Files

main

Go to file t

.github
2023
0ByteCTF 2023
0xL4ugh CTF 2023
1337UP LIVE CTF
24h@CTF 2023
ASC Cyber Wargames Qualificat...
AmateursCTF 2023
BDSec CTF 2023
BYUCTF 2023
BlueHens CTF 2023

daffainfo feat: grouped the challs e6c48e5 · last month History

Name	Last commit message	Last commit date
..		
images	feat: grouped the challs	last month
README.md	feat: grouped the challs	last month
encrypt.py	feat: grouped the challs	last month
output.txt	feat: grouped the challs	last month

README.md

babyRSA

babyRSA

> RSA in haystack

About the Challenge

We were given a python script called `encrypt.py` and `output.txt` (You can download the output here). Here is the content of `encrypt.py`

```python
from Crypto.Util.number import getPrime, bytes_to_long
from secret import FLAG

m = bytes_to_long(FLAG)
f = open ('output.txt', 'w')
e = 37
n = [getPrime(1024)*getPrime(1024) for i in range(e)]
c = [pow(m, e, n[i]) for i in range(e)]

with open ('output.py', 'w'):
    f.write(f"e = {e}\n")
    f.write(f"c = {c}\n")
    f.write(f"n = {n}\n")
```

This RSA encryption is vulnerable to `Hastad Broadcast Attack`

How to Solve?

In this case i created a script to solve this problem

```python
from Crypto.Util.number import inverse, long_to_bytes
import gmpy2

def hastad_broadcast_attack(e, c, n):
    # Apply Hastad's Broadcast Attack
    M = 1
    for modulus in n:
        M *= modulus

    result = 0
    for i in range(len(n)):
        Mi = M // n[i]
        Mi_inv = inverse(Mi, n[i])
        result += c[i] * Mi * Mi_inv

    result = result % M

    # Use gmpy2 for nth root
    m = int(gmpy2.iroot(result, e)[0])

    return long_to_bytes(m)

# Load the values from the file
with open('output.txt', 'r') as f:
    exec(f.read())

# Perform the Hastad's Broadcast Attack
recovered_message = hastad_broadcast_attack(e, c, n)
print("Recovered Message:", recovered_message.decode())
```

Run the program and voilà!

```
bash-3.2$ python3 solve-hasted.py
Recovered Message: nite{y0u_C@n_N3v3r_Gu3s5!!!}
bash-3.2$
```

```
nite{y0u_C@n_N3v3r_Gu3s5!!!}
```