Lab1

> Student ID: 3190104783
> Name: Ou Yixin
> Date: 2022-03-12

1 http://8.136.83.180:8080/

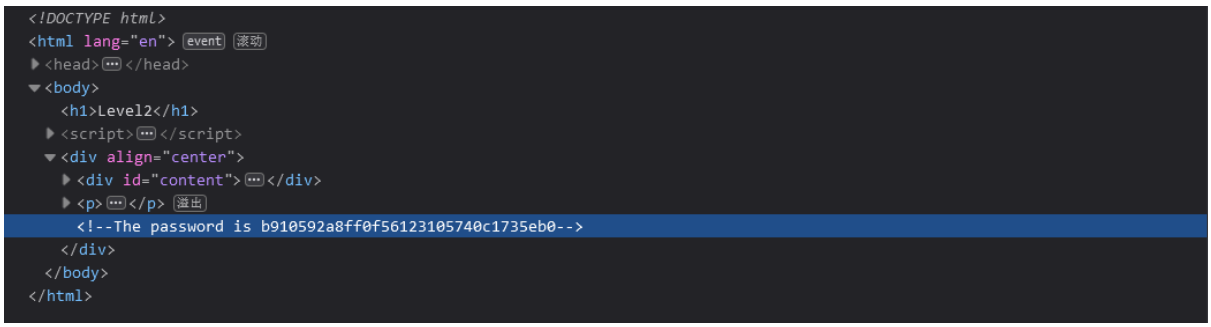
step 1. view page source

Open the browser's developer tools directly to view the HTML source code and find the hidden password in the comments

The password is 029c64152b6954e91d39183f8d2e07a9

step 2. view page source

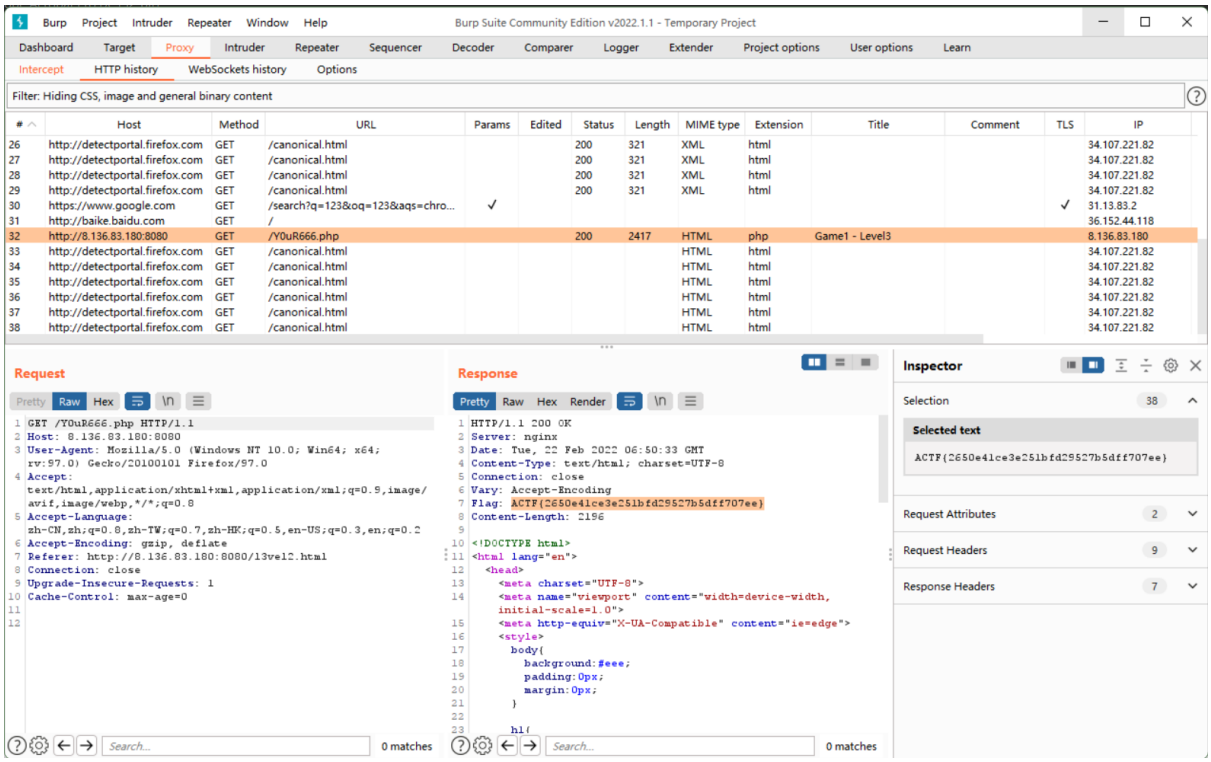
Open the browser's developer tools directly to view the HTML source code and find the hidden password in the comments



The password is b910592a8ff0f56123105740c1735eb0

step 3. capture RESPONSE packet header using Burp Suite

Use the Burp Suite tool to capture and view the Response header after the GET method requests a web resource

