web

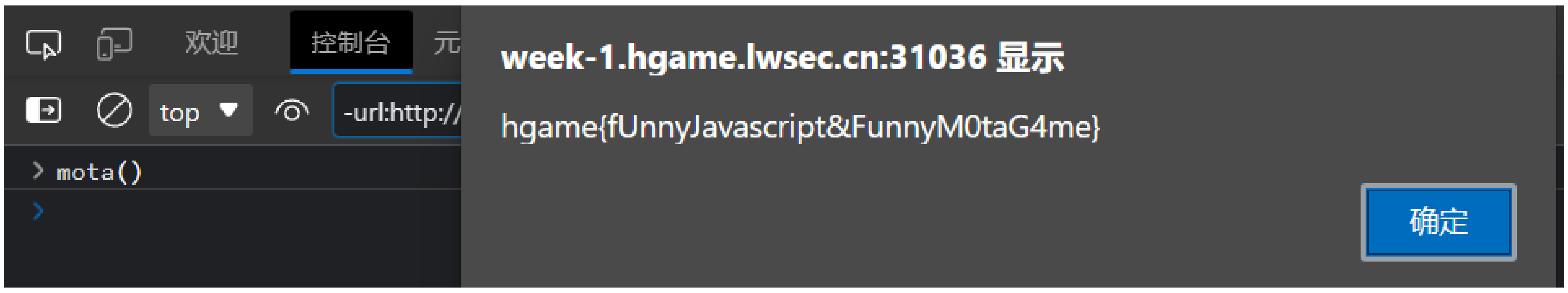
Classic Childhood Game

起初是想玩一下的，改个数值还是卡关了很难受，无奈只能去翻代码

发现 `/Res/Events.js` 里面有个可疑的函数

```
function mota() {
  var a =
['\x59\x55\x64\x6b\x61\x47\x4a\x58\x56\x6a\x64\x61\x62\x46\x5a\x31\x59\x6d\x35\x73\x53\x31\x6c\x59\x57\x6d\x68\x6a\x4d\x6b\x35\x35\x59\x56\x68\x43\x4d\x45\x70\x72\x57\x6a\x46\x69\x62\x54\x55\x31\x56\x46\x52\x43\x4d\x46\x6c\x56\x59\x7a\x42\x69\x56\x31\x59\x35'];
  (function (b, e) {
    var f = function (g) {
      while (--g) {
        b['push'](b['shift']());
      }
    };
    f(++e);
  }(a, 0x198));
  var b = function (c, d) {
    c = c - 0x0;
    var e = a[c];
    if (b['CFrzVf'] === undefined) {
      (function () {
        var g;
        try {
          var i = Function('return\x20(function()\x20' + '{}.constructor(\x22return\x20this\x22)(\x20)' +
');');
          g = i();
        } catch (j) {
          g = window;
        }
        var h = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';
        g['atob'] || (g['atob'] = function (k) {
          var l = String(k)['replace'](/=+$/, '');
          var m = '';
          for (var n = 0x0, o, p, q = 0x0; p = l['charAt'](q++); ~p && (o = n % 0x4 ? o * 0x40 + p : p, n++
% 0x4) ? m += String['fromCharCode'](0xff & o >> (-0x2 * n & 0x6)) : 0x0) {
            p = h['indexOf'](p);
          }
          return m;
        });
      }());
      b['fqlkGn'] = function (g) {
        var h = atob(g);
        var j = [];
        for (var k = 0x0, l = h['length']; k < l; k++) {
          j += '%' + ('00' + h['charCodeAt'](k)['toString'](0x10))['slice'](-0x2);
        }
        return decodeURIComponent(j);
      };
      b['iBPtNo'] = {};
      b['CFrzVf'] = !![];
    }
    var f = b['iBPtNo'][c];
    if (f === undefined) {
      e = b['fqlkGn'](e);
      b['iBPtNo'][c] = e;
    } else {
      e = f;
    }
    return e;
  };
  alert(atob(b('\x30\x78\x30')));
}
```

