

2025 HACKTHEON SEJONG

팀 이름 Team Name	HAINT
문제 이름 Question	Bridge

문제 풀이과정 작성 (캡처화면 필수) / Write-up Details (The screenshot is mandatory)

apktool를 사용하여 apk파일을 풀어준다.

이름	수정한 날짜	유형	크기
assets	2025-04-26 오전 9:43	파일 폴더	
lib	2025-04-26 오전 9:43	파일 폴더	
original	2025-04-26 오전 9:43	파일 폴더	
res	2025-04-26 오전 9:43	파일 폴더	
smali	2025-04-26 오전 9:43	파일 폴더	
smali_classes2	2025-04-26 오전 9:43	파일 폴더	
unknown	2025-04-26 오전 9:43	파일 폴더	
AndroidManifest.xml	2025-04-26 오전 9:43	Microsoft Edge H...	3KB
apktool.yml	2025-04-26 오전 9:43	Yaml 원본 파일	4KB

스마트폰에서 apk를 실행시켜보았더니, url을 입력하는 칸이 있고 GO! 버튼을 누르면 해당 url 링크로 연결되는 간단한 어플리케이션이었다.

smali_classes2\com\hacktheon\bridge\MainActivity.smali 를 확인해보면
입력값을 받아서 WebViewActivity 클래스로 넘겨줌을 확인할 수 있다.

WebViewActivity.smali 에서는 JSInterface를 참조,
JSInterface.smali에서는 BridgeLib에서 decode만 함을 할 수 있다.
BridgeLib.smali 에서는 bridge_lib 파일을 사용하는데

lib폴더 속에 arm64, armeabi-v7a, x86, x86_64 각각의 libbridge_lib.so 파일이 들어있다.

IDA로 Java_com_hacktheon_bridge_BridgeLib_decode() 부분을 확인해보았다.

2025 HACKTHEON SEJONG

```
1  __int64 __fastcall Java_com_hacktheon_bridge_BridgeLib_decode(__int64 a1, __int64 a2, __int64 a3)
2  {
3      unsigned __int8 *v3; // rbx
4      __int64 v4; // rcx
5      __int64 v5; // rax
6      __int64 v6; // r14
7      __int64 v7; // r14
8      __m256i v9; // [rsp+0h] [rbp-A8h] BYREF
9      __int128 v10; // [rsp+20h] [rbp-88h]
10     __int64 v11; // [rsp+30h] [rbp-78h]
11     __int64 v12; // [rsp+38h] [rbp-70h] BYREF
12     __m256i v13; // [rsp+40h] [rbp-68h] BYREF
13     __int128 v14; // [rsp+60h] [rbp-48h]
14     __int64 v15; // [rsp+70h] [rbp-38h]
15     __int64 v16; // [rsp+78h] [rbp-30h] BYREF
16     size_t v17; // [rsp+80h] [rbp-28h] BYREF
17     unsigned __int8 *v18; // [rsp+88h] [rbp-20h]
18     __int64 v19; // [rsp+90h] [rbp-18h]
19
20     v12 = a1;
21     v16 = a3;
22     sub_1AB20(&v13, &v12, &v16);
23     if ( v13.m256i_i8[0] != 15 )
24     {
25         v11 = v15;
26         v10 = v14;
27         v9 = v13;
28         sub_55F00(1LL, 0LL, &v9, &off_5F830, &off_5FA38);
29     }
30     v9.m256i_i64[2] = v13.m256i_i64[3];
31     *(_OWORD *)v9.m256i_i8 = *(_OWORD *)&v13.m256i_u64[1];
32     sub_1C480(&v17, (__int64)&v9);
33     v3 = v10;
34     sub_189D0(&v9, v18, v19);
35     if ( v9.m256i_i32[0] == 2 )
36     {
37         v4 = v9.m256i_i64[1];
38         v5 = v9.m256i_i64[3];
39         v6 = v9.m256i_i64[2];
40     }
41     else
42     {
43         v6 = 1LL;
44         if ( v9.m256i_i64[1] )
```

브레이크포인트를 걸고 주어진 secret을 넣고 해독한다.

FLAG{1325ed439e52bba40fedefaf5bec9458}