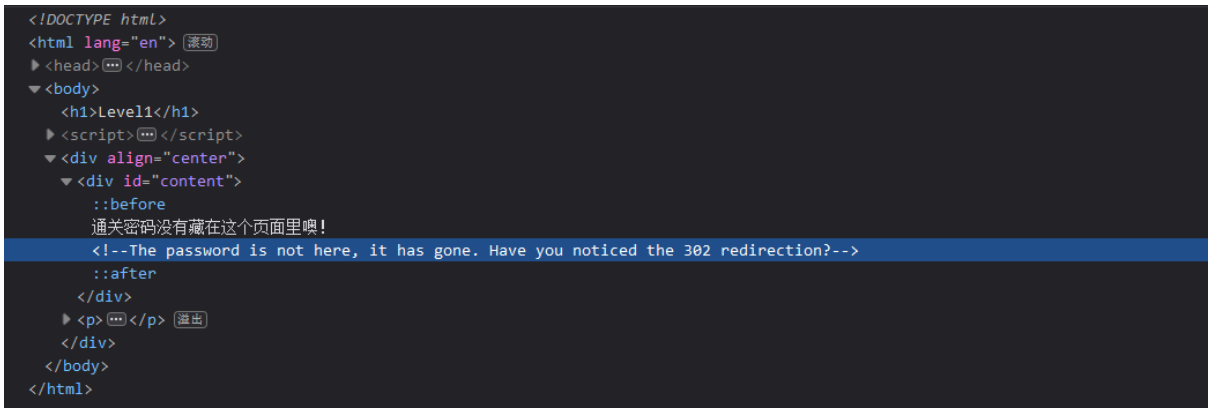


ACTF{2650e41ce3e251bfd29527b5dff707ee}

2 http://8.136.83.180:8081/

step 1. view page source

Open the browser's developer tools directly to view the HTML source code, prompting for a 302 redirect

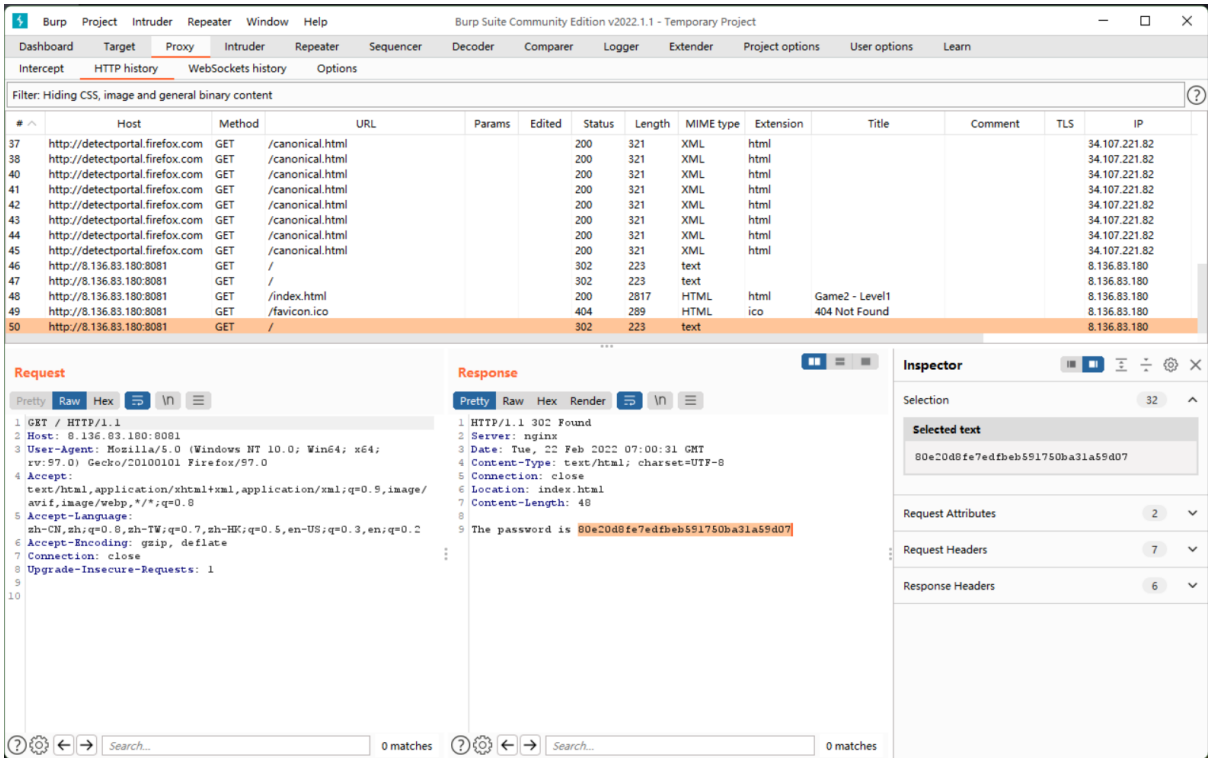


step 2. understand 302 redirection

A 302 is a status code in the HTTP protocol that can be interpreted to mean that the resource did exist, but has been temporarily redirected. For servers, the HTTP Location header is usually sent to the browser to redirect to the new location.

