Vulnerable SQL Injection allowing attacker inject malicious query without authentication in login page

Date: 01/05/2024

Site: secure.srlfloan.edu.bb

Exploit Author: Spcyio.Kon

Contact me:

+) **Facebook**: www.facebook.com/s1mpl3Love

+) **Github**: github.com/tiyeume25112004

Description: The vulnerable exists in the "/Methods.asmx/DoLogin" and can be exploited throught "email_address" and "password" parameters.

Impact: Allowing attacker inject and access, disclosure of all data on system

Suggestion: User input should be santinized, escaping and parameterized query

Payload exploit: konchanabc' or '1' = '1'-- -@gmail.com

Proof of Concept

Request and Response