[ACTF新生赛2020]crypto-rsa0

原创

2er0!=O 于 2021-05-26 11:05:18 发布 497 收藏 1

分类专栏： buuctf wp 文章标签： unctf

本文链接：https://blog.csdn.net/m0_52727862/article/details/117284459

buuctf 同时被 2 个专栏收录

28 篇文章 0 订阅

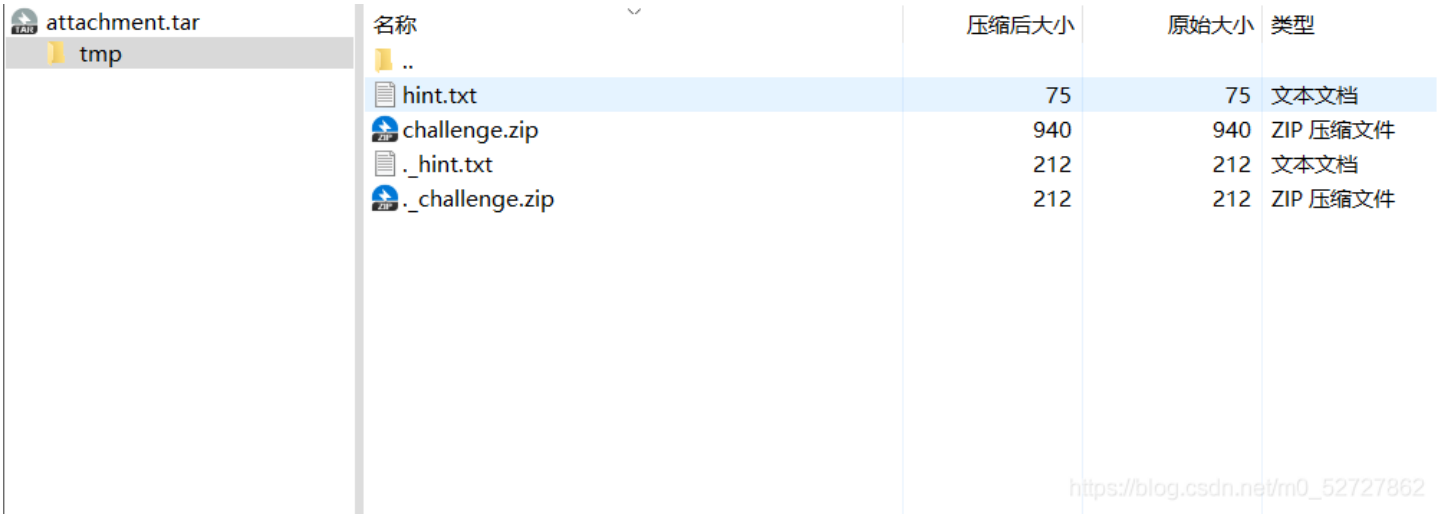
订阅专栏

wp

54 篇文章 0 订阅

订阅专栏

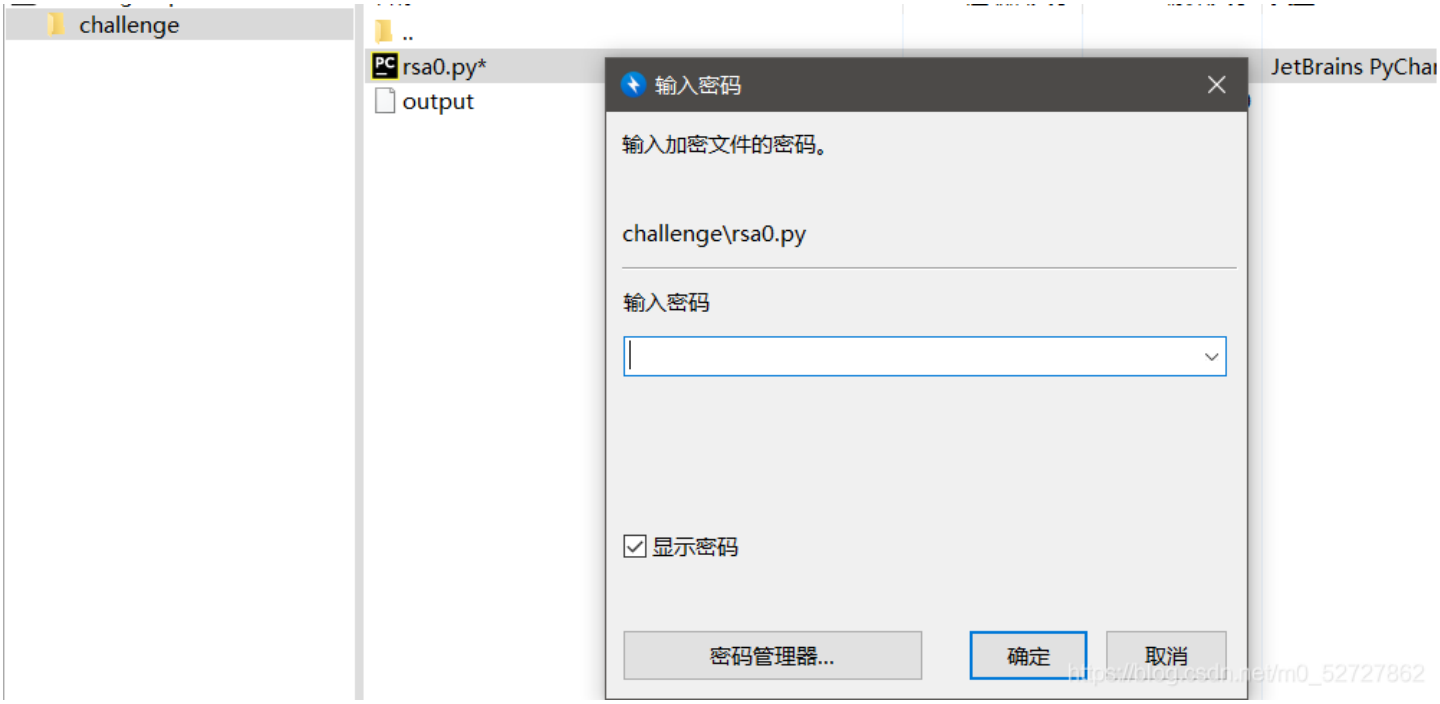
[ACTF新生赛2020]crypto-rsa0



hint.txt

怎么办呢，出题人也太坏了，竟然把压缩包给伪加密了！

challenge



output

```
90185880664342063772402771624767392713862401730886765262953151639909683470229228412991282745514829264909083992371538834949647434361938539784599470602104117547005673877738257835729760037765213340036696350766324229143613179932145122130685778504062410137043635958208805698698169847293520149572605026492751740223509962069259610194152560033947435941060614738650327920730359549258750560797626266484523488562555758401666405193348626900639493165157502565459374982134762866374558034528907812644460307323698710448703598385686181765862060410550002979817332728160898060144008463923077420655593318749722748449920478494722033903501858806643420637724027716247673927138624017308867652629531516399096834702292284129912827455148292649090839923715388349496474343619385397845994706021041175470056738777382578357297600377652133400366963507663242291436131799321451221306857785040624101370436359582088056986981698472935201495726050264927517402235099620692596101941525600339474359410606147386503279207303595492587505607976262664845234885625557584016664051933486269006394931651575025654593749821347628663745580345289078126444603073236987104487035983856861817658620604