就是他了



```
> mota()
```

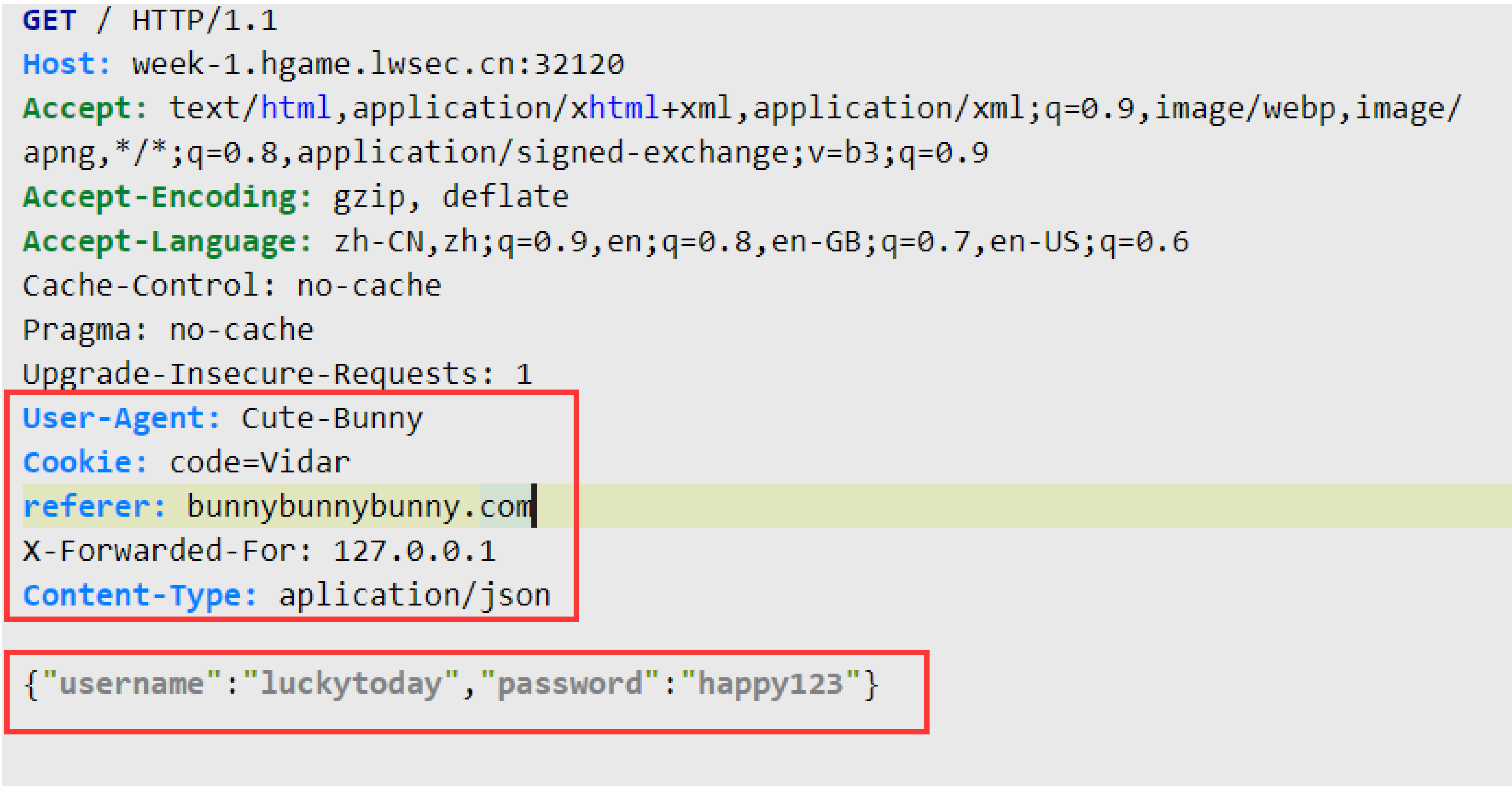
week-1.hgame.lwsec.cn:31036 显示

hgame{fUnnyJavascript&FunnyM0taG4me}

Become A Member

和hgame mini有道题比较像，其实倒不如说是祖传题目

说什么就加什么就好了



```
GET / HTTP/1.1
Host: week-1.hgame.lwsec.cn:32120
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cache-Control: no-cache
Pragma: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Cute-Bunny
Cookie: code=Vidar
referer: bunnybunnybunny.com
X-Forwarded-For: 127.0.0.1
Content-Type: aplication/json

{"username":"luckytoday","password":"happy123"}
```

Guess Who I Am

上脚本，去vidar爬数据再回来答题

```
package main

import (
    "encoding/json"
    "fmt"
    "github.com/PuerkitoBio/goquery"
    "html"
    "io"
    "log"
    "net/http"
    "net/url"
```

```go
    "os"
    "strings"
)

var members = make(map[string]string)

type req struct {
    Message string `json:"message"`
}

func main() {
    f, _ := os.Open("a.html")
    doc, _ := goquery.NewDocumentFromReader(f)
    s := doc.Find(".profile")
    s.Each(func(i int, selection *goquery.Selection) {
        name, _ := selection.Find("a").First().Attr("title")
        dsc := selection.Find("p").First().Text()
        members[dsc] = name
    })
    var session = "MTY3MjkzMDg1N3xEdi1CQkFFQ180SUFBUkFCRUFBQVBQLUNBQUlHYzNSeWFXNW5EQTBBQzJOb1lXeHNaVzVuWlVsa0EybHVkQVFEQVAtT0JuTjBjbWx1Wnd3SUFBWnpiMngyWldRRGFXNTBCQUlBQWc9PXz2bXHqNnL5kKLCz6cCmltqza7IAlCzQxabpocymDnF0w=="
    for i := 0; i < 99; i++ {
        request, _ := http.NewRequest(http.MethodGet, "http://week-1.hgame.lwsec.cn:31467/api/getQuestion", nil)
