WEB:

21:这TM是啥
去掉奇怪的js代码最后的 (); 剩余部分复制到chrome控制台中运行。即可得到正常的js代码

```
function anonymous() {
var f = "hctf{j5fuck_1z_m1233}"; alert("Hack by LoRexxar, 你的flag被我拿走了")
}
```

22:我是谁我在哪？？？
burpsuite抓包，查看response头
```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Fri, 20 Jan 2017 08:28:19 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.4.41
flag: hctf{1t_iz_4_4mall_tr1ck}
location: index.html
Content-Length: 94
```

25: 神奇的数字
is_numeric函数会跳过space,\t,\n,\r,\v,\f
trim会删去space,\t,\n,\r,\v,\0.没有\f
因此只要加上%0c就能绕过。
ps: php7.1下测试0.1e1通过。

26: 不可能拿到的flag
由于sha1的参数不支持数组，所以，只需要发送name[]="123"&password[]="456"即可通过
sha1得到结果均为false

27:php真可怕我要回农村
(int)(0.1+0.7100000000000)*10=8
虽然我不知道为什么，但反正结果就是这样的

RE:

28: 你看看，逆向多简单！
IDA查一下字符串就出来了

PWN:

24: pwn step0
IDA看一下，有个判断要求123456==aaaaa (大概是这样的，具体忘了)
实际操作的时候只需要发足够多的a就能栈溢出覆盖数字

MISC:

30: Explorer的图库之三
Stegsolve打开加密图片后，选择Analyse-DataExtract
Bit Planes 选中Reg、Green、Blue的第0位
然后就看到一段base64加密的数据。解密后即为flag

31:Explorer的图库之二
Binwalk -Me downloadfile 就跑出来了。直接明文显示。

32:Explorer的图库之一
右键-文本打开 就看见了。

38：explore的奇怪番外1
写了个python脚本

```
import socket
import sys
import binascii
HOST = '121.42.25.113'    # The remote host
PORT = 20000              # The same port as used by the server
s = None
for res in socket.getaddrinfo(HOST, PORT, socket.AF_UNSPEC, socket.SOCK_STREAM):
    af, socktype, proto, canonname, sa = res
    try:
        s = socket.socket(af, socktype, proto)
    except socket.error, msg:
        s = None
        continue
    try:
        s.connect(sa)
    except socket.error, msg:
        s.close()
        s = None
        continue
    break
if s is None:
    print 'could not open socket'
    sys.exit(1)
data=s.recv(1024)
print data,
data=s.recv(1024)
print data.encode("hex"),
while data!='':
        if data.encode("hex")=="72656164793f3a" or data.encode("hex")=="0a72656164793f3a":
                send="yes\n"
                s.sendall(send)
                print send,
                data=s.recv(1024)
                print data,
        else:
                while 1:
                        s.sendall("ready\n");
                        data=s.recv(1024);
                        print data
s.close()
```

写的不咋样。有些地方怪怪的主要是遇到了些奇怪的问题。

CRYPTO：
19：密码学教室入门（二）
最基本的凯撒，{}_不需要替换

```
#include "stdio.h"
int main(){
        char c;
        c=getchar();
        while(c!='\n'){
                printf("%c",c-17);//这里没管{}_，最后人工替换
                c=getchar();
        }

        return 0;
}
```

18：密码学教室入门（一）
写了个脚本

```
import os
import sys
import math

def my_RSA_decrypt(src, e, n):
    y = pow(src, e, n)
    print '*'*77
    print "Decrypted Data is:"
    print hex(y)
    print '*'*77
    return y
```

n=p*q，e=d，src=c
打印出的结果decode("hex")即可

33：密码学教室入门（四）
跟18题相同。n直接给出

PENTEST：

14：lightless的渗透教室入门篇（一）
burpsuite修改表单

```
POST /pentest/01/?hacker=HelloGet HTTP/1.1
headers......
....
....
...

hacker=HelloPost
```

16:lightless的渗透教室入门篇（三）
burpsuite查看response头，可以cookiecontent: admin=1 and isLogin=true
添加cookie，admin=1和isLogin=true即可

PS:页面注释里那行<!-- Post me a hint can give you some hints... --> 是骗我的吗！！