## *ABSTRACT*

*The advancement of innovation on the planet remains to progress together with the advancement of the moments in today. According to the advancement of the web currently, the variety of individuals is actually enhancing. This way it will certainly be actually extremely susceptible towards cyberpunk assaults. Assaults that are actually frequently utilized through cyberpunks towards get into a data source utilizing SQL Shot methods. SQL Shot is among the hacking methods utilized towards go into or even penetrate the site data source body, which intends towards discover the components of the data source as well as the info included on the webinternet web site. Within this particular examine, scientists utilized the Infiltration Screening Implementation Requirement (PTES) technique towards evaluate susceptabilities as well as permeate the site of SMA Negeri 1 Sokaraja. The Infiltration Screening Implementation Requirement (PTES) technique has actually 7 phases. The outcomes of the safety and safety evaluation of the SMA Negeri 1 Sokaraja site, discovered 11 susceptabilities that were actually effectively checked utilizing the OWASP ZAP devices. Of the 11 susceptabilities that were actually effectively checked, 1 was actually one of the absolute most in danger. The susceptability is actually discovered in SQL Shot assaults, within this particular examine scientists handled towards go into the MySQL data source body on the SMA Negeri 1 Sokaraja site utilizing SQL Shot assault methods. On the site data source of SMA Negeri 1 Sokaraja, scientists handled towards discover essential information like the username as well as code for the admin site of SMA Negeri 1 Sokaraja.*



***Keywords***: ***Database, SQL Injection, Website***