Security Testing of TeamMentor WebServices - Part 1

In terms of testing the security of the WebServices there are a couple tools and techniques that were developed that really help to gain visibility into the actual behaviour of the webservices:

This document covers the direct use of UnitTests to execute these requests (see part 2 for a more advanced and powerful GUI)

SecurityInnovation.TeamMentor.WebServices.OnlineStorage_Invoke_Query_UnitTests.cs

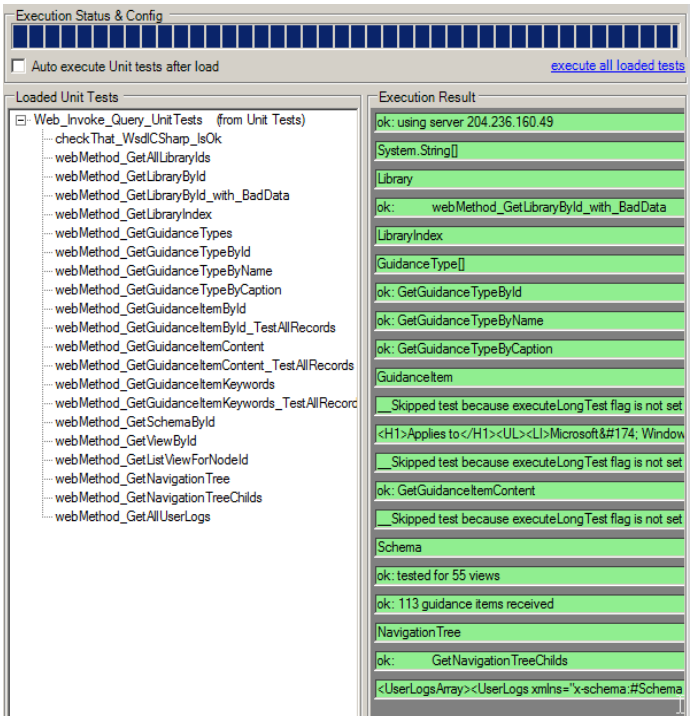
This unit tests is the one the makes Queries to the database

Executing as Admin

if you look at the constructor of this test, you will notice that there is an 'login_As_Admin' call which will make all requests execute with an account with 'Admin' privileges:

```
39
40          public Web_Invoke_Query_UnitTests()
41          {
42              executeLongTests =false;// true;// false;
43
44              targetServer = "204.236.160.49";
45              onlineStoragePort = 9124;
46
47              onlineStorage = new OnlineStorage();
48              onlineStorage.Url = "http://{0}:{1}/OnlineStorage.asmx".format(targetServer,onlineStorage
49              TMLoginHelper.authentication.Url = "http://{0}:{1}/WebServices/Authentication.asmx".forma
50
51              //setup Credentials
52              var sessionID = TMLoginHelper.login_As_Admin();
53              //var sessionID = TMLoginHelper.login_As_Test();
54              onlineStorage.CredentialsValue = new Credentials() {AdminSessionID = sessionID};
55          }
```

which when executed will look like this:

