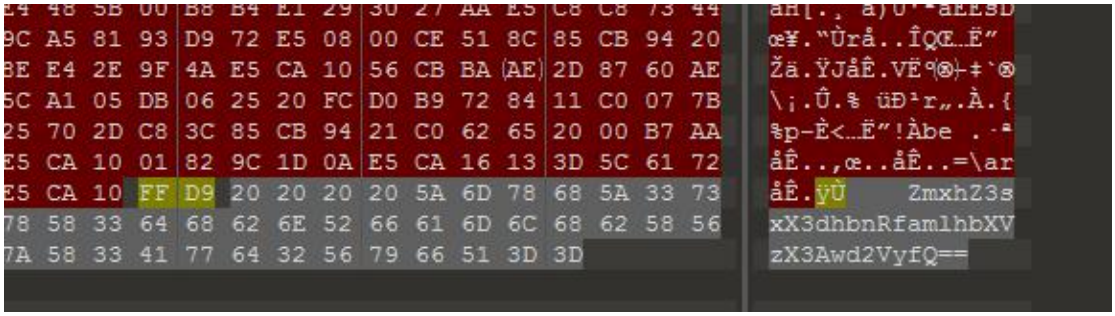
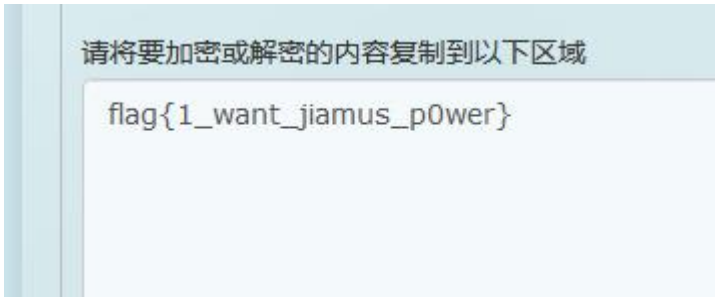
misc-签到

