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：卢佳盈

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：3180103570

指导教师：卜凯

年　　月　　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

实验要求：Lab 01 aims to practice commonly used tools for packet sniffing, packet crafting, and port scanning.For packet sniffing and packet crafting, we use basic web exploitation CTF challenges for example. Solving these challenges helps to understand the HTTP protocol and technologies involved in information transfer and display over the internet like PHP, CMS's (e.g.,Django), SQL, Javascript, and more.For port scanning, we use Nmap to determinewhich ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

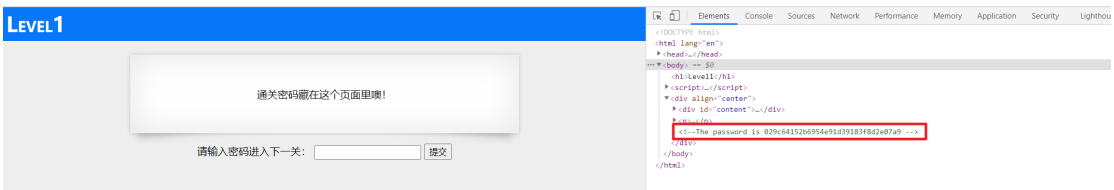
实验过程：

1.https://actf.lol/challenges#Game1-97

Level 1

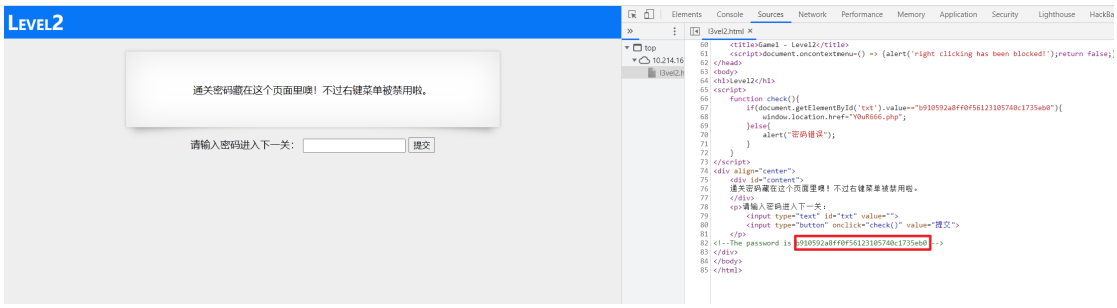
Check the source code to get the level 1 password:

