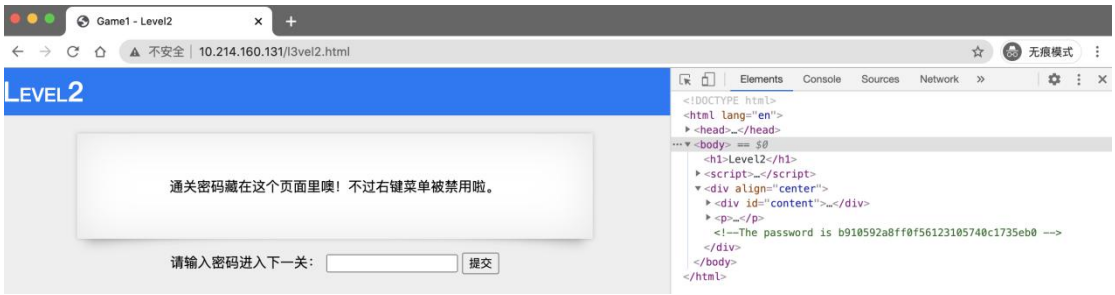


Then the password of the first level is shown as a comment of the HTML text.

When it comes to level2 we find the right clicking has been blocked.

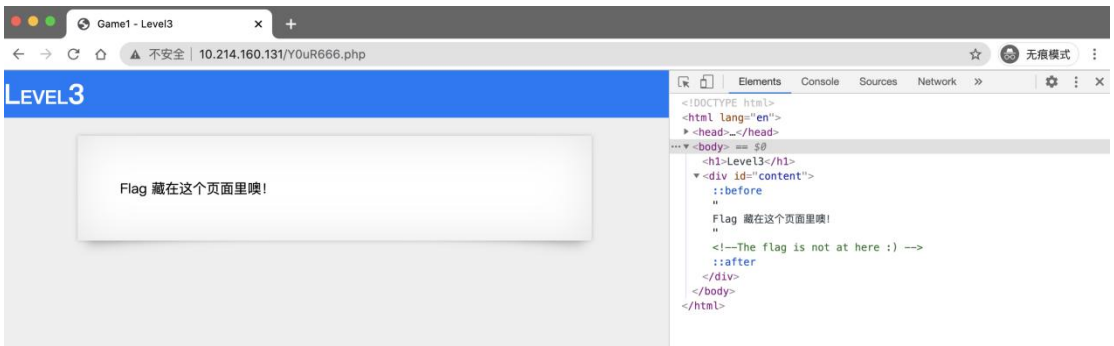


But we can open the developer tools through its hot key, F12.

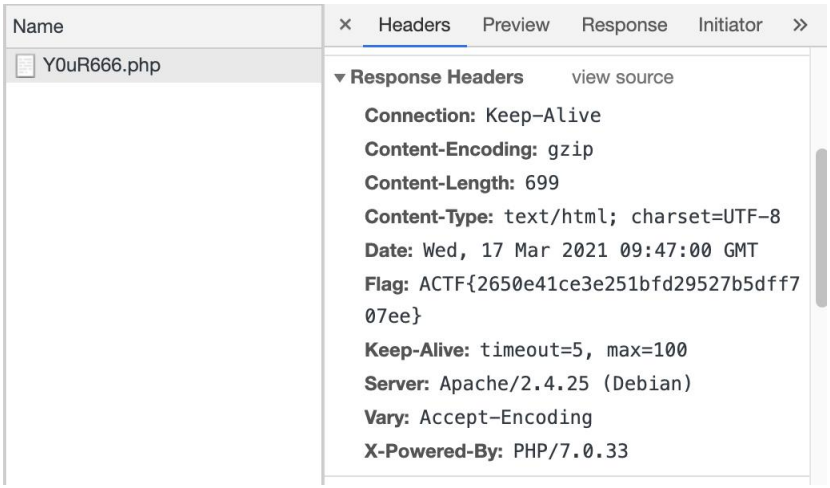


And the password is shown as a comment, too.

When it comes to the third level the flag is not hidden in source code but in the current page yet.

