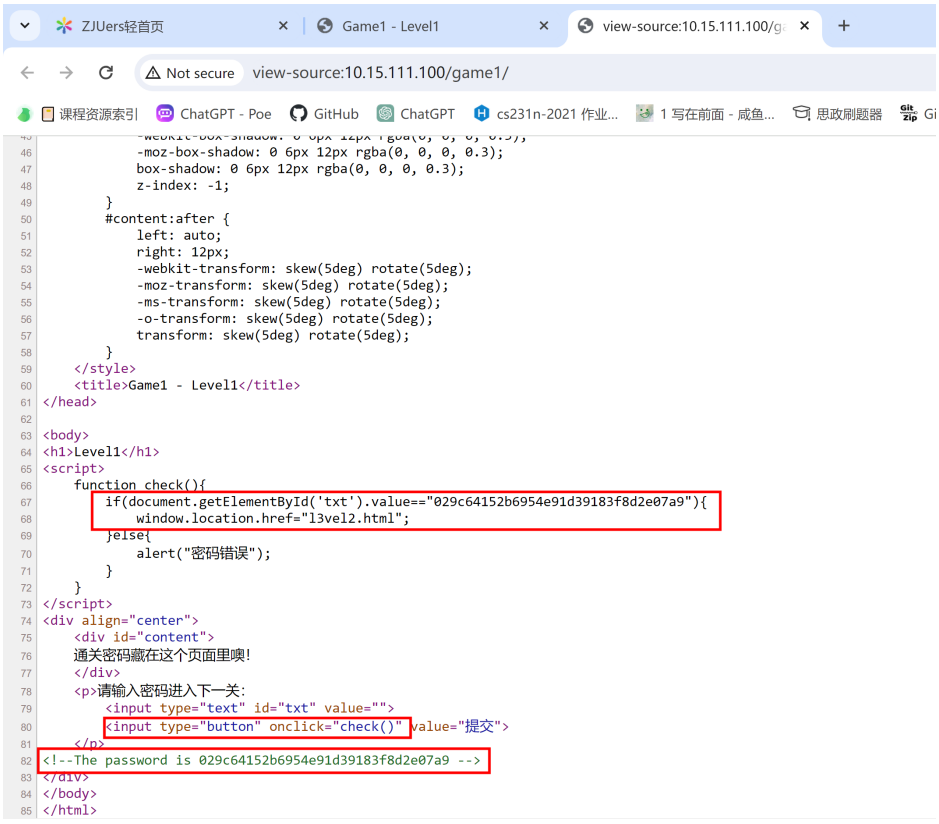
浙江大学实验报告

课程名称：网络安全原理与实践

实验名称：Lab 01

1 Task1

We press F12 to use the developer tools of the browser and get the HTML code of the website below. We mark several useful information with red blanks.



From comment info, we can know the password is

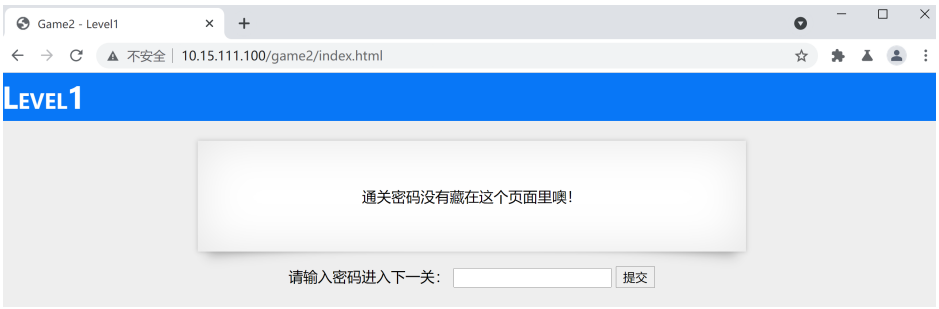
029c64152b6954e91d39183f8d2e07a9

If we enter the password, we can go to the next level:

If we check the onclick function of the button, we can find check(), which compare the input string with a literal(the correct password).