029c64152b6954e91d39183f8d2e07a9



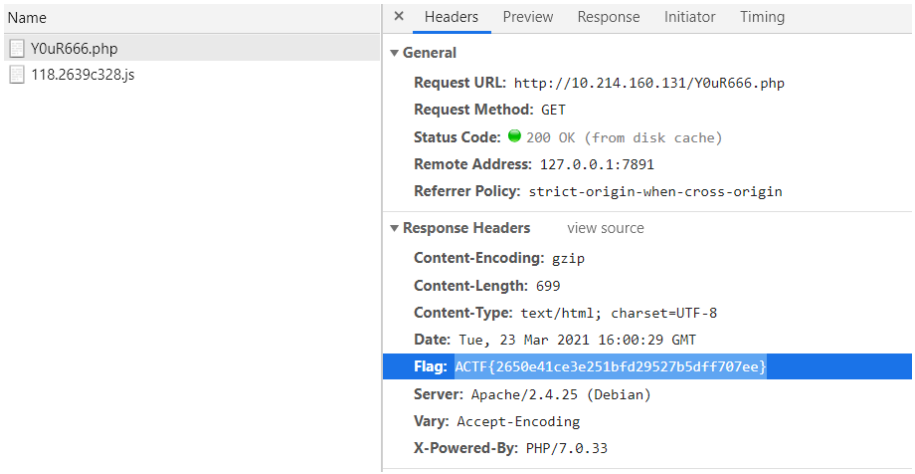
Level 2

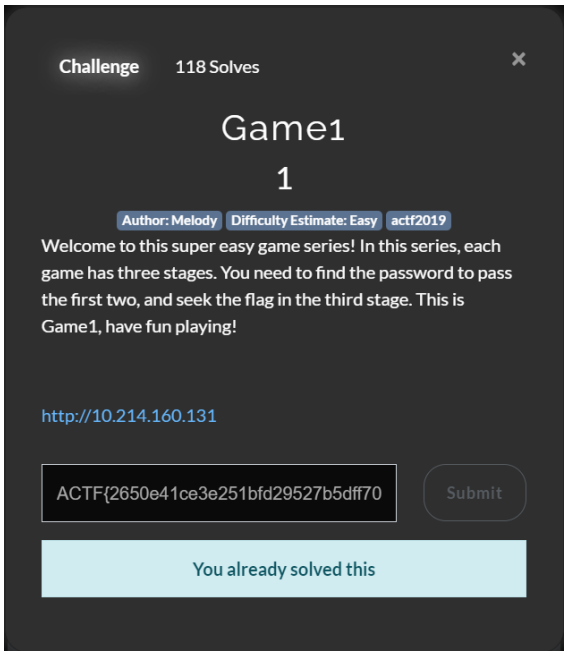
Page disable right-click, so F12 shortcut to open the source code. Get level 2 password: b910592a8ff0f56123105740c1735eb0



Level3

Find flag in source file: ACTF{2650e41ce3e251bfd29527b5dff707ee}





2.https://actf.lol/challenges#Game2-98

Level1

Enter it on the command line, where authentic comes from the authentication

information of the original web page

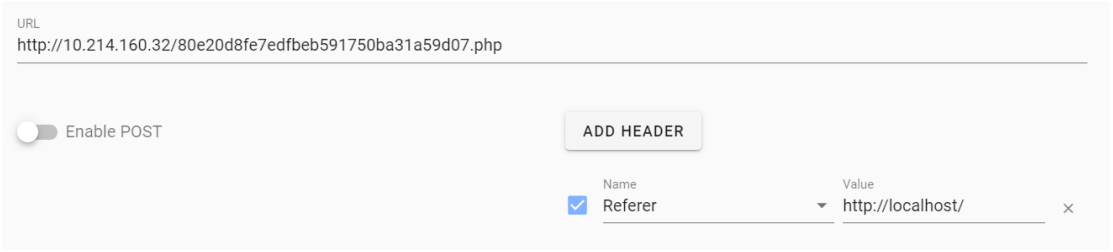
```
C:\Users\ljy28>curl http://10.214.160.32/index.php --cookie "authtoken=3180103570.cf0d686dd25fd7f8d0b8ecf08b706aeb"
The password is 80e20d8fe7edfbeb591750ba31a59d07
```

得到密码：80e20d8fe7edfbeb591750ba31a59d07

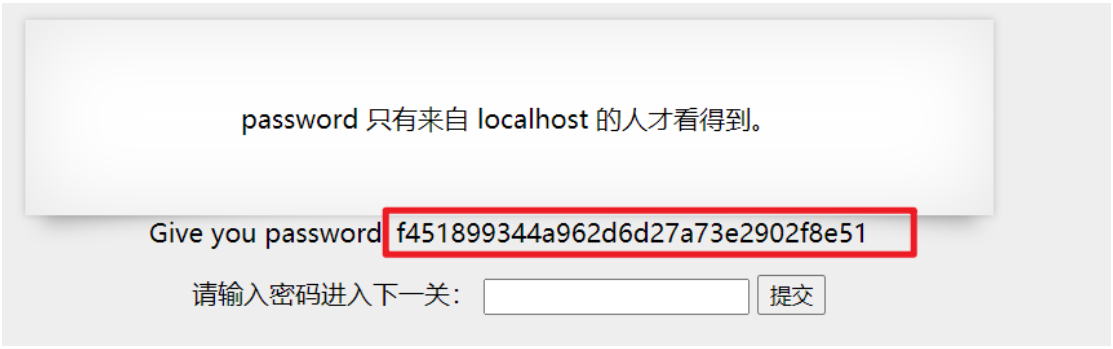
Level2

It can be seen from the page prompt that my referer is not localhost at this time, so I need to forge my own referer