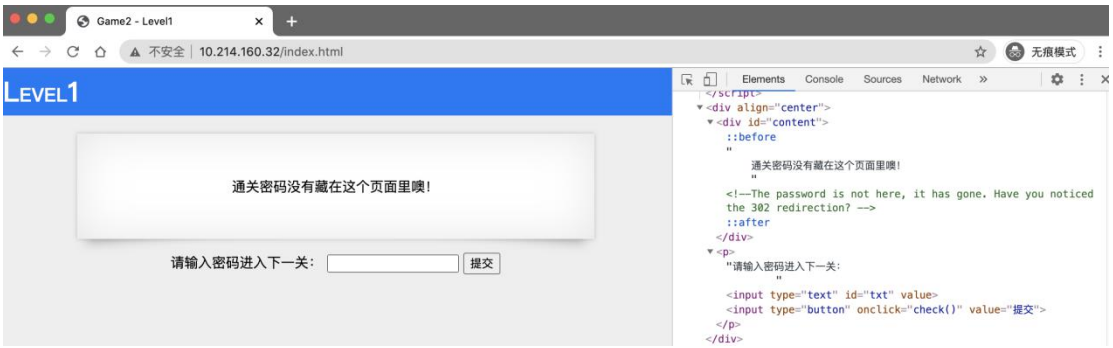


Fortunately we can find it in the response header.



3.2 Part 2

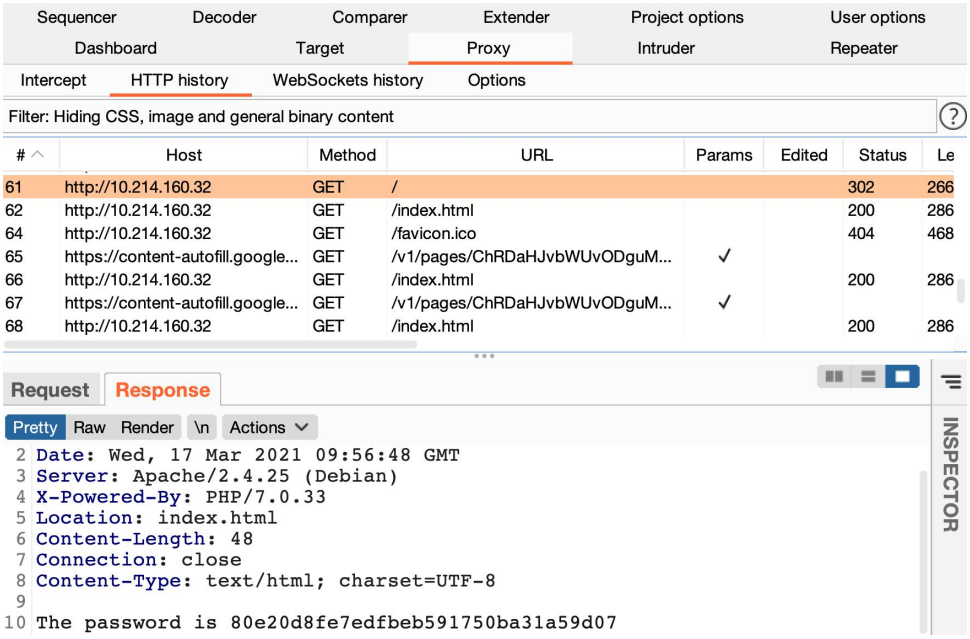
Click the link and the browser comes to a page like that in part1.



From the comment we get the hint “302 redirection”.