We can also see that when the password is correct, browser will access l3vel2.html referenced by the hypertext reference href. So we can also directly visit l3vel2.html, and we will get a same result.

2 Task2

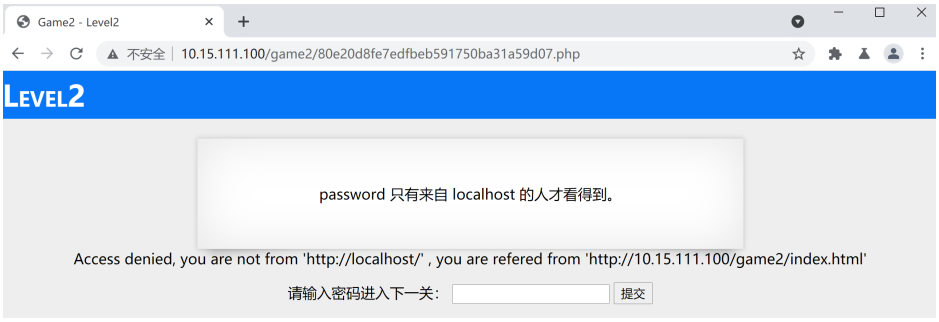


We use Burp to capture the 302 redirection packet and find the password in the response packet. A 302 redirect is a temporary redirect used by web servers to tell a browser that the requested resource has been temporarily moved to a new location. The browser will then automatically redirect to the new URL, but will continue to use the original URL for subsequent requests.

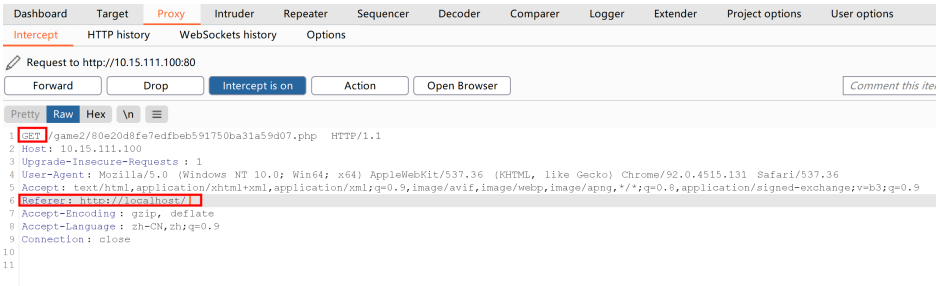
From response info, we can know the password is

80e20d8fe7edfbeb591750ba31a59d07

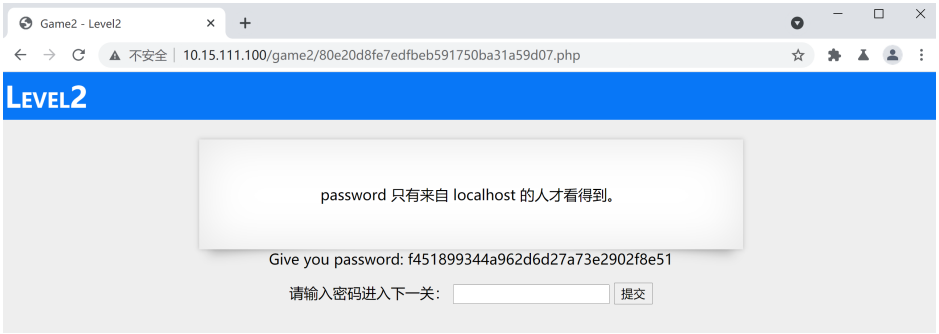
If we enter the password, we can go to the next level:



Because we are not visit from localhost. Then we should modify the Referer in the request packet to pretend that we are from localhost as follows:



after that, we get the password2:

