

# 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 determine which 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.

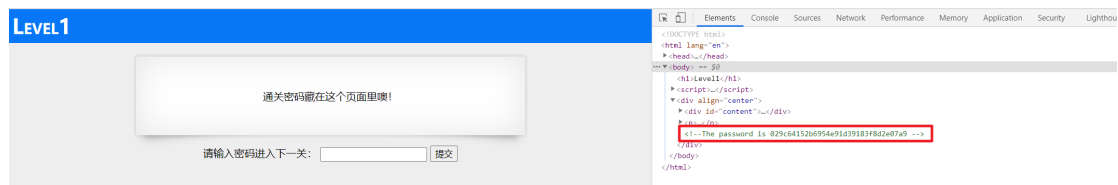
实验过程：

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

### Level 1

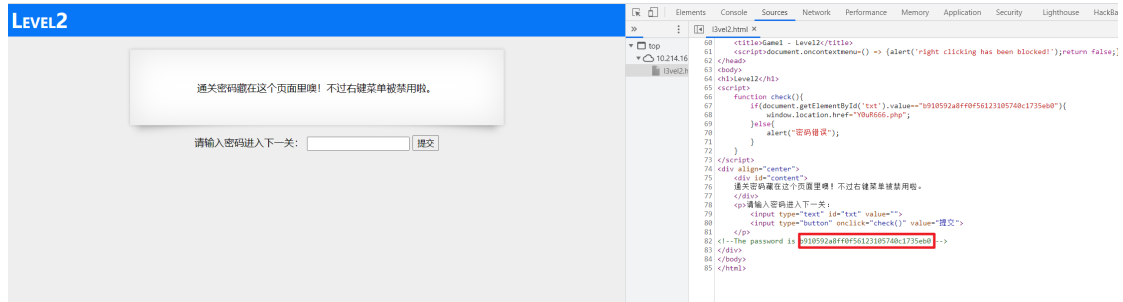
Check the source code to get the level 1 password:

029c64152b6954e91d39183f8d2e07a9



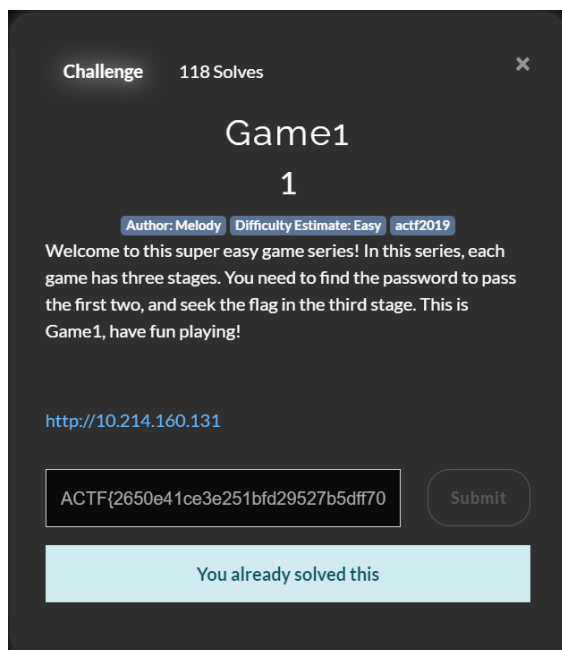
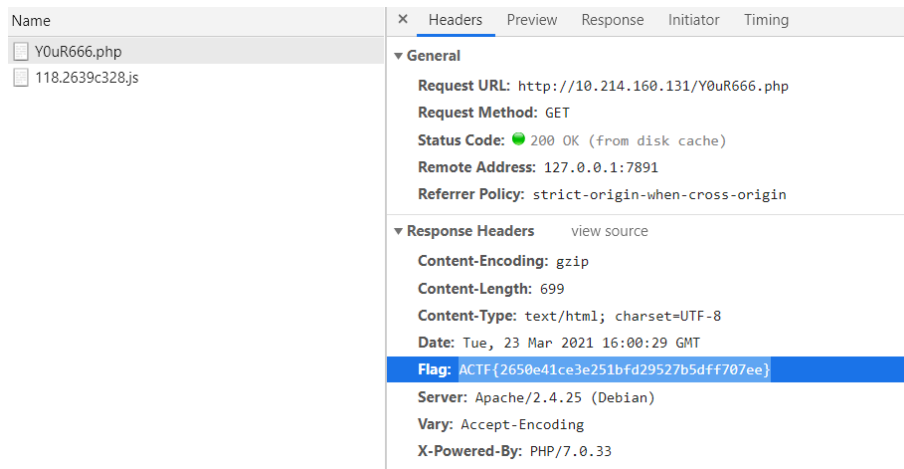
### Level 2