step 3. locate redirected pages and find password

Check the GET request with status code 302 and find the password in the Response header



The password is 80e20d8fe7edfbeb591750ba31a59d07

step 4. understand HTTP Referer field

Referer is a common field in the header of HTTP requests that provides information about the source of the access. The client sends the request with or without this field at its own discretion. Servers generally use the referer to identify the source of a visit, which may be used for statistical analysis, logging, and cache optimization.

step 5. capture GET-packet and rewrite Referer field using Burp Suite

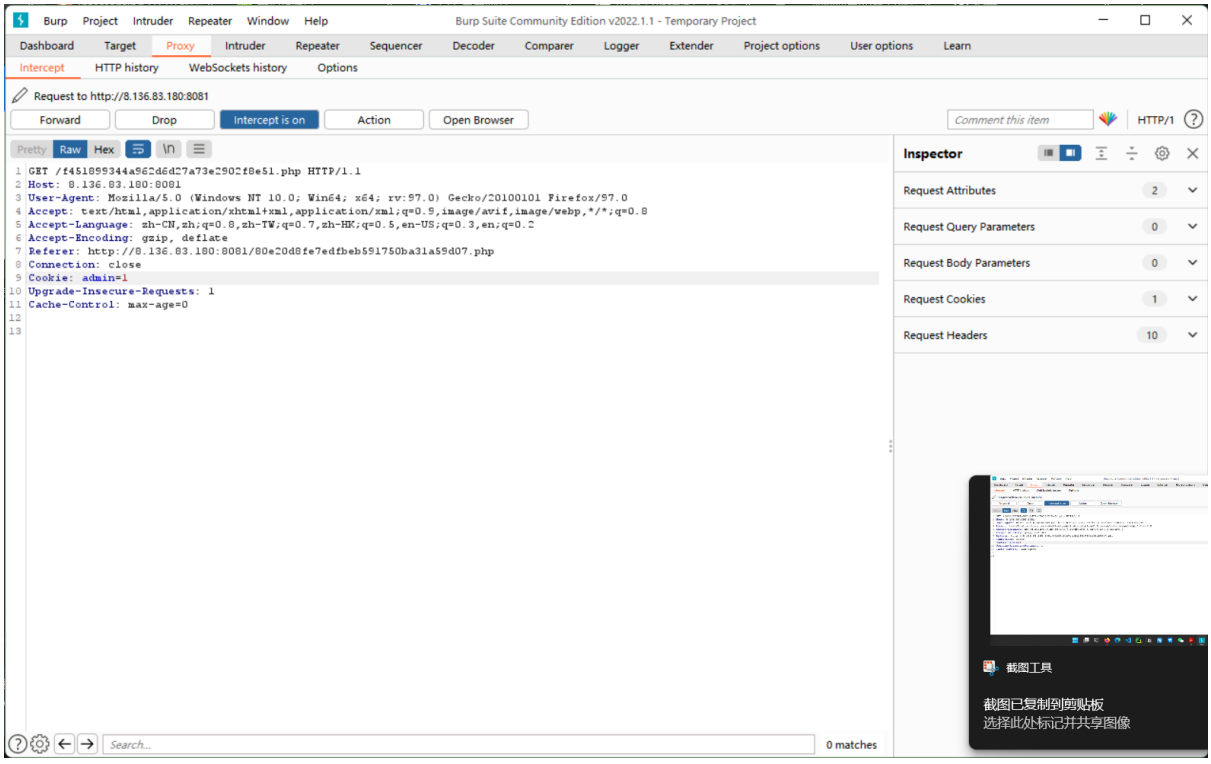
Use the Burp Suite tool to capture GET request packets and rewrite the Referer field and resend it

```
<!DOCTYPE html>
<html lang="en"> 滚动
 <head> ... </head>
 <body>
   <h1>Level2</h1>
  <script> ... </script>
  <div align="center">
   <div id="content"> ... </div>
   <div id="password">
     Give you password: f451899344a962d6d27a73e2902f8e51
    </div>
   <p> ... </p> 溢出
   </div>
  </body>
</html>
```

Give you password: f451899344a962d6d27a73e2902f8e51

step 6. capture GET-packet and rewrite Cookie field with admin privilege using Burp Suite

Use the Burp Suite tool to capture the GET request packet and rewrite the cookie field and admin privilege and resend it




```
<!DOCTYPE html>
<html lang="en">
 <head> ... </head>
 <body>
   <h1>Level3</h1>
  <div id="content">
    ::before
    Flag 只有来自 admin 才看得到。 Ok, give you flag: ACTF{47ca8aa874ba92a43621d5ff8cde0cdf}
    <!--Do you know how http cookie worked?-->
    ::after
   </div>
  </body>
</html>
```

