Site:

http://testaspnet.vulnweb.com/Comments.aspx?id=1

Problem:

The automatic analysis tools indicated that an SQL injection is possible at the parameter id. SQL injections may grant us access to data we are not supposed to see or even alter them on the database.

Exploit example:

In this case we can exploit the comments table of the http://testaspnet.vulnweb.com/ database with an Inferential SQL injection

1. Table guessing:
   since we don't know the names of the table on the remote database we can use a query like:
   http://testaspnet.vulnweb.com/Comments.aspx?id=1+AND+1=
   (SELECT+COUNT(*)+FROM+comments) his query will cause ether an error or return a result depending on wether or not the table users exists this way we figured out that the table with the name comments exists on the database

2. Table manipulation:
   at this part I tried to drop or truncate the table which didn't work but the following delete query was successful and all comments on the server where deleted
   http://testaspnet.vulnweb.com/Comments.aspx?id=0;+DELETE+FROM+comments+WHERE+1=1

Fix:

To avoid SQL Injections use parameterized queries with bind variables.

since we are dealing with .NET It should be like this (there is a bit of guessing because I don't know the actual query and never wrote .NET)

```
public DataSet GetDataSetFromAdapter(
  DataSet dataSet, string connectionString, integer id)
{
  using (OleDbConnection connection = new
OleDbConnection(connectionString))
  {
      // The important part is that we define the id with ? and then use
OleDbType.Integer as a type
      // so all other imput will be result in an error
      queryString = "SELECT * FROM comments WHERE id = ?"
      OleDbDataAdapter adapter = new OleDbDataAdapter(queryString,
connection);
      adapter.SelectCommand.Parameters.Add("@id", OleDbType.Integer).Value
= id;
```

```
        try
        {
            connection.Open();
            adapter.Fill(dataSet);
        }
        catch (Exception ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
    return dataSet;
}
```