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\lly28>curl http://10.214.160.32/index.php --cookie "authtoken=3180103570.cf0d686dd25fd7f8d0b8ecf08b706aeb"
The password is 80e20d8fe7edfbeb591750ba31a59d07
```

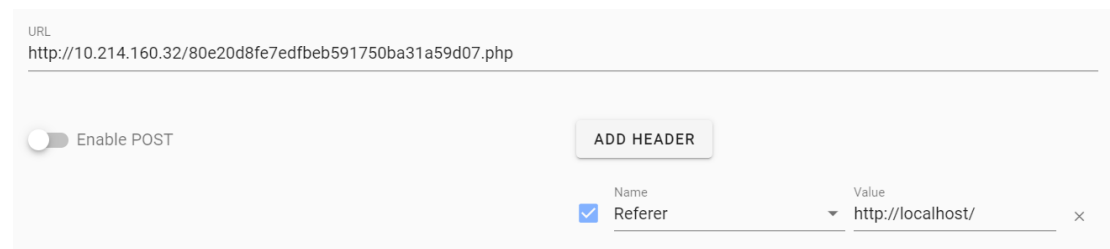
得到密码: 80e20d8fe7edfbeb591750ba31a59d07

## Level2

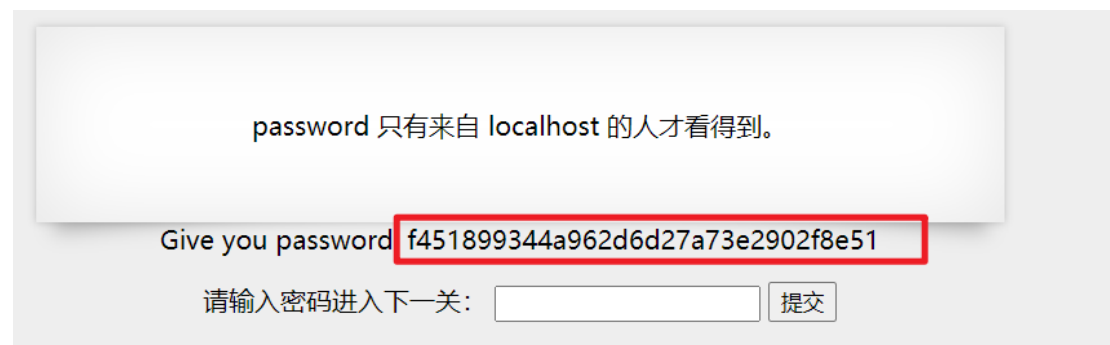
It can be seen from the page prompt that my referer is not localhost at this time, so I need to forge my own referer



Using the hackbar tool, the configuration is as follows

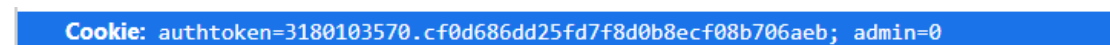


The password will pop up in the page: f451899344a962d6d27a73e2902f8e51



## 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

URL  
http://10.214.160.32/f451899344a962d6d27a73e2902f8e51.php

☐ Enable POST

ADD HEADER

Name	Value
<input checked="" type="checkbox"/> Cookie	!b8ecf08b706aeb; admin=1

We can get flag: actf {47ca8aa874ba92a43621d5ff8cde0cdf}

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

Challenge 90 Solves

## Game2

1

Author: Melody Difficulty Estimate: Easy actf2019

Welcome to this super easy game series! In this series, each game has three stages. You need to find the password to pass the first two, and seek the flag in the third stage. This is Game2, have fun playing!

<http://10.214.160.32>

ACTF{47ca8aa874ba92a43621d5ff8cde0cdf} Submit

You already solved this

### 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" content="text/html">
  <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>