ACTF{47ca8aa874ba92a43621d5ff8cde0cdf}

3 https://zjusec.com/challenges/19

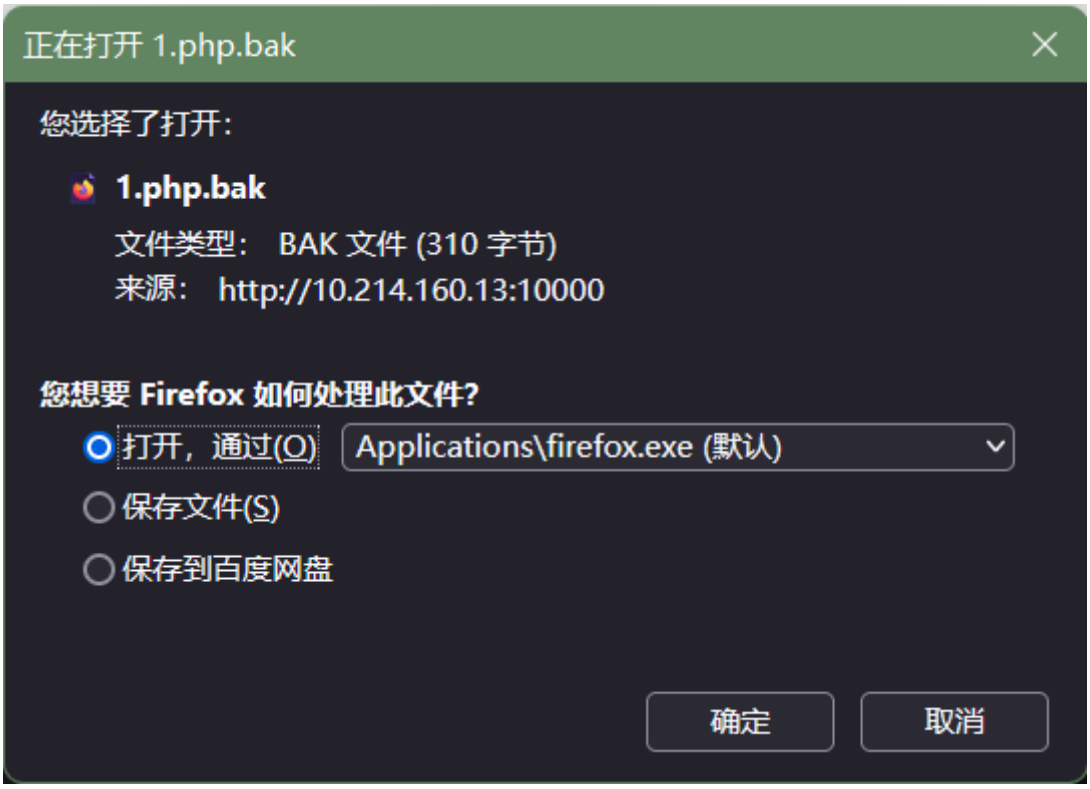
step 1. view page source

View web page HTML source code

```
<html>
▶ <head> ⋯ </head>
▼ <body>
  ▶ <div align="center"> ⋯ </div>
    <!--删除1.php.bak-->
  </body>
</html>
```

step 2. get link from .bak file

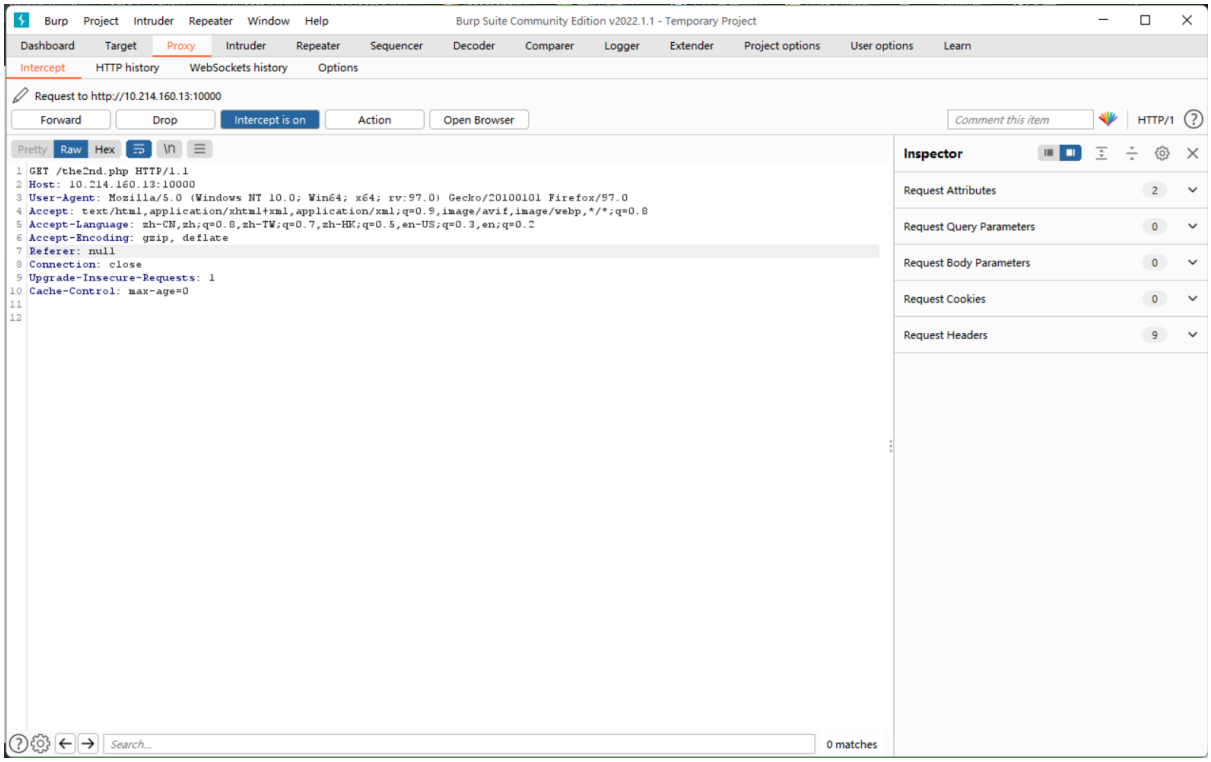
Change the URL to get the 1.php.bak file and open it in browser

