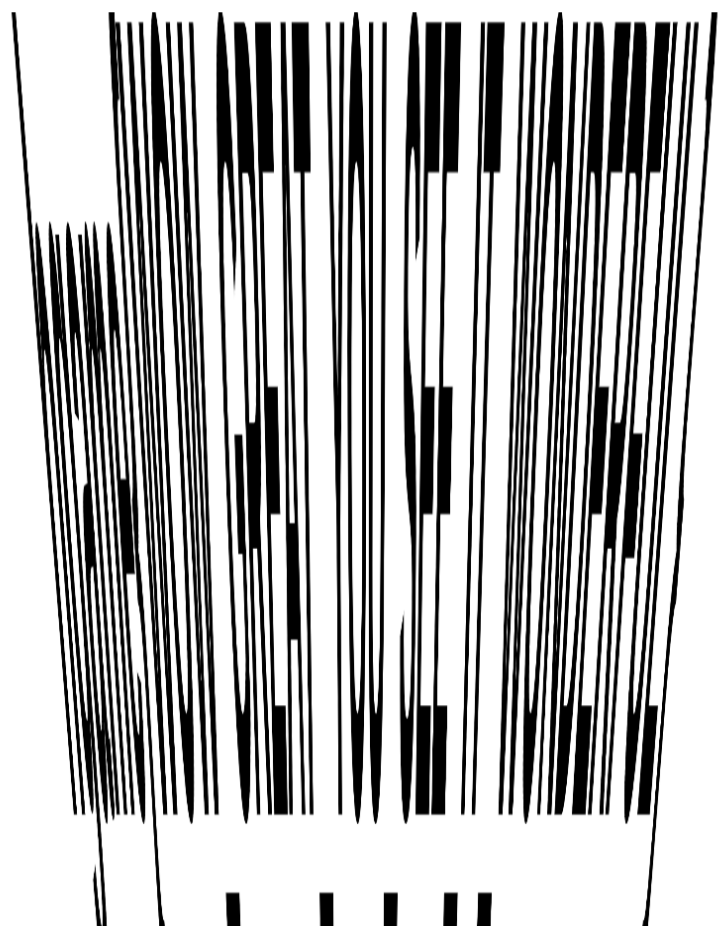


MISC

SignIn

打开附件是一张图片



换一种视角吧

从下方看即可看见flag

签到

关注“凌武科技”微信公众号，发送“HGAME2024”获得 Flag

PWN

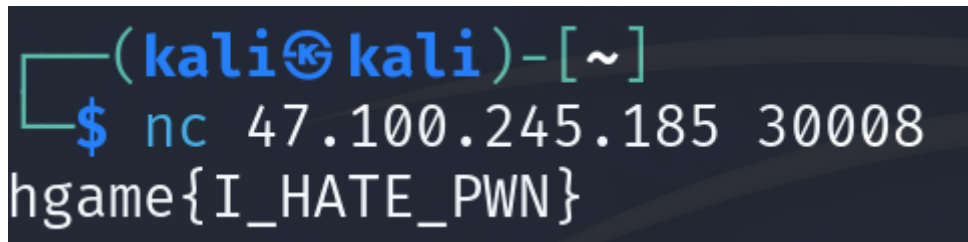
EzSignIn

打开题目得到下面的东西

```
nc 47.100.245.185:30008
```

放进浏览器里发现这个并不是网站，于是上网搜了一下，发现nc是Linux里的命令

于是打开Kali-Linux，在终端输入 `nc 47.100.245.185 30008`，得到flag



```
(kali㉿kali)-[~]  
$ nc 47.100.245.185 30008  
hgame{I_HATE_PWN}
```

WEB

ezHTTP

进入网站后看到下面一句话：

```
请从vidar.club访问这个页面
```

于是打开Burpsuite抓包，发送到Repeater模块，添加请求头：

```
Referer:vidar.club
```

得到：

```
请通过Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0访问此页面
```

于是再次修改请求头：

```
User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
```

得到：

```
请从本地访问这个页面
```

于是继续添加请求头：

```
X-Forwarded-For:127.0.0.1
```

发现好像没什么用，看响应发现有提示：

```
Hint: Not XFF
```

于是上网搜了一下，发现不止XFF这种方法，试了半天发现了可以用的：

```
X-Real-IP:127.0.0.1
```

得到：

```
Ok, the flag has been given to you ^-^
```

看了一眼源代码，并没有找到flag

找了半天也没找到flag，只在响应处看见下面的东西有点可疑：

Authorization: Bearer

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwc1Q0bnR9In0.VKMdRQl1G6lJTReFhmbcfIdq7MvJDncYpjaT7ztEDc

上网搜了一下，发现是jwt编码，解码得到：

JSON Web Tokens (JWT) 在线解密

提示： JWT是目前最流行的跨域认证解决方案, 是一个开放式标准(RFC 7519), 用于在各方之间以JSON对象安全传输信息。我们不记录令牌，所有验证和调试都在客户端进行。

Encoded 请在以下文本框粘贴令牌

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwc1Q0bnR9In0.VKMdRQl1G6lJTReFhmbcfIdq7MvJDncYpjaT7ztEDc

Decode 以下是解密的内容

HEADER

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD

```
{
  "Fl4g": "hgame{HTTP_!s_1mP0rT4nt}"
}
```

STATUS

Decode Success

jwt在线解码：<https://www.box3.cn/tools/jwt.html>

Select Courses

打开发现是选课界面，显示要选到所有课程才能拿到flag

看了看源码，没什么发现

偶然间发现原本已满的课居然选上了，猜测只要一直点就能选到

最后得到：

谢谢啦！这是给你的礼物：hgame{w0w_!_1E4Rn_To_u5e_5cripT_^_^}

看来这题应该是写脚本来解的

REVERSE

ezASM

打开附件，是一段汇编代码

这段代码需要用户输入的值与预设的加密字符匹配

于是写一段代码：

```
#include <stdio.h>
#include <string.h>

char c[] = {74, 69, 67, 79, 71, 89, 99, 113, 111, 125, 107, 81, 125, 107, 79,
82, 18, 80, 86, 22, 76, 86, 125, 22, 125, 112, 71, 84, 17, 80, 81, 17, 95, 34};
char flag[33];

int main() {
    int i;
    for (i = 0; i < 33; i++) {
        flag[i] = c[i] ^ 0x22;
    }
}
```

```

}
printf("%s\n", flag);

return 0;
}

```

运行得到:

```
hgame{ASM_Is_Imp0rt4nt_4_Rev3rs3}
```

ezIDA

将ezIDA.exe拖进IDA后, 直接看见了flag

