Write-Up CTF KKST2021 Kategori Mahasiswa

NAMA TIM : Kung Lao Chicken

INSTITUSI : Institut Teknologi dan Bisnis STIKOM Bali

Rabu, 15 September 2021

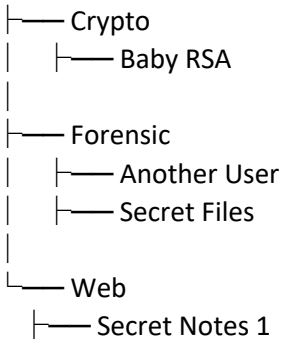
Ketua Tim

1. I Made Wahyudi

Member

1. I Putu Pramayasa Anesa Putra
2. Christopher Hendratno

Table of Content


Crypto
Baby RSA
Forensic
Another User
Secret Files
Web
Secret Notes 1

Crypto

Baby RSA

Soal

-

Attachment: out.txt, yourchall.py

Pembahasan

Diberikan file out.txt dan yourchall.py. Berikut penampakan dari yourchall.py

```
from Crypto.Util.number import getPrime, bytes_to_long, long_to_bytes
from Crypto.PublicKey import RSA

flag = b"KKST2021{1337_babying_rsa}"

p = getPrime(2048)
q = getPrime(2048)

n = p*q

e = 112

m = bytes_to_long(flag)
assert pow(m,e)>n
c = pow(m, e, n)

print('p = ', p)
print('q = ',q)
print('e =', e)
print('c =', c)
```

dan berikut penampakan dari out.txt

```
p =
174302708291532199704746594499099993107158077615976637810020756707719413
307846621433849422177093130961620210984382354931563829741495743361296415
548482820306786815695534631260628286587659583063514971991984354947170137
797770518843173660774032636499245766080416371404275984887325613542751546
746388597620117028466562931327258267477577826542863682328151714675266937
372457754497819483788338393558622203547111723417387445477544193324996255
816038930148651137387992076052389525737164443085011133444570191571800550
465455602573312073676623734619091452459281788067562364603042032170891351
77550407607787303876517195754781748656481673199
q =
241209510818309932999646108500482042958528952987428561066716815766575515
802202645473508788813180360636237594761556076139820537947167966774142198
168003684782293149985296186749000866452358867710498039820545149920463676
841193623942203684997854224025442179672233472660180715908257548252 7
```

```
734523782808657517353145399908642363936877588316903449363623584859469960461232521561681173961758168973768873896988941953874791143688840128656042726000591352169974029344678613353455702113625642938272866051843499524163998153009591046189091773301564858394991255724310724102773975702139890091251430096487849369613699809532415284109488607
e = 112
c = 14672350601751274304003169640358504354758853101311645067291449048317779678928694810564118950469744408616788934958737527011655230783446131808936701800442133351058475400560466795126543038090838351554740181801050533523758870383339981019932687349772013379978944697984965713867760727916204935090814821055003034191962606587741610602341255791407332872488906716137278223921540031926952900214034199092397808162408820999378180864934794465418049595953160460595027341719172721828634602415957338394177197979564296971971964516814226635261920334857189634437579505016769078537235705108336520718344280714638734335248338160892257800031168085140595482894003303653703789671315458175743031897831556154369600318081711321869125951989787568533121154805785772279086767854491446404735503072772566446139447274981711633503828015693936375509324086109709423141661431726884643699031302242622634284395711548021761887813439622499784251113180826999432116004667156057927449472101449534049399439252900301069010850601336120975373678751168967400228564097792789388876665082191131906934708937257069597628276285995472930230603888129336701801838743371109149289258526844054166965526698963654087622743921188963518228928795752879053567139600830570602425102784265090167876401494
```

Terlihat cukup sederhana, hanya mencari nilai d, decrypt, flag didapat. Tetapi karena nilai $e = 112$ mengakibatkan nilai $GCD(e, \varphi n) = 4$

Setelah searching-searching di google, kami menemukan diskusi dari stackoverflow

https://stackoverflow.com/questions/43141980/given-values-for-p-q-and-e-but-gcde-phi-is-not-1-then-how-to-find-n-d-in

pada jawaban yang terpilih, dia juga mencoba mencari λn. Dia juga mengatakan kalau λnhanya $\frac{\varphi n}{2}$, jadi saya mencoba $\frac{\varphi n}{4}$karena $GCD(e, \varphi n) = 4$, dan ternyata flag didapat.

