Greetings,

I am Aditya Shinde, The student of Bharat College of Second year computer science I am a certified Ethical hacker, Certified information security expert and newbie bug bounty hunter.

INTROCUTION

This is a Bug bounty report of one of the domain of a Bharat college (<http://bharatcollege.org/>)

Project developed by : [Inficare Solutions Pvt. Ltd.](http://www.inficare.in) I am creating this report as a Bug Bounty Hunter, please do not share this document with anyone else until the vulnerability is patched because the vulnerability found on the domain (<http://bharatcollege.org/>) is not that hard to exploit if the syntax formed correctly as I did.

INTROCUTION OF THE VULNERABILITY

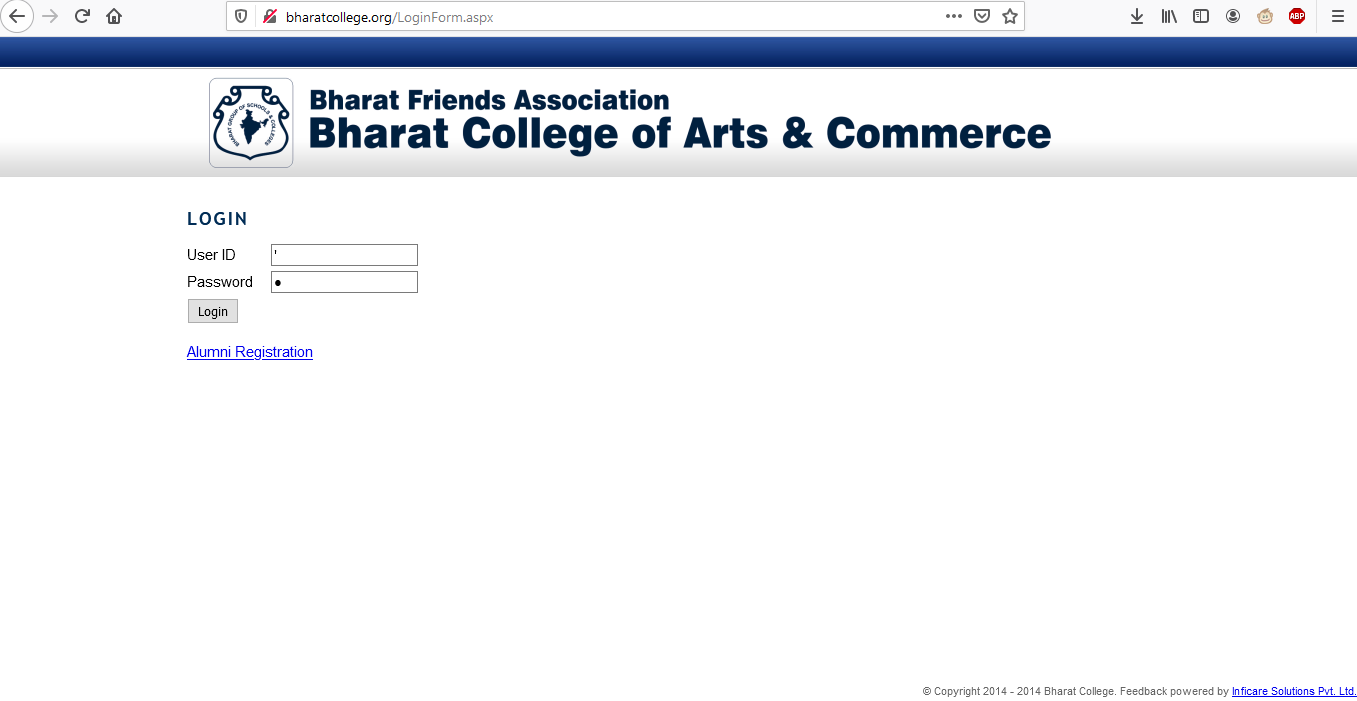
The vulnerability is known as “SQL INJECTION” which is found on the “Feedback” Section of the domain (<http://bharatcollege.org/>)

