Week 1 WP 19906767892

0 sign in

Base64 解密

1 Show me your beauty

由题意可以上传不同后缀文件，想到木马

上传文件漏洞 使用一句话木马修改后缀名为 png 后 burp 抓包修改后缀名为 Php（大小写绕过）蚁剑连接成功

遍历后发现 flag 文件

2 elephant want a girlfriend

hgame{e99p1ant_want_a_girlfriend_qq_524306184}

通过 tweakpng 知道 CRC 校验错误并用 winhex 将 A8586645 改为 01374779 再使用 tweakpng 改高使底部的 flag 出现

3 classic childhood game

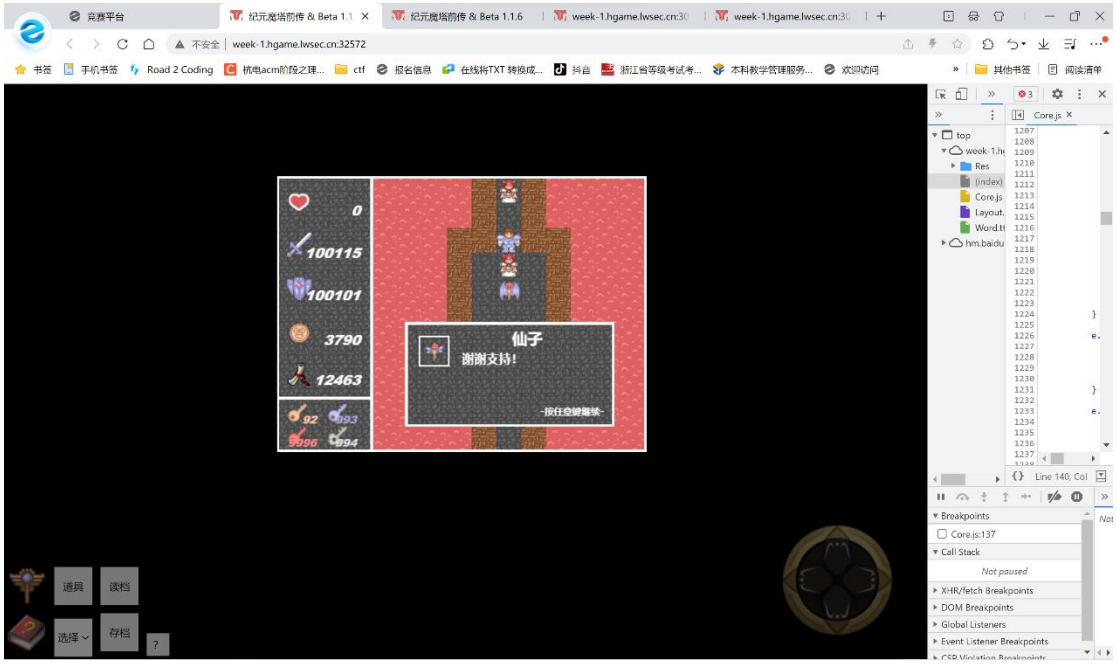
由题意知是纯前端的，想到可以改变变量值

在 core.js 中找到了初始化语句，通过设置 source 中 core.js 的断点（要把一整个执行完之后的断点，不然有 hero 未定义），

断成功后到 console 中发送参数赋值（如 Hero["HP"] = 1000000），取消断点并继续执

行，达到开挂效果

最后一幕使用凿子和万能门通过，发现假的公主，并被公主击杀，弹出 flag



4 become a member

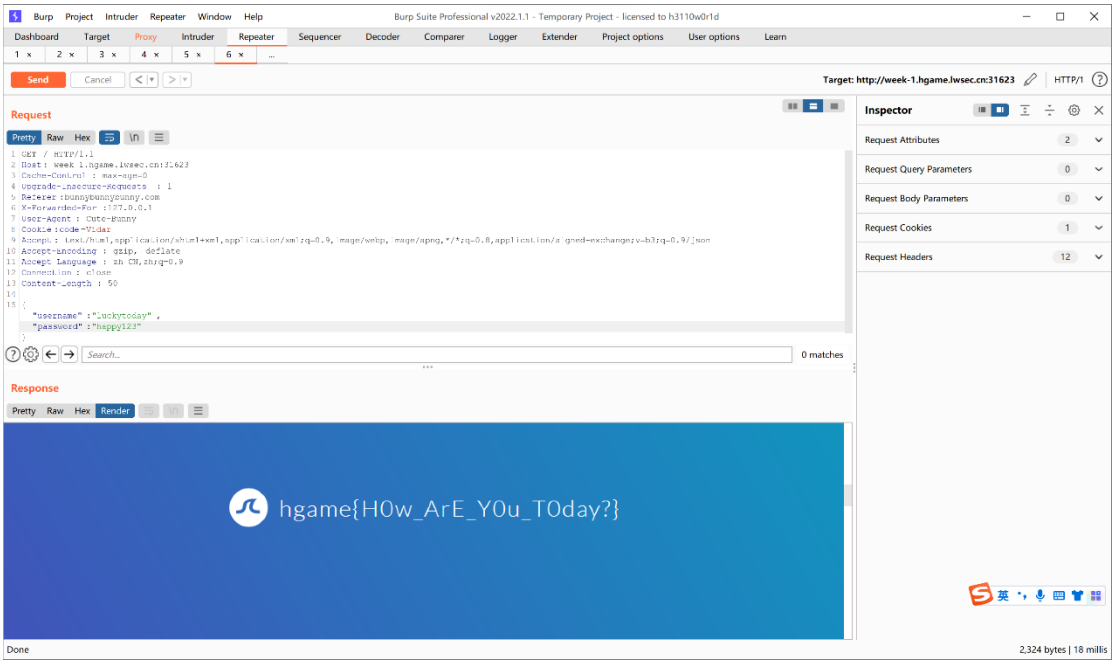
首先是用户身份证明，归 user-agent 管用户信息，改为 cute-bunny

然后邀请码是 vidar （经学长提醒看请求头）发现 set-cookie 中 code 为 guest,于是将 cookie 的 code 改为 Vidar

然后是从 bunnybunnybunny.com 来，这归 REFER 管，加入 refer 即可

本地访问，一眼 X-FORWARED-FOR

然后用 JSON 方式登陆（最麻烦，其实是用 JSON 语法表示字符串）{“A”:”B”}就是字符串



A 值为 B，用这个语法表示即可

5 test your IDA

Reverse 签到题 下载 IDA 查看源码

6 RSA

是 RSA 解密，用 git 上有脚本可以解，ctf rsa tool master,运行 python 输入 e c n

7 test nc

测试 netcat ， nc 后下载到文件，记事本打开即可

8easy asm

读汇编，是异或的 0X33，也用脚本解

9be stream

读代码，是 32 的循环，使用脚本

(i//2)**6 再整除 32