

Hgame week 1 writeup

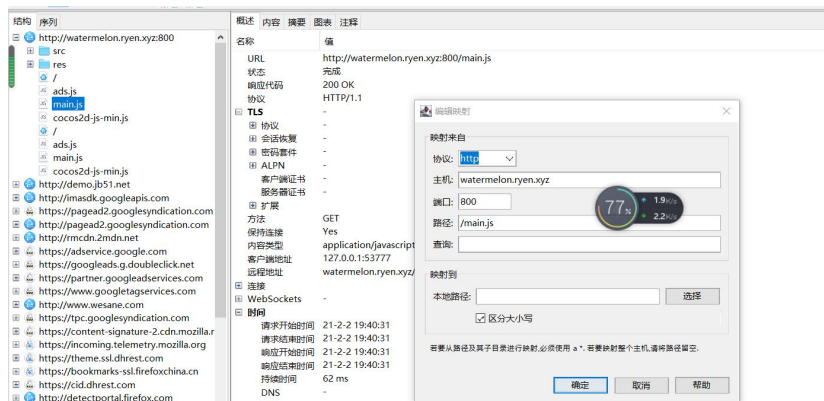
Web.2 大西瓜

1. 第一反应修改合成水果分数，网上找到大西瓜分数计算源代码

```
2, t.prototype.onbeginContact = function (c, t) {
    var o = this;
    if ("downwall" == n.node.group && (t.node.parent = cc.find("Canvas/fruitNode"), 0 == this.wallColl && (d.default.Instance.Play(5, !1, 1), this.wallColl++)),
    if (this.endCtrl = !0, t.node.y < n.node.y) return;
    t.node.parent = cc.find("Canvas/fruitNode"), i.default.Instance.fruitHeigh = i.default.Instance.findHighestFruit(), null != t.node.getComponent(cc.RigidBody) && (t.fruitNumber = n.node.getComponent("fruitData").fruitNumber;
    c == r && c < 9 && r < 9 ? (this.pengzhuangCount += 1, 0 == t.node.getComponent("fruitData").getNumber() && (a.default.score += this.fruitNumber + 1, u.
    position: n.node.position
    }).call(function () {
        i.default.Instance.createFruitSui(o.fruitNumber, n.node.position), i.default.Instance.createFruitI(o.fruitNumber, n.node.position, n.node.width), i.
    }).start(): c == r && 9 == c && 9 == r && (this.pengzhuangCount += 1, 0 == t.node.getComponent("fruitData").getNumber() && (a.default.score += this.f.
    position: n.node.position
    }).call(function () {
        i.default.Instance.createFruitSui(o.fruitNumber, n.node.position), i.default.Instance.createFruitI(o.fruitNumber, n.node.position, n.node.width), i.
    }
}
```

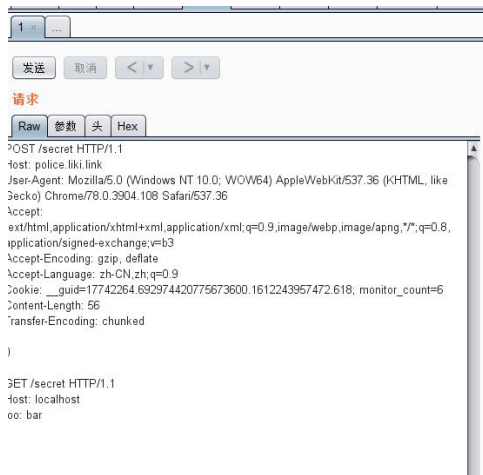
2.

3. 网页不能直接修改,于是百度查到 charles 可以修改,网站下载源代码 project.js 并修改上传到 charles 使用本地映射再刷新网页就可以得到修改后的大西瓜



Web3 宝藏走私者与 web5 走私者的愤怒

刚开始没有头绪,但后来出题人给了资料 <https://paper.seebug.org/1048/> 根据资料在 burpsuite 修改请求头,运用走私攻击,偷渡完成本地登录,两者考点相同

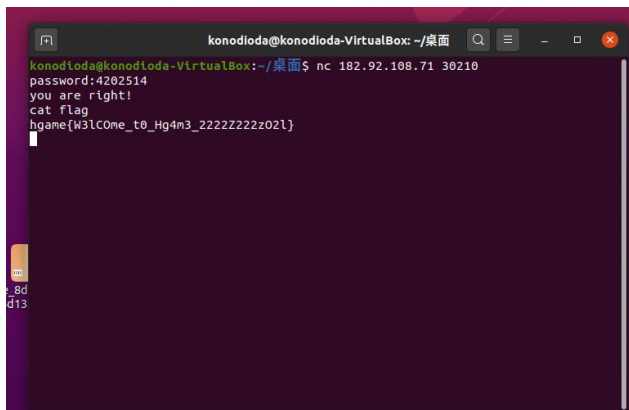


4 智商检测仪

写一百道微积分,刚开始发现修改网页源码没有用,于是想到用 python 编写脚本(由于当时没有意识到要写 wp, 代码没有截图)即可快速完成 100 道题目得到 flag

Pwn

1. Pwn 选手只做出最简单的签到题实在是太丢人了，下周继续努力。（签到题不难，只要会 gdb 调试就可。）



```
konodioda@konodioda-VirtualBox: ~/桌面
konodioda@konodioda-VirtualBox:~/桌面$ nc 182.92.108.71 30210
password:4202514
you are right!
cat flag
hqame{W3lC0me_t0_Hg4m3_222222222021}
```

- 2.

Misc

1. base 全家福

提示是 base 全家，于是便将

R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUIRHTVIETVJCV0dVMIVNTlpVR01ZREtSUIVI
QTJET01aVUdSQ0RHTVpWSVlaVEVNWIFHTVpER01KWEIRPT09PT09 先后分别用 base64 ,
base32, base16 解码得到 flag

2. 不起眼压缩包的培养的方法

1 到 foremost 分解得到 zip , 第一个 zip ARCHPR 是纯数字爆破, 得到密码: 70415155, 里面是 plain.zip
和 NO PASSWORD.txt 发现第二个 zip 也有密码, 而且爆破不了, 直接用 winhex , 用 16 位读取, 发现
里面有一大串 &#xxxxx, 猜测这就是 flag , 解码后得到 flag

3.Word RE:MASTER

下载附件后得到两个文档, 第一个文档是打开第二个文档的密码, 于是将第一个文档后缀修改为 zip, 解
压得到多个文件, 发下其中有一个文件名为 password

于是用 txt 打开, 发现一串全为 ++- 的字符,

Fuck! 我的脑子好疼! 这可能是音游瘾发作最严重的一次.躺在床上很想打交互, 嘴里
念叨: O-ooooooooo AAAAE-A-A-I-A-U JO-ooooooooooooo AAE-O-A-A-U-U-A
E-eee-ee-eee AAAAE-A-E-I-E-A JO-ooo-oo-oo-oo EEEEE-O-A-AAA-AAAA, 不行我得在
brainpower 耗尽前把密码记下来。

根据文档的提示得出用 brainfuck 解码得到文档 2 密码, 文档 2 打开是一张照片



发现 hint 是雪, 于是百度得到 snow 加密, 将文档后缀改为 txt , 用 snow 解密可得到 flag