此篇为信息安全月writeup

不是按照难度排序

建议大家从低分题开始对照

Code 部分

Decrypt题

查看源代码发现

此题模拟简单加密类漏洞，使用简单加密方法传输存储的数据，极易被解密。



注释部分提示BASE64解密

将题目中的字符串多次base64解密得到flag

VmpKMFYyRXlTWGxUYTFwcFVsZG9XVmx0Y3pGWlZscHhVMnM1YVdKSGVGaFpWVlV4V1ZVeGMxWnFXbGhoTWxFd1ZrWmtTMlJHVm5WYVJuQm9UV3hHTmxkcldtdFViVlpYVjI1U2JGSlVSbkJaYkdodVpWWmtjbGRyTlU1V01EVkpWVEkxUTFReFdYbGhTRUphWWtaS2VWcEVSbk5XYkhCSFdrZDRWMWRIWjNoV1ZtTXhWREZrYzFkWVpFOVhSVFZvV1d0V1ZrNVdWa2RTVkd4UlZWUXdPUT09

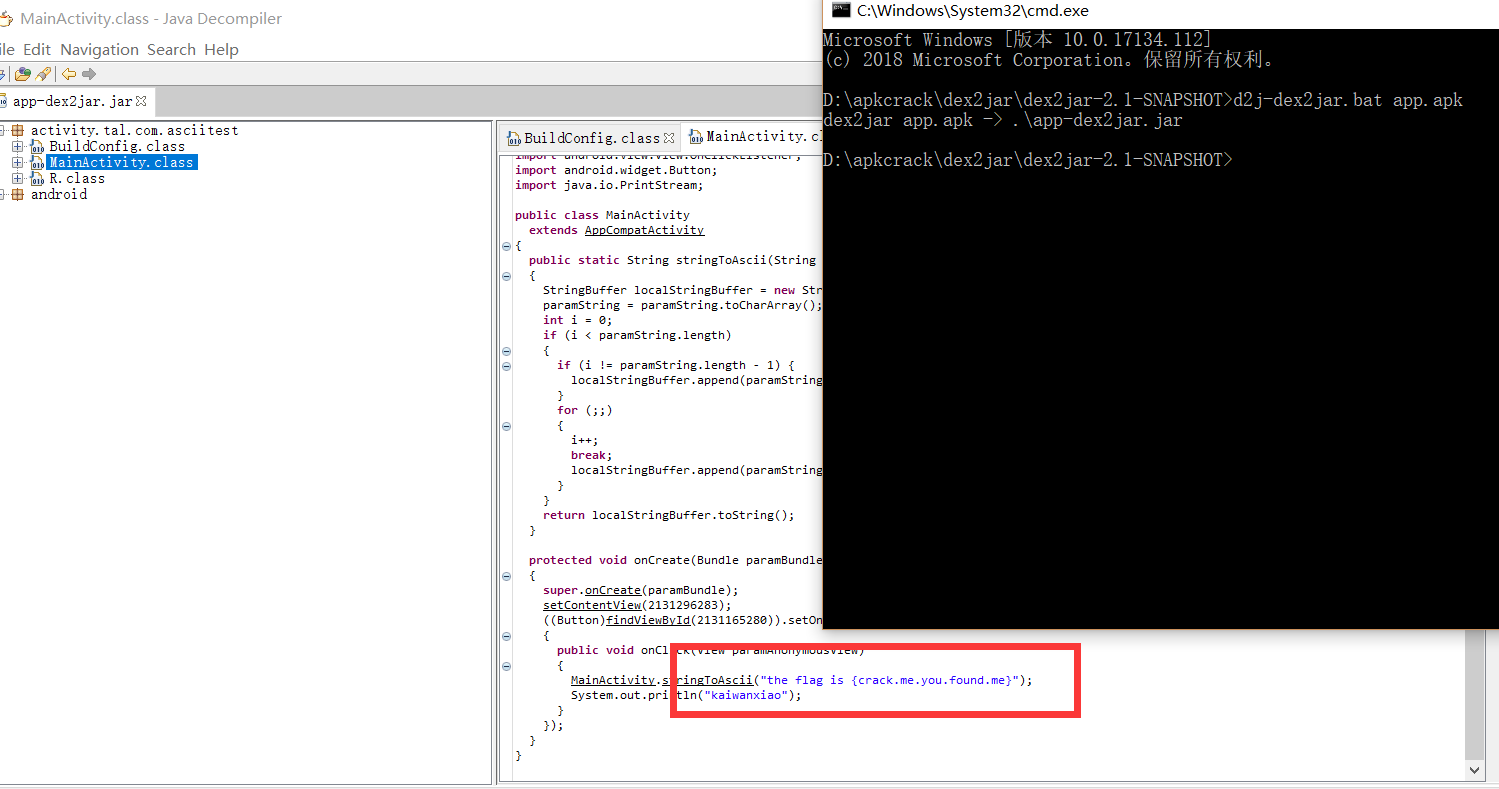
the flag is {we.will.see.you.in.another.place}

flag 意思是 查看源代码要经常用到

APP题

此题模拟APP破解漏洞。未加壳的APP可以被破解出源代码。

将题目中的APP下载下来，破解之后，在main源码里找到flag



the flag is {crack.me.you.found.me}

此题是 提示普通打包的APP 都是可以破解的。发布上线的时候要去加固一下。

code 题

纯算法题



由题面信息可知：题目信息为 flag 的乱序输出，并且给出了 flag 的md5值。

因此只要将剩余字母排序计算md5即可。

剩下字符一共9位，其中多个重复，计算次数为 （9\*8\*7\*6\*5\*4\*3\*2\*1 ）/ （2\*2\*2）=45360

答案为：the flag is {my.nickname.is.scopioncn}

此题答案跟其他题目有交互。

codemix 题

此题为 简单加密以及爆破 的 混合题。

此题为混合题，设计有点失误，没有另外一个简单的抓包改包题来做铺垫，所以这道题 参加队伍全军覆没，没有一个解出来。



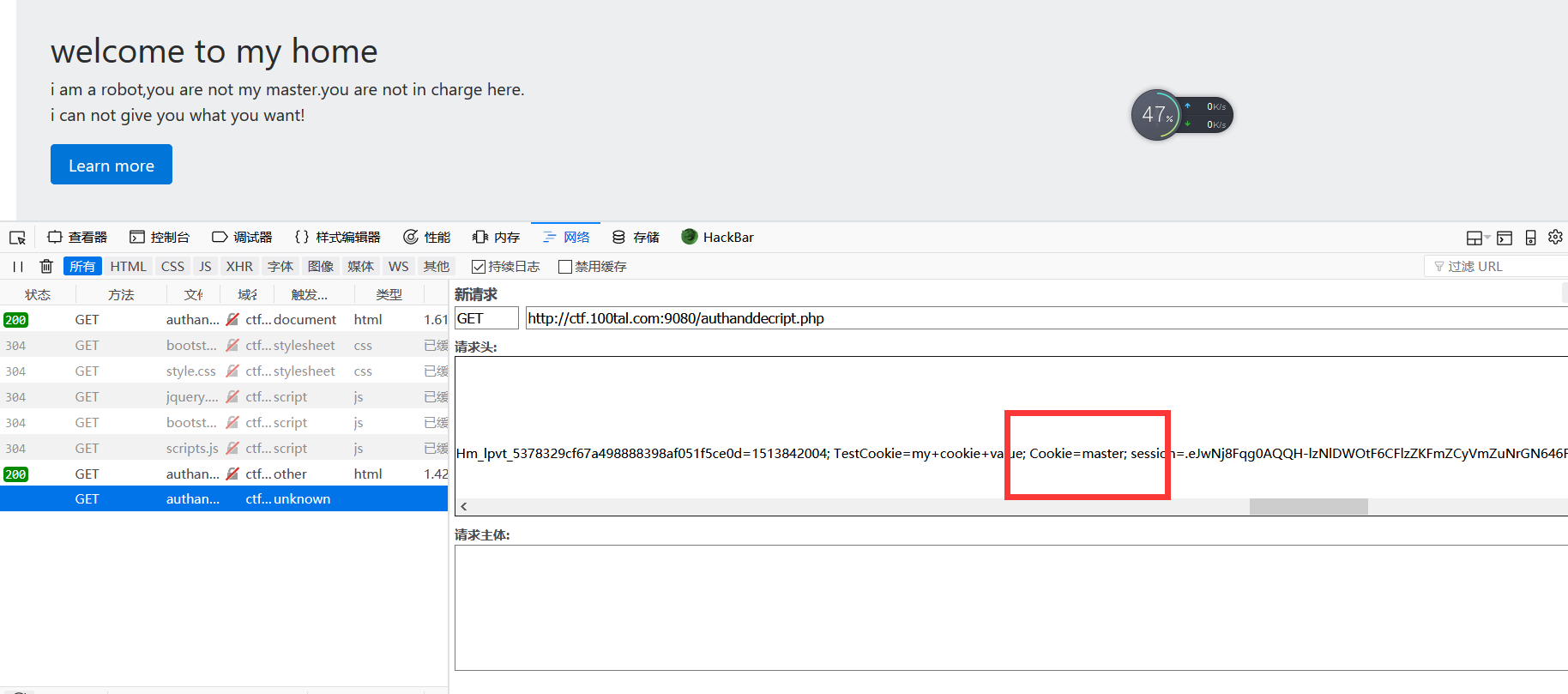
查看访问请求，发现返回有setcookie，auth-algorithm字段

Set-Cookie: Cookie=Ce01oaILOq13bEvCSw%3D%3D

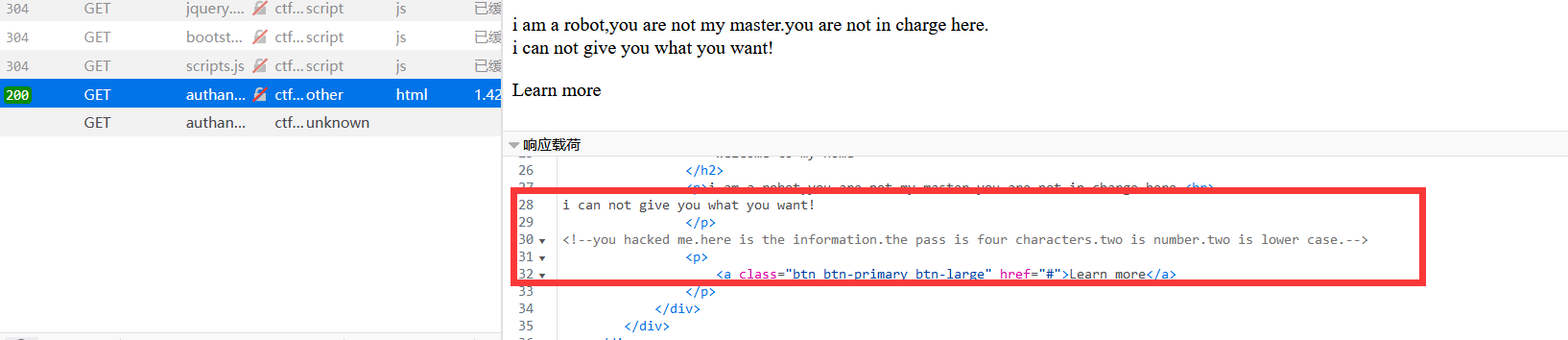
auth-algorithm: base64\_encode(rc4('user', 'pass')

可知，cookie值 Ce01oaILOq13bEvCSw%3D%3D是由 base64\_encode(rc4('user', 'pass') 方法得来。目前源码中没有信息。

由题面信息，将cookie值改成master 再次请求



查看源代码



由注释信息

<!--you hacked me.here is the information.the pass is four characters.two is number.two is lower case.-->

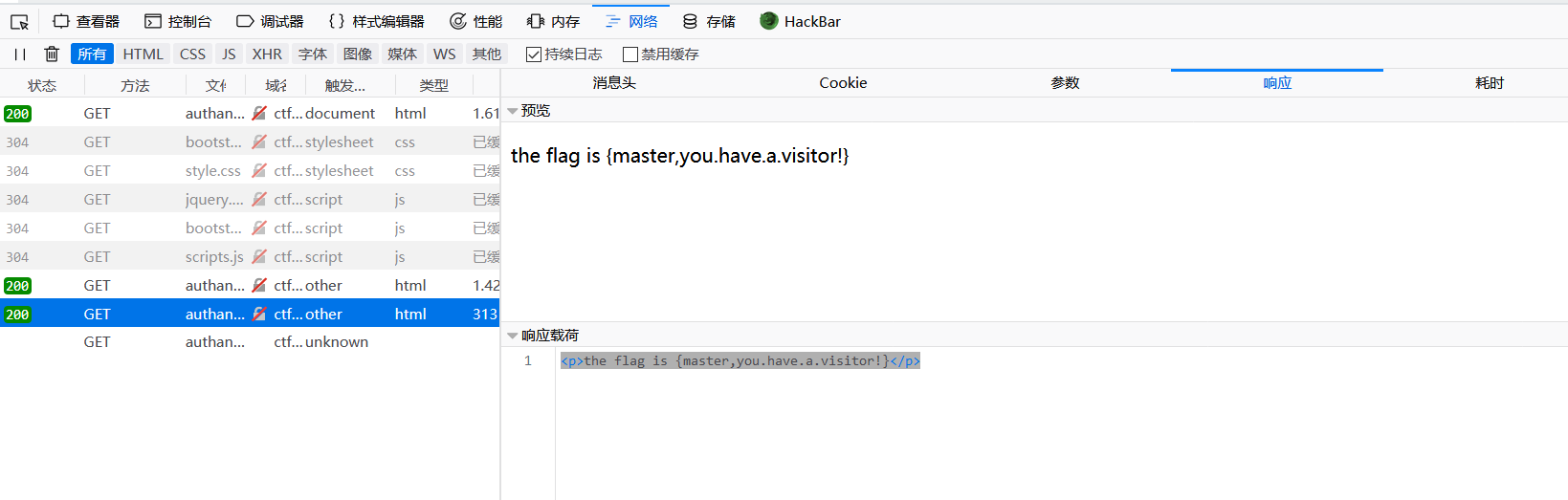
可知，auth-algorithm: base64\_encode(rc4('user', 'pass') 中pass字段为4位字符。其中2位为注释，2位为小写字母。