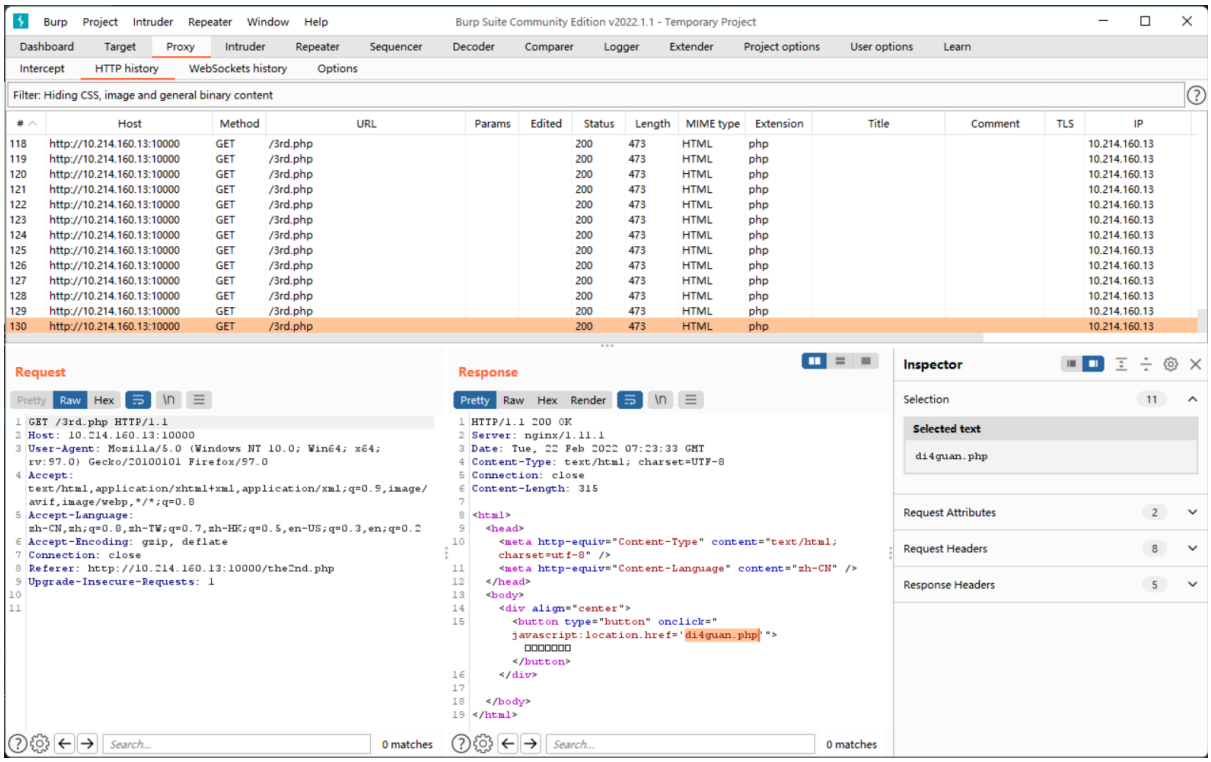



```
<html>
▶ <head> ⋯ </head>
▼ <body>
  ▶ <div align="center"> ⋯ </div>
    <!--删除1.php.bak-->
    <a href="the2nd.php">进入第二关</a>
  </body>
</html>
```