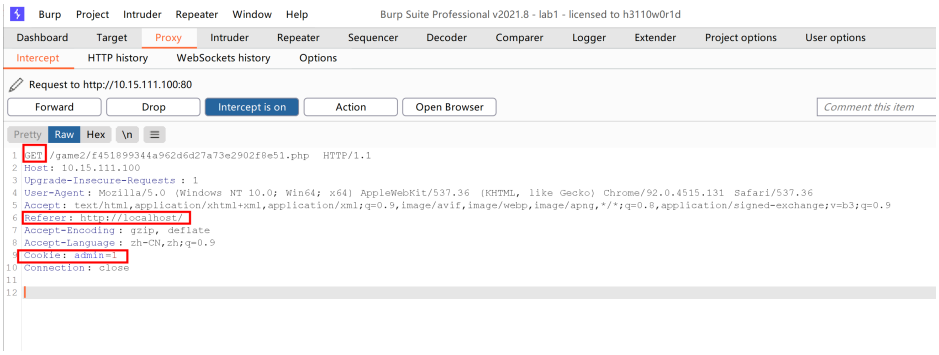


From plain info, we can know the password is

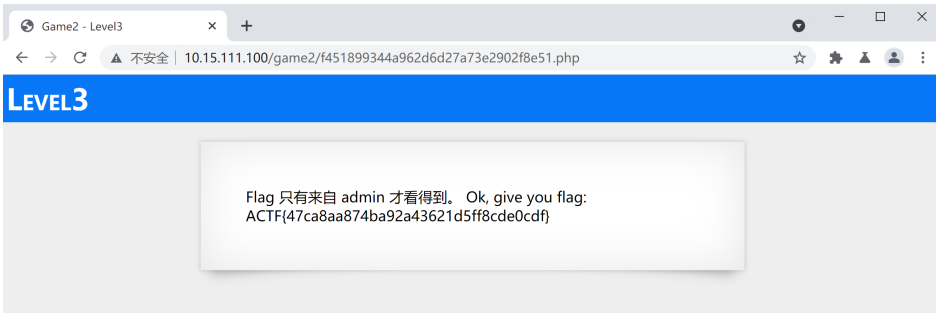
f451899344a962d6d27a73e2902f8e51

If we only enter the password, we can go to the website as follows:

Because we are not admin. Then we should modify the cookie in the request packet to pretend that we are admin as follows:



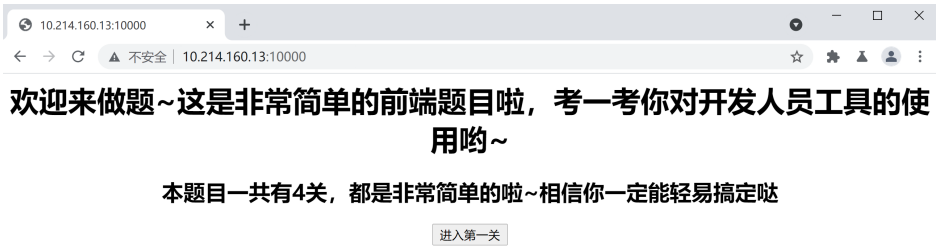
Then we can get the flag of task 2.



From plain info, we can know the flag is

ACTF{47ca8aa874ba92a43621d5ff8cde0cdf}

3 Task3



After we press the button, we can get the page:

To get the url for next level, we add ".bak" after "1.php" to get the bak file.

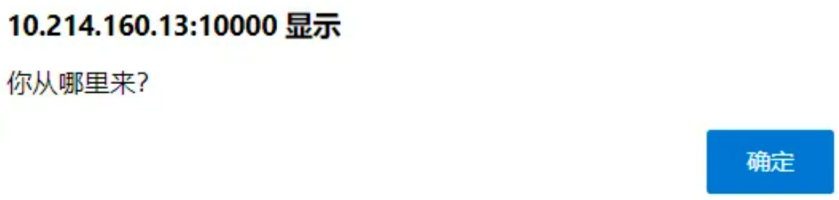
In the bak file, we can get "the2nd.php" is next url:

