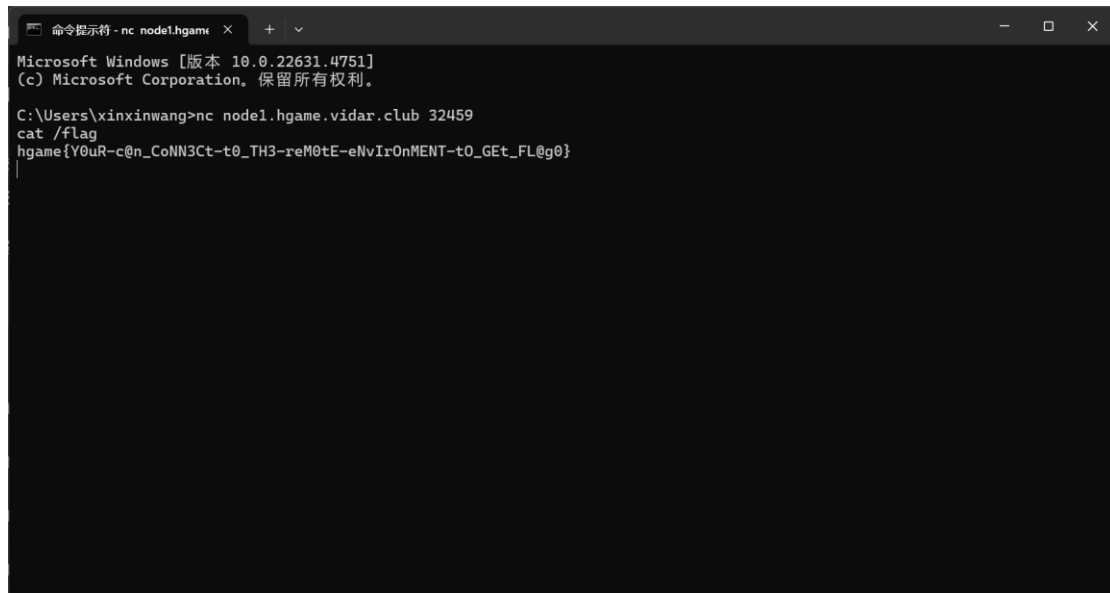


wang7 #000265

TEST NC

根据提示有 netcat 和 pwntools。我这里使用的是 netcat。



```
Microsoft Windows [版本 10.0.22631.4751]
(c) Microsoft Corporation. 保留所有权利。


C:\Users\xinxinwang>nc node1.hgame.vidar.club 32459
cat /flag
hgame{Y0uR-c@n_CoNN3Ct-t0_TH3-reM0tE-eNvIrOnMENT-t0_GET_FL@g0}
```

从这里开始的序章。

直接输入答案 `hgame{Now-I-know-how-to-submit-my-flag!}`

1 首先 f12 打不开 要用右键检查 查看源代码

2 一般从末尾找



```
..._0x3c0cce['createItem']({
  'x': _0x5e1765['width'] / 0x2,
  'y': _0x5e1765[_0x4bff30(0x14f)] * 0.5,
  'draw': function(_0x413b57) {
    var _0x5dcc17 = _0x4bff30;
    _0x413b57[_0x5dcc17(0x159)] = '#FFF',
    _0x413b57['font'] = _0x5dcc17(0x16a),
    _0x413b57[_0x5dcc17(0x129)] = _0x5dcc17(0x154),
    _0x413b57[_0x5dcc17(0x150)] = _0x5dcc17(0x101);
    var _0x82b005 = _SCORE + 0x32 * Math[_0x5dcc17(0x103)](_LIFE - 0x1, 0x0);
    _0x413b57[_0x5dcc17(0x10c)](_0x5dcc17(0xf7) + _0x82b005, this['x'], this['y']),
    _0x82b005 > 0x270f ? (_0x413b57[_0x5dcc17(0xf4)] = _0x5dcc17(0x164),
    _0x413b57['fillText'](_0x5dcc17(0x10d), this['x'], this['y'] + 0x28),
    console['log'](_0x5dcc17(0x10d))) : (_0x413b57[_0x5dcc17(0xf4)] = _0x5dcc17(0x164),
    _0x413b57['fillText']('here is your gift:aGfLcGFpZW1rc3ByZXRNbXtydGNfYWVfZWZjfQ==', this['x'], this['y'] + 0x28),
    console[_0x5dcc17(0x125)](_0x5dcc17(0x166)));
  }
}),
..._0x3c0cce['createItem'](_0x413b57[_0x5dcc17(0x129)] = _0x5dcc17(0x154),
..._0x413b57[_0x5dcc17(0x150)] = _0x5dcc17(0x101);
...var _0x82b005 = _SCORE + 0x32 * Math[_0x5dcc17(0x103)](_LIFE - 0x1, 0x0);
..._0x413b57[_0x5dcc17(0x10c)](_0x5dcc17(0xf7) + _0x82b005, this['x'], this['y']),
..._0x82b005 > 0x270f ? (_0x413b57[_0x5dcc17(0xf4)] = _0x5dcc17(0x164),
..._0x413b57['fillText'](_0x5dcc17(0x10d), this['x'], this['y'] + 0x28),
...console['log'](_0x5dcc17(0x10d))) : (_0x413b57[_0x5dcc17(0xf4)] = _0x5dcc17(0x164),
..._0x413b57['fillText']('here is your gift:aGfLcGFpZW1rc3ByZXRNbXtydGNfYWVfZWZjfQ==', this['x'], this['y'] + 0x28),
...console[_0x5dcc17(0x125)](_0x5dcc17(0x166)));
...}
```

其实是假的 flag 但解密方式与正确相同

3 继续寻找

```
' , 'here is your gift:aGFldTRlcGNhXzR0cmdte19yX2Ftbm1zZX0='
```

4 看到等号 大概确定为 base 加密 逐一尝试 最后确定 base64

aGFldTRlcGNhXzR0cmdte19yX2Ftbm1zZX0=

base64 ▼ 🔒 Encode 🔒 Decode 🔒 Quote escape

haeu4epca_4trgm{r_amnmse}

5 看到关键{} 和 h g a m e 猜测栅栏加密尝试

AmanCTF - 栅栏加密/解密

在线栅栏(RailFence)加密/解密

haeu4epca_4trgm{r_amnmse}

栏数 加密 解密 枚举加密 枚举解密

标准型

W型

hgame{u_4re_pacman_m4ster}|

hgame(u_4re_pacman_m4ster)

结束得到结果