PENCEGAHAN SERANGAN SQL *INJECTION* DENGAN MELAKUKAN ENKRIPSI PARAMETER *UNIFORM RESOURCES LOCATOR* (URL) MENGGUNAKAN ALGORITMA KRIPTOGRAFI HASH DAN *FILTER* ESCAPE STRING

Ghozi Ihza Humamda

ABSTRAK

SQL *Injection* merupakan salah satu jenis atau teknik serangan *website* yang paling sering dijumpai bahkan menurut *website* owasp.org teknik atau serangan berjenis *Injection* ini masih menempati posisi teratas, cara kerja dari serangan ini yaitu dengan memanfaatkan celah keamanan yang terjadi pada layer basis data dari sebuah aplikasi. Hal tersebut dapat terjadi karena data yang diinputkan oleh pengguna akan divalidasi dan dimuat dalam baris perintah *query* SQL. Dengan demikian data tersebut akan menjadi bagian dari query SQL. Serangan ini memberikan dampak yang cukup serius ini dikarenakan pada serangan berjenis injeksi ini langsung menargetkan sebuah *database* dari suatu *website*. Terdapat banyak cara untuk mencegah serangan berjenis injeksi ini, salah satunya dengan menggunakan Enkripsi pada parameter *Uniform Resource Locator* (URL) dan menerapkan *filter Escape String*, selain mudah diterapkan sebuah salah satu kelebihan dari enkripsi juga dapat dimanfaatkan untuk menyembunyikan parameter asli dari URL, sehingga penyerang kesulitan untuk memodifikasi URL tersebut. Hasil yang didapat dari pengujian dengan menerapkan metode Enkripsi parameter URL dan *filter Escape String* serangan SQL *Injection* tidak berhasil menembus *database website*.

Kata Kunci : SQL *Injection*, Enkripsi, *Uniform Resources Locator* (URL), *Escape String*

SQL INJECTION ATTACK PREVENTION BY ENCRYPTING UNIFORM RESOURCES LOCATOR (URL) PARAMETER USING CRYPTOGRAPHIC HASH ALGORITHM AND FILTER ESCAPE STRING

Ghozi Ihza Humamda

ABSTRACT

SQL Injection is one of the most common types or techniques of website attacks even according to the website owasp.org techniques or attacks of this type of Injection still occupy the top position, the way this attack works is by utilizing security gaps that occur in the database layer of an application. This can happen because the data inputted by the user will be validated and loaded in the SQL query command line. Thus the data will be part of the SQL query. This attack has a serious impact because this type of Injection attack directly targets a database of a website. There are many ways to prevent attacks of this type of Injection, one of which is by using Encryption in uniform resource locator (URL) parameters and applying the Escape String filter, in addition to being easy to implement one of the advantages of encryption can also be used to hide the original parameters of the URL, making it difficult for attackers to modify the URL. Results obtained from testing by applying url parameter encryption method and Escape String filter SQL Injection attack did not successfully penetrate the website database.

Keywords : SQL Injection, Encryption, Uniform Resources Locator (URL), Escape String