

HGAME 2022 Week1 writeup by cl0ud1

● WEB

1. Classic Childhood Game

查看源码，发现

```
function mota() {  
    var a = ['\x59\x55\x64\x6b\x61\x47\x4a\x58\x56\x6a\x64\x61\x62\x46\x5a\x31\x59\x6d\x35\x73\x53\x31\x6c\x59\x57\x6d\x68\x6a\x4d\x6b\x35\x35\x59\x56\x68\x43\x4d\x45\x70\x72\x57\x6a\x46\x69\x62\x54\x55\x31\x56\x46\x52\x43\x4d\x46\x6c\x56\x59\x7a\x42\x69\x56\x31\x59\x35'];
```

转换为对应的字符

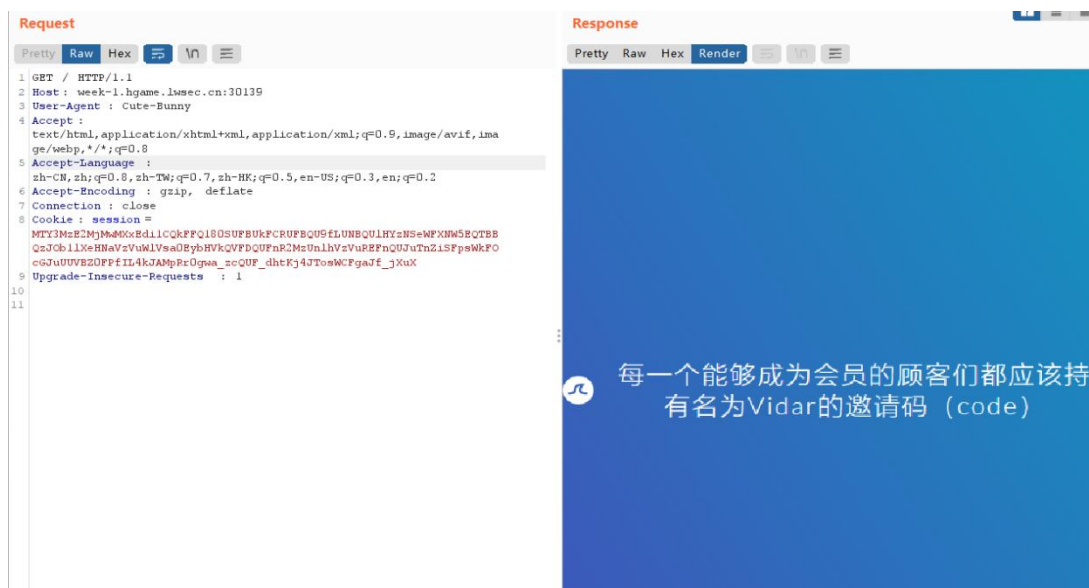
YUdkaGJXVjdabFZ1Ym5sS1lYWmhjMk55YVhCMEprWjFibTU1VFRCM

FlVYzBiV1Y5

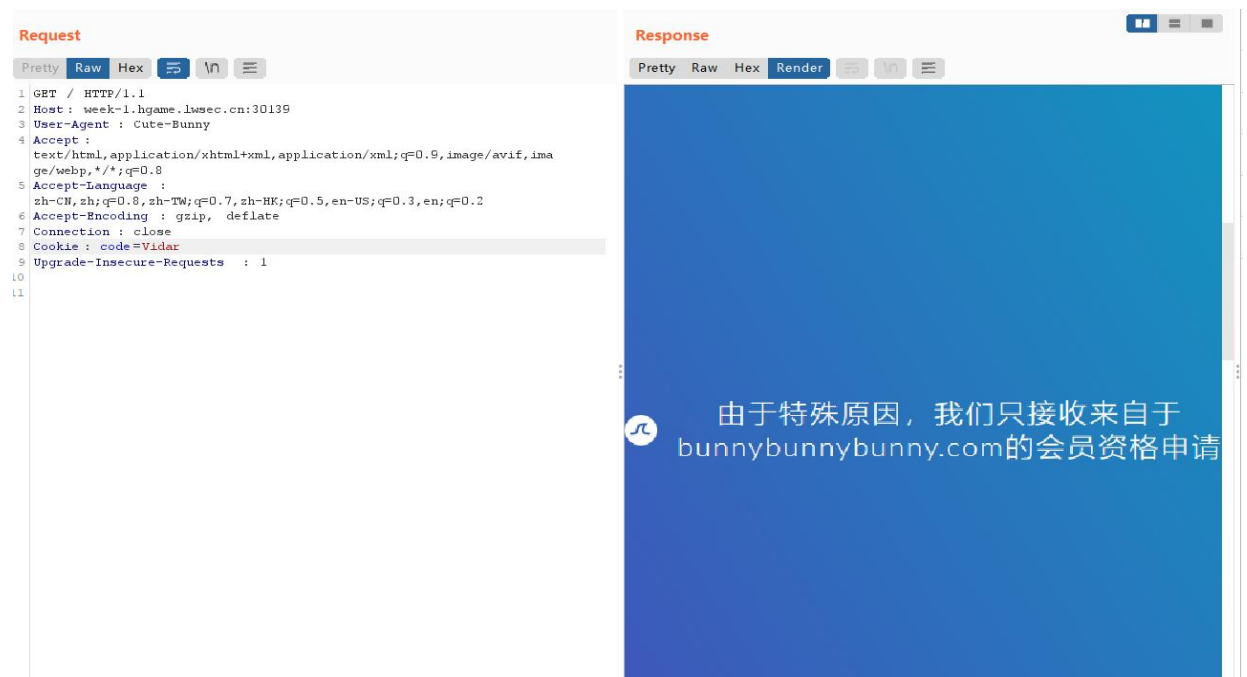
用 base64 解码两次得到 flag:hgame{fUnnyJavascript&FunnyM0taG4me}