Full script:

```
from Crypto.Util.number import *

chall = open("out.txt").read()
exec(chall)     # p, q, e, c

n = p*q
phi = (p-1)*(q-1)
divisor = GCD(e,phi)
d = inverse(e, phi//divisor)

m = pow(c,d,n)
print(long_to_bytes(m))
```

Hasil:

```
anehman@ubuntu:~/ctf/kks_tni/2021/crypto/baby_rsa$ python3 solve.py
b'KKST2021{b4by_RSA_1337}'
anehman@ubuntu:~/ctf/kks_tni/2021/crypto/baby_rsa$
```

FLAG: **KKST2021{b4by_RSA_1337}**

Forensic

Another User

Soal

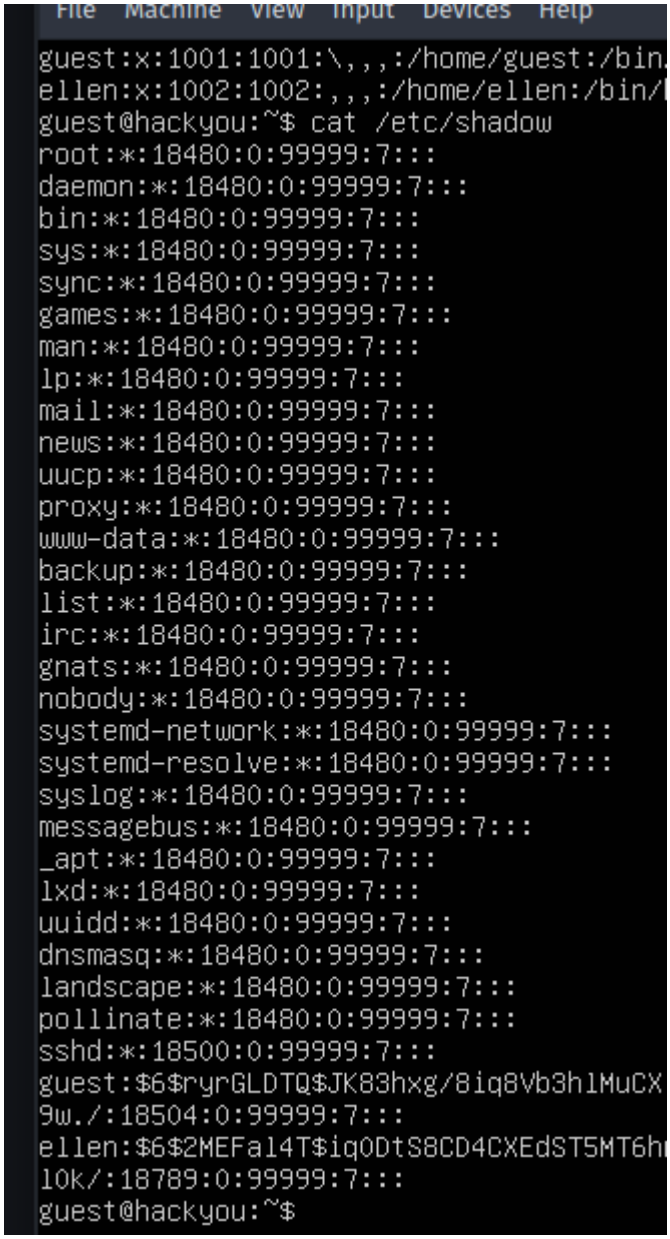
Kami menyita sebuah mesin dari terduga pelaku perentasan pada website sebuah perusahaan, di situ diberikan sebuah akun yang dapat masuk ke dalam sebuah mesinnya, dapatkah kamu mendapatkan akun selain **guest**? KKST2021{username:password}