计算次数为：26\*26\*100=67600

使用解密算法暴力破解默认cookie：Ce01oaILOq13bEvCSw==。当 pass 为 0o9s 时，破解user 为 buyaoyongroot (不要用root)

所以，使用base64 (rc4(root ，0o9s)) 获得COOKIE值 GfcjtA==

请求得到 flag



<p>the flag is {master,you.have.a.visitor!}</p>

此题为纯算法题，答案无其他意义。希望看到这里的老师亲手实现一下算法，如果有什么问题可以钉钉问我。

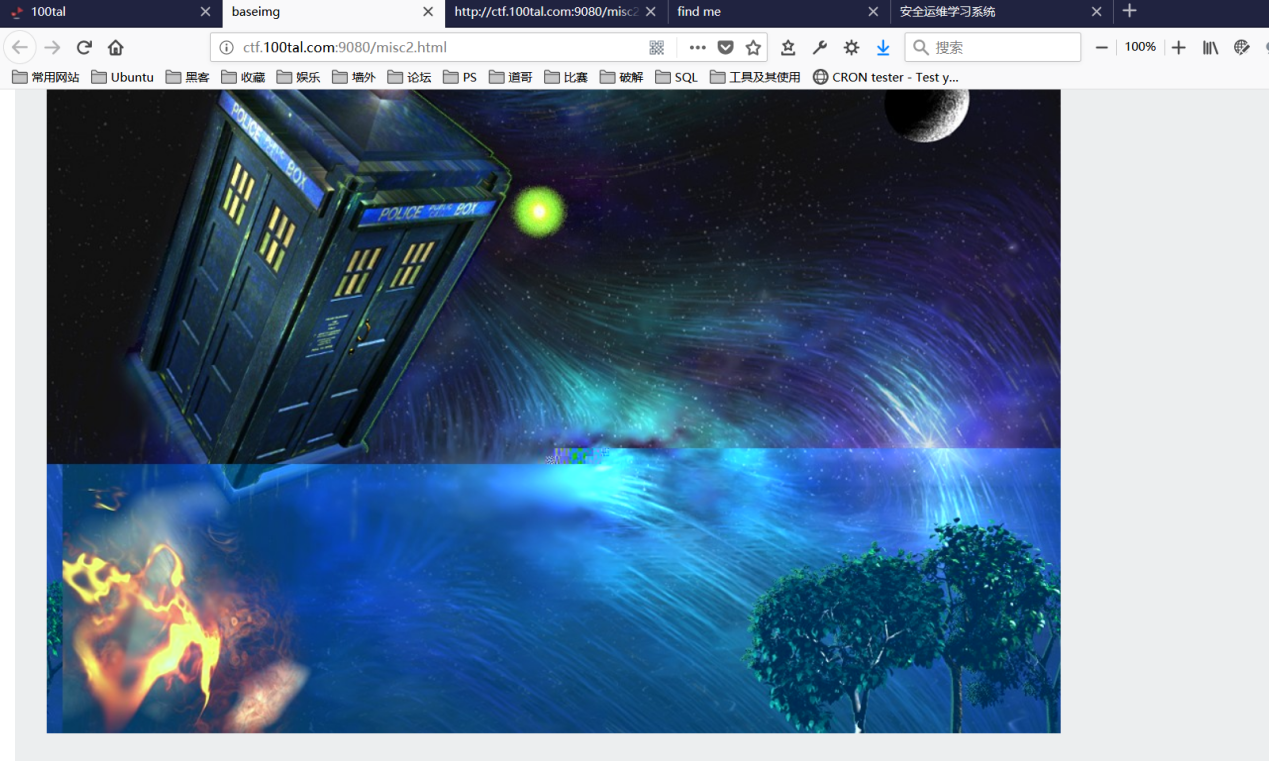
Misc 部分

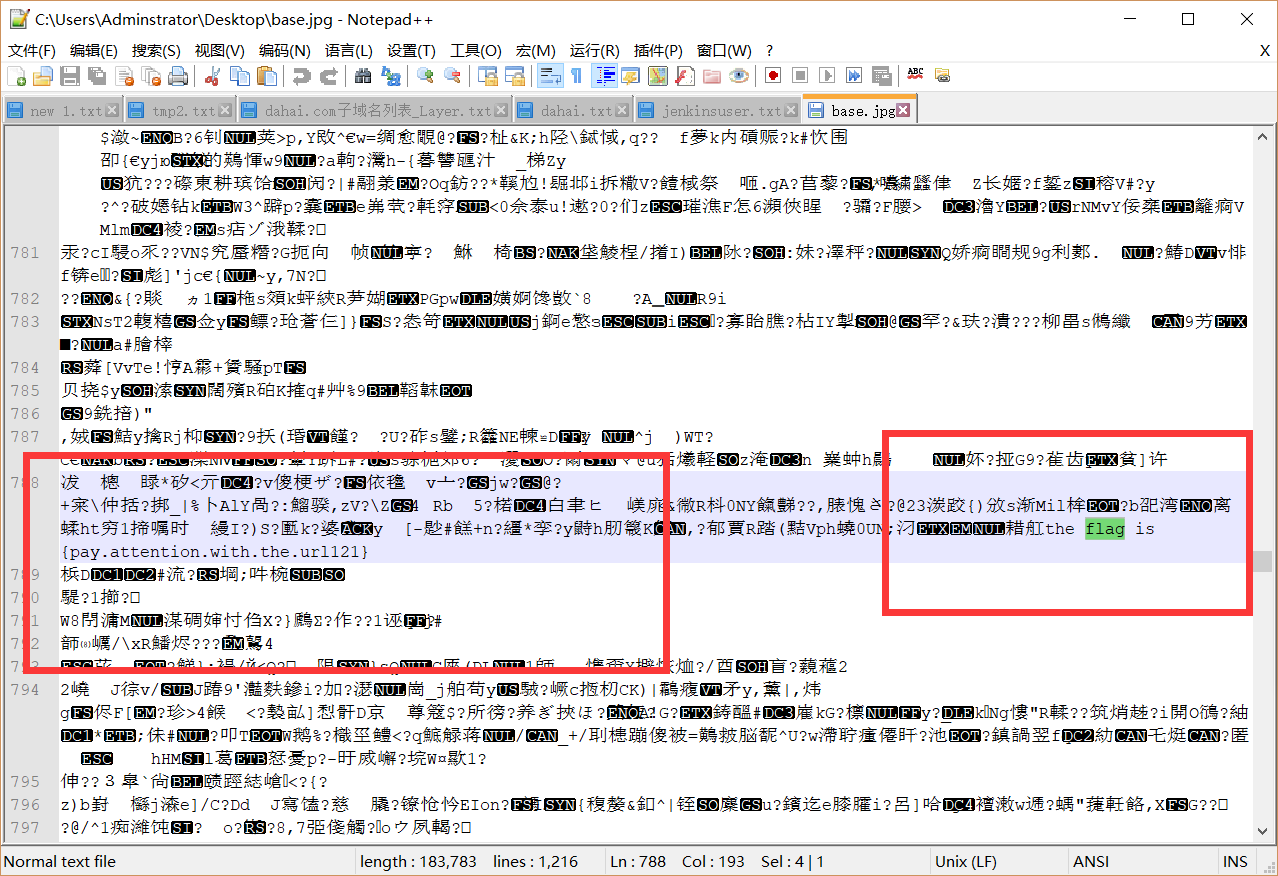
Baseimg题

图片隐写题，图片木马。在特殊环境下，图片内容可以被当成 脚本 解析，所以可以在图片内容中写入网马进行入侵。

从题图就能看出不和谐。

将图片下载下来，使用txt方式打开，在相应比例的位置处发现flag

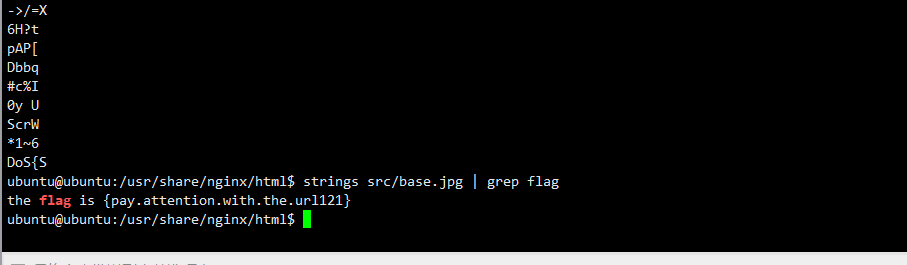




得到

the flag is {pay.attention.with.the.url121}

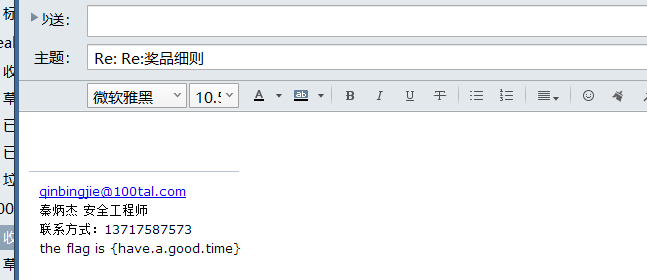
或者使用linux系统



此题最简单的隐写术。答案 意为让你注意url，找规律。是安全测试常用技巧。

总结题

此题为 反馈建议题 。将自己的建议想法 发给我。只要认真写的我都回复。不认真写的，我也回复让认真写了。回信签名里有 flag 。



the flag is {have.a.good.time}

poem题

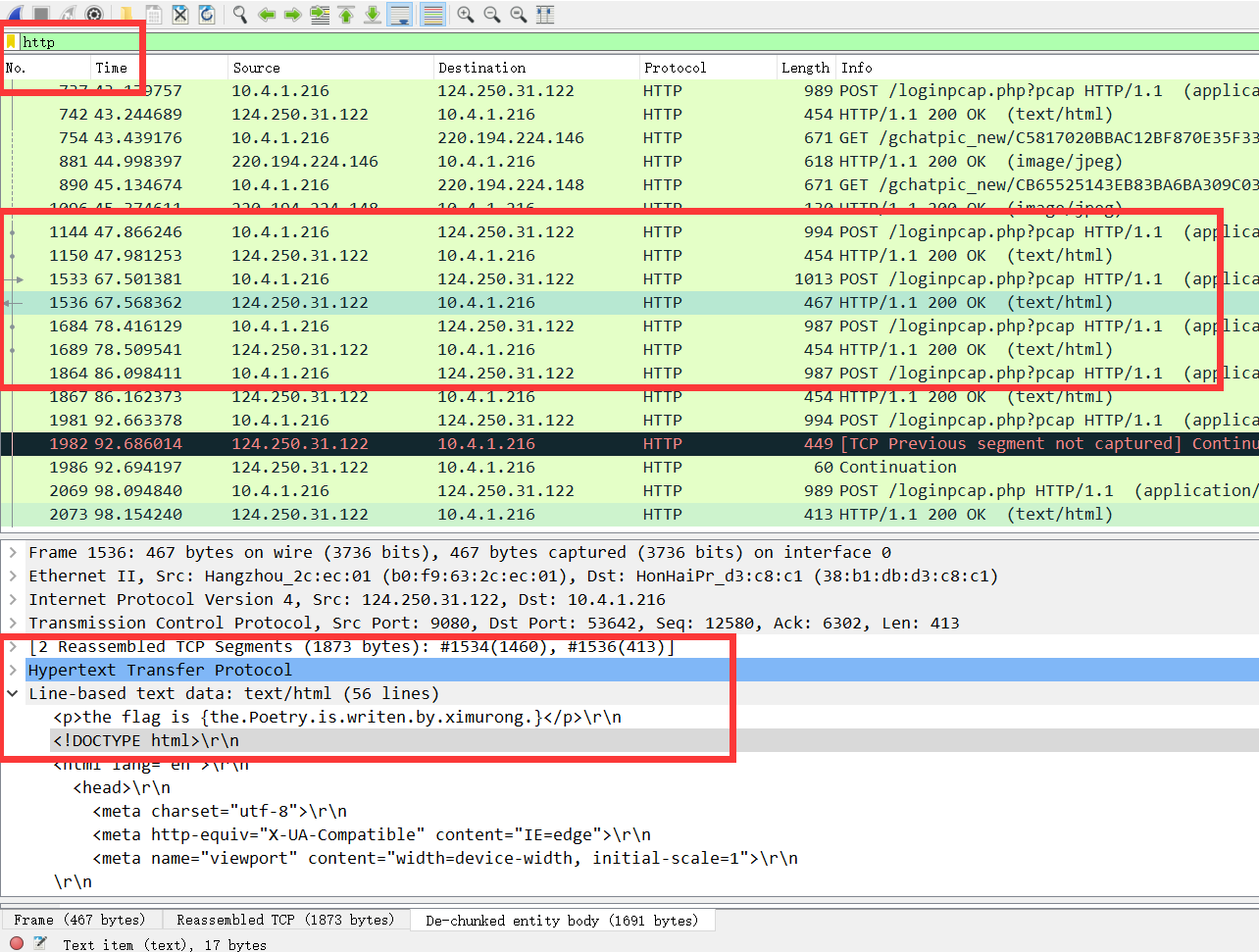
此题为网络包分析题。

下载文件，将后缀改成pcap格式。

url中的文件名，跟标题名都有pcap的提示。

使用iwreshark等打开。

获取 flag



<p>the flag is {the.Poetry.is.writen.by.ximurong.}</p>