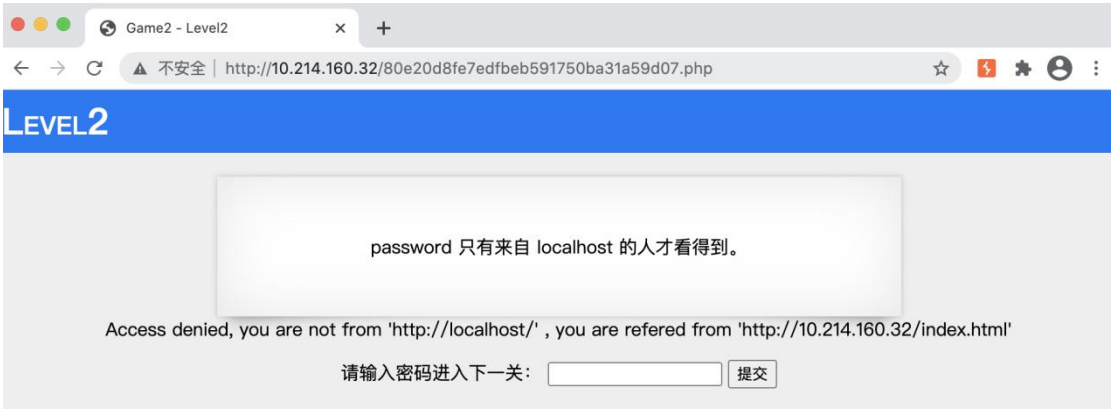
We can only see the page without password because the truly useful page is redirected soon. We can use Burp suite to see the whole process and the details of TCP packets.

Burp Suite supplies a function which records the requests history and the according responses, then we can see the details of the redirection.

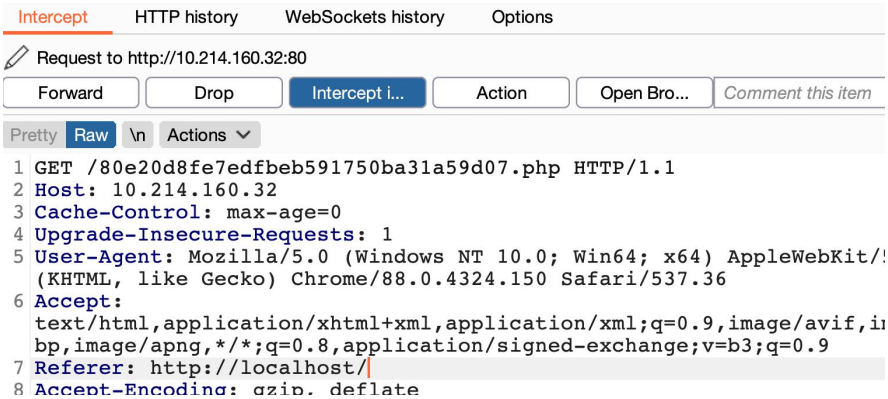


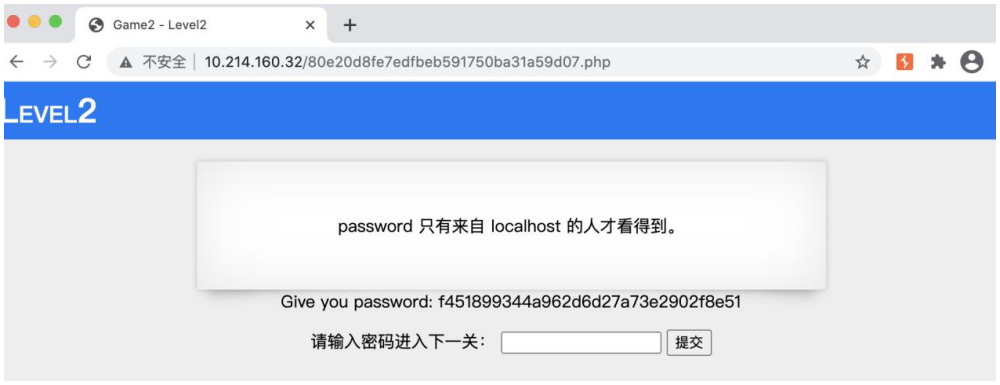
The password is hidden in the response header of the 302 redirection.

Enter the password and come to level 2.

