**SEPTIC: Detecting Injection Attacks and Vulnerabilities Inside the DBMS**

**Abstract:**

Databases continue to be the most commonly used backend storage in enterprises, but they are often integrated with vulnerable applications, such as web frontends, which allow injection attacks to be performed. The effectiveness of such attacks stems from a semantic mismatch between how SQL queries are believed to be executed and the actual way in which databases process them. This leads to subtle vulnerabilities in the way input validation is done in applications. In this paper, we propose SEPTIC, a mechanism for DBMS attack prevention, which can also assistontheidentiﬁcationofthevulnerabilitiesintheapplications. The mechanism was implemented in MySQL and evaluated experimentally with various applications and alternative protection approaches. Our results show no false negatives and no false positives with SEPTIC, on the contrary to other solutions. They also show that SEPTIC introduces a low performance overhead, in the order of 2.2%.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/UBUNTU.
* Implementation : NS2
* NS2 Version : 2.28
* Front End : OTCL (Object Oriented Tool Command  Language)
* Tool : Cygwin (To simulate in Windows OS)