此题中需要改后缀名，低分题中也有一个要改后缀名的。所以题目外放顺序是从低到高的。题目本身也有提示。

File题

由HINT知，文件加载用的为常用单词。所以使用load等尝试



the flag is {check.the.auth}

此题 模拟的是 安全测试中的任意文件读取/加载漏洞。

find题

此题模拟的是 平行越权漏洞。场景有 订单，用户信息，学生考试分数等查询功能的越权

查看题目URL，id=1，遍历ID到1101的时候，查看源代码。



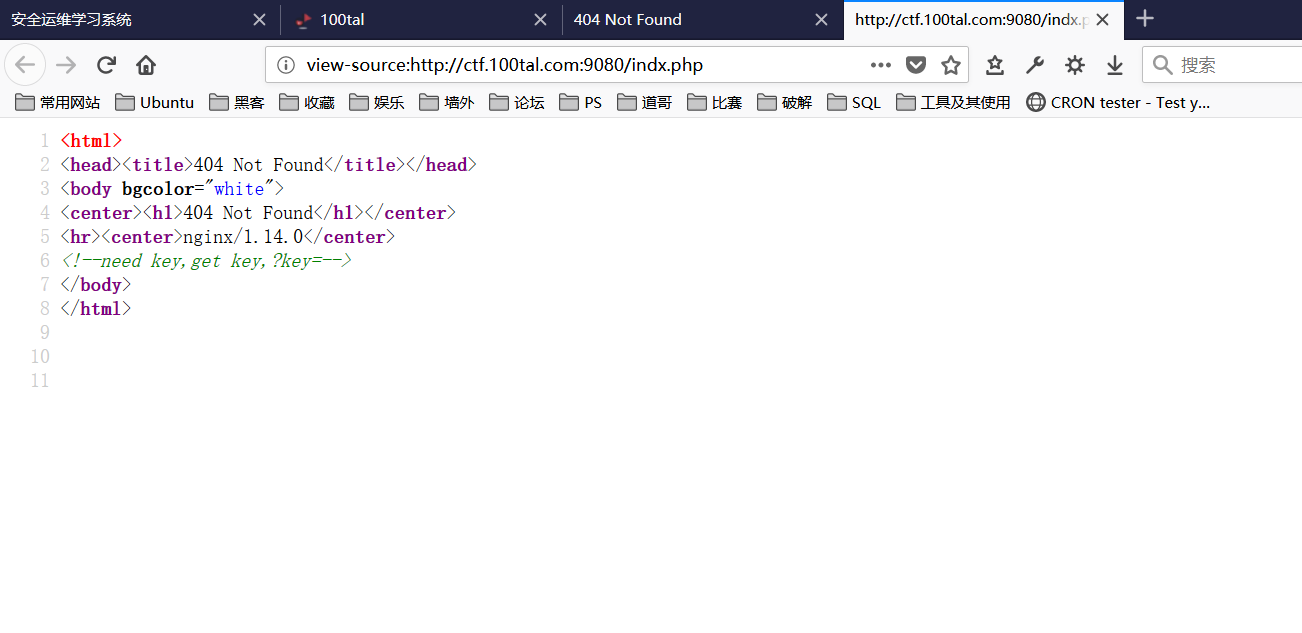
将 注释中的 数字 ASCII解码，获得flag

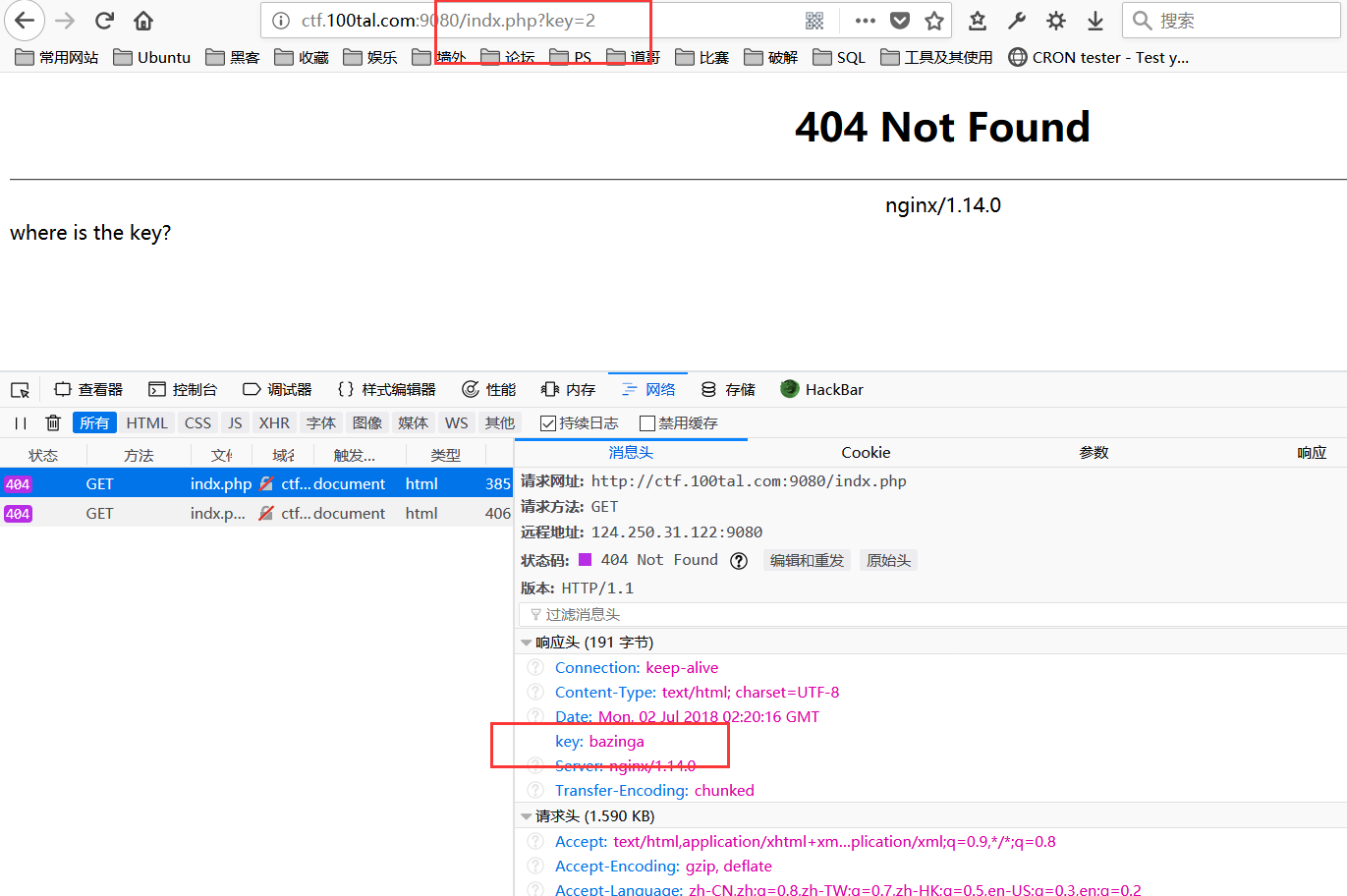
The flag is {yahaha!you.found.me}

眼见为假亦为真 题

观察题。观察请求包，返回包。

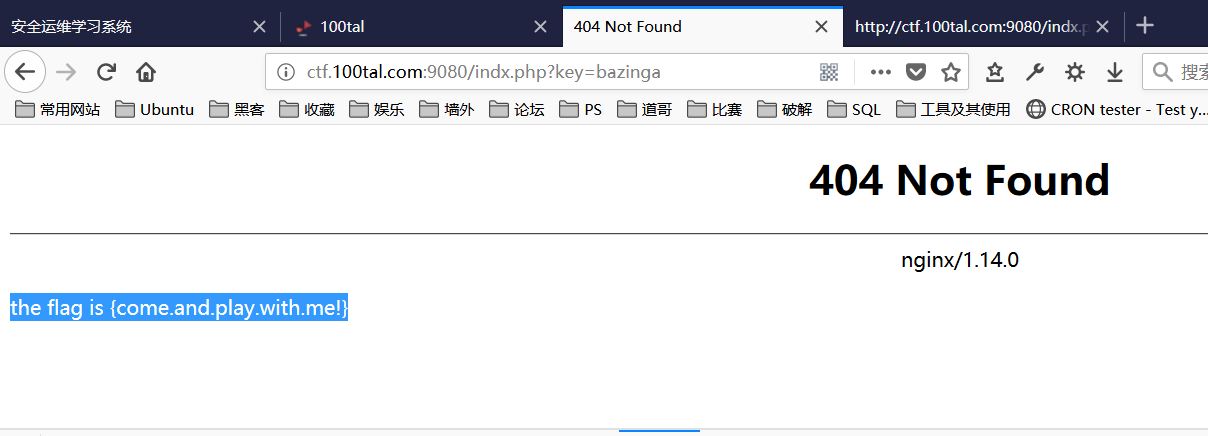
查看源代码发现提示

使用提示



查看请求包发现返回 key

使用key



the flag is {come.and.play.with.me!}

hide 题

隐写 加解密的混合题

查看源代码发现，除了图片还有一个迅雷链接



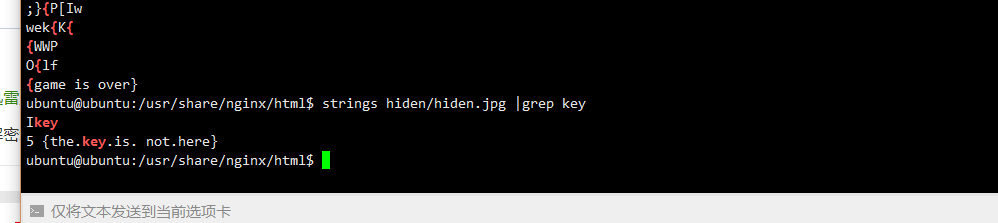
thunder://QUEuL2hpZGVuLzlhMmQ4Y2UzZmZkY2RmMjEyM2JkZGQ5NGQ3OWVmMjAwLnppcFpa 此链接为迅雷加密连接，解密为



下载图片，下载压缩包

将图片以txt等方式打开，可以找到几个字符串

关键信息为

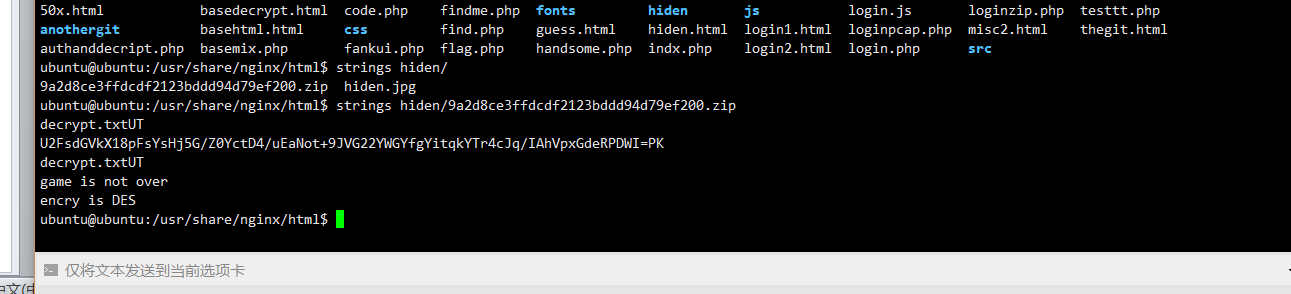


{the.key.is. not.here}

{game is over}

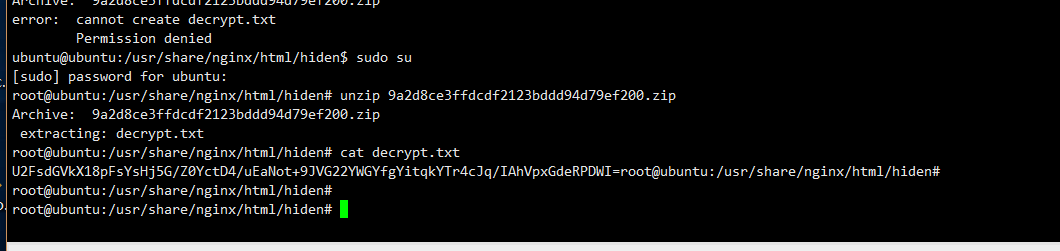
图片信息并没有 the flag is {}字样。图片信息有 game is over 字样。