Password VM : **4d1b54eeaceb5277ea022f7b42b53113**

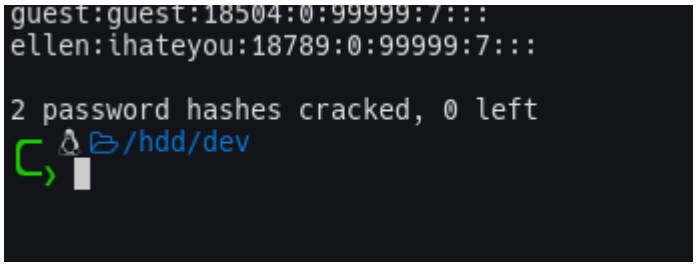
Pembahasan

Setelah berhasil masuk kedalam machine kami langsung menjalankan perintah **cat /etc/passwd** untuk melihat list user yang terdapat pada sistem. Kami melihat ada user lain bernama **ellen** dengan uid 1002.

Disini kami awalnya mengira harus mendapatkan akses root untuk membaca file /etc/shadow setelah dicoba ternyata tidak.



pada file /etc/shadow terdapat password dari user **guest** dan **ellen** yang telah di enkripsi. kemudian kami mencoba untuk melakukan bruteforce dengan bantuan tool JohnTheRipper.



Tinggal submit flag **KKST2021{ellen:ihateyou}**

Forensic

Secret Files

Soal

Saat melakukan introgasi terhadap terduga, dia mengatakan menyimpan sebuah file yang telah diamankan dengan sebuah password, isi dari file yang diamankan adalah sebuah teks bernama secret, saat ditanya apa passwordnya, dia hanya memberi clue bahwa terdiri dari 5 karakter, karakter awal dan akhir adalah huruf besar lalu karakter di tengahnya adalah huruf kecil, serta sisanya adalah sebuah angka, bantu kami!

Pembahasan

Setelah mendapatkan username dan password user lain, kami langsung mengecek home directory (/home/ellen). Ada 2 direktori, **document** dan **tools**.

```
ellen@hackyou:~$ ls
document  tools
ellen@hackyou:~$ _
```

Didalam direktori document, terdapat file .pdf dan hidden file .secret yang ternyata adalah zip file.

```
ellen@hackyou:~/document$ ls -la
total 972
drwxrwxr-x 2 ellen ellen   4096 Jun 11 03:12 .
drwxr-xr-x 7 ellen ellen   4096 Sep 15 16:34 ..
-rw-rw-r-- 1 ellen ellen 982296 Jun 11 03:12 gdpr.pdf
-rw-rw---- 1 ellen ellen    238 Jun 11 02:46 .secret
ellen@hackyou:~/document$ file .secret
.secret: Zip archive data, at least v2.0 to extract
ellen@hackyou:~/document$
```

Langsung saja kami zip lalu pindahkan ke shared folder agar bisa dibuka diluar VM. Ketika kami coba unzip .secret, seperti yang tertera pada soal, ternyata password-protected. pada deskripsi soal diberikan hint sebagai berikut.

1. Panjang password 5 karakter
2. Karakter pertama dan terakhir huruf besar
3. Karakter ketiga huruf kecil
4. Sisanya adalah angka (karakter kedua dan keempat)

Berdasarkan hint diatas, kami memutuskan untuk membuat wordlist yang nantinya akan digunakan untuk brute-force dengan John The Ripper. Berikut adalah wordlist generatornya:

```
import string

uppercase = string.ascii_uppercase
lowercase = string.ascii_lowercase
number = string.digits
```

```
password = ""

for a in uppercase:
   for b in number:
       for c in lowercase:
           for d in number:
               for e in uppercase:
                   password += a+b+c+d+e+"\n"

with open("pass.txt","w") as f:
   f.write(password)
```

Hasil:

```
anehman@ubuntu:~/ctf/kks_tni/2021/foren/secret_file/document$ head pass.txt
A0a0A
A0a0B
A0a0C
A0a0D
A0a0E
A0a0F
A0a0G
A0a0H
A0a0I
A0a0J
```