        request.Header.Set("Cookie", "code=Cute-Bunny; session="+session)
        resp, _ := http.DefaultClient.Do(request)
        bytes, _ := io.ReadAll(resp.Body)
        var m req
        _ = json.Unmarshal(bytes, &m)
        var ans string
        if m.Message == "什么都不会 / 咸鱼研究生 / <del>安恒</del>、<del>长亭</del> / SJTU" {
            ans = "陈斩仙"
        } else {
            ans = members[strings.ReplaceAll(html.UnescapeString(m.Message), "  ", " ")]
        }
        log.Println(ans, m.Message)
        request, _ = http.NewRequest(http.MethodPost, "http://week-1.hgame.lwsec.cn:31467/api/verifyAnswer", strings.NewReader("id="+url.QueryEscape(ans)))
        request.Header.Set("Cookie", "code=Cute-Bunny; session="+session)
        request.Header.Set("Content-Type", "application/x-www-form-urlencoded")
        post, _ := http.DefaultClient.Do(request)
        b, _ := io.ReadAll(post.Body)
        fmt.Println(string(b))
        session = post.Header.Get("Set-Cookie")[8:]
        log.Println(session)
        getScore(session)
    }
}

func getScore(session string) {
    req, _ := http.NewRequest(http.MethodGet, "http://week-1.hgame.lwsec.cn:31467/api/getScore", nil)
    req.Header.Set("Cookie", "code=Cute-Bunny; session="+session)
    resp, _ := http.DefaultClient.Do(req)
    b, _ := io.ReadAll(resp.Body)
    fmt.Println(string(b))
}
```

并不能完全对上，会有一点问题，题目给的描述有一些类似于~~这种标签，但是我爬的话我当时用了.Text()，那这些标签就没了，导致了一定的错误率，还挺高的，以至于需要手动修正提高正确率，现在想想应该用.Html()~~