查看压缩包



发现 game is not over字样，加密方式为DES加密。

解压压缩包，发现decrypt.txt 文件。



使用DES方式解密字符串



获取flag

the flag is {the.show.is.doctor.who}

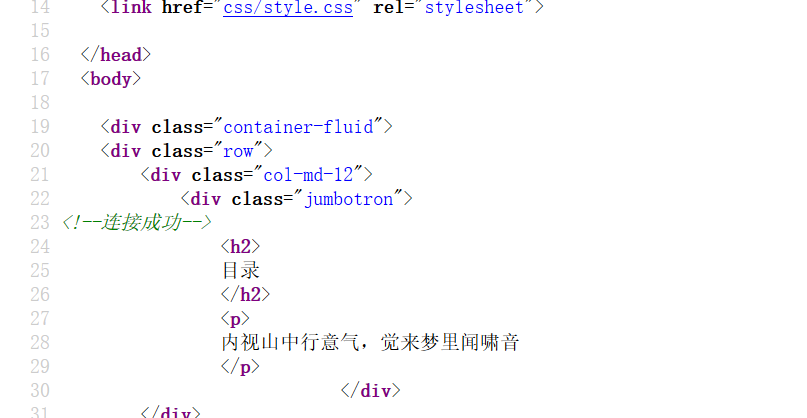
information 部分

findme 题

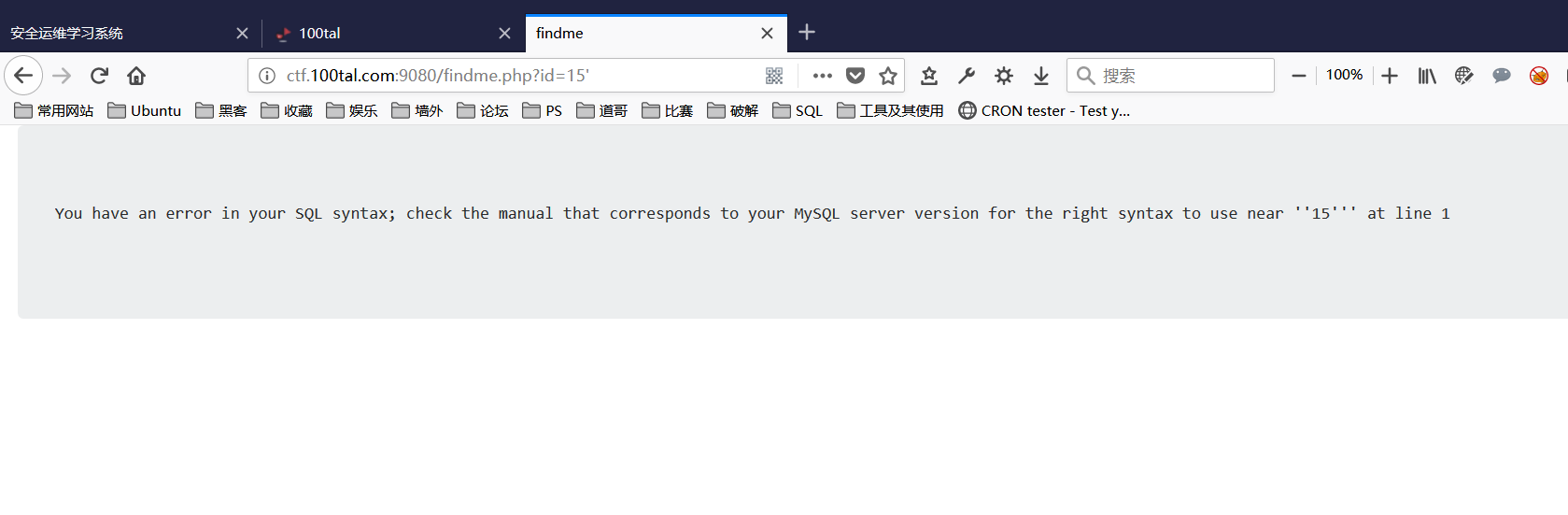
SQL注入题

查看URL发现ID=字样，改变ID数值，发现内容随之改变。

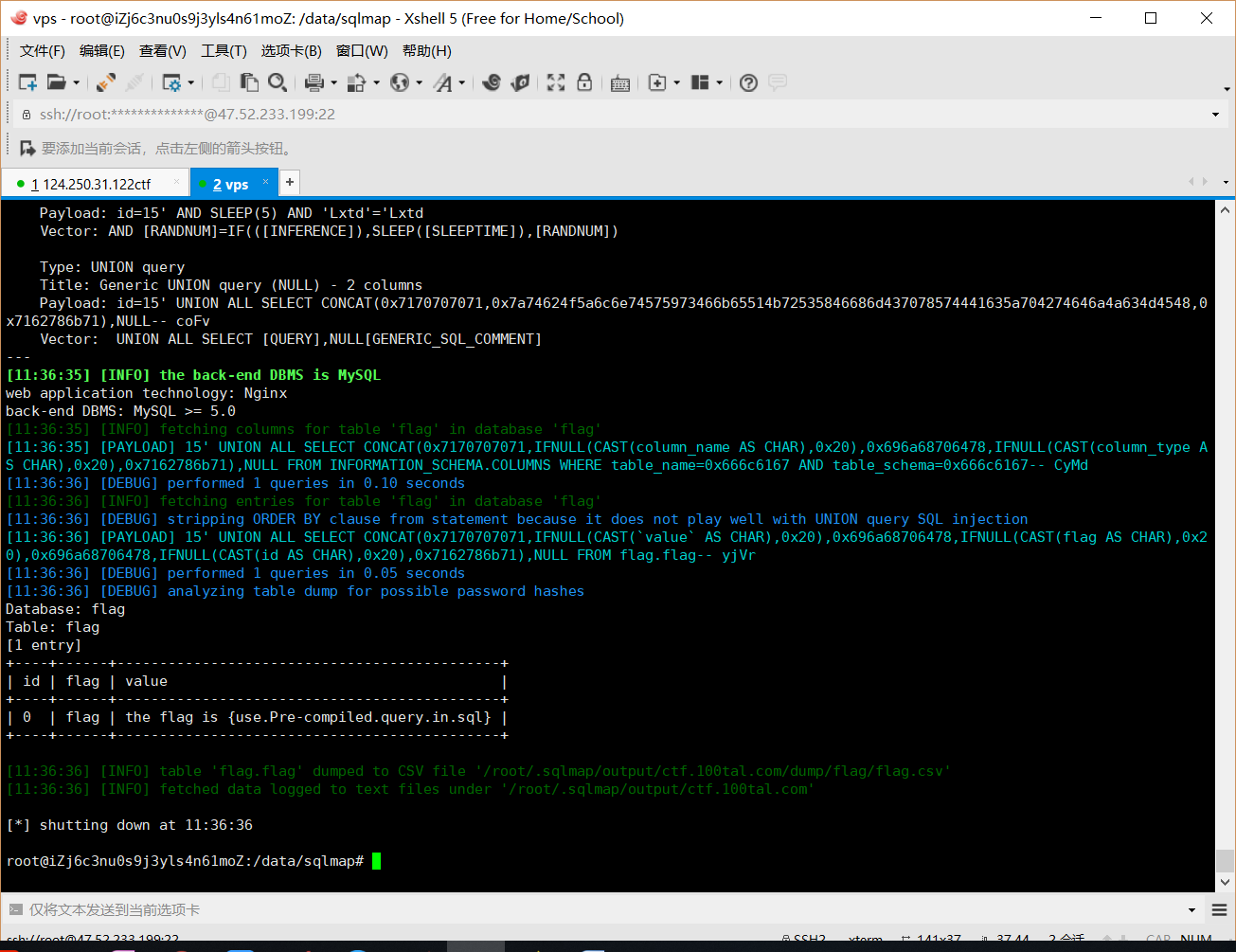
查看源代码，发现



使用 ’ 字符来测试是否是sql 注入，发现报数据库错误

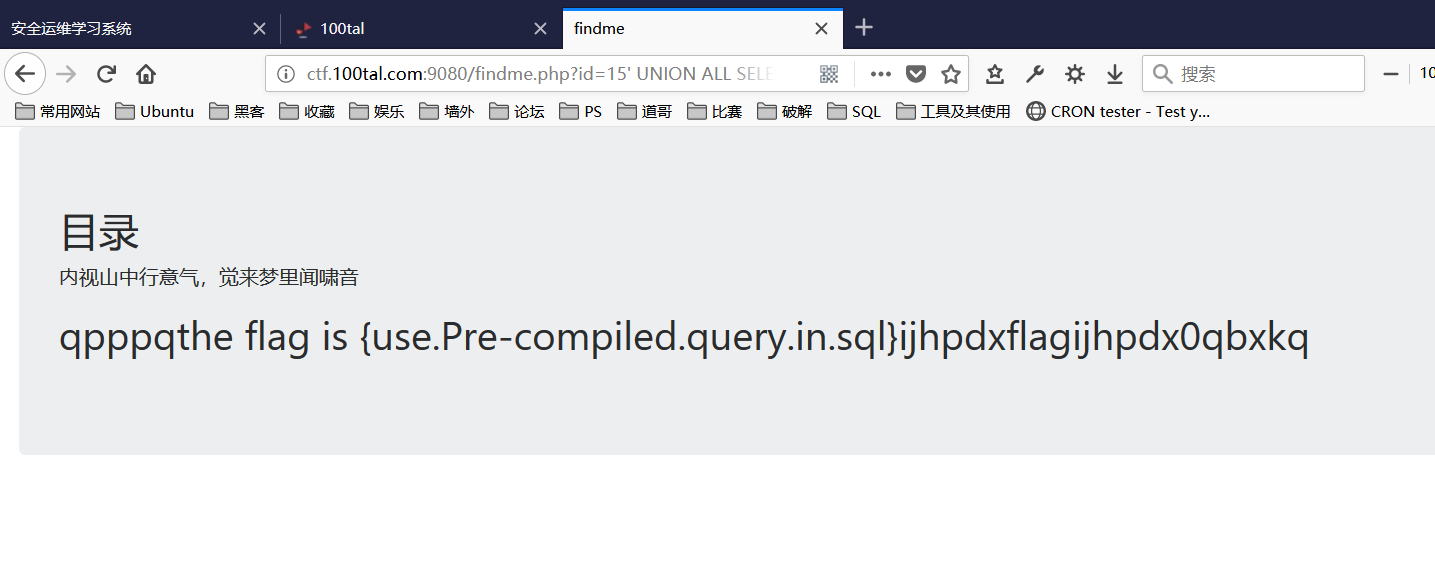


确定存在sql注入，使用sqlmap测试



完整url 为

ctf.100tal.com:9080/findme.php?id=15' UNION ALL SELECT CONCAT(0x7170707071,IFNULL(CAST(`value` AS CHAR),0x20),0x696a68706478,IFNULL(CAST(flag AS CHAR),0x20),0x696a68706478,IFNULL(CAST(id AS CHAR),0x20),0x7162786b71),NULL FROM flag.flag—yjVr