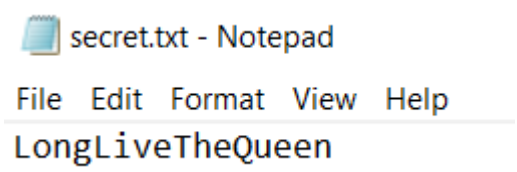
Selanjutnya tinggal brute dengan John The Ripper

```
anehman@ubuntu:~/JohnTheRipper/run$ ./zip2john /home/anehman/ctf/kks_tni/2021/foren/secret_file/do
cument/secret.zip > /home/anehman/ctf/kks_tni/2021/foren/secret_file/document/secret.zip.hash
anehman@ubuntu:~/JohnTheRipper/run$ ./john --wordlist=/home/anehman/ctf/kks_tni/2021/foren/secret_
file/document/pass.txt /home/anehman/ctf/kks_tni/2021/foren/secret_file/document/secret.zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
No password hashes left to crack (see FAQ)
anehman@ubuntu:~/JohnTheRipper/run$
```

(output beda karena ini ss reka ulang *hiks*)

password ada di john.pot

```
$zip2$*0*3*0*68b4f611ab1afdfe2dde936c1e2f1ae8*226c*12*6565d232e3243a3e3fd0f0301d96411d436b
*03d19a52228b3d726121*$/zip2$:R4c3K
```



FLAG: **KKST2021{LongLiveTheQueen}**

Web

Secret Notes 1

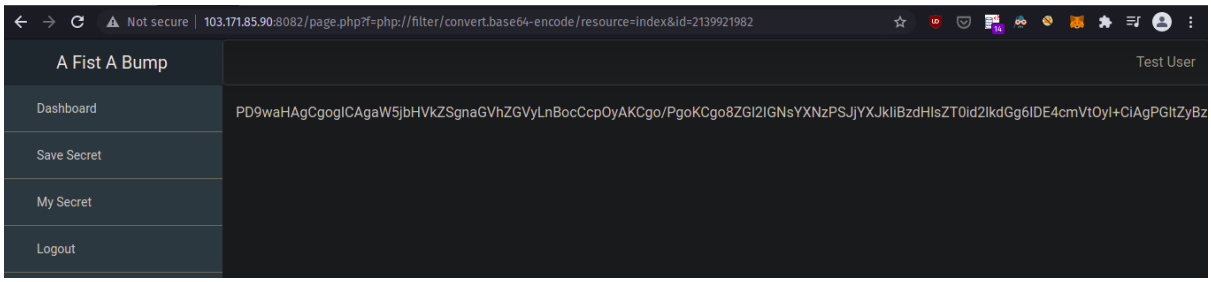
Soal

Percayakan rahasiamu pada kami, kami akan menjaganya sepenuh hati seperti n---skip---

http://103.171.85.90:8082

Pembahasan

Setelah melakukan investigasi yang mendalam kami menyadari bahwa parameter **?f** pada saat melakukan edit secret /page.php terdapat LFI. Disini kami memanfaatkan wrapper php://filter untuk melakukan inclusion berikut penampakannya:



kami menemukan credentials database pada file **conn.php**

```
❯ d64 PD9waHAgCiAgICBzZXNzaW9uX3N0YXJ0KCk7CgogICAgJGNvbm4gPSBteXNxbGlfY2
aWUobXlzcWxpX2Nvbm5lY3RfZXJyb3IoKSk7CiAgICB9CgogICAgZnVuY3Rpb24gYXNxbGko
0sICRkYXRhKTsKICAgIH0KCj8+Cg==
<?php
    session_start();

    $conn = mysqli_connect("db_fist", "uceng", "uceng123", "fist");

    if(!$conn){
        die(mysqli_connect_error());
    }

    function asqli($data){

        return mysqli_real_escape_string($GLOBALS['conn'], $data);
    }

?>
```

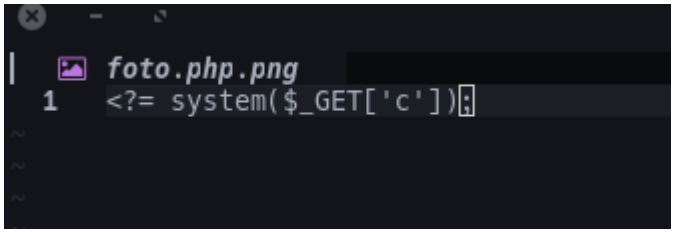
lalu kami mencoba melakukan koneksi ke database menggunakan program cli **mysql**

```
❯ mysql -h 103.171.85.90 -P 3306 -uuceng -puceng123
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 229
Server version: 5.6.51 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| fist               |
+--------------------+
2 rows in set (0.050 sec)

MySQL [(none)]>
```

