

**Nama : Daffa Damar Ardhika**

**NIM : 20190801247**

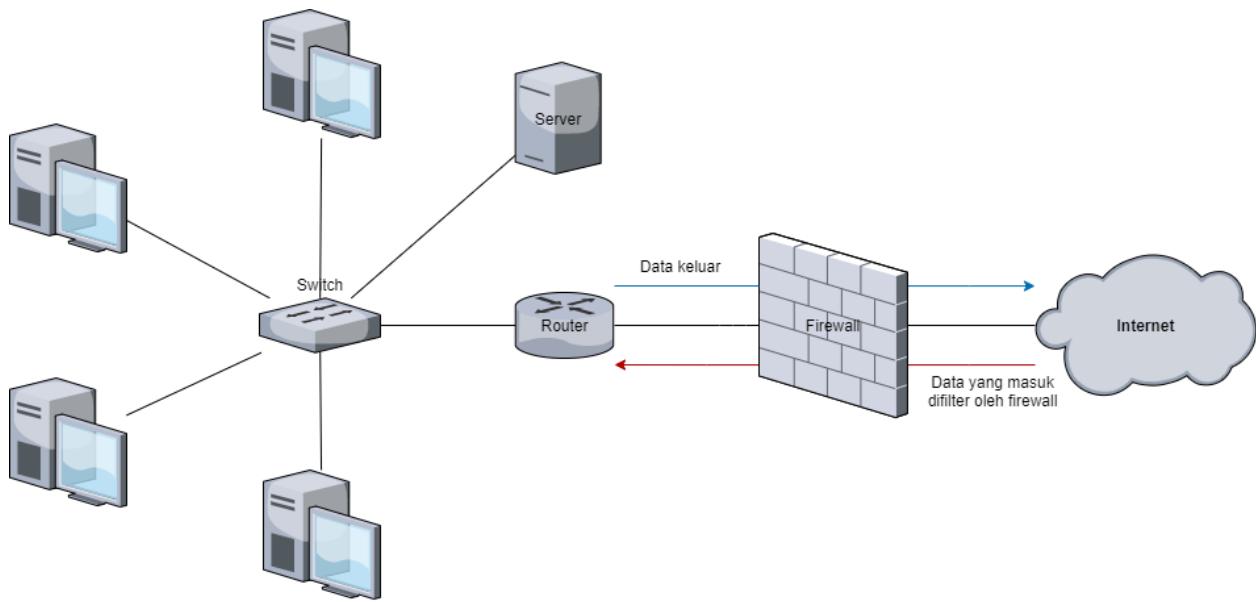
**UTS Keamanan Informasi EU003**

Soal :

Buatlah 1 buah video youtube dan 1 buah dokumen yang berisi:

- a. Desain keamanan jaringan yang anda desain sendiri dan jelaskan desain tersebut.
- b. Buatlah sebuah logic (Snippet Code) untuk yang dapat menghasilkan sanitasi data dari serangan mysql injections
- c. Buatlah sebuah lakukan pengujian terhadap logic tersebut.
- d. Buatlah 1 buah public private key (PPK) dari perangkat komputer / laptop, PPK tersebut harus menggunakan password dengan minimum length 8 dan kombinasi huruf dengan angka.
- e. Lakukan PUSH Programming Code Ke Account Github, dan cantumkan link git pada saat input jawaban Ujian.

### A. Desain keamanan jaringan



Kemanan jaringan di desain ini menggunakan firewall yang berfungsi untuk menyaring/memfilter data yang masuk ke router. Lalu router dihubungkan ke switch yang menghubungkan jaringan kepada end user. Server di sini dihubungkan ke switch yang berguna sebagai server, bisa diatur menjadi ip static maupun ip dhcp. Jika menggunakan ip static, masing-masing pc harus dikonfigurasi ip-nya secara manual, tetapi jika menggunakan ip dhcp masing-masing pc tidak usah dikonfigurasi karena ip-nya sudah otomatis ter-setting.