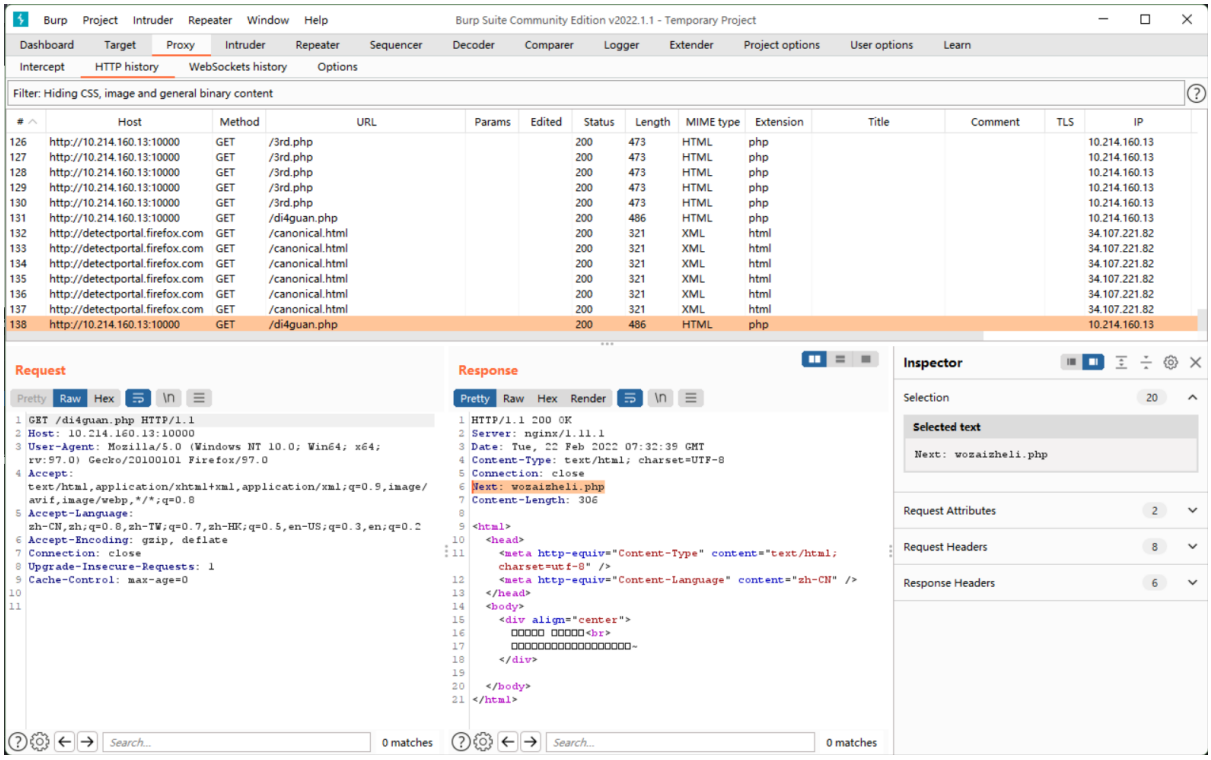
step 3. capture GET-packet and null Referer field using Burp Suite

Use the Burp Suite tool to capture GET request packets and rewrite the Referer field and resend it



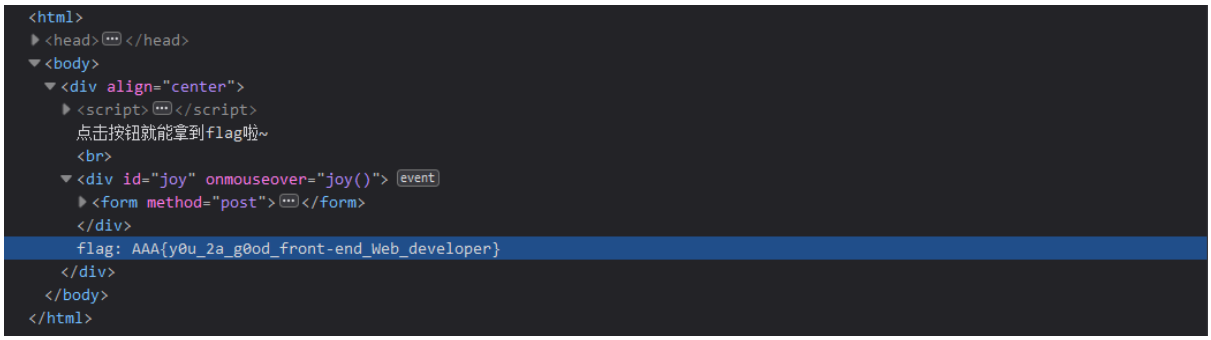


step 4. capture RESONSE-packet header with next link included using Burp Suite



step 5. view page source and try to click the button or craft packet with button click effect

Modify the page source code to disable the script to click the button normally



AAA{y0u_2a_g0od_front-end_Web_developer}

4 http://8.136.83.180:????/

Scanning ports with the nmap tool

```
nmap 8.136.83.180
```

```
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
8083/tcp open  us-srv
```

AAA web5 端口扫描与目录爆破 (part2)

非常棒，你已经成功扫描出端口了！
如果你还没有加qq群，请收好part1的flag(这个flag对已经加群了的小伙伴无效)：
AAA{web5_part1_passed_and_welcome_to_aaa_qq_group_386796080}