1.php.bak - 记事本

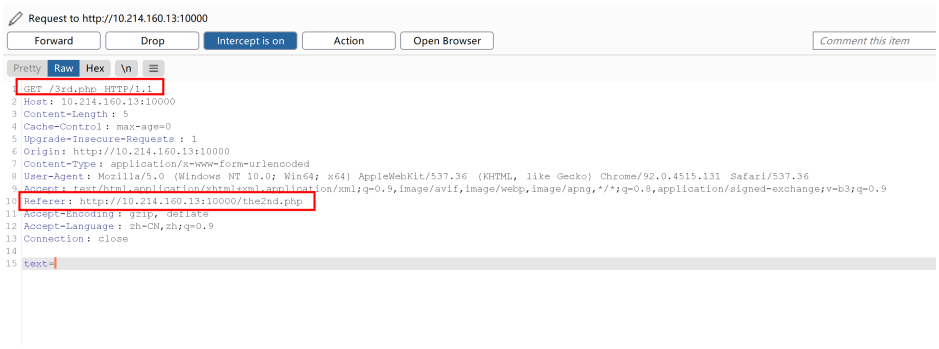
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<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">
<h1>欢迎来到第一关</h1>
</div>
<!-- 删除1.php.bak -->
<a href="the2nd.php">进入第二关</a>
</body>
</html>
```

When we press the button, we will visit "3rd.php", but it shows an alert and send us back:



Then we can modify the request packet to pretend that we are at "the2nd.php" and we want to get "3rd.php".



After that, we can get another page:

When we press the button, we can get the next url information("wozaizheli.php") as follows since we look into the response packet carefully.

But when we first try to press the button, it disappears. Then we modify the " " in the HTML source code with developer tools, so that we can disable the onmousemove event. Once the onmousemove event is disabled, the button will not disappear when we click it.

Figure 1: disable the onmousemove event

Finally we get the result after F5:

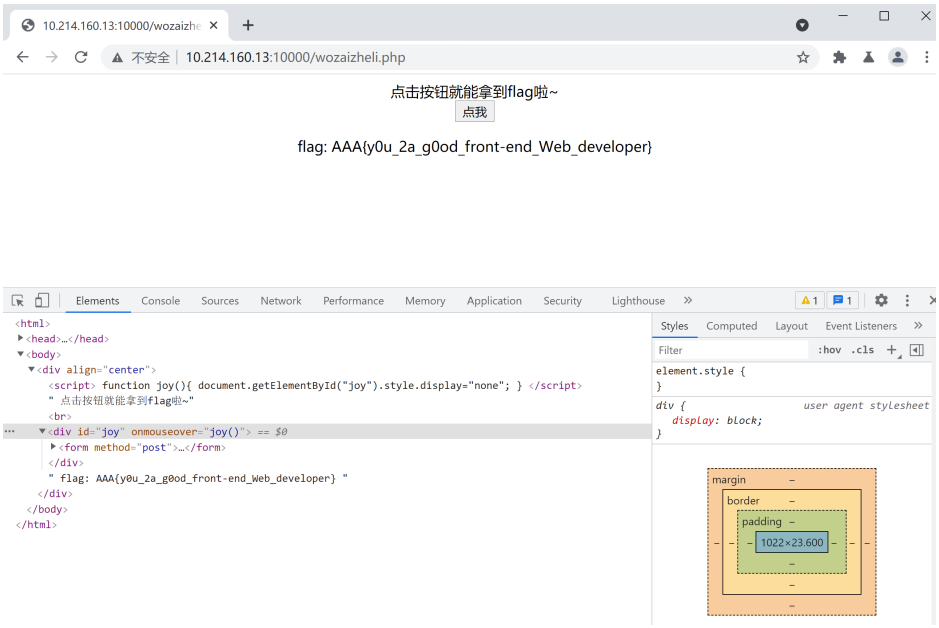


Figure 2: disable the onmousemove event

From plain info, we can know the flag is

AAA{y0u_2a_g0od_front-end_Web_developer}