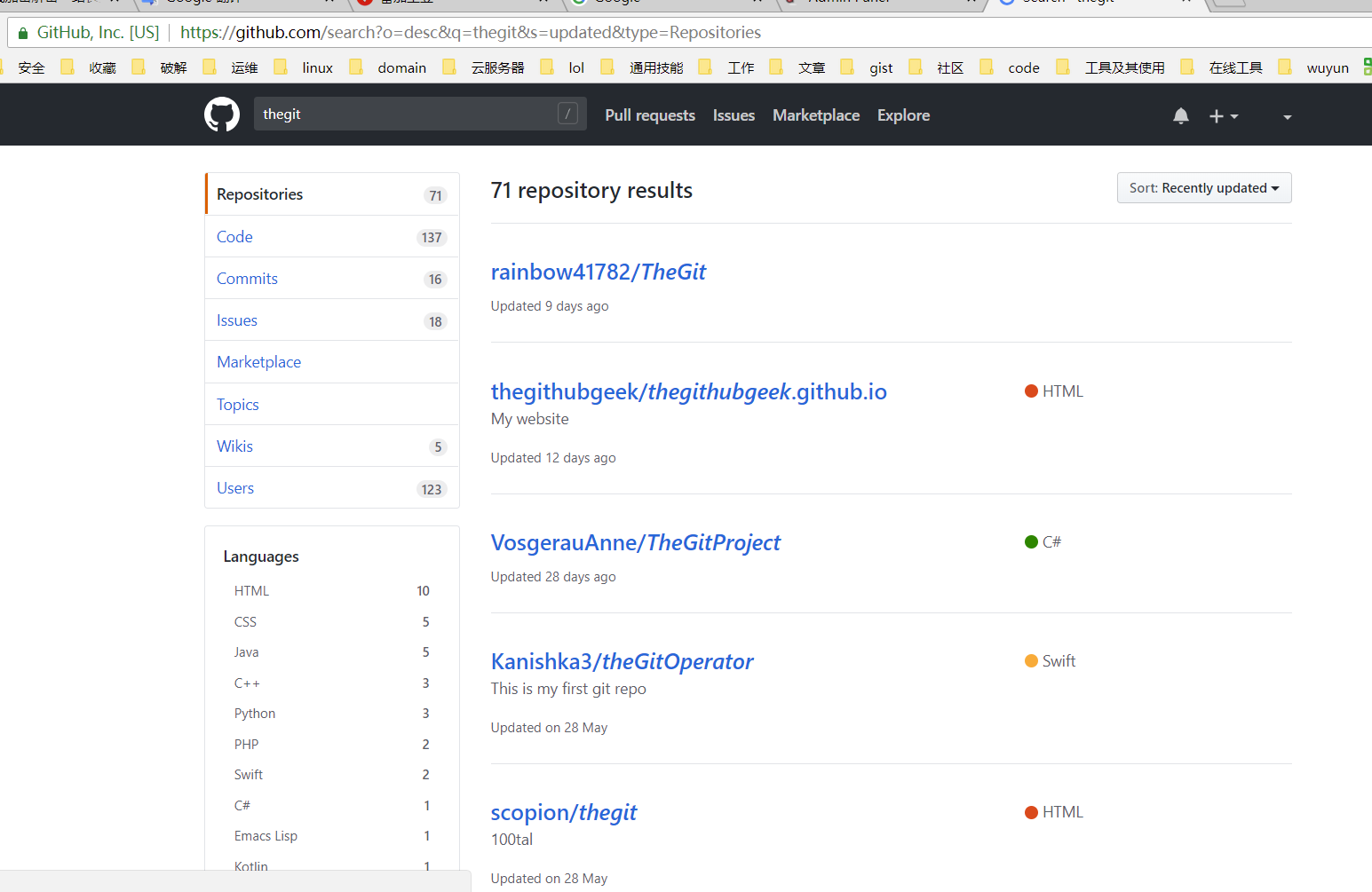


获取flag

the flag is {use.Pre-compiled.query.in.sql}

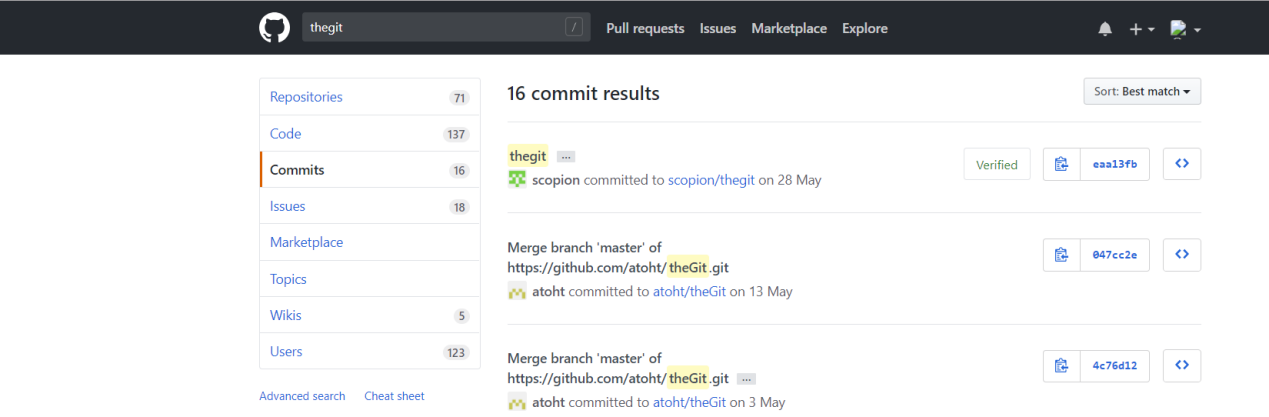
thegit 题

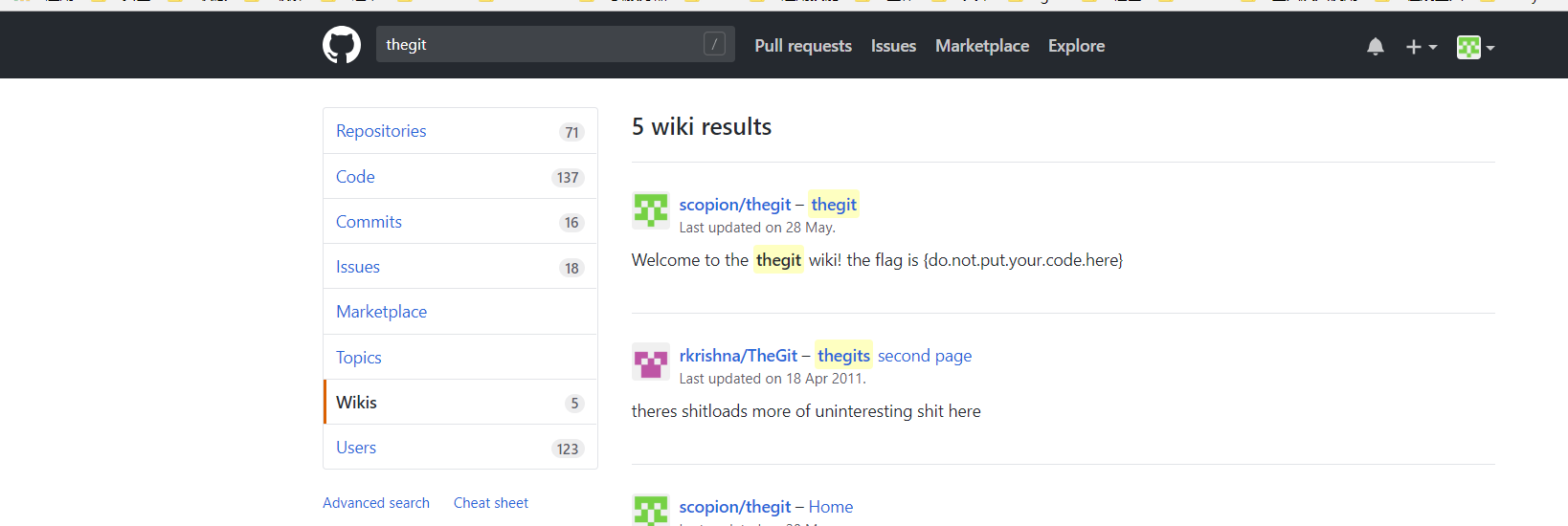
本题为 信息搜索题。Thegit 意指 GitHub 。在 GitHub中搜索 thegit 字符