以下是part2的说明(目录爆破)：
Q：什么是目录爆破？为什么要爆破目录？
A：正常情况下，网站的某些目录是没有直接进入的入口的，比如
  www.foo.com/secret/admin.php
  ~~melody.com/resource/小电影.torrent~~
  这些隐藏的目录可能会给攻击带来很大的方便，提供网站的更多信息或者增加攻击面.
  目录爆破就是根据一个庞大的字典，来一个个测试这个目录是否存在. 当然还会加上爬虫的辅助
  google是最好的老师

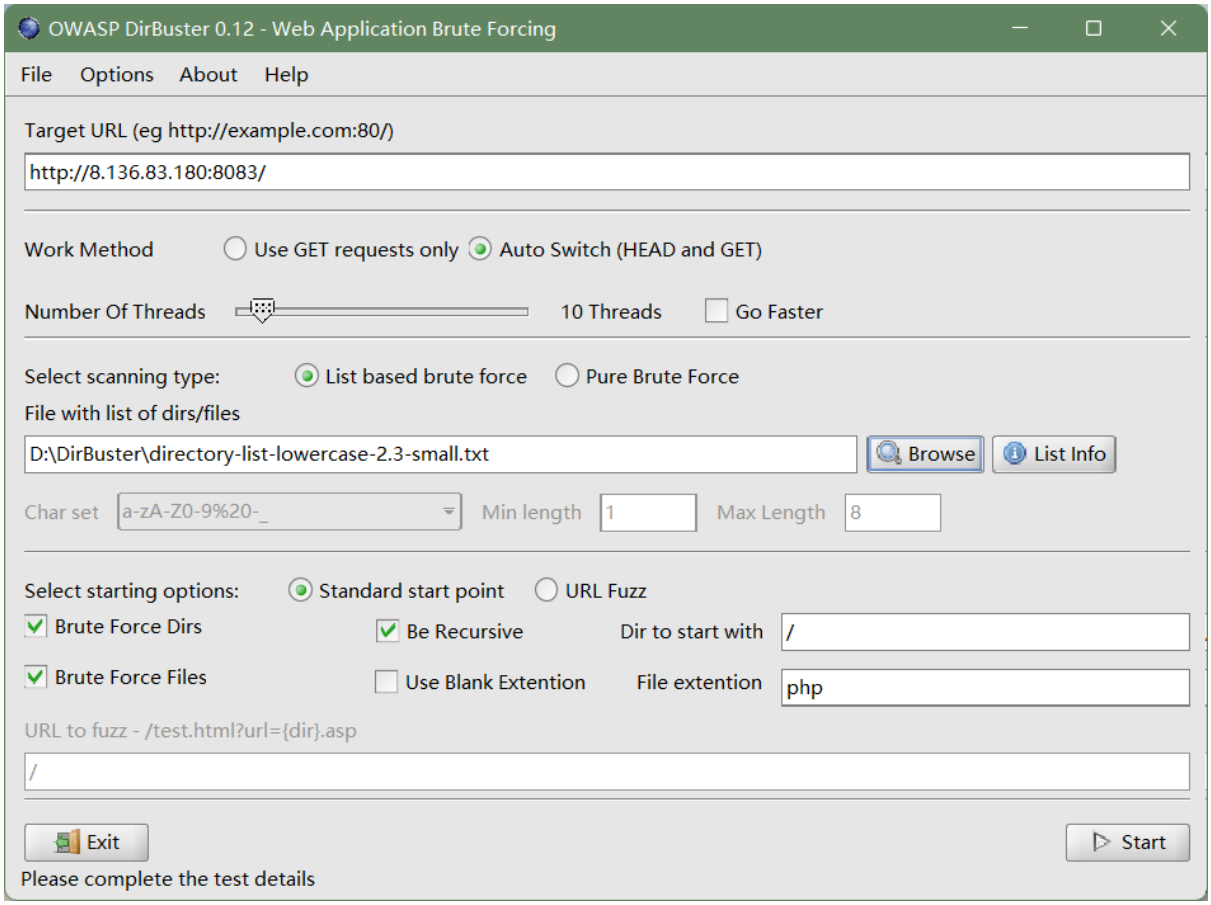
Q：使用什么工具？
A：DirBuster 或者它的集成版 Zap（看喜好，zap整体功能比较强，但是就扫目录这个功能上可定制性比较差）
  burpsuite也可以用于目录爆破