### B. Snippet code yang dibuat adalah menggunakan prepared statement pada bahasa pemrograman PHP

Ketika tidak menggunakan prepared statement code akan terlihat seperti di bawah ini

```
<?php

$servername = "localhost";
$username = "root";
$password = "";

$conn = new PDO("mysql:host=$servername;dbname=sql_injection_test",
$username, $password);
$conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);

$result= $conn->query("SELECT * FROM user");
$total = $result->rowCount();

$username = "apaaja' OR '1='1";;
```

```
$query = "SELECT * FROM user WHERE username = '$username'";
var_dump( $conn->query($query)->fetch(PDO::FETCH_ASSOC));
?>
```

Lalu digunakan prepared statement untuk menghindari SQL injection

```
<?php

$servername = "localhost";
$username = "root";
$password = "";

$conn = new PDO("mysql:host=$servername;dbname=mysql_injection_test",
$username, $password);
$conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);

$result= $conn->query("SELECT * FROM user");
$total = $result->rowCount();

$username = "apaaja' OR '1='1";

#prepared statement
$query = $conn->prepare("SELECT * FROM user WHERE username = ?");
$query->execute(array($username));

var_dump($query->fetch(PDO::FETCH_ASSOC));
?>
```

### C. Pengujian logic

- Ketika tidak menggunakan prepared statement

Username yang dipanggil benar dan dilakukan var\_dump(), outputnya seperti ini:

```
array(3) { ["id"]=> string(1) "1" ["username"]=> string(10) "daffadamar" ["password"]=> string(13) "daffadamar123" }
L
```

lalu ketika username yang dipanggil salah dan dilakukan var\_dump(), outputnya seperti ini:

```
bool(false)
```

Tetapi, ketika seseorang yang jahat melakukan SQL injection dengan memasukan “ OR ‘1’ = ‘1’ ” terhadap website ini, maka outputnya seperti ini:

```
array(3) { ["id"]=> string(1) "1" ["username"]=> string(10) "daffadamar" ["password"]=> string(13) "daffadamar123" }
```

Hal seperti ini menyebabkan data user bocor ke seseorang yang jahat

- Lalu digunakanlah prepared statement  
ketika seseorang yang jahat melakukan SQL injection dengan memasukan “  
OR ‘1’ = ‘1’ ” terhadap website ini, maka outputnya seperti ini:  
`bool(false)`

#### D. Generate Public Key

Di sini saya men-generate public key menggunakan openSSL

Pada folder openSSL>bin buka CMD, lalu jalankan openssl

```
Z:\openssl-0.9.8h-1-bin\bin>openssl  
OpenSSL>
```

Lalu masukan perintah:

```
genrsa -des3 -out privateKeySaya.pem 2048
```

Saat diminta memasukan password, masukan password: daffadamar12

```
Z:\openssl-0.9.8h-1-bin\bin>openssl  
OpenSSL> genrsa -des3 -out privateKeySaya.pem 2048  
Loading 'screen' into random state - done  
Generating RSA private key, 2048 bit long modulus  
.....++  
.....++  
e is 65537 (0x10001)  
Enter pass phrase for privateKeySaya.pem:  
Verifying - Enter pass phrase for privateKeySaya.pem:  
OpenSSL> -
```

Perintah di atas menghasilkan file bernama privateKeySaya.pem yang berisi:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,8285BB1A54FDA211