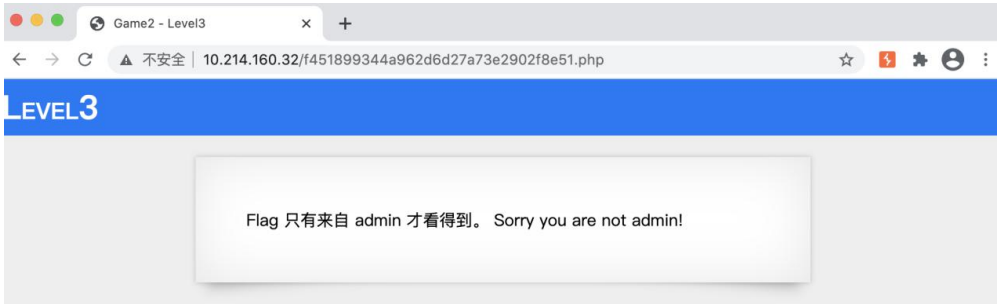


Since the page says we need to access the password from “http://localhost/”, we can intercept the request packet and modify the “referrer” field before forward it.

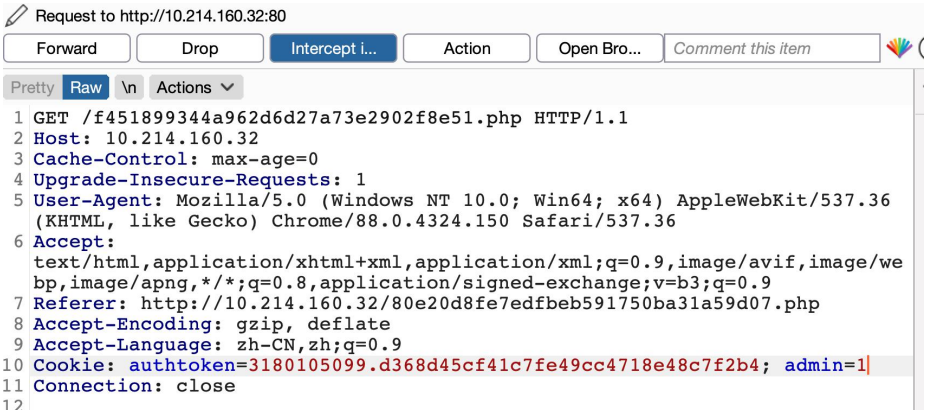


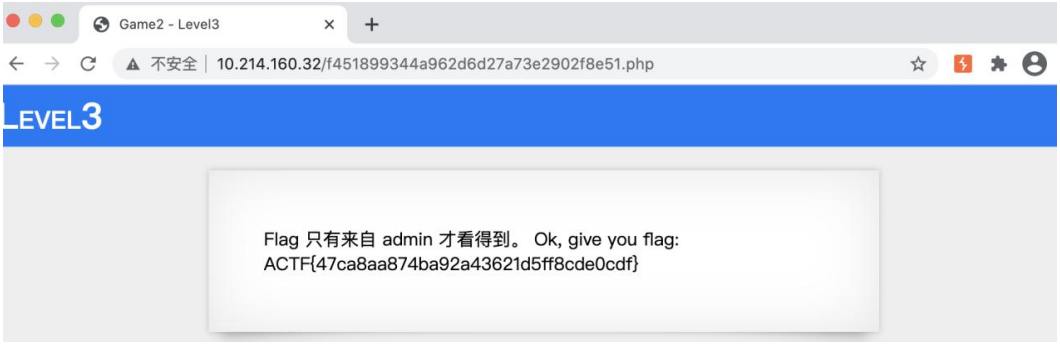


When we try to find the flag it says that flag can only be seen by admin, then we can attempt to fake our identity to be admin.



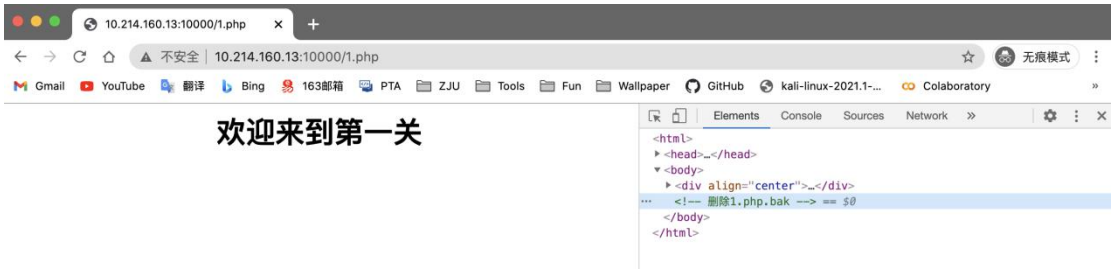
After modify the "admin" segment to 1 instead of 0, and forward the packet, the server has already regard us as admin and gives the flag.