```

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

---

点击进入第三关

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

```

7 <div align="center">
8 <form method="post">
9 <input type="text" name="text">
10 <input type="submit" value="点击进入第三关">
11 </form>
12 jumping...
13 <script>
14   function jump(url){
15     document.body.appendChild(document.createElement('iframe')).src="javascript:<script>top.location.replace('\'+url+'\')</script>";
16   }
17   setInterval("jump('3rd.php')",2000);
18 </script>
19 </div>
20
21 </body>
22 </html>

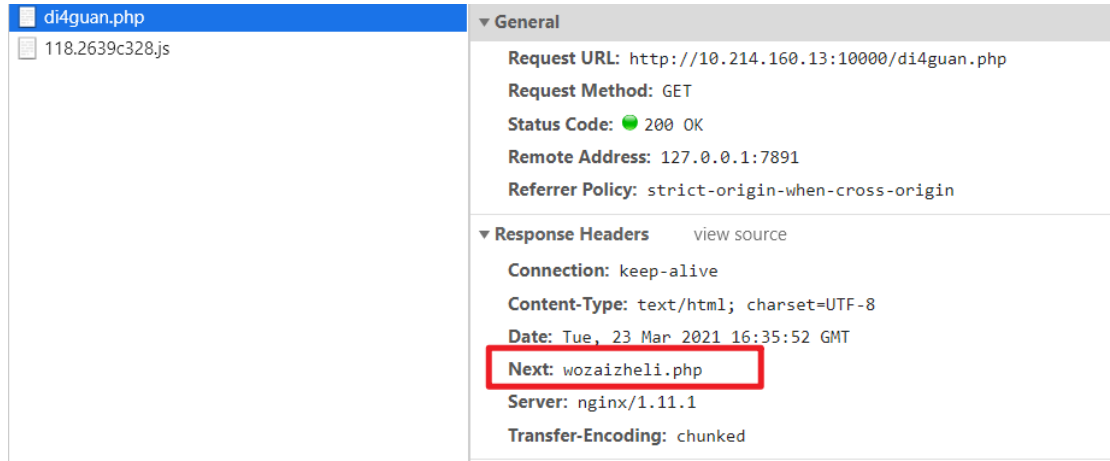
```

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}

点击按钮就能拿到flag啦~

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)

```
C:\Users\lly28>ping zju.tools

正在 Ping zju.tools [103.205.8.47] 具有 32 字节的数据:
来自 103.205.8.47 的回复: 字节=32 时间=78ms TTL=52
来自 103.205.8.47 的回复: 字节=32 时间=77ms TTL=52
来自 103.205.8.47 的回复: 字节=32 时间=81ms TTL=52
来自 103.205.8.47 的回复: 字节=32 时间=92ms TTL=52
```

Find the target port 10822 under this IP

```
C:\windows\system32>nmap -sS -p 9000-11000 103.205.8.47
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-16 23:03 ?D1ú±ê×?ê±??
Nmap scan report for 103.205.8.47
Host is up (0.16s latency).
Not shown: 1999 closed ports
PORT      STATE SERVICE
9996/tcp  filtered palace-5
10822/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 534.74 seconds
```

Scanning with dirbuster <http://121.196.146.56> : 10822 contents



OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)  
http://121.196.146.56:10822

Work Meth... ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads  10 Thre... ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files  
C:\Program Files (x86)\DirBuster\directory-list-2.3-small.txt

Char set a-zA-Z0-9%20- Min length 1 Max Length 8

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☒ Be Recursive Dir to start with //

☒ Brute Force Files ☐ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp  
//121.196.146.56:10822146.56:10822

Please complete the test details

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

File Options About Help

http://121.196.146.56:10822//

List View Tree View

Type	Found	Response	Size	Include	Status
Dir	//	200	1417	<input checked="" type="checkbox"/>	Scanning
Dir	//icons/	403	452	<input checked="" type="checkbox"/>	Waiting
Dir	//bbs/	200	748	<input checked="" type="checkbox"/>	Waiting
Dir	//config/	200	610	<input checked="" type="checkbox"/>	Waiting
Dir	//sex/	200	1006	<input checked="" type="checkbox"/>	Waiting
Dir	//flag/	200	477	<input checked="" type="checkbox"/>	Waiting
Dir	//a4/	200	457	<input checked="" type="checkbox"/>	Waiting
Dir	//secret/	200	457	<input checked="" type="checkbox"/>	Waiting
Dir	//bonus/	200	505	<input checked="" type="checkbox"/>	Waiting
Error	/		39	<input type="checkbox"/>	IOException
Dir	//phpmyadmin/	200	497	<input checked="" type="checkbox"/>	Waiting
Dir	//melodies/	200	420	<input checked="" type="checkbox"/>	Waiting

Current speed: 196 requests/sec (Select and right click for more options)

Average speed: (T) 189, (C) 161 requests/sec

Parse Queue Size: 0

Total Requests: 24975/1795864

Current number of running threads: 10

Time To Finish: 03:03:19

Brute forcing dirs in // //saveicon/

Key is: AAA{Earth\_Three-body-Organization}

# Flag

AAA{Earth\_Three-body-Organization}

Scan - 77 pts

AAA web5 端口扫描与目录爆破 (part1)

Q: 什么是端口?

A: (google是最好的老师)

端口范围为1-65535 (端口0在RFC规范中是没有的)

http的默认端口是80 https是443

ftp是21 ssh是22

Congratz, you have solved it.

Solved

<b>Category</b> welcome	<b>Completed</b> Linxi Clapeysron maybe zuhxs Sleepy icefires TyteKa Pale Shadow
<b>Type</b> web	<b>Writeups</b> <a href="#">Submit Your Writeup!</a>
<b>Solved</b> 187	