Nwz34IW/wzz6xj/6tOQI4LoX0GUttM11YXlgtvCD+nB8uICgkpAXb9jWXFk1IUc
HLOgs+zvGEdgFfWAWUyr7uh9ugdMadC0iB4cg6bMLxjPDPutOAlmA6AeW6c7rjv0
IDG1pWvx1G0FieoPr035noMdVCCPLJ0W5saAlg+OqMq9BiHtwkft3MQhCTb5xIu
xvw/p9gcXAkwspz0yf7b1VJdJA0EKCZQdt5Rb51GcoHU8HWkp8GTnJiKZP/TqMJm
VsUG8ToZF8ecSL7nLA5Cdf8pvDtRltajMHHD5i40V22InDl+o9fu29mFfdjGOjsC
PCI1dppPjJR4JpbDsWzIm9uD6xjh9DYGCPv5EsgV3vfGq0m4/7iLNj6FOYizEHjp
Kxjbdk6xMWCGtB01cWImtuodzhE8ZuIegCvoLp1oq7RhLUQvys63/DzL85kQS9xR
+/0FEA8MReRw5CqNFQReWf9lBttjBMXyTKj3egxDX0yWYVIgLU2gv9R0lwvi8mP20
1cjtsOuw/2TpGN/eDPT01S8vpbQ8PZNcwMxqw4BuVhJKTQasPyC5QfvIVE4EoUqV
NPMe0p6vS09p1cc271L4M1gBvNfMhIAGpN1Ojs3hQS3zzs1nh3AM23s5CmLJq7w
0biP3oiYL08Res7B7fpUUA5NHNrIApMjrun5n3b4V4hc3HpI8vXOY1jURNj84nZ
JHUTJ+i2Cy564i/GD/vyepOZ/zHle7Nryr2rPualVU4A8DW4+SUP8TXmRjt7eDxd
w3qr/0tiJ8F6ku3tLaamDiRVpzBYLj0AEftRWi+beaz8XJ/XnE88Sh8YfpCM7n9p
ubMzmEXq+lZkPCg9Iqqrv+toY+3bhVqRaax68UQL07S506eXIBf0w+t9API2maF5
1h3F5w0J40PGCV3E2LzwGFgT9BuRpkaYObfp+B144J/v8BFXMOs7khz4x4p0AgYP
wcdTFTWp7EWJUCxVQP0AEjfWcbFFLao4fCdVI9IEomlVuT42UK/I1do9qNf2TVnb
9LZ7WmEnROgdeU88LdTlwdxRFNxewAEcR1nAVwi4aJpqHEsRVvZp0SmqHon10Wen
fcykU6C8HAxgDzeORhCTKHbI2EmakNKHffo1K0fZaEf6bLgDVIPqMcm5102F8io
0g61YUNOLbIyaQpwhRg9LJCc4J4426tp4+KcEAqDUJmXrg/XrL6UziuXLqmKFB20
+H8W9Mvu2Ecm0t5prE2XBEBMBKX0cwSWF9GEsPYm328oLq9oH3BFFmD10/biNsQq
kttHdjEYGHkDTgD/NeZGp8Q7LvCGBDJpvfKbNcrX8fozK4NjCQX6MvlbGGVFpC16
Ln18CV/HMakgEeBmnLAD6W91ahy6jmpae3nrBtAtagD2up05vcCeKqLBEBpyMfH+
XLA5u1DFdI30Wri36vcxFHPGzhvnkv2rLQg2ZgB3hdEFZAI86uLpLDwY11PeWDF
JKgQ2PIq4tLuLNk/qAwcH1IJesZxouxQ1bNmrd0RLbr0kzWNxQssC90QoairkLPr
uMG01tPuIw2WhcebNpOxi+eTwgrR9wJxivtODh3sOZXyRIzmIMQ7hoqr5Pyzb4IS
-----END RSA PRIVATE KEY-----
```

Lalu untuk men-generate public key-nya, pada CMD masukan perintah:

```
rsa -in privateKeySaya.pem -outform PEM -pubout -out publicKeySaya.pem
```

Saat diminta memasukan password, masukan password yang tadi kita input untuk membuat private key yaitu: daffadamar12

```
OpenSSL> rsa -in privateKeySaya.pem -outform PEM -pubout -out publicKeySaya.pem
Enter pass phrase for privateKeySaya.pem:
writing RSA key
OpenSSL>
```