使用 010 Editor 打开图片，拉到尾部。



发现 base64 编码

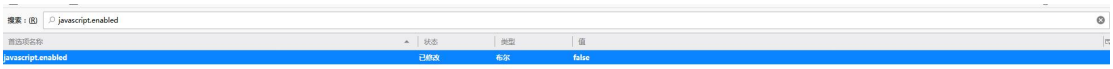
解码得到 flag



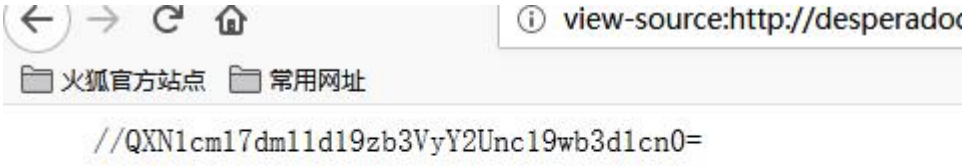
baby-web-九曲十八弯

进入页面，发现无法查看源代码
猜测通过 js 禁止

打开 firefox，禁用 js



可以查看源代码



一段 base64 编码，解码得

medium_web_justburp

打开页面，提示密码藏在某页面中

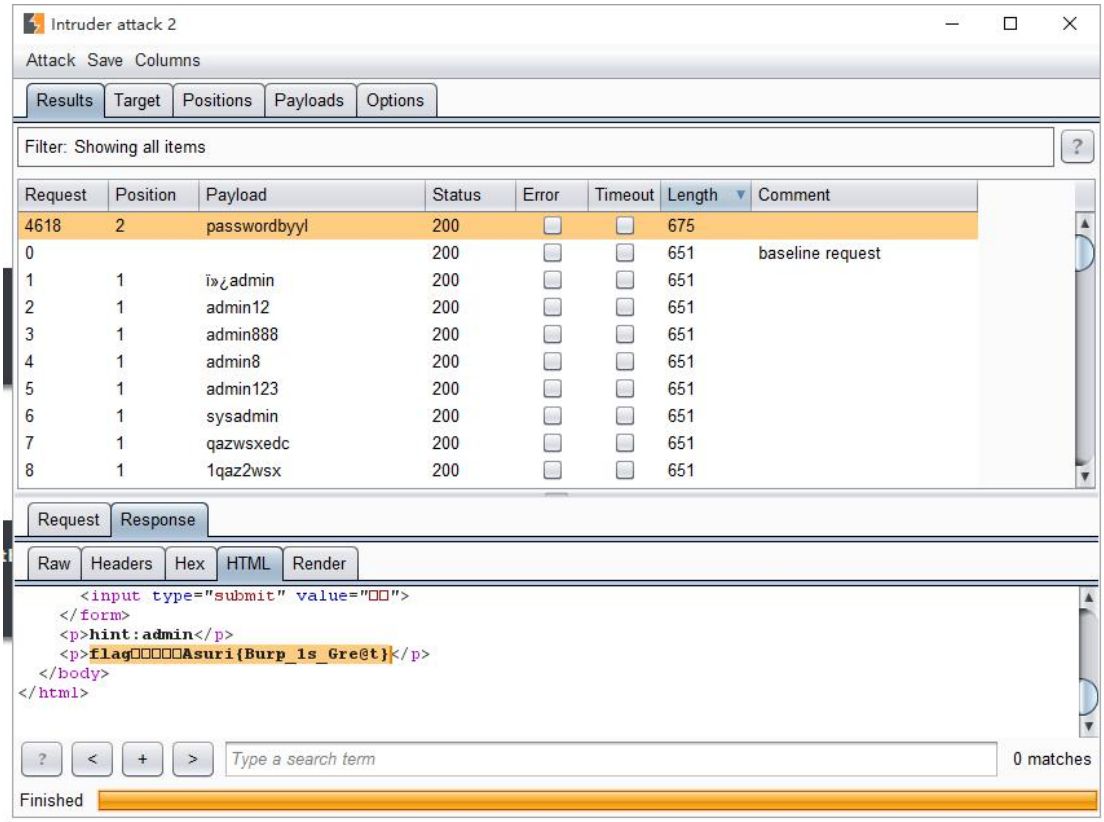
用御剑扫一下

发现 robot.txt

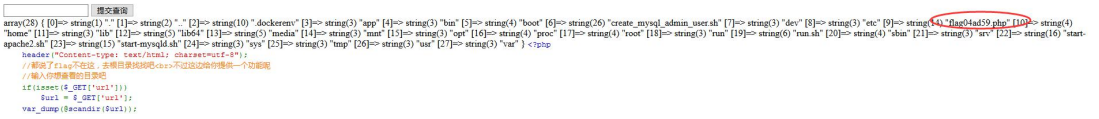
发现 hint.php

下载得到密码文件

用 burp 爆破一波

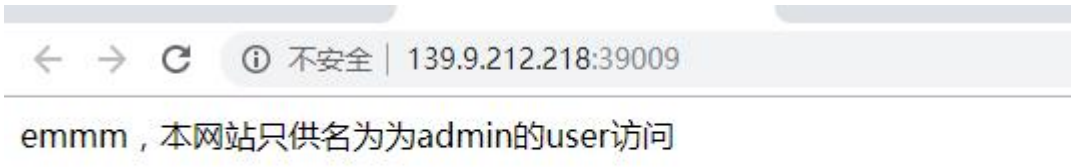

Intruder attack 2
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Position Payload Status Error Timeout Length Comment
4618 2 passwordbyyl 200 675
0 200 651 baseline request
1 1 ï»¿admin 200 651
2 1 admin12 200 651
3 1 admin888 200 651
4 1 admin8 200 651
5 1 admin123 200 651
6 1 sysadmin 200 651
7 1 qazwsxedc 200 651
8 1 1qaz2wsx 200 651
Request Response
Raw Headers Hex HTML Render
<input type="submit" value="□□">
</form>
hint:admin
flag□□□□□Asuri{Burp_1s_Gre@t}
</body>
</html>
Type a search term
0 matches
Finished