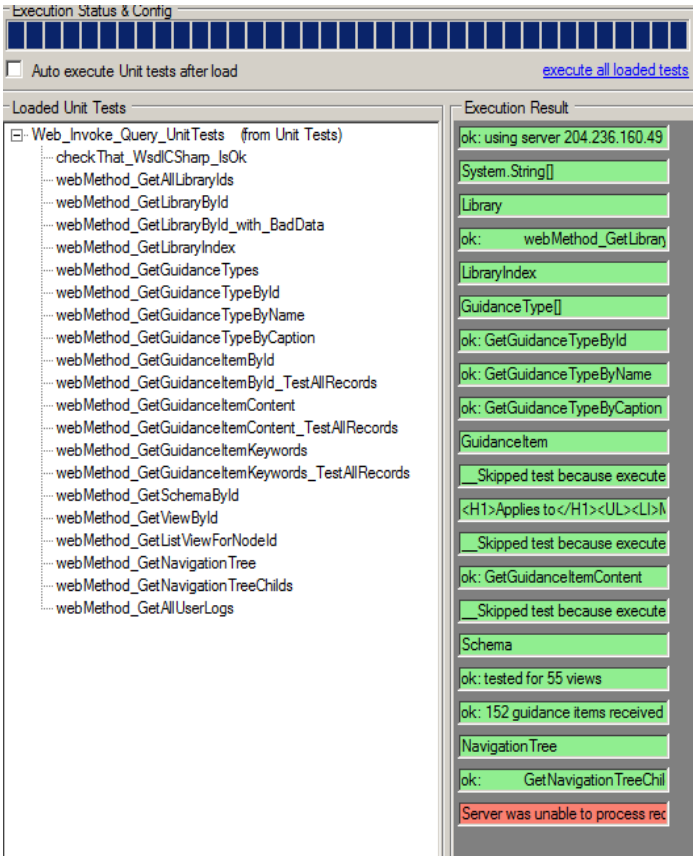


Executing as User

and if we change the session id to a 'user' account

```
51              //setup Credentials
52              //var sessionID = TMLoginHelper.login_As_Admin();
53              var sessionID = TMLoginHelper.login_As_Test();
54              onlineStorage.CredentialsValue = new Credentials() {AdminSessionID = sessionID};
55          }
```

we will get the following results:



This is exactly the same as before except for the last test which fail.

This **`webMethod_GetAllUserLogs`** test

```
440         ///**********************
441         ///*** GetAllUserLogs
442         ///
443         [Test]
444         public string webMethod_GetAllUserLogs()
445         {
446             var allUserLogs = onlineStorage.GetAllUserLogs();
447             Assert.That(allUserLogs.notNull(), "No data received");
448 
449             var userLogs = allUserLogs.xRoot().elements();
450             Assert.That(userLogs.size() > 0, "no user log fetched");
451 
452             var userLog = userLogs[0];
453 
454             var UserGUID = userLog.attribute("UserGUID").value();
455             var FirstLog = userLog.attribute("FirstLog").value();
456             var LastLog  = userLog.attribute("LastLog").value();
457             var NumLogs  = userLog.attribute("NumLogs").value();
458             Assert.That(UserGUID.valid() && FirstLog.valid() && LastLog.valid() && NumLogs.valid()
459             return allUserLogs;
460         }
```

calls the `onlineStorage.`**`GetAllUserLogs`**`();` WebMethod which has a Security demand for the 'Admin' role

```
25      public partial class OnlineStorage
26      {
27          [WebMethod]
28          [SoapHeader("credentials")]
29          [PrincipalPermission(SecurityAction.Demand, Role = "Admin")]
30          public string GetAllUserLogs()
31          {
32              XmlReader reader = null;
33              StringBuilder outputString = new StringBuilder();
34              using (SqlConnection conn = GetConnection())
35              {
36                  SqlCommand cmd = new SqlCommand("dbo.GetAllUserLogs", conn);
37                  cmd.CommandType = CommandType.StoredProcedure;
```

This is why the **webMethod_GetAllUserLogs** test failed with the message:

[3:32:47 PM] ERROR: InnerException value: Server was unable to process request. ---> **Request for principal permission failed.**
[3:32:47 PM] ERROR: in UnitTestSupport.executeXRuleMethod: System.String webMethod_GetAllUserLogs() threw error: Exception has been thrown by the target of an invocation.
[3:32:47 PM] INFO: executing method: webMethod_GetAllUserLogs

For reference, here is what one of the WebMethods that were sucessfully invoked by the current user looks like (note the demand for the 'ReadArticles' role:

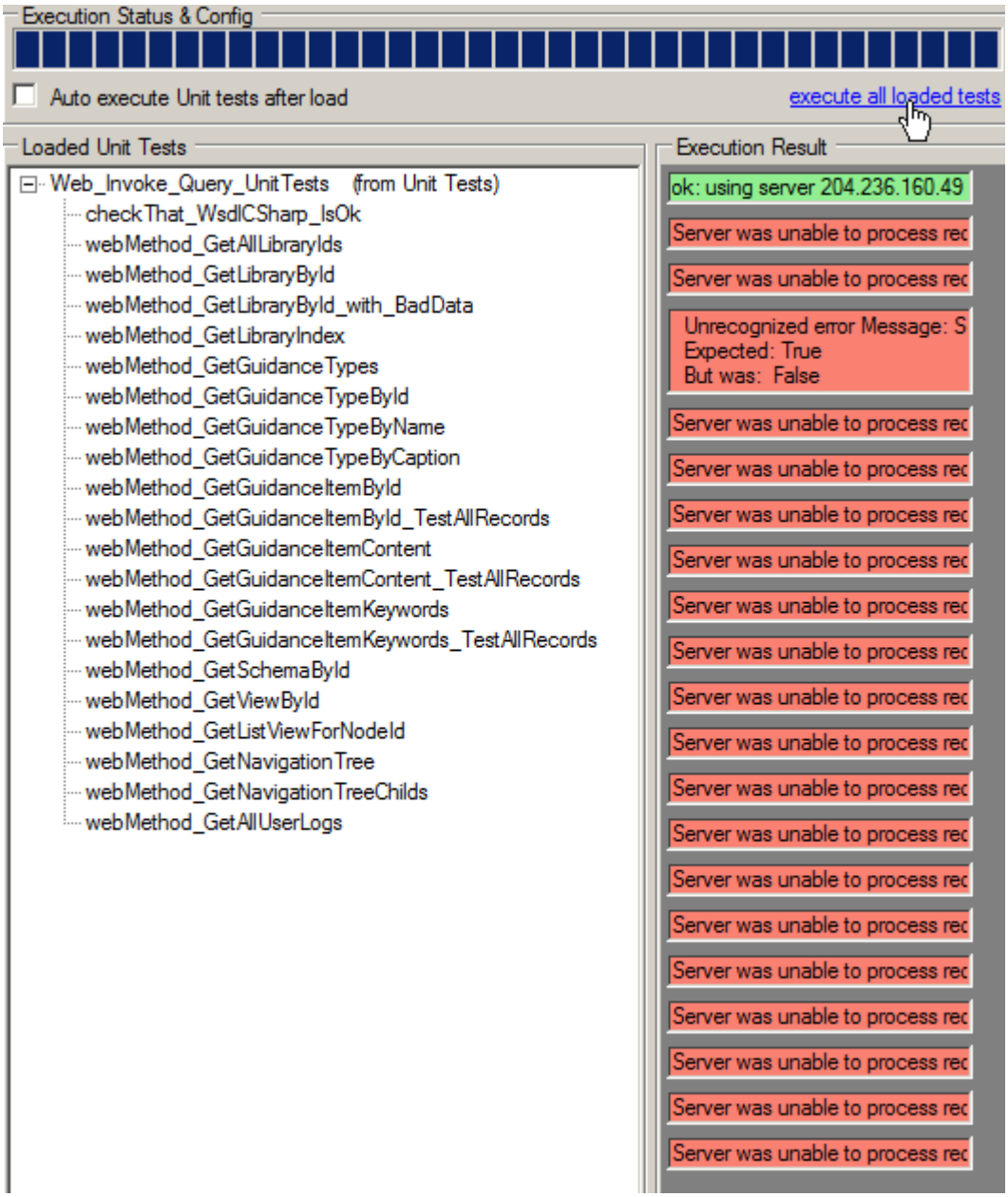
```
165         [WebMethod]
166         [SoapHeader("credentials")]
167         [PrincipalPermission(SecurityAction.Demand, Role = "ReadArticles")]
168         public GuidanceType GetGuidanceTypeById(string guidanceTypeId)
169         {
170             using (SqlConnection conn = GetConnection())
171             {
172                 SqlCommand cmd = new SqlCommand("dbo.GetGuidanceTypeById", conn);
173                 cmd.CommandType = CommandType.StoredProcedure;
```