3.3 Part 3

Open the link and the develop tools first, and from the comment in the source code we can get the hint “1.php.bak”.



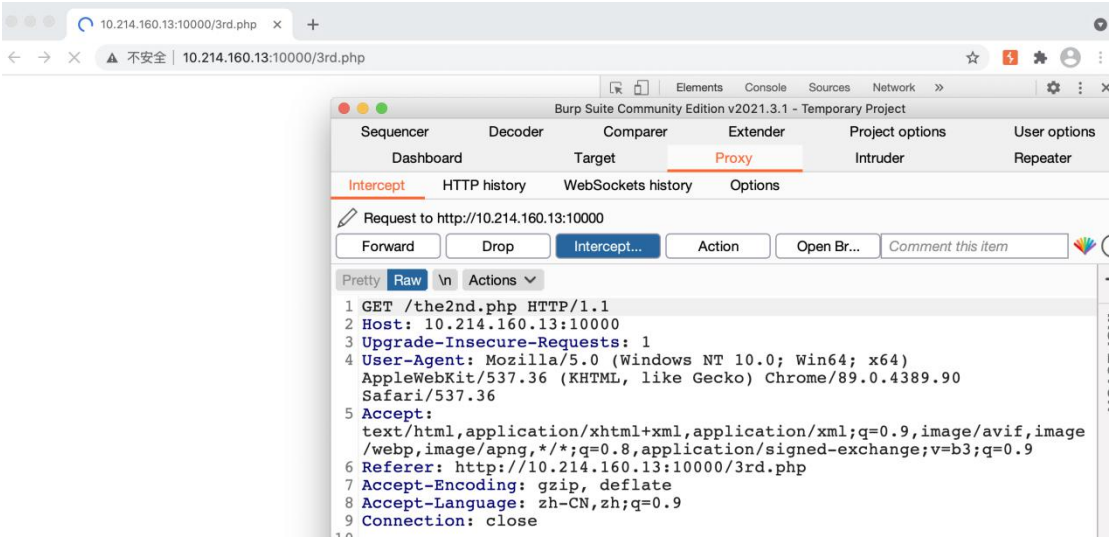
Some developers will forget to delete the backup files before deploying their project, it seems that we can exploit this point.

Visit “1.php.bak” from the address bar, and we can get a file named “1.php.bak”.

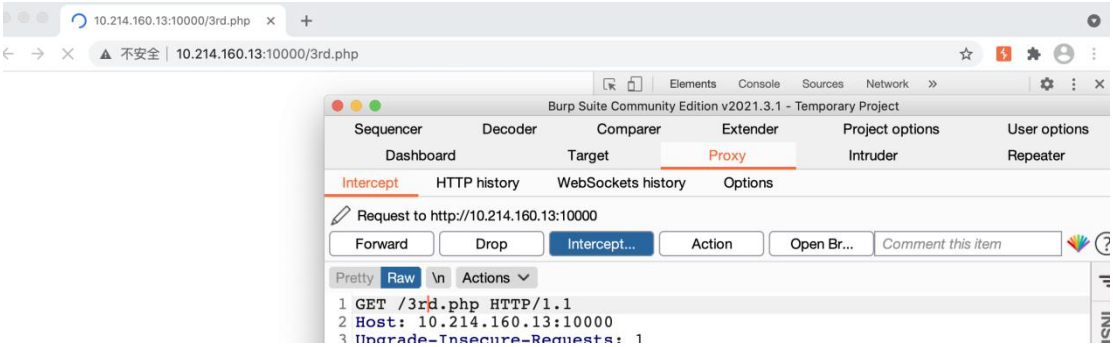
From the file we can get that the next checkpoint is “the2nd.php”.

