**Tugas 2**

**Cynthia Caroline | 09011281520101**

Common Vulnerability Exposure pada MySQL

1. Deskripsikan

MySQL remote root code execution atau privilege escalation vulnerability. CVE-2016-662 dilaporkan sebagai eksploitasi kritis yang dapat memungkinkan penyerang local dan remote untuk mengeksekusi kode sewenang-wenang dengan hak istimewa di server MySQL yang rentan. Oracle MySQL melalui 5.5.52, 5.6.x sampai 5.6.33, dan 5.7.x sampai 5.7.15; MariaDB sebelum 5.5.51, 10.0.x sebelum 10.0.27, dan 10.1.x sebelum 10.1.17; dan Percona Server sebelum 5.5.51-38.1, 5.6.x sebelum 5.6.32-78.0, dan 5.7.x sebelum 5.7.14-7 memungkinkan pengguna lokal untuk membuat konfigurasi sewenang-wenang dan melewati mekanisme perlindungan tertentu dengan menetapkan general\_log\_file ke konfigurasi my.cnf. vulnerability dapat dimanfaatkan untuk mengeksekusi kode sewenang-wenang dengan hak akses root dengan mengatur malloc\_lib. Serangan SQL injection adalah salah satu isu paling sering pada website, vulnerability CVE-2016-6662 bisa menempatkan aplikasi website pada kondisi yang kritis jika SQL injection berhasil dilakukan.

1. Bagaimana cara melakukan penyerangannya?

Penyerang dapat melakukan eksploitasi pada server vulnerability setelah mendapatkan akses ke server database dengan salah satu cara:

1. Mendapatkan akses otentik ke database MySQL, detail database user login dapat dicuri dengan banyak cara. Akun dengan password yang mudah dan tidak aman dapat diakses melalui koneksi jaringan atau web interface seperti phpMyAdmin.
2. Menyerang melalui SQL injection. Aplikasi web seperti PHP rentan terhadap SQL Injection. Sql injection adalah teknik injeksi dengan kalimat SQL yang dimasukan kedalam kode dan informasi database yang dibocorkan oleh penyerang.
3. Apa vulnerabilitynya?

MySQL / MariaDB / Percona - Remote Root Code Execution / Privilege Escalation (0day)

MySQL <= 5.7.14

5.6.32

5.5.51

MySQL clones yang juga terdampak, termasuk:

MariaDB

Percona

Di sistem debian

root@debian:~# dpkg -l | grep -i mysql-server

ii mysql-server 5.5.50-0+deb8u1

ii mysql-server-5.5 5.5.50-0+deb8u1

ii mysql-server-core-5.5 5.5.50-0+deb8u1

root@debian:~# service mysql start

altenatif :

root@debian:~# /etc/init.d/mysql start

server MySQL

root 14967 0.0 0.1 4340 1588 ? S 06:41 0:00 /bin/sh /usr/bin/mysqld\_safe

mysql 15314 1.2 4.7 558160 47736 ? Sl 06:41 0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mysql/plugin --user=mysql --log-error=/var/log/mysql/error.log --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=3306

mysqlld\_safe dijalankan sebagai root, sedangkan proses mysqld utama menjatuhkan hak istimewanya kepada pengguna mysql.