Executing as Annoymous

now, if we remove any of these authentication calls from the constructor:

```
51              //setup Credentials
52              //var sessionID = TMLoginHelper.login_As_Admin();
53              //var sessionID = TMLoginHelper.login_As_Test();
54              //onlineStorage.CredentialsValue = new Credentials() {AdminSessionID = sessionID};
55          }
```

and run the UnitTests



we will get all a security exception of all but the first test:

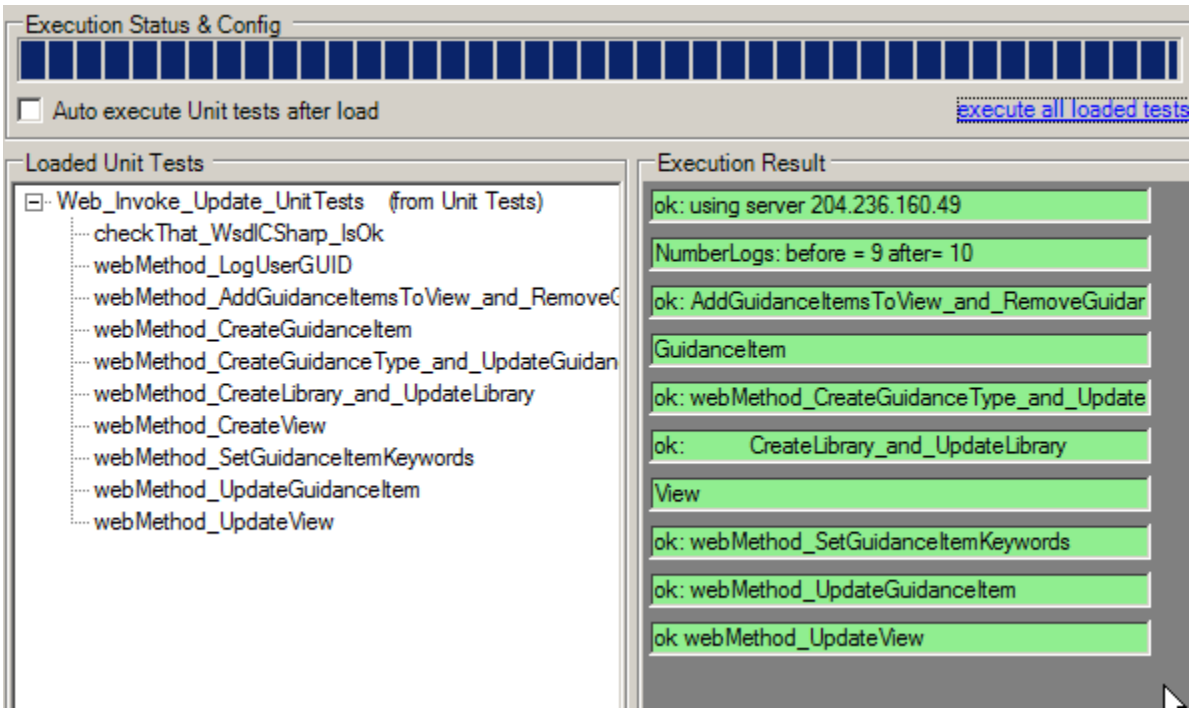
[3:44:26 PM] ERROR: InnerException value: Server was unable to process request. ---> Request for principal permission failed.
[3:44:26 PM] ERROR: in UnitTestSupport.executeXRuleMethod: System.String webMethod_GetAllUserLogs() threw error: Exception has been thrown by the target of an invocation.
[3:44:26 PM] INFO: executing method: webMethod_GetAllUserLogs
[3:44:26 PM] DEBUG: Execution result was: false
[3:44:26 PM] ERROR: InnerException value: Server was unable to process request. ---> Request for principal permission failed.
[3:44:26 PM] ERROR: in UnitTestSupport.executeXRuleMethod: System.String webMethod_GetNavigationTreeChilds() threw error: Exception has been thrown by the target of an invocation.
[3:44:26 PM] INFO: executing method: webMethod_GetNavigationTreeChilds
[3:44:26 PM] DEBUG: Execution result was: false
[3:44:26 PM] ERROR: InnerException value: Server was unable to process request. ---> Request for principal permission failed.
[3:44:26 PM] ERROR: in UnitTestSupport.executeXRuleMethod: NavigationTree webMethod_GetNavigationTree() threw error: Exception has been thrown by the target of an invocation.
[3:44:26 PM] INFO: executing method: webMethod_GetNavigationTree