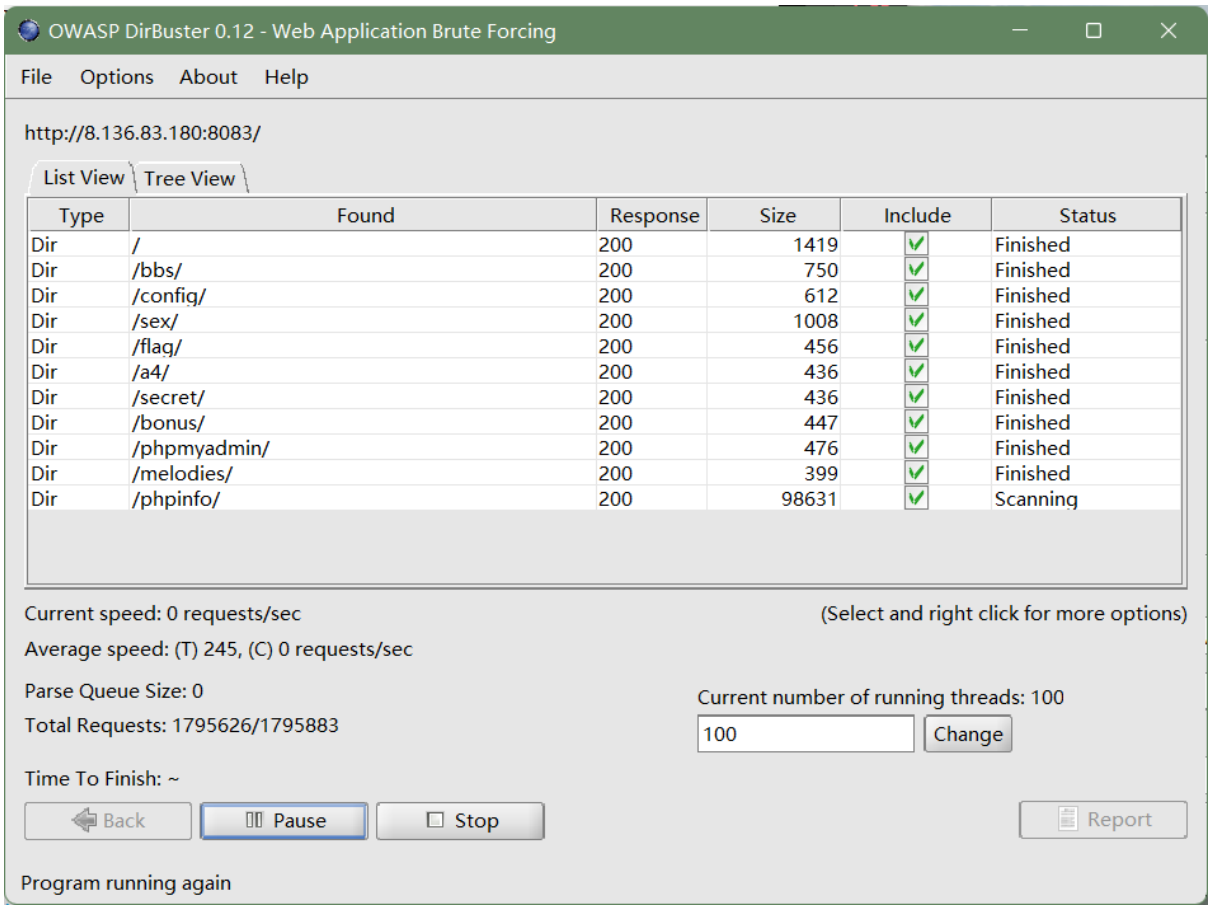
Q：目录字典呢？
A：DirBuster(0.12) 自带目录字典，zap被阉割了，如果是用zap的话请下载DirBuster里面的目录字典
  在本次扫描中，为了减轻服务器压力，请使用 directory-list-lowercase-2.3-small.txt 这个

Hints:
  本次扫描中，只会出现 .html 后缀的文件
  目录爆破可能需要非常长的时间，请耐心等待(*￣﹀￣*)

---
author: Aploium

Directory bursting with the DirBuster tool


OWASP DirBuster 0.12 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://8.136.83.180:8083/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 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
Browse
List Info
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
/
Exit
Start
Please complete the test details


OWASP DirBuster 0.12 - Web Application Brute Forcing
File Options About Help
http://8.136.83.180:8083/
List View
Tree View
Type Found Response Size Include Status
Dir / 200 1419 Finished
Dir /bbs/ 200 750 Finished
Dir /config/ 200 612 Finished
Dir /sex/ 200 1008 Finished
Dir /flag/ 200 456 Finished
Dir /a4/ 200 436 Finished
Dir /secret/ 200 436 Finished
Dir /bonus/ 200 447 Finished
Dir /phpmyadmin/ 200 476 Finished
Dir /melodies/ 200 399 Finished
Dir /phpinfo/ 200 98631 Scanning
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 245, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 1795626/1795883
Current number of running threads: 100
100
Change
Time To Finish: ~
Back
Pause
Stop
Report
Program running again

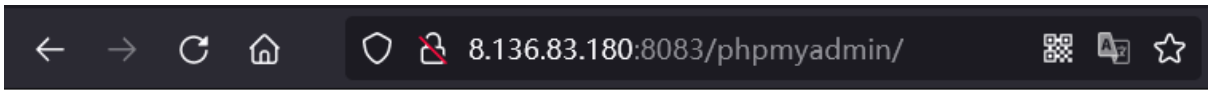
```
DirBuster 0.12 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Mon Feb 28 15:35:49 CST 2022
--------------------------------

http://8.136.83.180:8083
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/bbs/
/config/
/sex/
/flag/
/a4/
/secret/
/bonus/
/phpmyadmin/
/melodies/
/phpinfo/


--------------------------------
--------------------------------
```



Flag

AAA{Earth_Three-body-Organization}

AAA{Earth_Three-body-Organization}