这里注意排序方式，使用时间最近排序。因为CTF比赛是6月刚刚弄。所以在本题出现时使用此排序方式，第一个应该就是我。简介中有100tal字符。

另为了使搜索方便，此项目中多处有关键字。



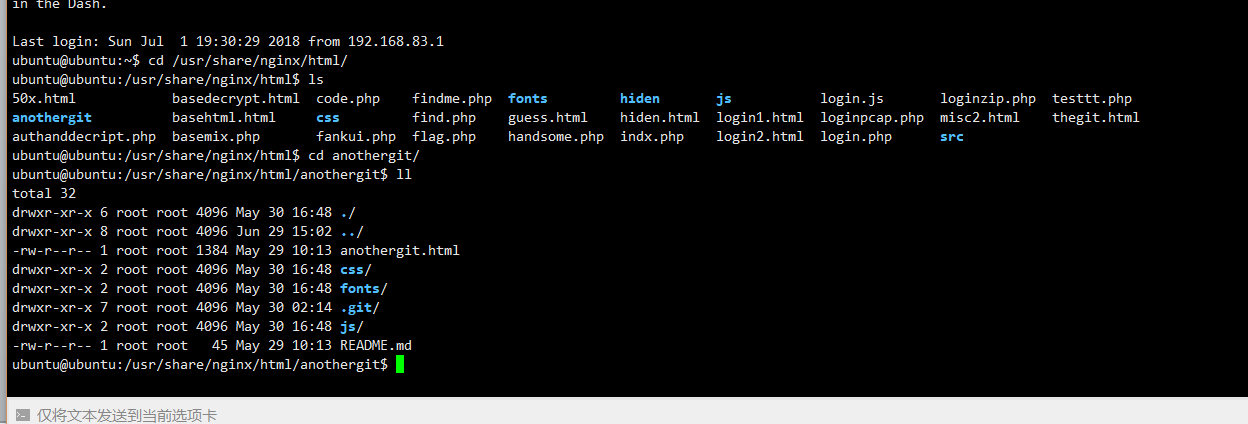


使用wiki选项搜索的时候，可以直接获得flag

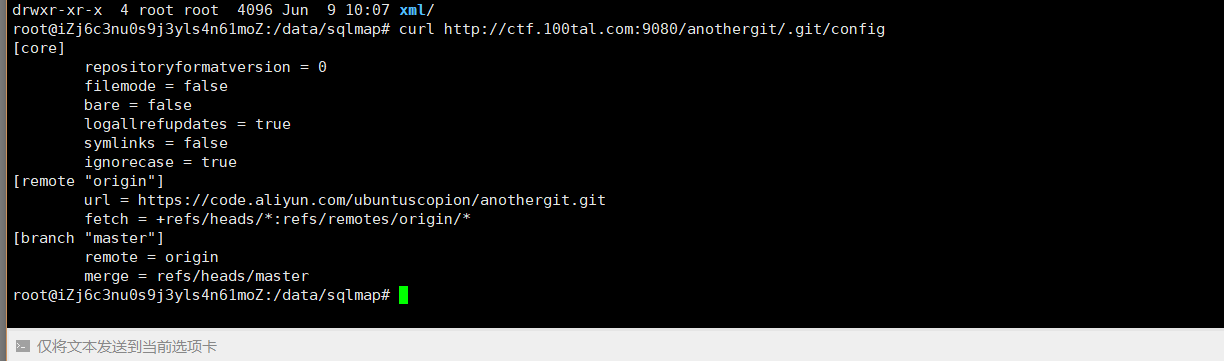
the flag is {do.not.put.your.code.here}

another 题

此题为 文件下载题。模拟了git文件泄露的情况。在git项目中存在.git的隐藏文件夹，若是项目上线的时候，将此文件夹一同上线，那么就会有代码泄露的风险。

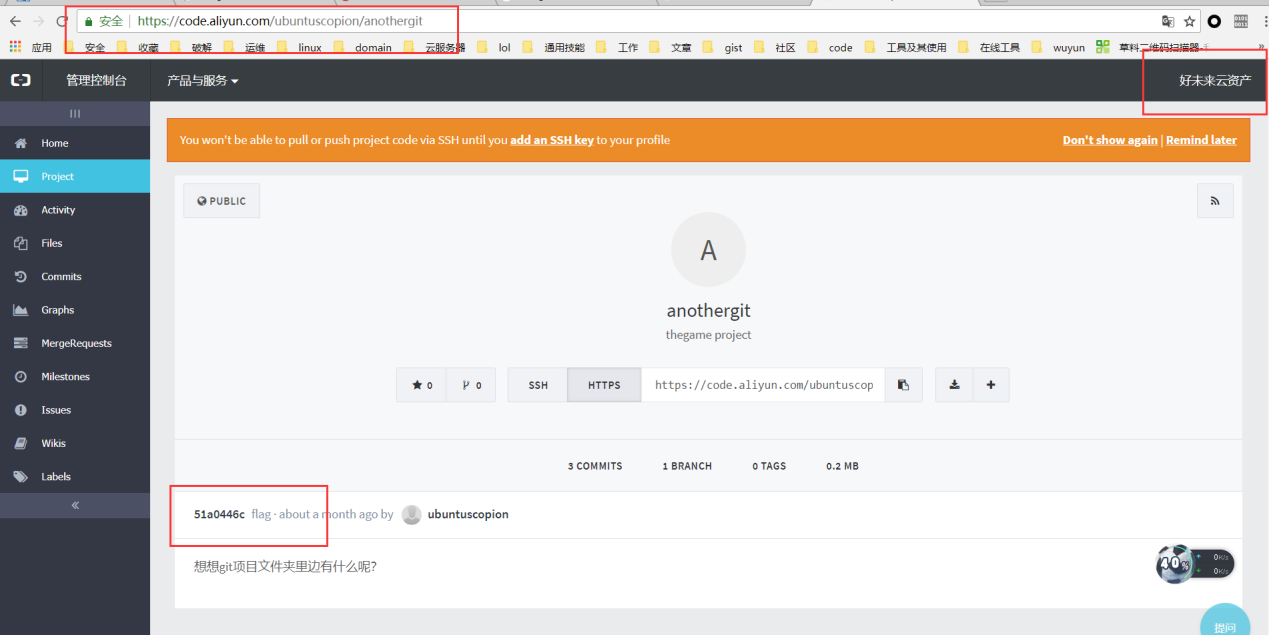


一般测试步骤是请求 /.git/config文件。



如图，可得项目地址

使用阿里云账户访问 项目地址



可得flag

the flag is {must.set.private.project}

every thing is connected 题

此题模拟 社工攻击，信息收集攻击

根据 ”让兴趣，更有趣“ 搜索得出，此为 网易乐乎 的广告词。



乐乎中个人主页地址为 昵称.lofter.com

结合code题的答案 ，我的个人主页地址为 <http://scopioncn.lofter.com/>

查找博文，得flag

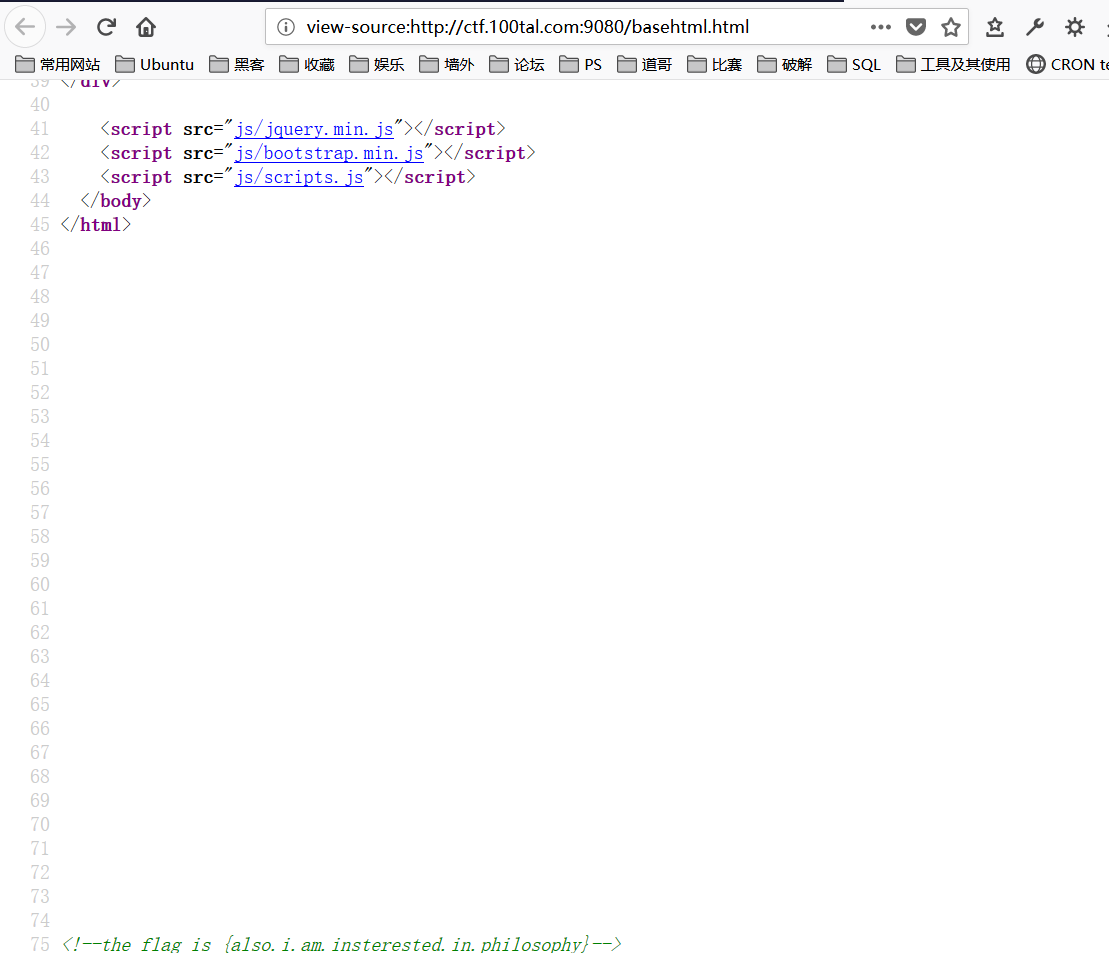
the flag is {i.get.these.from.novel}

base 部分

basehtml 题

此题为 简单信息泄露题。开发过程中的注释，测试代码，to do list 等信息上线时没有处理的话可能会造成敏感信息泄露

查看源代码，拉到最后，获取flag

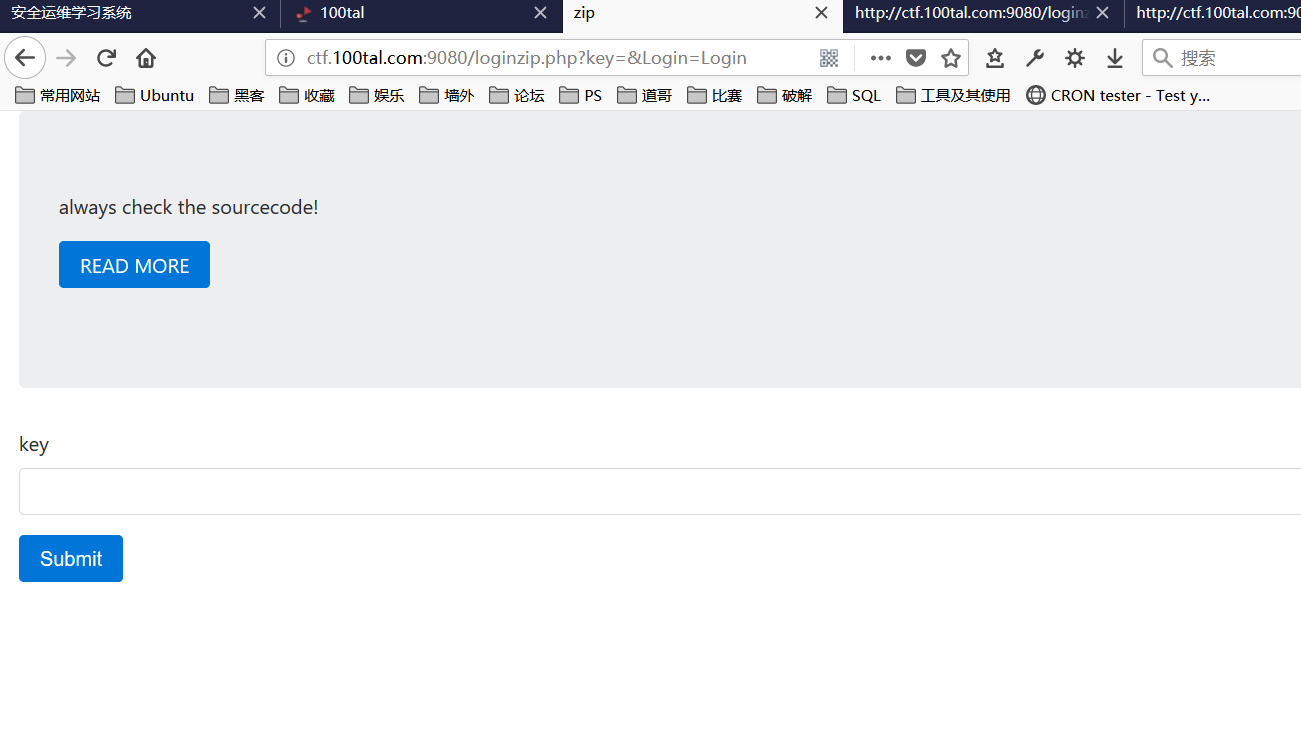


<!--the flag is {also.i.am.insterested.in.philosophy}-->

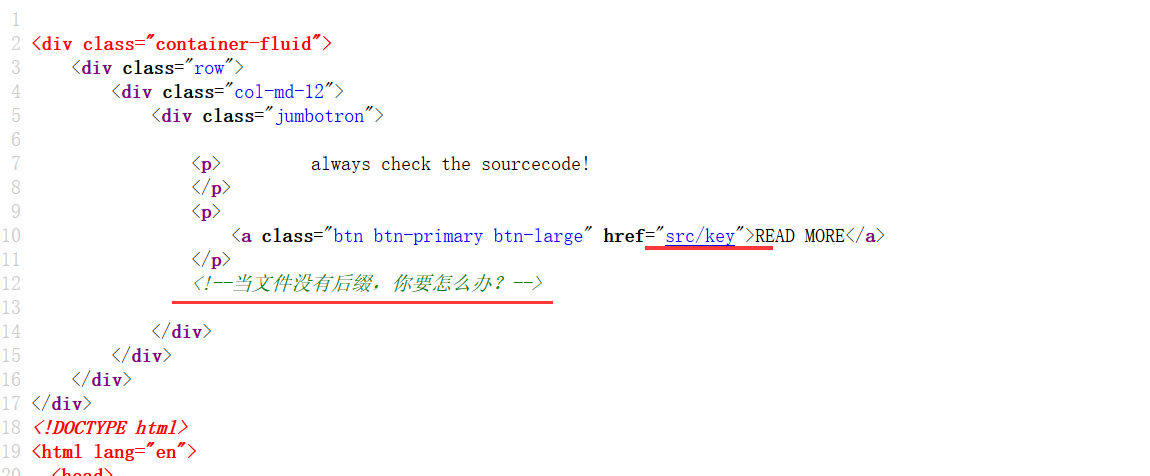
Basesuffix题

Suffix 意为后缀。此题要改后缀，乃是为后面的网络包分析题铺路。

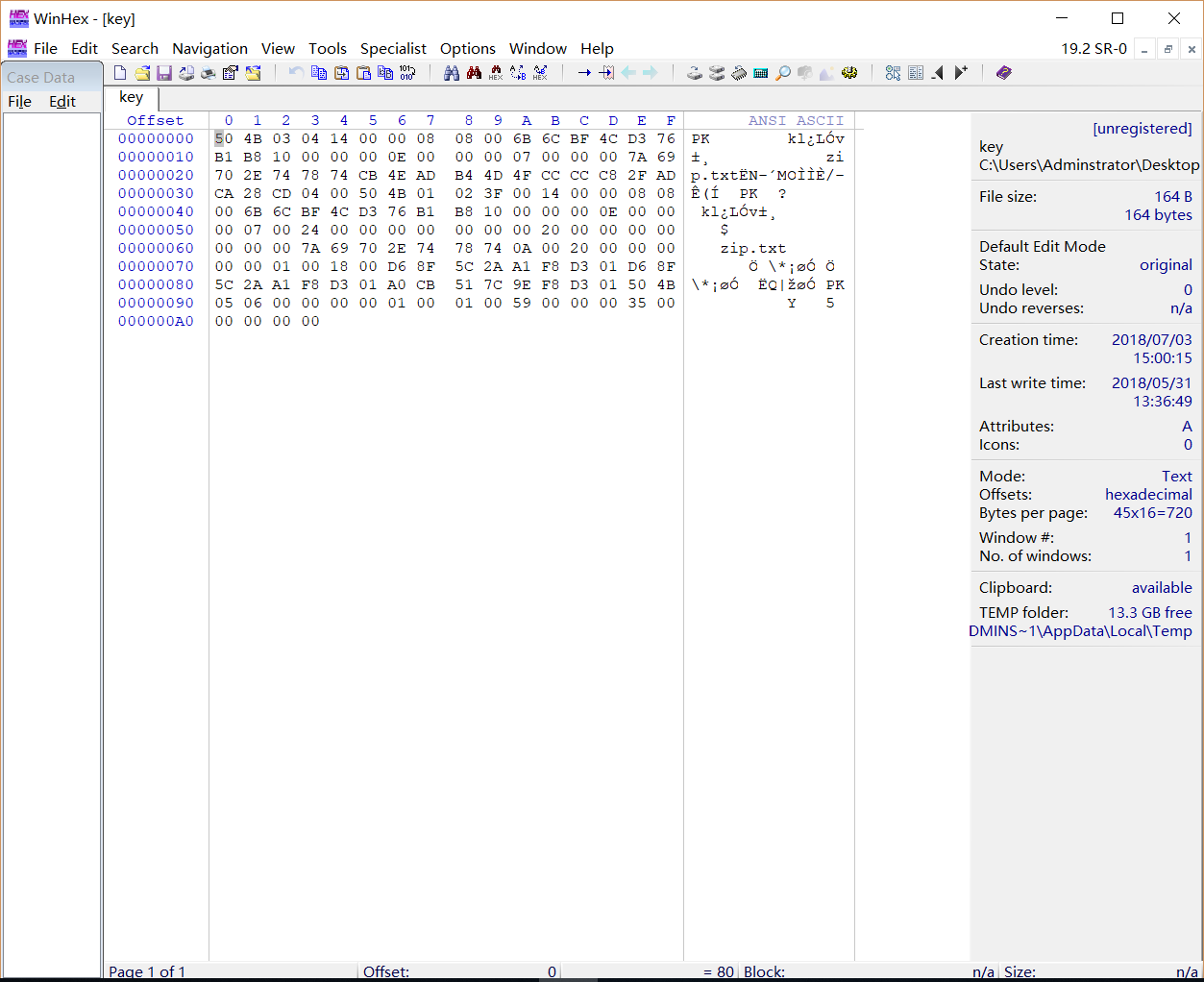
题目只有一个登录框，在源代码，消息头头没有任何提示，所以随便提交什么，返回这个页面