But we can access the third checkpoint directly from the second checkpoint because the page will jump back to “the2nd.php” automatically.

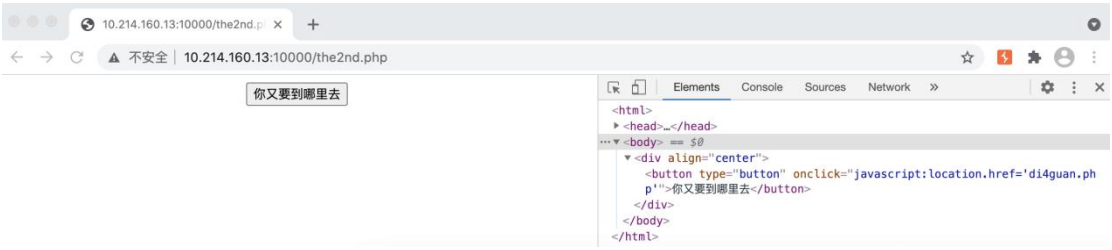
Reopen the page in Burp Suite, and we can see there is a request to jump back to the second page.



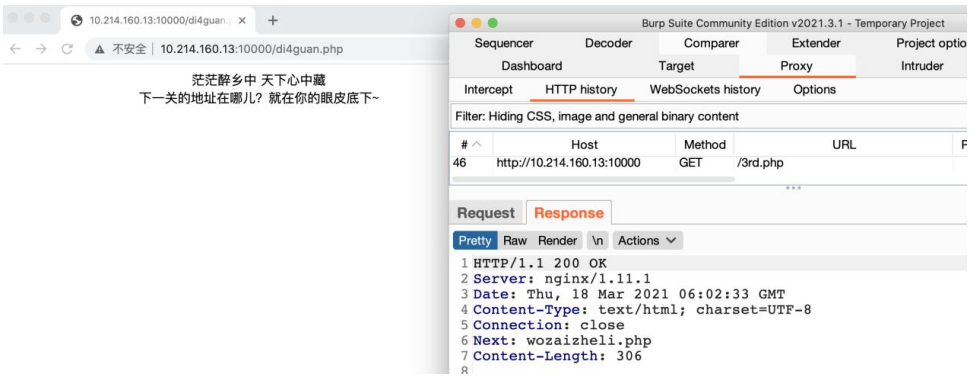
Modify the request packet and forward it.



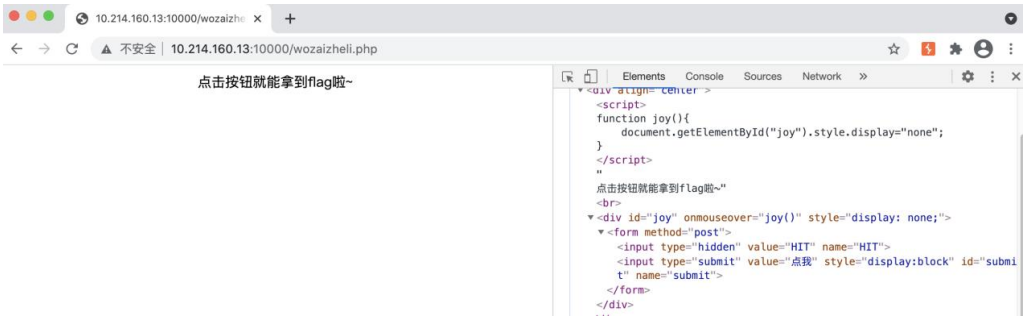
And we can see the third page.



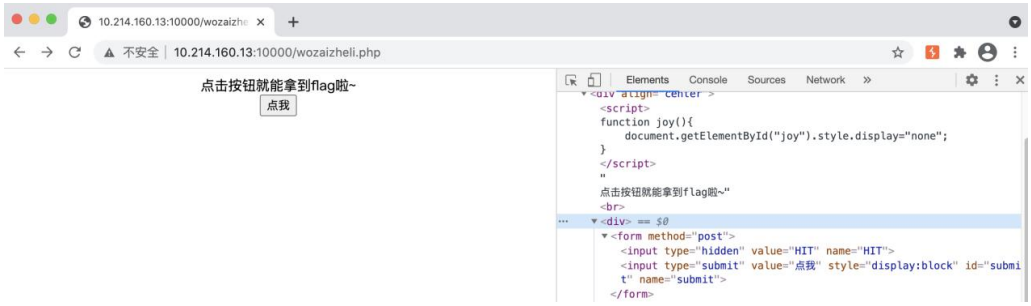
From the response packet of the fourth page, we can find the address of the fifth checkpoint.