2. Become A Member

根据提示改 User-Agent:为 Cute-Bunny



根据提示改 cookie 为 code=Vidar



Request

```
1 GET / HTTP/1.1
2 Host: week-1.hgame.lwsec.cn:30139
3 User-Agent: Cute-Bunny
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: code=Vidar
9 Upgrade-Insecure-Requests: 1
```

Response

由于特殊原因，我们只接收来自于 bunnybunnybunny.com 的会员资格申请

根据提示添加 Referer: bunnybunnybunny.com



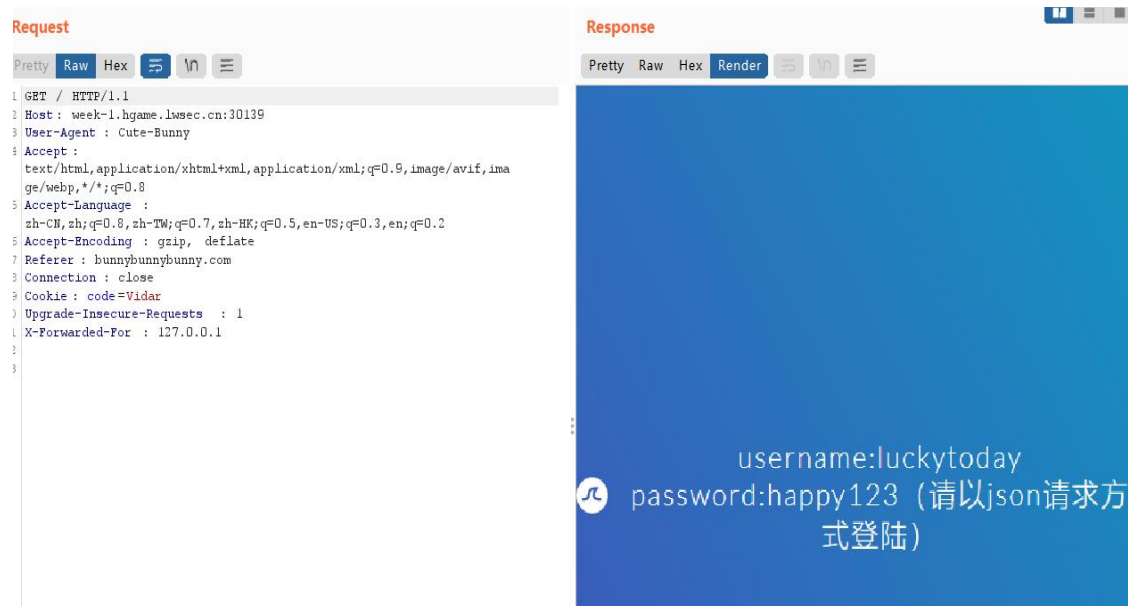
Request

```
1 GET / HTTP/1.1
2 Host: week-1.hgame.lwsec.cn:30139
3 User-Agent: Cute-Bunny
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: code=Vidar
9 Upgrade-Insecure-Requests: 1
10 Referer: bunnybunnybunny.com
```

Response

就差最后一个本地的请求，就能拿到会员账号啦

根据提示添加 X-Forwarded-For: 127.0.0.1



根据提示添加 Content-Type: application/json

和 {"username": "luckytoday", "password": "happy123"}



得到 flag:hgame{H0w_ArE_Y0u_T0day?}

● MISC

1. Sign In

Base64 解码得到 flag

hgame{Welcome_To_HGAME2023!}

控制台

调试器

网络

样式编辑器

性能

内存

存储

无障碍环境

应用程序

Encoding SQL XSS LFI XXE Other

}

hgame{Welcome_To_HGAME2023!}