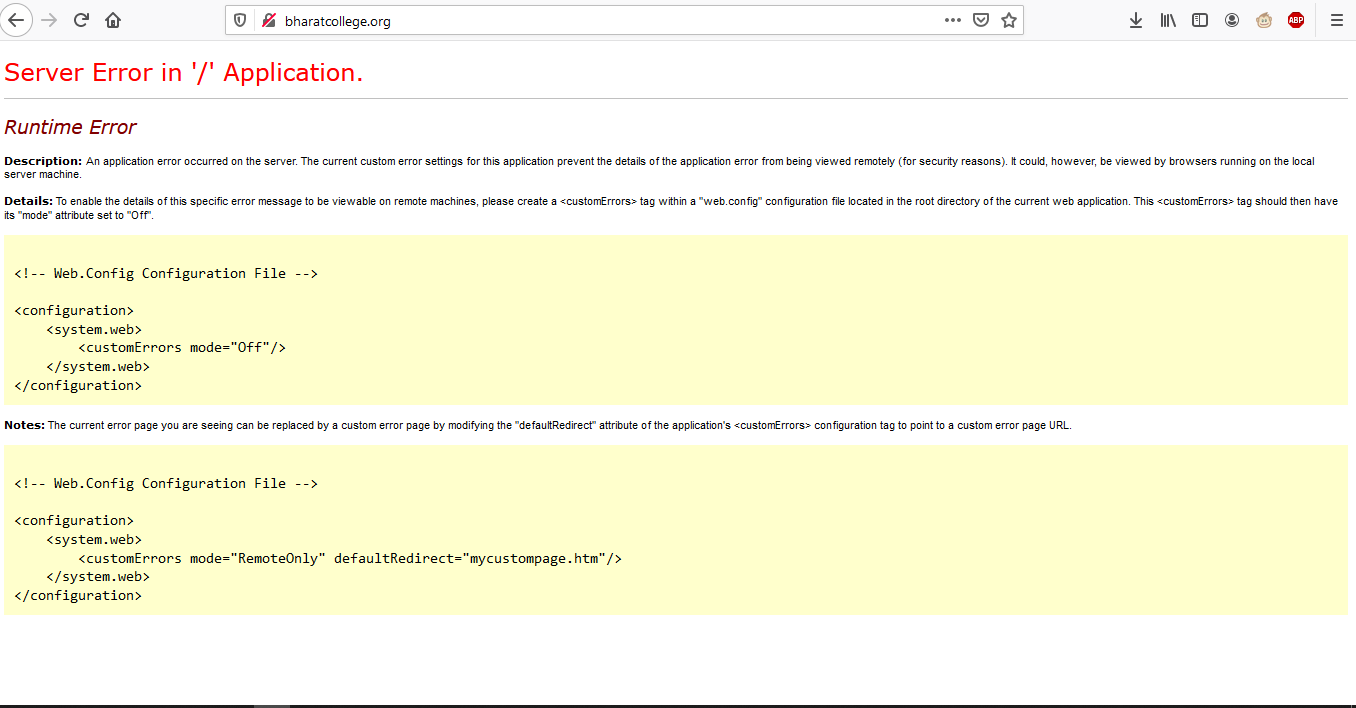
SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

WHAT ARE THE CAUSED OF VULNERABILITY(SQL INJECTION)

As I found the Vulnerability is persist on the complete website, if a Bad Hacker or Attacker formed a correct query then he/she may get access to personal information of students. Which can be used for bad intentions or he can destroy the database tables. I have no Idea how complicated this vulnerability can be but the vulnerability should be patched before anyone takes advantage of it.

