**Bharatcollege.org – Using SQL Injection to Bypass Authentication**

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.

A SQLi authentication bypass vulnerability exists in one of the college websites.

Vulnerable Link - <http://bharatcollege.org/LoginForm.aspx>

Payload used to check vulnerability – (**‘**)

Payload used to exploit vulnerability – (**1’ or 1=1 --)**

Severity – High

Mitigation – Input validation is required

PoC Steps

1. Open following link - <http://bharatcollege.org/LoginForm.aspx>
2. Add following payload in both Username and Password fields - **1’ or 1=1 –**
3. Reset to new password and login with the same