Show Me Your Beauty

一眼webshell，后缀黑名单，php8不考虑%00这些奇怪手法，yakit抓一下改个后缀，.pHp成功上传，是大小写敏感

mics

Sign in

base64 decode

Where am I

wireshake里唯二的http请求就是在文件上传，导出出来一个rar

7z不认识这个rar我以为要怎么修一下什么的，拿010比对了一下，结果是rar伪加密，文件头 bit flag 加密位4改0，解压，图片右键看看属性gps信息就在那了

神秘的海报

图片看起来很正常，010也看不出来，考虑一下LSB隐写

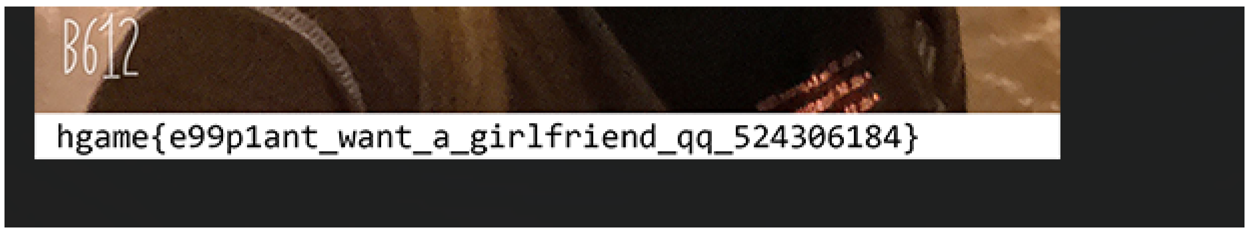
stegsolve真就提出来了，拿到了一半flag和一个wav的网盘链接，明确提示了steghide和6位数字密码

考虑一下弱密码 `steghide extract -sf Bossanova.wav -p 123456`

提取出flag2.txt，拼接一下就好了

e99p1ant_want_girlfriend

提示crc，撞crc，改宽高，撞出来是高度改为706



hgame{e99p1ant_want_a_girlfriend_qq_524306184}

blockchain

Checkin

看看代码感觉只需要调用一下setGreeting就可以了

本来想用remix的，但是他估算gas的rpc调用失败之后我就啥也不会了

就拿js写了，gas随便填了一下这样子

```
const Web3 = require("web3");
const Tx = require("ethereumjs-tx").Transaction;
const senderAddress = "";
const privateKey =
  "";
```

```
const DAI_ADDRESS = "";

var web3 = new Web3(
  new Web3.providers.HttpProvider("http://week-1.hgame.lwsec.cn:31126")
);

const ABI = [
  {
    inputs:[],
    name: "greet",
    type: "function",
    outputs: [
      {
        type: "string",
      },
    ],
  },
  {
    inputs: [
      {
        name: "_greeting",
        type: "string",
      },
    ],
    name: "setGreeting",
    type: "function",
    outputs: [],
  },
  {
    inputs:[],
    name: "isSolved",
    type: "function",
    outputs: [
      {
        type: "bool",
      },
    ],
  },
];

const contract = new web3.eth.Contract(ABI, DAI_ADDRESS);

const rawTx = {
  to: DAI_ADDRESS,
  gasLimit: "0x5710",
  data: contract.methods.setGreeting("HelloHGAME!").encodeABI(),
  gasPrice: web3.utils.toHex("10000000000"),
  gasLimit: web3.utils.toHex("3000000"),
  value: web3.utils.toHex("0"),
};


web3.eth.accounts.signTransaction(rawTx, privateKey).then(function (value) {
  web3.eth
    .sendSignedTransaction(value.rawTransaction)
    .then(function (response) {
      console.log("response:" + JSON.stringify(response, null, " "));
    });
});
```