Using the hackbar tool, the configuration is as follows

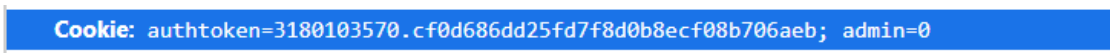


The password will pop up in the page: f451899344a962d6d27a73e2902f8e51

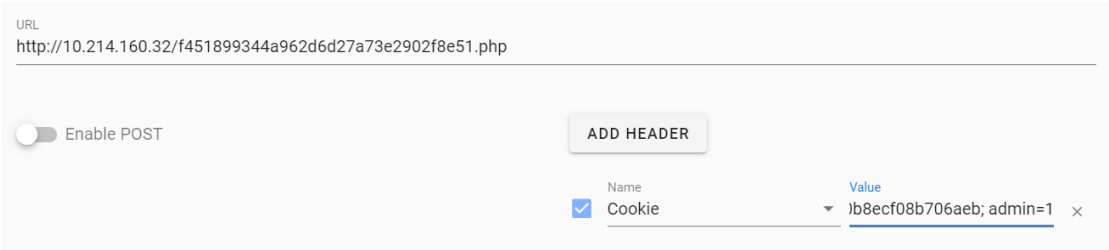


Level3

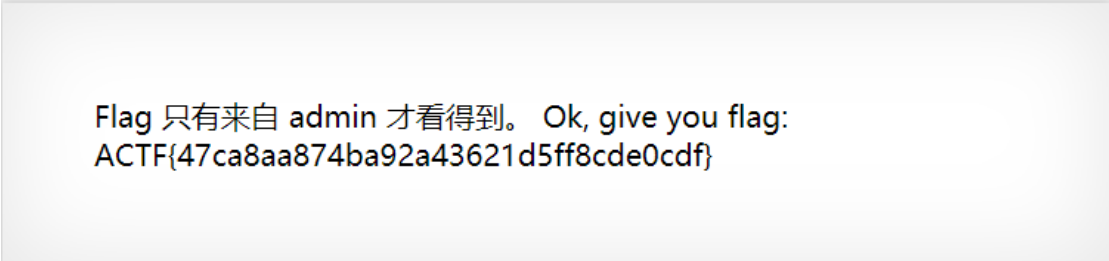
The webpage prompts us to pay attention to admin. From the source code, we can see that in the cookie attribute, our admin is 0

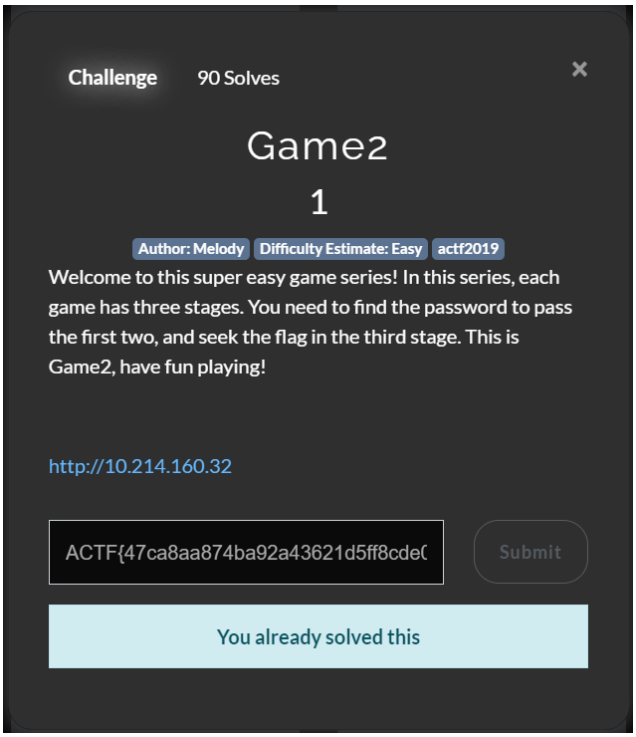


To be admin, we use the hackbar tool, which is configured as follows



We can get flag: actf {47ca8aa874ba92a43621d5ff8cde0cdf}





3. https://zjusec.com/play?q=19

Level1

Prompted by the source code, through the path http://10.214.160.13 :10000/1. php.bak

Download bak file

```
<html>
<head>
  <meta http-equiv="Content-Type" cont
  <meta http-equiv="Content-Language"
</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>
```