扫出来了

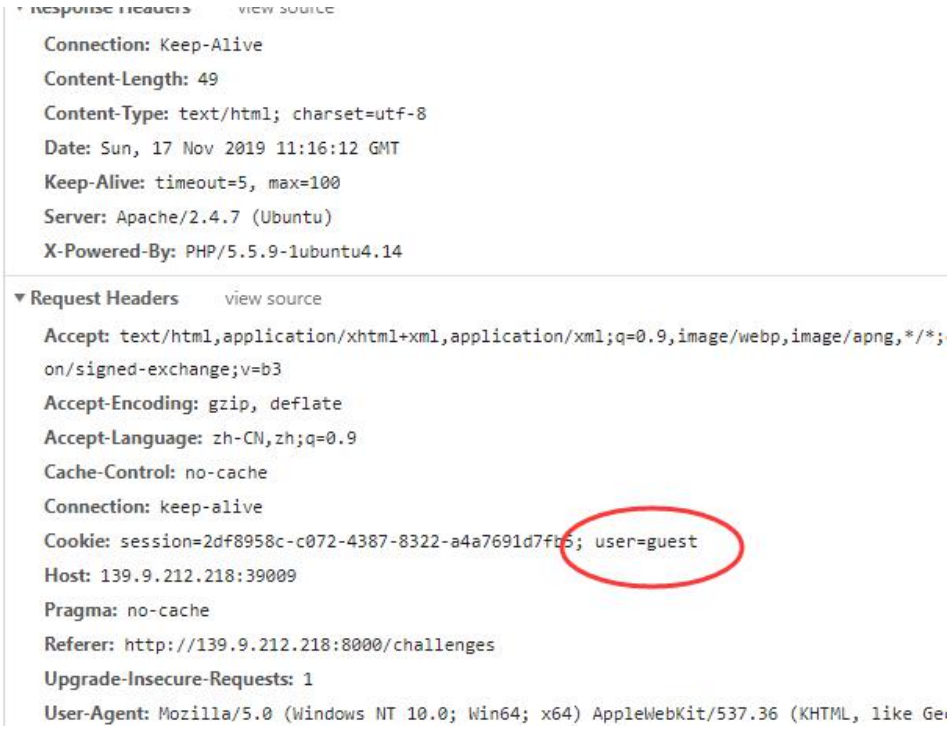

提交查询
array(28) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(3) "app" [4]=> string(3) "bin" [5]=> string(4) "boot" [6]=> string(26) "create_mysql_admin_user.sh" [7]=> string(3) "dev" [8]=> string(3) "etc" [9]=> string(14) "flag04ad59.php" [10]=> string(4) "home" [11]=> string(3) "lib" [12]=> string(5) "lib64" [13]=> string(5) "media" [14]=> string(3) "mnt" [15]=> string(3) "opt" [16]=> string(4) "proc" [17]=> string(4) "root" [18]=> string(3) "run" [19]=> string(6) "run.sh" [20]=> string(4) "sbin" [21]=> string(3) "srv" [22]=> string(16) "start-apache2.sh" [23]=> string(15) "start-mysqld.sh" [24]=> string(3) "sys" [25]=> string(3) "tmp" [26]=> string(3) "usr" [27]=> string(3) "var" } <?php
header("Content-type: text/html; charset=utf-8");
//解决了flag不在这，去根目录找找吧
不过这边暗示提供一个功能呢
//输入你想查看的目录吧
if(isset($_GET['url']))
$url = $_GET['url'];
var_dump(@scandir($url));