When we attempt to click the button to get the flag, it just disappears, and we can see the style of the form is set to “display:none”.



This owns to the script function “joy”. Since it is just run on the page, we can modify the source code to disable it.



And click the button, the flag appears out.

flag: AAA{y0u_2a_g0od_front-end_Web_developer}

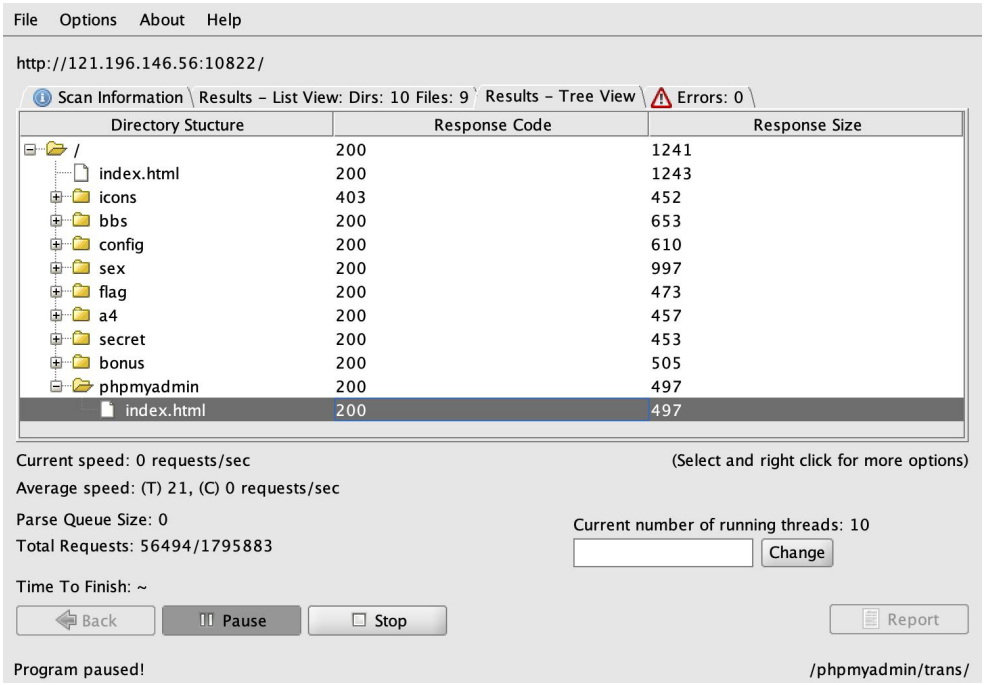
3.4 Part 4

Scan ports on the server using Nmap.

```
➜  ~ nmap zju.tools -p 9000-11000
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-18 14:15 CST
Nmap scan report for zju.tools (103.205.8.47)
Host is up (0.11s latency).
Not shown: 1999 closed ports
PORT      STATE    SERVICE
9996/tcp  filtered palace-5
10822/tcp open     unknown
```

The only open port is 10822.

Scan directories on “http://121.196.146.56:10822/” using DirBuster.



Visit “http://121.196.146.56:10822/phpmyadmin/index.html” and get the flag.

4. Experience and Thinking

All problems are easy and interesting and I get a lot from them.

The first challenge introduces the develop tools supplied by the browser; the second challenge is mainly about the basic usage of Burp Suite and trivial HTTP knowledge; the third challenge is about HTTP request and response; the fourth challenge is about port scanning and directory bursting.

After finishing these four problems, I have learned a lot about Network Security. Hope to do better in the following studying.