webassembly

发表于 2021-01-04 分类于 Challenge， 2019， 强网杯， Misc
Challenge | 2019 | 强网杯 | Misc | webassembly

点击此处获得更好的阅读体验

题目考点

- *WebAssembly逆向*

解题思路

将wasm转成c再编译。 主要校验代码如下：

xtea加密 输入38字节。前32字节经xxtea加密。38字节与硬编码数据校验。 38字节校验数据（hex）： `959668e7b75517c9ad031ecf6fc5614b0290fd2d22ed0a93307ec9ec8c96b1e065363862627d`*前32字节直接xtea解密即可。*

```
t = '959668e7b75517c9ad031ecf6fc5614b0290fd2d22ed0a93307ec9ec8c96b1e0'
flag = ''
for i in range(4):
    ci = xtea.new('\x00'*16)
    m = ci.decrypt(t[16*i:16*(i+1)-8].decode('hex')[::-1]+t[16*(i+1)-8:16*(i+1)].decode('hex')[::-1])
    flag += m[:4][::-1]+m[4:][::-1]
flag += '65363862627d'.decode('hex')
print flag
```

Flag

```
flag{1c15908d00762edf4a0dd7ebbabe68bb}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/强网杯/Misc/8HvmYuRcUsUBw5zLfSnP9A.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Misc # 2019 # 强网杯
JuseRe
强网先锋_AD