You can see that the page will jump to the2 nd.php page

enter path http://10.214.160.13 :10000/the2 nd.php Go to the next level

Level2

Click the XSS button, and you can see that the source code is likely to change

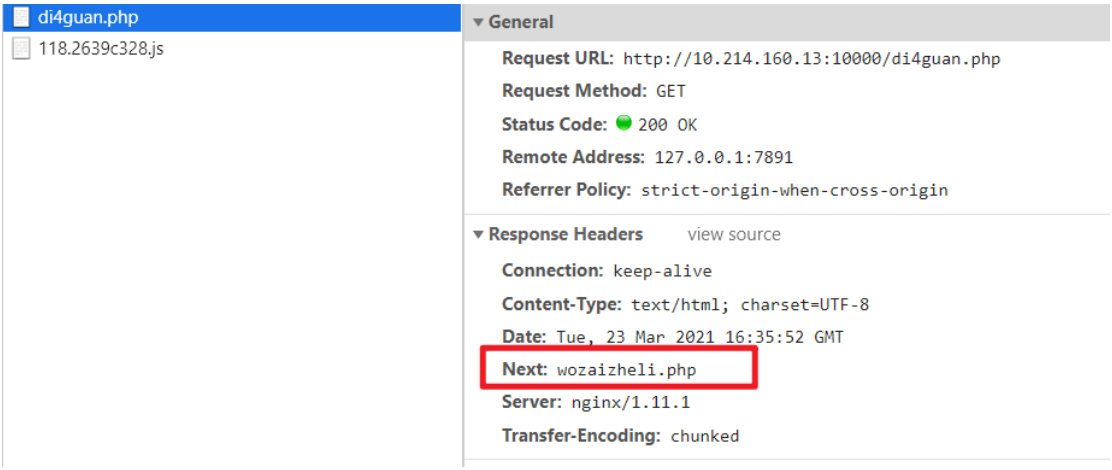
```
<div align="center">
<form method="post">
<input type="text" name="text">
<input type="submit" value="点击进入第三关">
</form>
    jumping...
    <script>
        function jump(url){
            document.body.appendChild(document.createElement('iframe')).src='javascript:"<script>top.location.replace(\''+url+'\')<\/script>"';
        }
        setInterval("jump('3rd.php')",2000);
    </script>
    </div>

</body>
</html>
```

Click the XSS button, and you can see that the source code is likely to change

Level3

As you can see from the source code, the next page is wozaizheli.php

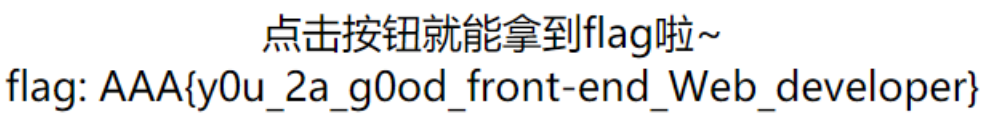
Through the path http://10.214.160.13 :10000/ wozaizheli.php Make a jump



Level4

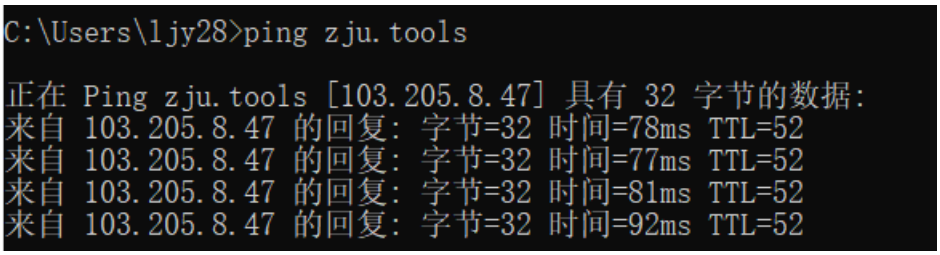
Delete the element action under OnMouseOver action, and then click the button on the page

