K999-WriteUp

本题为简单的Lua游戏逆向题目，玩家可以通过各种方法例如锁血、无限弹药杀死999个敌人后可以获得一串信息：

```
”MOON\r\n”
”157 89 215 46 13 189 237 23 241\r\n”
”49 84 146 248 150 138 183 119 52\r\n”
”34 174 146 132 225 192 5 220 221\r\n”
”176 184 218 19 87 249 122\r\n”
”Find a Decrypt!\r\n”
```

寻找游戏程序中的flag加解密脚本：

```
function to8(n)
    return n % 256
end

function bxor(a, b)
    local p = 0
    local i = 0
    for i = 0, 7, 1 do
        p = p + 2 ^ i * ((a % 2 + b % 2) % 2)
        a = math.floor(a / 2)
        b = math.floor(b / 2)
        if a == 0 and b == 0 then break end
    end
    return p
end

function encrypt(v, k)
    local sum = 0
    local delta = 0x37
    local i = 0
    for i = 1, 8, 1 do
        sum = to8(sum + delta)
        v[1] = to8(v[1] + to8(bxor(bxor(to8((v[2] * 16) + k[1]), to8(v[2] + sum)), to8(math.floor(v[2] / 32) + k[2]))))
        v[2] = to8(v[2] + to8(bxor(bxor(to8((v[1] * 16) + k[3]), to8(v[1] + sum)), to8(math.floor(v[1] / 32) + k[4]))))
    end
end

function decrypt(v, k)
    local sum = 0xB8
    local delta = 0x37
    local i = 0
    for i = 1, 8, 1 do
        v[2] = to8(v[2] - to8(bxor(bxor(to8((v[1] * 16) + k[3]), to8(v[1] + sum)), to8(math.floor(v[1] / 32) + k[4]))))
        v[1] = to8(v[1] - to8(bxor(bxor(to8((v[2] * 16) + k[1]), to8(v[2] + sum)), to8(math.floor(v[2] / 32) + k[2]))))
        sum = sum - delta
    end
end

function passGen()
    local pw = ””
    local j
    for i = 1, 4, 1 do
```

```
        j = math.random(33, 126)
        if j == 96 then pw = pw .. ”_”
        else pw = pw .. string.char(j) end
    end
    return pw
end

function strDecrypt(s, k)
    local b = {}
    local c = {}
    local i
    local j
    j = string.gmatch(k, ”.”)
    b = { string.byte(j()), string.byte(j()), string.byte(j()), string.byte(j()) }
    j = ””
    for i = 1, string.len(s) / 2, 1 do
        c = { string.byte(string.sub(s, i * 2 – 1, i * 2 – 1)), string.byte(string.sub(s, i * 2, i * 2)) }
        decrypt(c, b)
        j = j .. string.char(c[1])
        if c[2] == 0 then break end
        j = j .. string.char(c[2])
    end
    return j
end

function Decrypt()
    local key = ”MOON”
    local s = {157, 89, 215, 46, 13, 189, 237, 23, 241, 49, 84, 146, 248, 150, 138, 183, 119, 52, 34, 174, 146, 132, 225, 192, 5, 220, 221,176, 184, 218, 19, 87, 249, 122}
    flag = ””
    for i = 1, #s, 1 do
        flag = flag .. string.char(s[i])
    end
    flag = strDecrypt(flag, key)
    print(flag)
end

Decrypt()
```

稍作修改，即可解密最后获得Flag：

RCTF{1_Rea11y_Want_t0_Y0ur_H0use}