提示我们查看源代码，发现

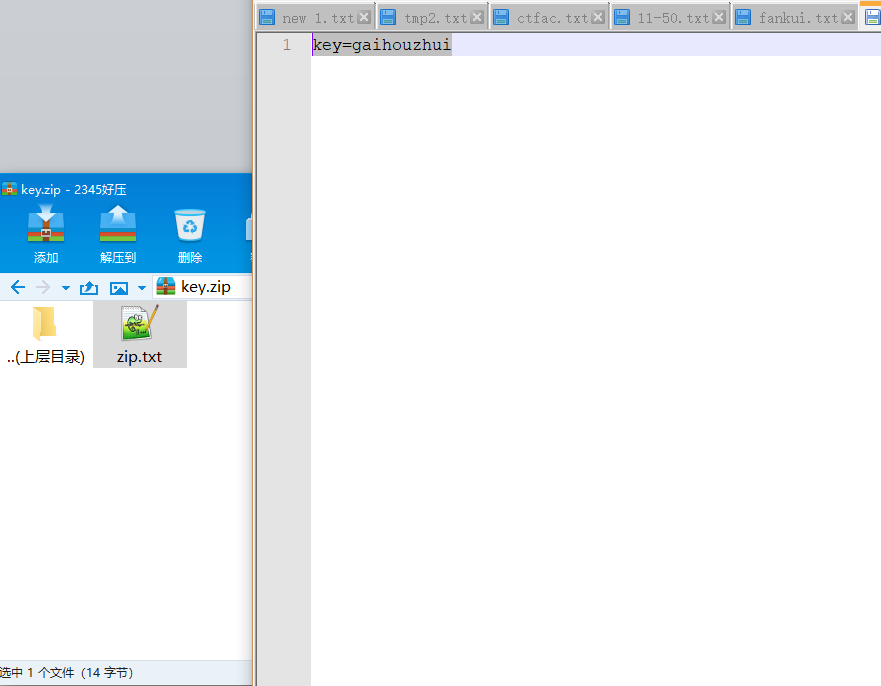


下载此文件，使用hex打开查看文件头为PK

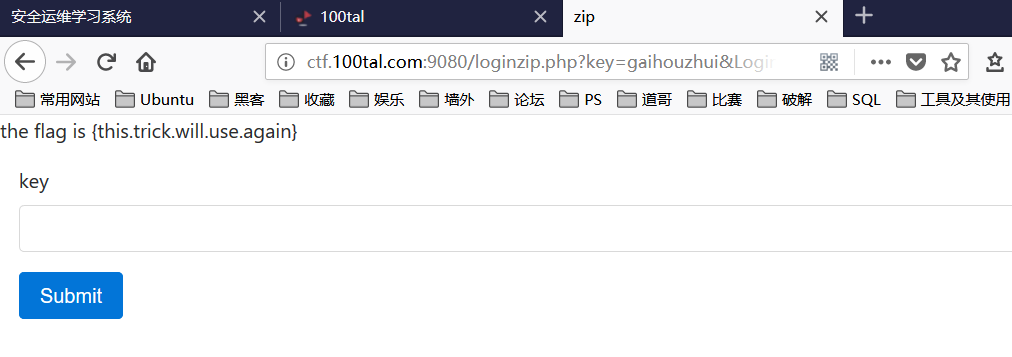


得知此为zip文件，结合题目标题以及url确定

将此文件解压获取txt



提交key,获取flag



the flag is {this.trick.will.use.again}

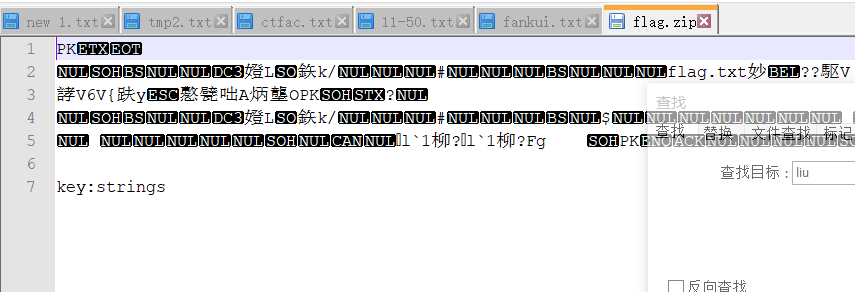
意指 改后缀会再次用到，也指 先获取key ，再获取 flag 的步骤。

after baseimg 题

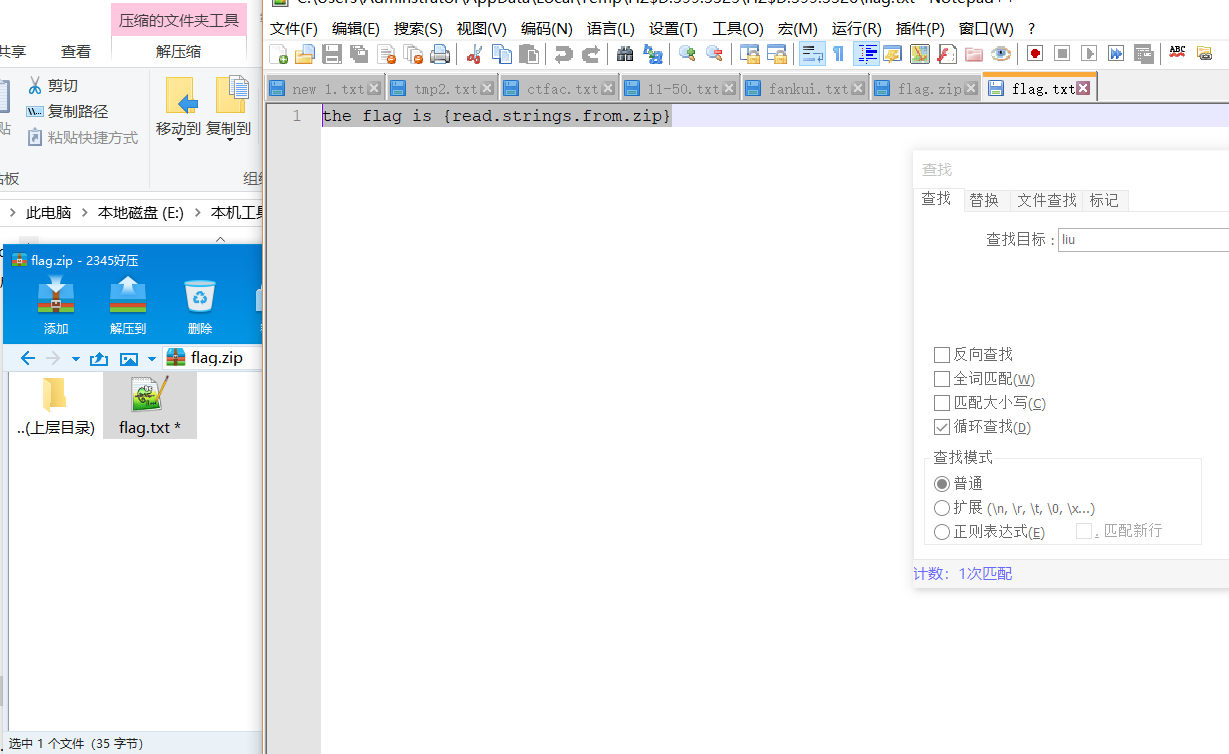
此题的关键提示点就在题名

在img题中，是用txt 方式查看图片，获取flag

在这，也是要用txt方式查看 zip 文件，获取解压密码



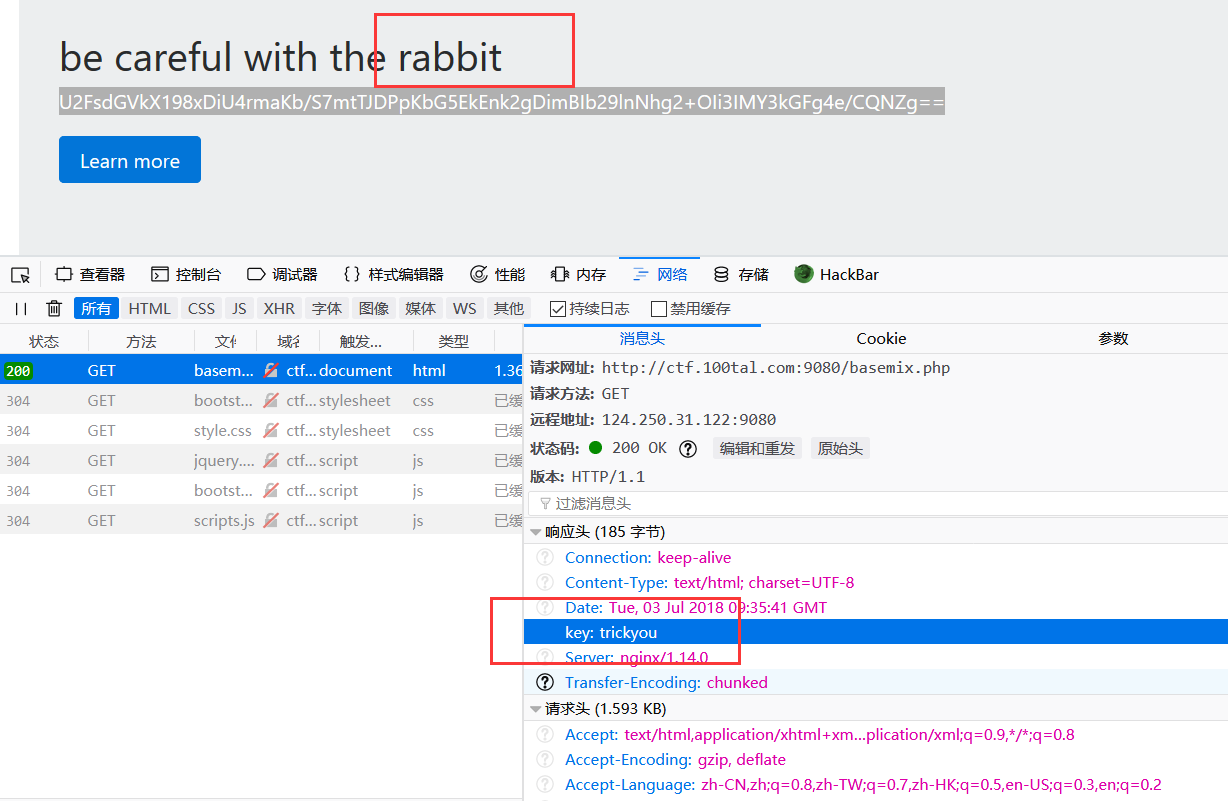
解压文件



the flag is {read.strings.from.zip}

the first mix 题

此题为rabbit 解密

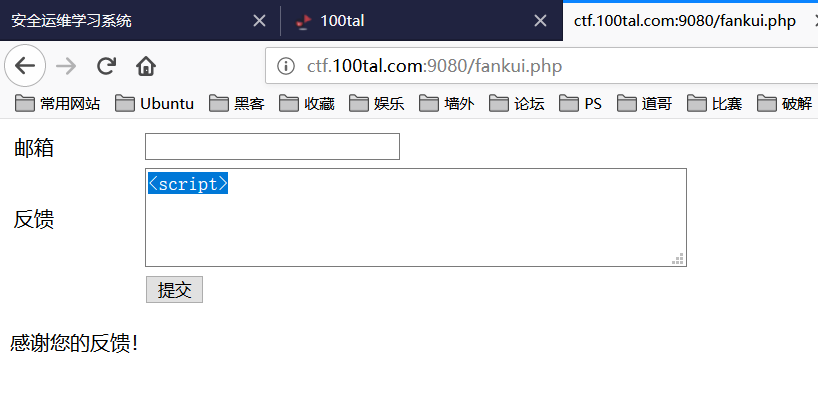




the flag is {every.thing.here.is.in.used.}

反馈 题

此题为XSS 题。模拟XSS攻击场景。提交内容中有 <script> 标签即可。



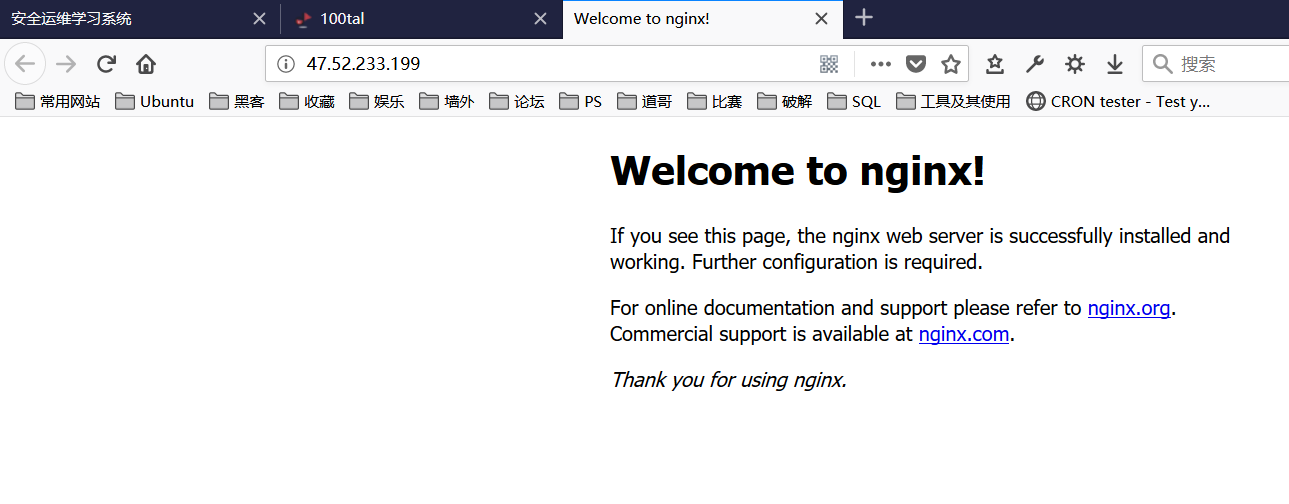
提交之后查看源代码



Nosql题

此题为第三方组件未授权访问。这里以mongo为例，介绍了第三方组件在使用时不设置用户校验会导致严重信息泄露。

题目地址给的是一个普通的nginx页面，而题名叫nosql。查看此IP端口，发现27017端口。



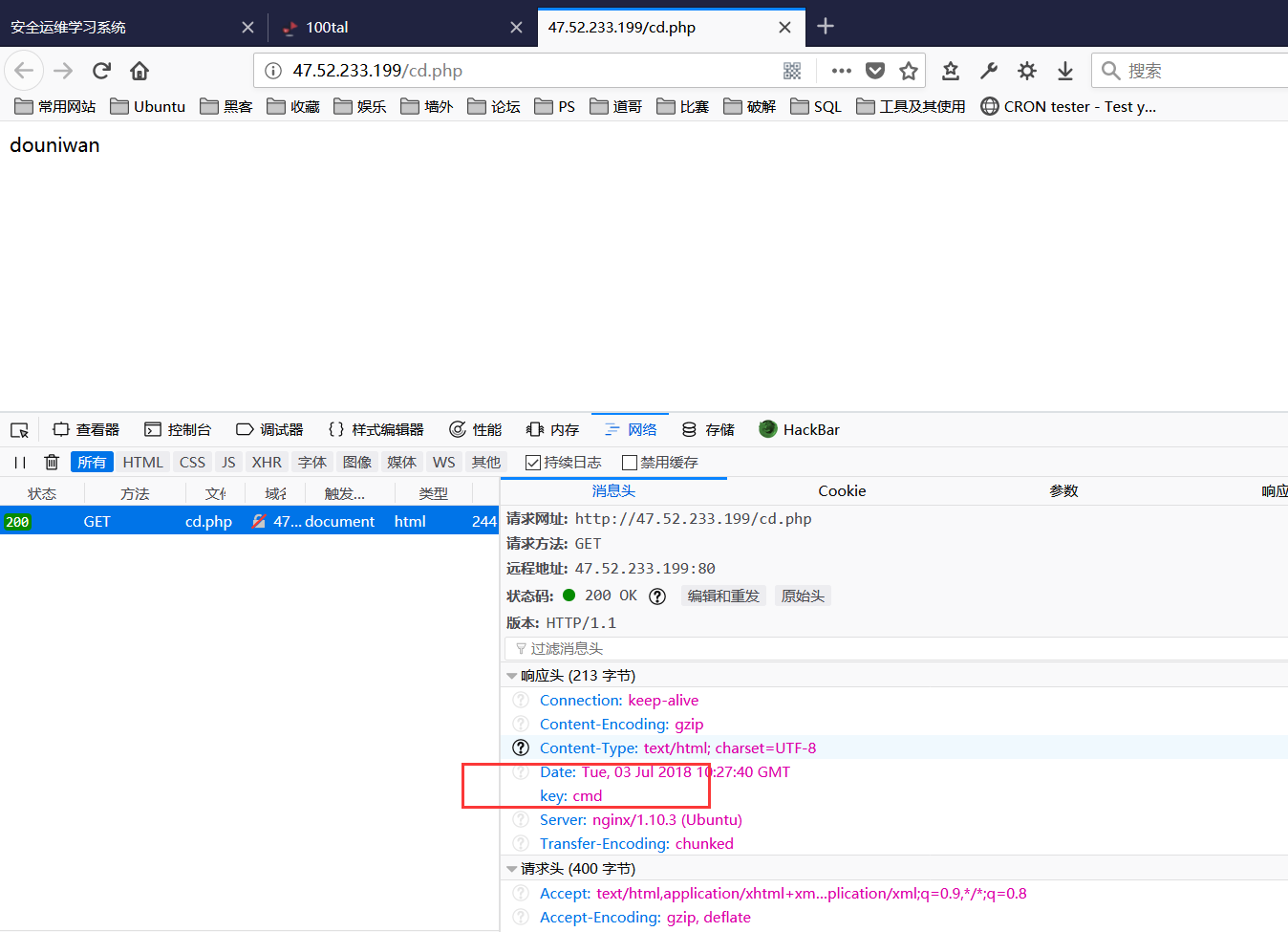
使用mongoclient连接端口，获取flag



the flag is {always.set.auth}

cd 题

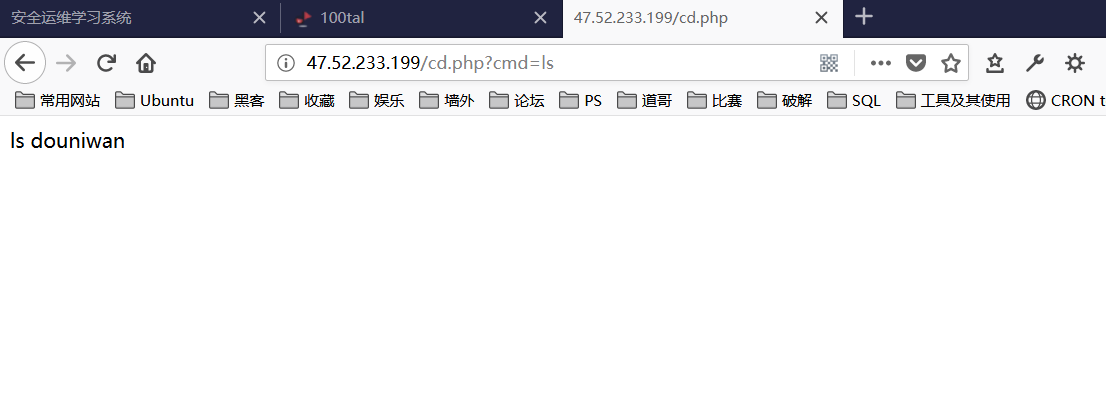
此题为命令执行漏洞。在实现命令执行功能/调用系统函数时，没有对用户输入进行过滤，导致任意命令执行。访问页面，发现key



Key=cmd

使用 <http://47.52.233.199/cd.php?key=cmd> 或 http://47.52.233.199/cd.php?key= X 访问，页面没有任何变化