Using SecurityInnovation.TeamMentor.WebServices.OnlineStorage_Invoke_Update_UnitTests.cs

These are the tests that can only be executed with an account with the 'Admin' role with the test's constructor looking like this:

```
31      [TestFixture]
32      public class Web_Invoke_Update_UnitTests
33      {
34          //public API_TeamMentor teamMentor { get; set; }
35          public string targetServer { get; set; }
36          public int onlineStoragePort {get;set;}
37          public OnlineStorage onlineStorage { get; set; }
38          public bool executeLongTests { get; set; }
39
40          public Web_Invoke_Update_UnitTests()
41          {
42              targetServer = "204.236.160.49";
43              onlineStoragePort = 9124;
44
45              onlineStorage = new OnlineStorage();
46              onlineStorage.Url = "http://{0}:{1}/OnlineStorage.asmx".format(targetServ
47              TMLoginHelper.authentication.Url = "http://{0}:{1}/WebServices/Authentica
48
49              onlineStorage.login_As_Admin();
50              //onlineStorage.login_As_Reader();  // this will fail all tests
51          }
```

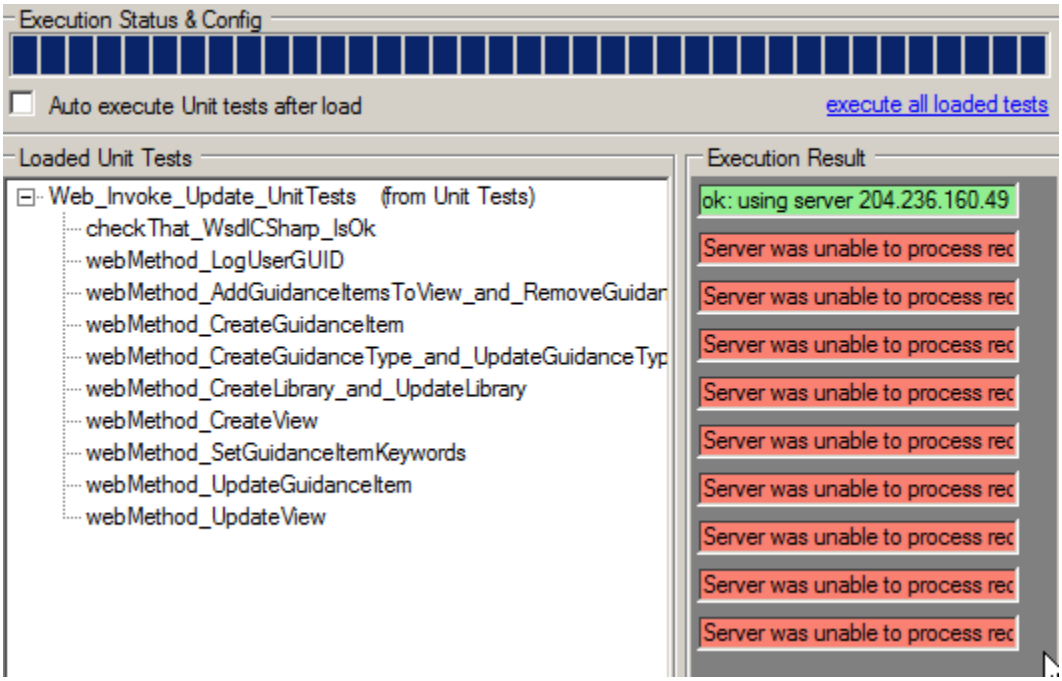
Note the 'login_As_Admin()' method which will setup the credentials so that all requests are made with an admin account:



If we change the login to an normal user account:

```
49              //onlineStorage.login_As_Admin();
50              onlineStorage.login_As_Reader();  // this will fail all tests
51          }
```

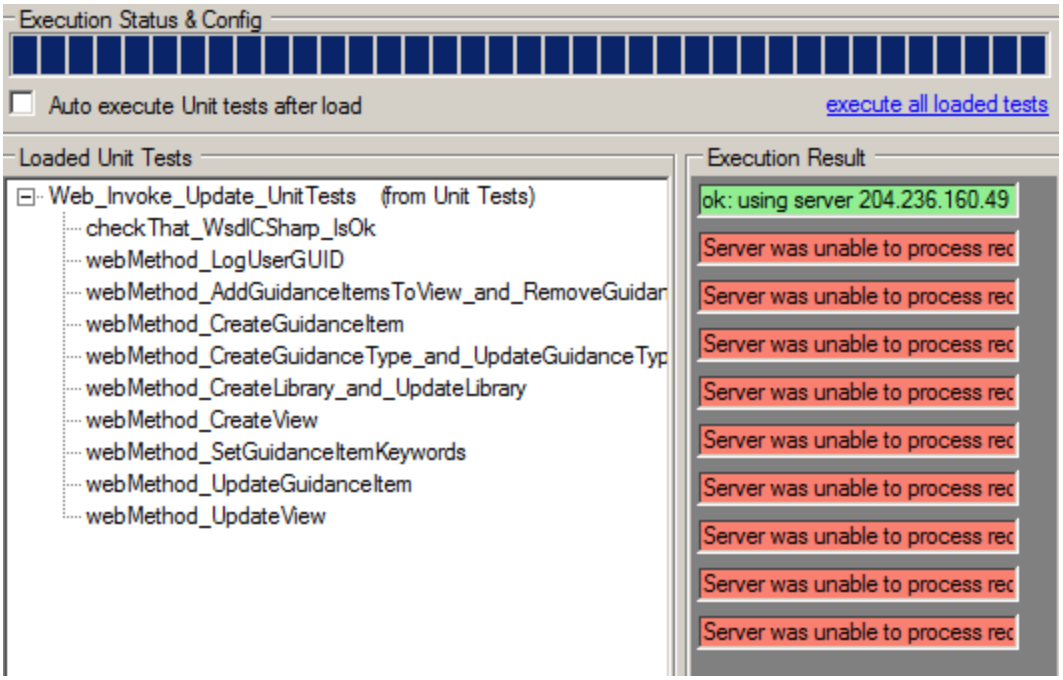
we will see that all Unit Tests will fail



And if we make the requests as an Anonymous user:

```
49              //onlineStorage.login_As_Admin();
50              //onlineStorage.login_As_Reader();  // this will fail all tests
51          }
```

we will get the same result:


Execution Status & Config
Auto execute Unit tests after load
execute all loaded tests
Loaded Unit Tests
Web_Invoke_Update_UnitTests (from Unit Tests)
checkThat_WsdlCSharp_IsOk
webMethod_LogUserGUID
webMethod_AddGuidanceItemsToView_and_RemoveGuidar
webMethod_CreateGuidanceItem
webMethod_CreateGuidanceType_and_UpdateGuidanceTyp
webMethod_CreateLibrary_and_UpdateLibrary
webMethod_CreateView
webMethod_SetGuidanceItemKeywords
webMethod_UpdateGuidanceItem
webMethod_UpdateView
Execution Result
ok: using server 204.236.160.49
Server was unable to process rec
Server was unable to process rec
Server was unable to process rec
Server was unable to process rec
Server was unable to process rec
Server was unable to process rec
Server was unable to process rec
Server was unable to process rec
Server was unable to process rec