hard_web_php 是世界上最好的语言

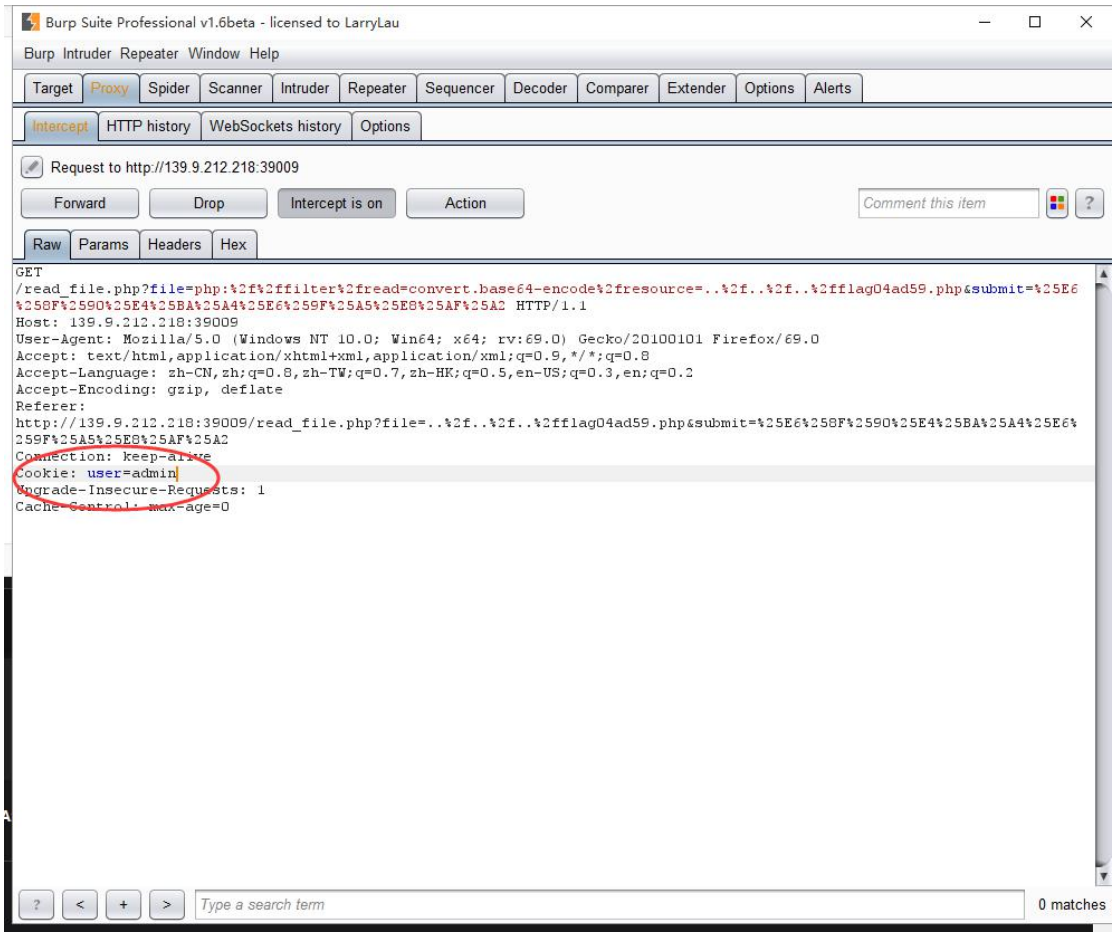
进入网页，发现提示信息



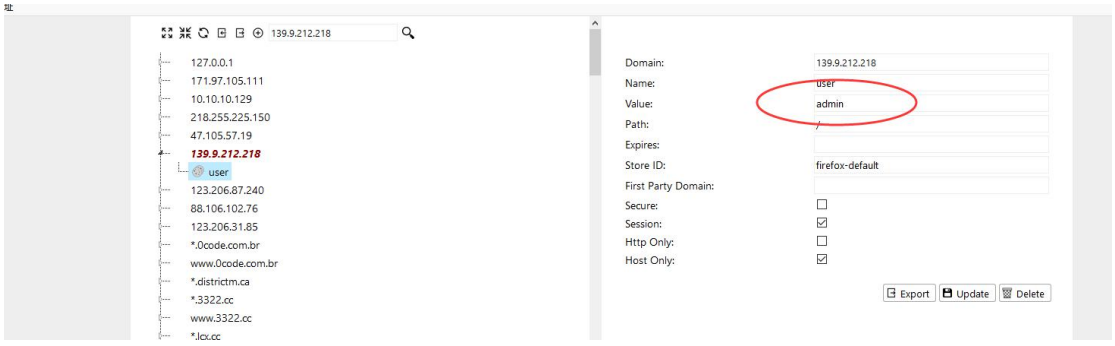
查看 cookie



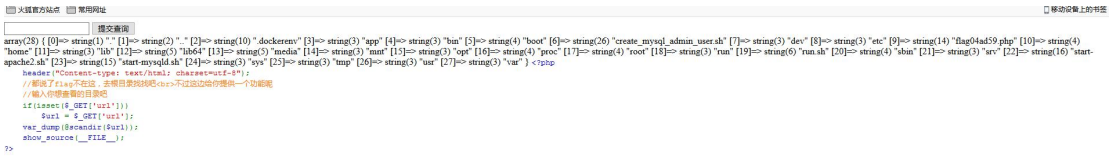
Burp 截包修改试试，成功

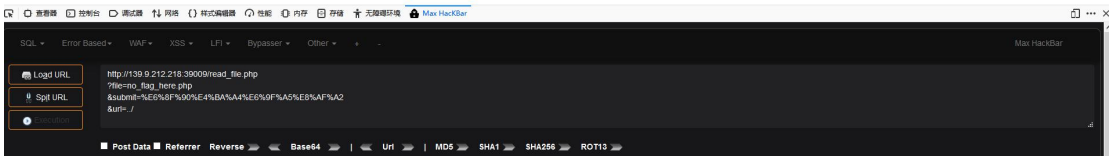


修改 cookies



获得提示





构造语句，得到根目录信息

一层一层查看文件夹/www/所在位置

发现网站目录位置，/var/www/html

构造语句：file=php://filter/read=convert.base64-encode/resource=../../../flag04ad59.php

得到 base64 编码，解码得

快速计算

脚本代码：

```
import requests
import re
from bs4 import BeautifulSoup
import time

url = "http://47.102.107.100:39012"
data = {'answer':'5'}

# response = requests.post(url,data)
# res = response.text
# soup = BeautifulSoup(res, features='html.parser')
# str = soup.find_all("div")[0].get_text()
# str = re.split("=",str,1)
# cal = eval(str[0])
# result = str[1]


s = requests.Session()
for i in range(20):
    req = s.get(url).text
    soup = BeautifulSoup(req, features='html.parser')
    str = soup.find_all("div")[0].get_text()
    str = re.split("=", str, 1)
    cal = int(eval(str[0]))
    result = int(str[1])
    print(cal, result)
    if cal == result:
        print('true')
        data = {'answer': 'true'}
        time.sleep(1)
        textT = s.post(url,data)
    elif cal != result:
        print('false')
        data = {'answer': 'false'}
        time.sleep(1)
        textT = s.post(url, data)

textT.encoding = 'utf-8'
print(textT.text)
```

```
34953 34952
false
20190144 20190145
false
166587 166587
true
Asuri{python_1s_th3_be3t_l4ngu4ge}
```