Iot

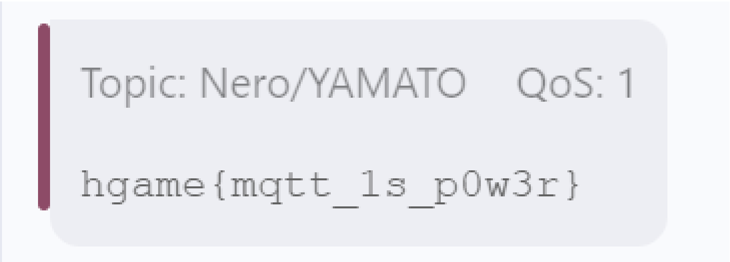
Help the uncle who can't jump twice

1883 mqtt

需要用户名和密码，题面提示了用户名为Vergil

题目提供了密码本，mqtt-pwn撞得密码为power

塞进mqttx，根据题面提示订阅Nero/#



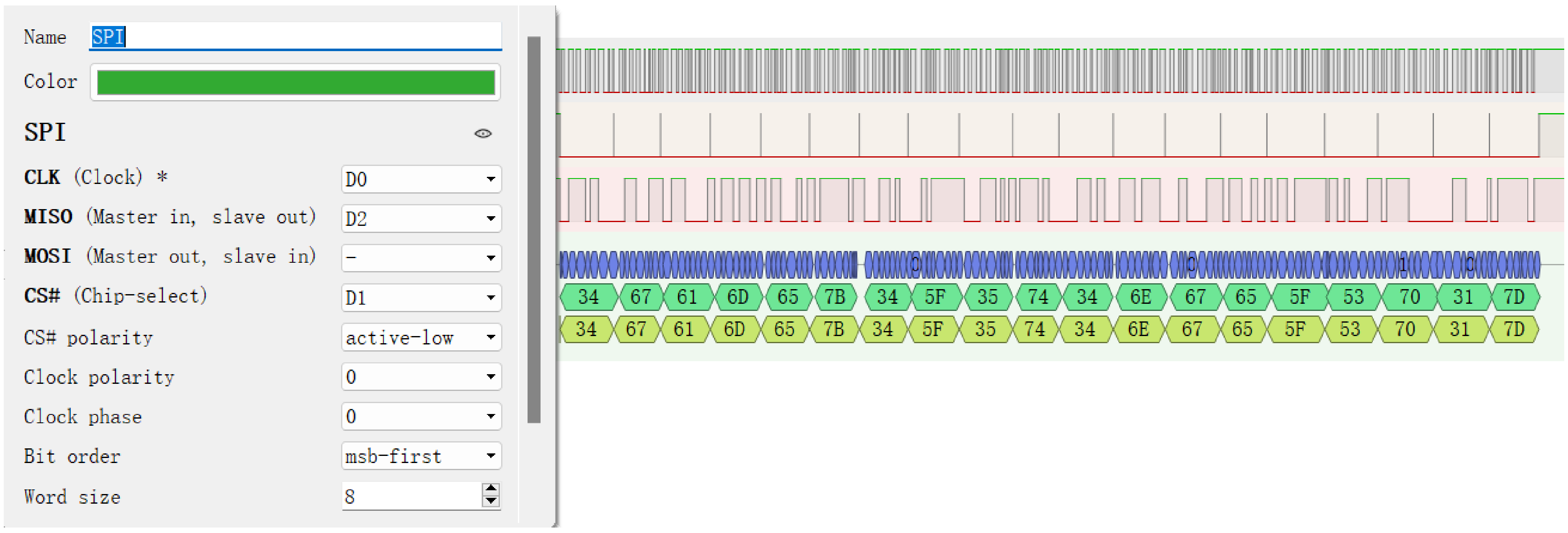
Topic: Nero/YAMATO QoS: 1

hgame{mqtt_1s_p0w3r}

Help marvin

谢谢apex

在网络上比对了不少协议，决定是spi



Name SPI

Color

SPI

CLK (Clock) * D0

MISO (Master in, slave out) D2

MOSI (Master out, slave in) -

CS# (Chip-select) D1

CS# polarity active-low

Clock polarity 0

Clock phase 0

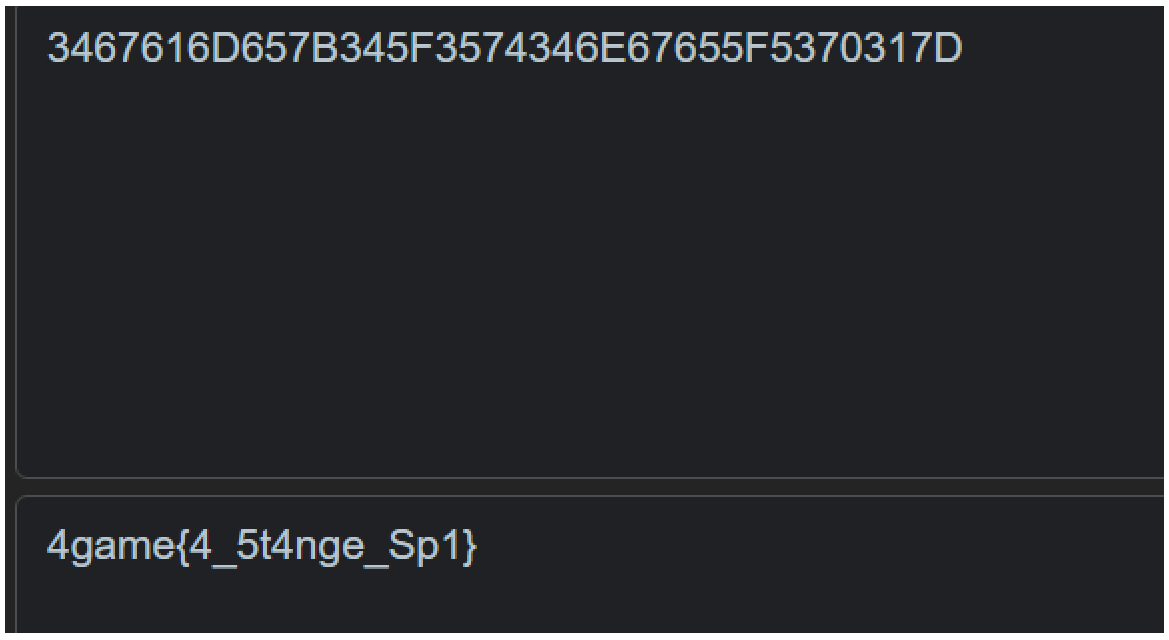
Bit order msb-first

Word size 8

34 67 61 6D 65 7B 34 5F 35 74 34 6E 67 65 5F 53 70 31 7D
34 67 61 6D 65 7B 34 5F 35 74 34 6E 67 65 5F 53 70 31 7D

D0和D2猜猜看应该是clk和数据，剩下的D1就给cs了

hex转string解得



```
3467616D657B345F3574346E67655F5370317D
```

```
4game{4_5t4nge_Sp1}
```

为什么第一个字符是4不是h，人工修正一下

Reverse

test your IDA

ida打开，看到是明文

easyasm

做了一个异或，弄回来就行了

```
#include <bits/stdc++.h>

int enc[] =
{0x5b,0x54,0x52,0x5e,0x56,0x48,0x44,0x56,0x5f,0x50,0x3,0x5e,0x56,0x6c,0x47,0x3,0x6c,0x41,0x56,0x6c,0x44,0x5c
,0x41,0x2,0x57,0x12,0x4e};

int main()
{
    for (int i = 0; i < 27; i++)
        printf("%c", enc[i]^0x33);
}
```

easyenc

是一个sub和一个xor

```
#include <bits/stdc++.h>

int enc[] =
{167640836,11596545,-1376779008,85394951,402462699,32375274,-100290070,-1407778552,-34995732,101123568};

int main()
{
    for (int i = 0; i < 10; i++){
        char *c = (char*)(enc+i);
        for (int j =0;j<4;j++)
            printf("%c", (c[j]+0x56)^0x32);
    }
    // 在内存里这个-7刚刚好排在前面那块的后面
    printf("%c", ((char)-7+0x56)^0x32);
}
```

pwn

test_nc

nc连上去发现能cat能ls，cat flag