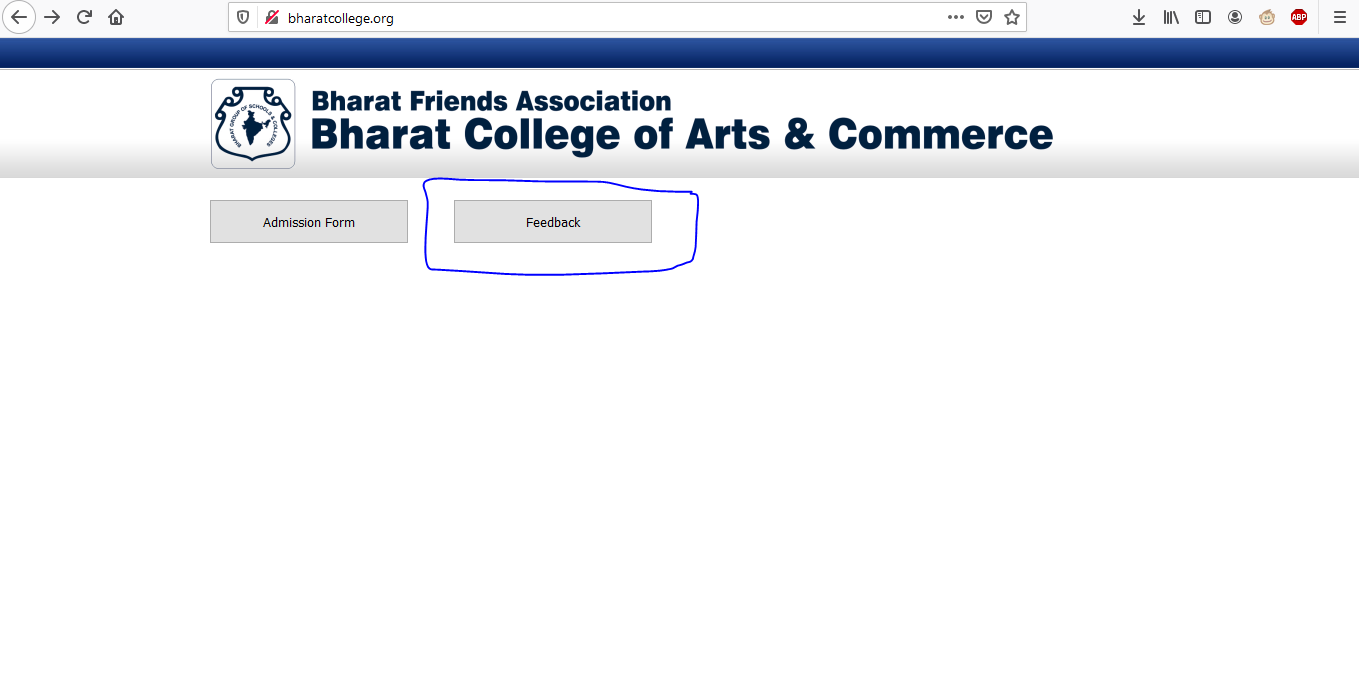


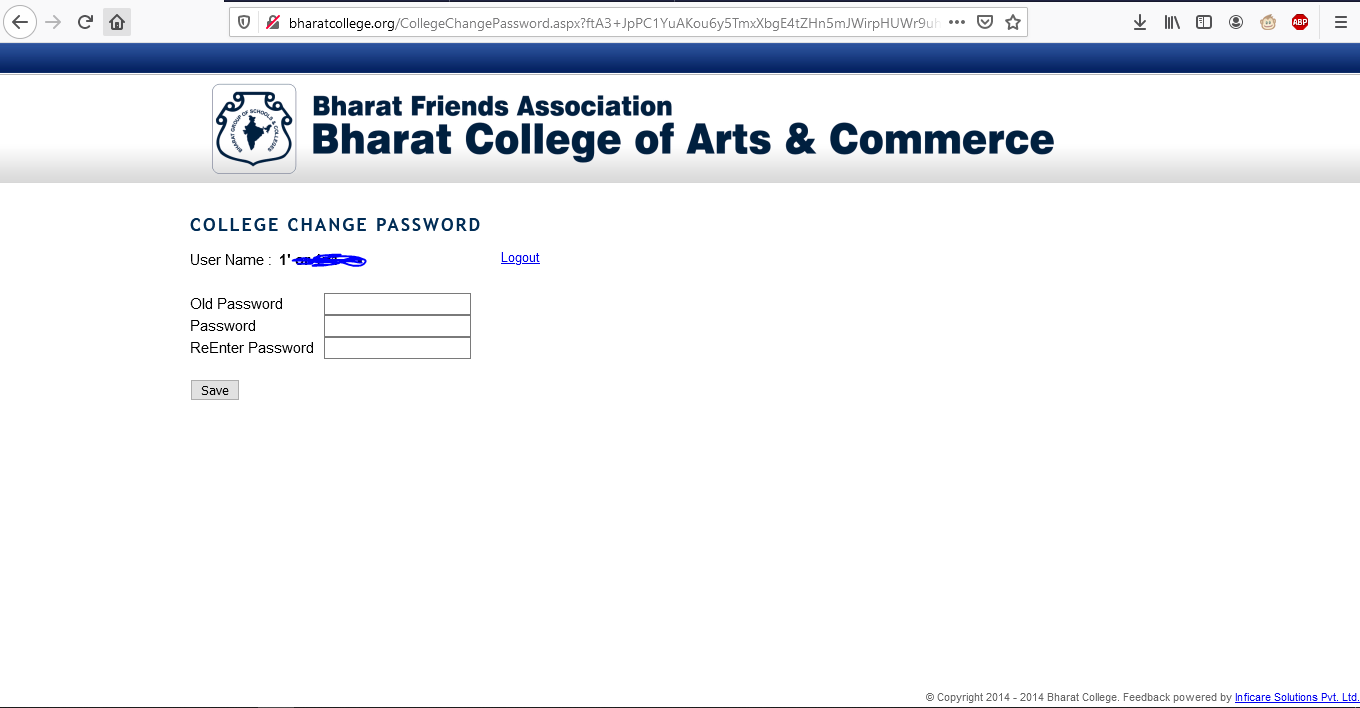


HOW DID I FOUND THE VULNERABILITY

While enumerating the “FEEDBACK” section of the domain I have found that after entering the escape character ( ‘ ) String after Single Quote runs as a SQL query. Results are given in the following image. The formed query is hidden because if in case the document leaked any one can use that single line query to change the Password of the first user of database “BHARAT”.

As this vulnerability is not that complicated anyone can form the correct query. Also it does looks like vulnerability is persist on the complete domain. I kindly request you to share this document with the Development team to get the vulnerability patched as soon as possible.





HOW TO FIX THIS VULNERABILITY

Developers are smart enough to fix this vulnerability they may fix it easily by adding Validation of input sting etc. I am not a developer but just giving an idea.

NOTES

In the Following domain I have changed the password of “BHARAT” (Admin user), but the next day I have discussed with my respective professors and fixed everything. The incident happed around 2-3 months ago.

As a student of the Bharat College I want to contribute as much I can.

Developers are much smarter than me but in case of any helpful information of my research on the domain kindly contact me on “9260608664” I will try to contribute as much as I can.

Thank you