get Flag：AAA{y0u_2a_g0od_front-end_Web_developer}

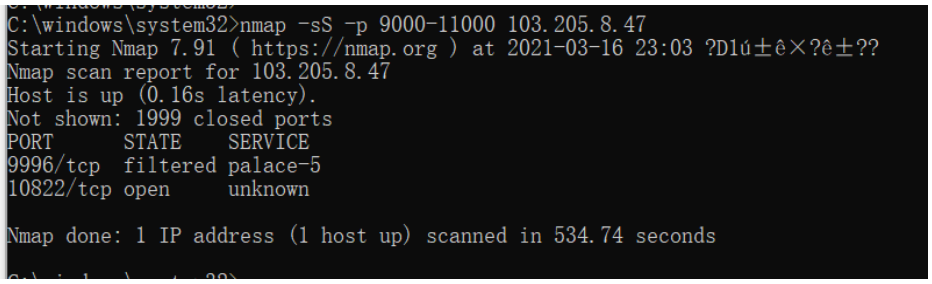


4. https://zjusec.com/play?q=2

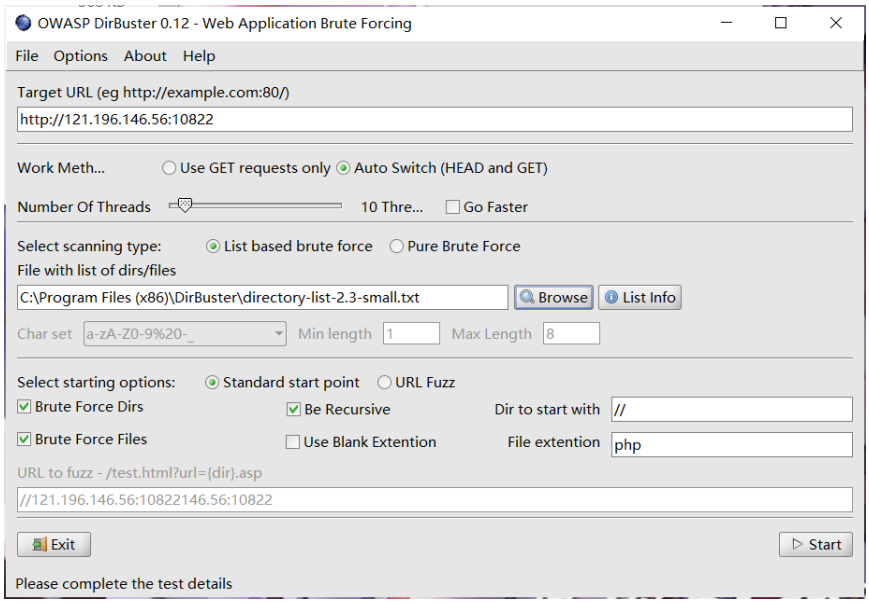
Ping to know zju.tools IP address of (103.205.8.47)



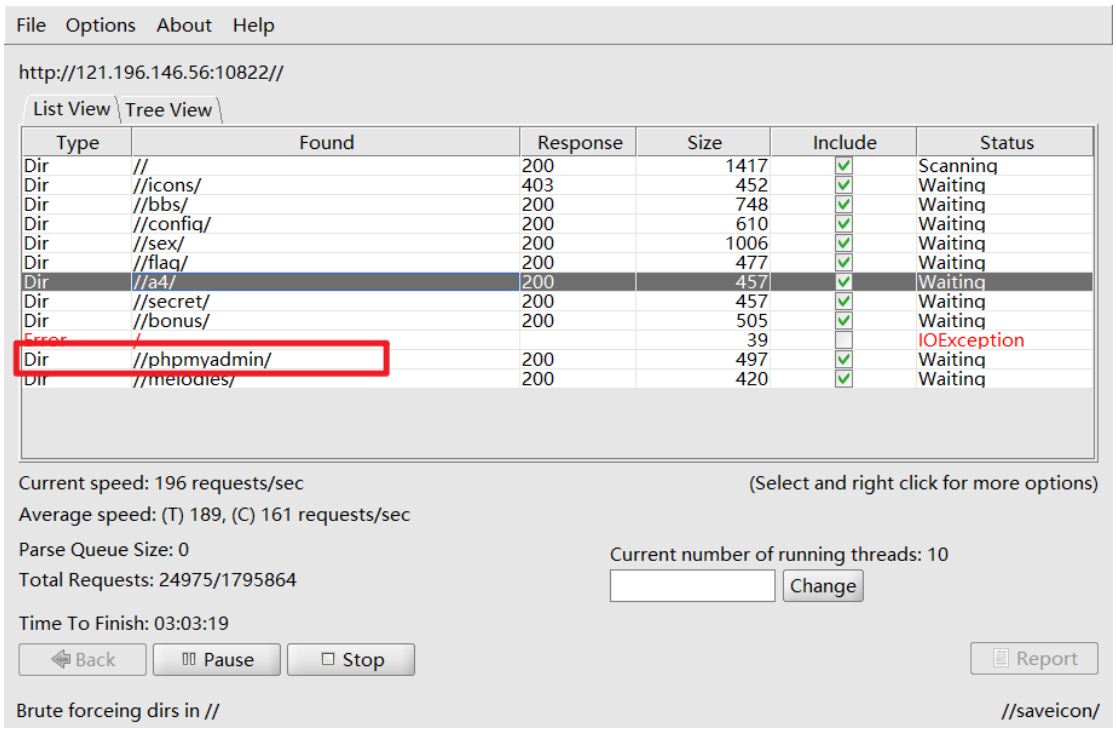
Find the target port 10822 under this IP



Scanning with dirbuster http://121.196.146.56 : 10822 contents



Enter the scanned directory in turn and find that the password is in / phpMyAdmin



Key is: AAA{Earth_Three-body-Organization}

Flag

AAA{Earth_Three-body-Organization}