105500029798173327281608980601440084639230774206555933187497227484499204784947220339035018588066434206377240277162476739271386240173088676526295315163990968347022922841299128274551482926490908399237153883494964743436193853978459947060210411754700567387773825783572976003776521334003669635076632422914361317993214512213068577850406241013704363595820880569869816984729352014957260502649275174022350996206925961019415256003394743594106061473865032792073035954925875056079762626648452348856255575840166640519334862690063949316515750256545937498213476286637455803452890781264446030732369871044870359838568618176586206041055000297981733272816089806014400846392307742065559331874972274844992047849472203390350
```

上脚本

```
p=90185880664342063772402771624767392713862401730886765262953151639909683470229228412991282745514829264909083992371538834949647434361938539784599470602104117547005673877738257835729760037765213340036696350766324229143613179932145122130685778504062410137043635958208805698698169847293520149572605026492751740223509962069259610194152560033947435941060614738650327920730359549258750560797626266484523488562555758401666405193348626900639493165157502565459374982134762866374558034528907812644460307323698710448703598385686181765862060410550002979817332728160898060144008463923077420655593318749722748449920478494722033903501n=p*qimport  gmpy2e=65537d=gmpy2.invert(e,(p-1)*(q-1))m=gmpy2.powmod(c,d,n)import binasciiprint(binascii.unhexlify(hex(m)[2:]))
```

运行得到

```
actf{n0w_y0u_see_RSA}
```

flag

```
flag{n0w_y0u_see_RSA}
```