所以key不是参数，cmd才是参数。http://47.52.233.199/cd.php?cmd=ls

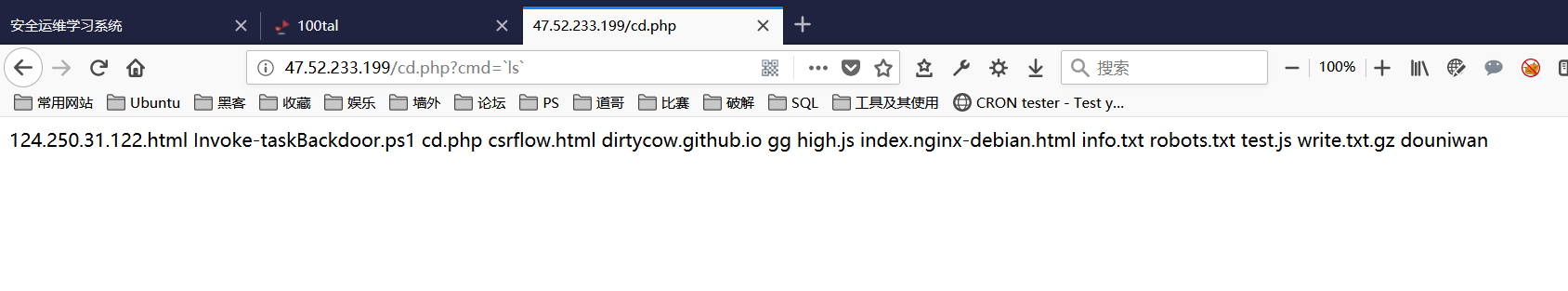


发现返回 ls字符，即返回参数内容。

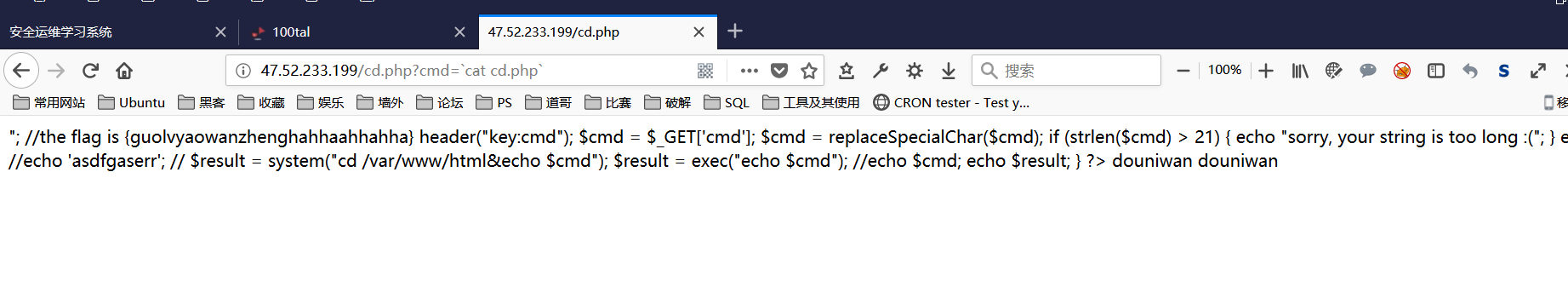
测试特殊符号，发现系统过滤了大部分的特殊字符，当使用` 字符时出现了异常，猜测关键点就在这。

在linux系统中，使用` 括起来的内容会被当做命令执行。

访问 [http://47.52.233.199/cd.php?cmd=`ls`](http://47.52.233.199/cd.php?cmd=%60ls%60)，发现执行了ls命令



输出文件本身 [http://47.52.233.199/cd.php?cmd=`cat%20cd.php`](http://47.52.233.199/cd.php?cmd=%60cat%20cd.php%60)，获取flag



the flag is {guolvyaowanzhenghahhaahhahha}

i am .handsome 题

此题为上传题，考任意文件上传。

按照一般思路，php环境上传php网马文件，返回



它说我的思路是对的。要更改后缀。

查看题名，发现线索，上传.handsome文件



thank you !the flag is {yes!i.am.so.good.}

auth 部分

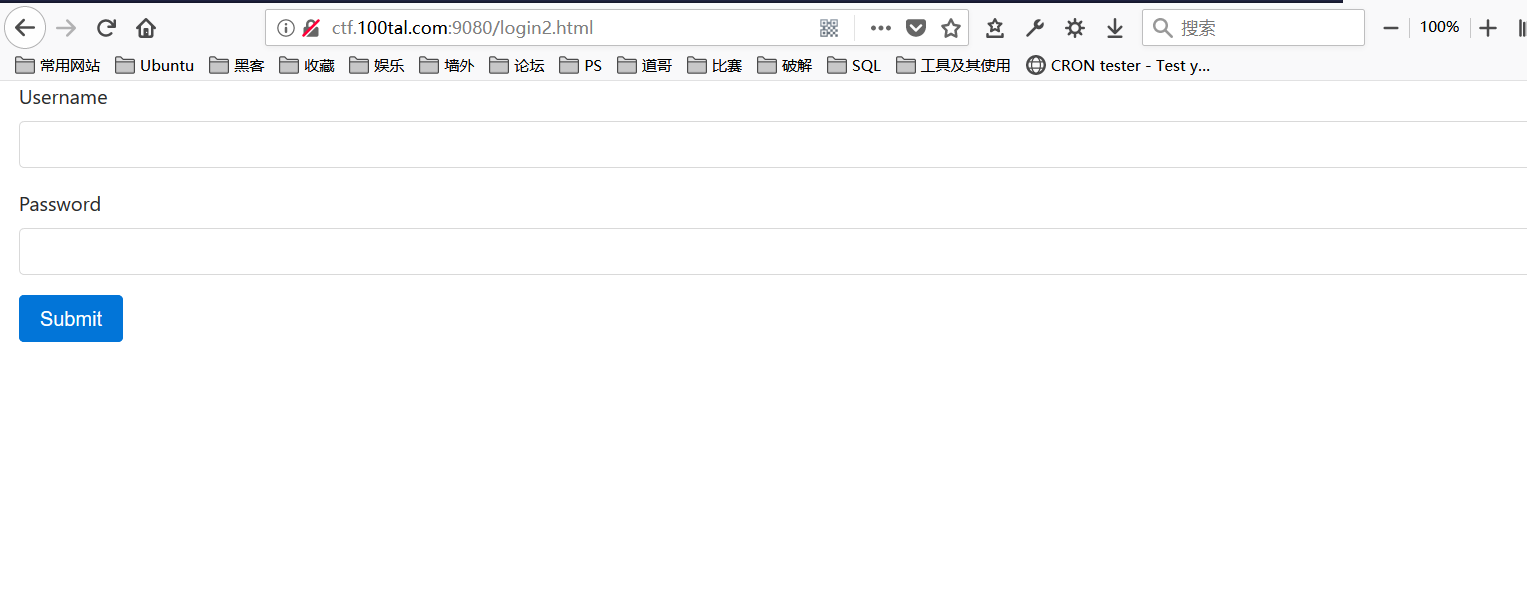
i am not alone 题

此题为脑洞 + 前端校验 混合题。场景为 多版本迭代 + 历史文件/代码 的管理问题。

访问题目地址 <http://ctf.100tal.com:9080/login1.html> ，查看注释以及提示

讲的是 121，121，121，121

观察url 发现 login1.html ，访问login2.html ，发现相同页面



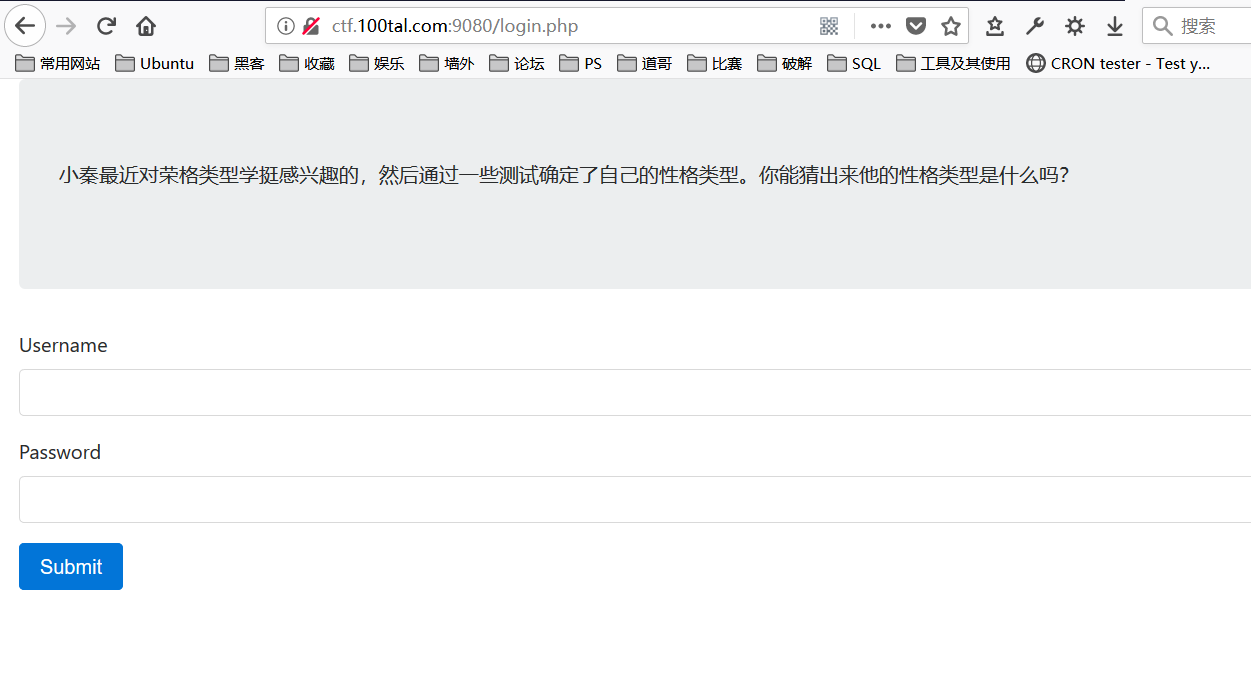
提交任意 用户名密码，发现js校验



alert("the flag is {oops.i.forget.the.old.version}")

mbti 题

此题为暴力破解题。查看源代码发现，注释说都用大写，用户名为xiaoqin,荣格性格类型共 16种。爆破



当使用INTJ 时，获取flag



the flag is {i.am.interested.in.psychology}