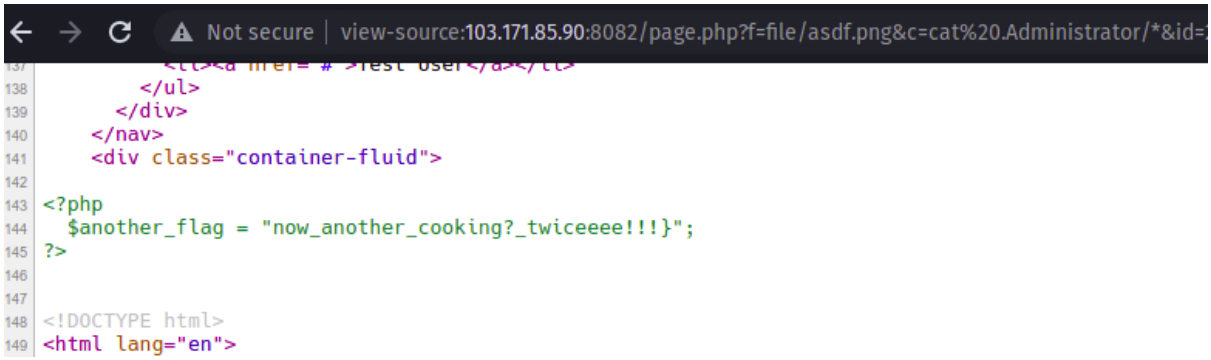
pada database ini kami hanya menemukan sebuah potongan flag pada database **fist** tabel **user**

```
Database changed
MySQL [fist]> show tables;
+----------------+
| Tables_in_fist |
+----------------+
| secret         |
| user           |
+----------------+
2 rows in set (0.055 sec)

MySQL [fist]> select * from user;
+----+---------------+--------------------+------+------------+------+
| id | username      | password           | role | pin        | foto |
+----+---------------+--------------------+------+------------+------+
|  1 | nikko         | 123                | user | 1672586651 | NULL |
|  2 | loona         | 123                | user | 1951903116 | NULL |
|  3 | baru          | baru               | user |       8175 | NULL |
|  4 | first-flag-is | KKST2021{do_you_k  | flag | 1231231231 | NULL |
|  5 | nikko         | 5                  | user |       7988 | NULL |
|  6 | yolo          | yolo               | user |       2992 | NULL |
|  7 | abcd          | abcd               | user |       8416 | NULL |
|  8 | xxx           | xxx                | user |       5716 | NULL |
|  9 | asdf          | asdf               | user |       8706 | NULL |
| 10 | ravidhr       | ravidhr            | user |       2920 | NULL |
| 11 | xxxx          | xxxx               | user |       7286 | NULL |
| 12 | foo           | 1                  | user |       5539 | NULL |
| 13 | foo           | 1                  | user |       7341 | NULL |
| 14 | loh           | loh                | user |       3723 | NULL |
| 15 | admin         | admin              | user |       9060 | NULL |
+----+---------------+--------------------+------+------------+------+
```

potongan flag lainnya kami temukan dengan cara melakukan RCE melalui file upload. Berikut payload RCE yang kami gunakan:



Terlihat pada file **upload.php** yang kami temukan sebelumnya bahwa payload <?php tidak diperbolehkan atau di filter maka dari itu kami menggantinya dengan <?=. untuk mengeksekusi nya kami perlu melakukan LFI ke file yang baru saja di upload yakni file/foto.php.png pada page.php seperti sebelumnya dengan tambahan parameter **c** untuk menjalankan perintah. Selanjutnya kami perlu mencari keberadaan flagnya, setelah melakukan pencarian ternyata flagnya berada pada .Administrator. Langsung saja kami cat semua dengan payload **cat .Administrator/*** seperti yang terlihat pada gambar berikut:



Flag setelah disatukan : **KKST2021{do_you_know_another_cooking?_twiceeee!!!}**