BabyRSA

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Extra
Challenge | 2017 | HCTF | Extra | BabyRSA

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

- *RSA*

解题思路

```
1 M = r * bytes_to_long('hctf{' + sha256(open('./flag').read()).hexdigest() + '}')
2 S = pow(M, d, n)
```

程序接收 r，然后同 flag 相乘后计算出它的数字签名先说下本来的思路，flag 为 m，单纯 flag 的签名为 S，返回的签名为 S',如果我们构造 `r=R^e`

e 的值未知，通过爆破 e 的值遍历提交 R^e，再根据上式得出 flag

但是题目忘记对 r 进行限制，导致也可以通过传入 r=2 来做出

因为 2m < n，所以直接对 S''^e 除以 2 就是 m

然后对 m^2 开方就是 flag 了

Flag

```
1 无
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2017/HCTF/Extra/rL4wYY1kEFvWwURoeF67W8.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 # 2017 # HCTF # Extra
New_Love_Song
WeakRSA