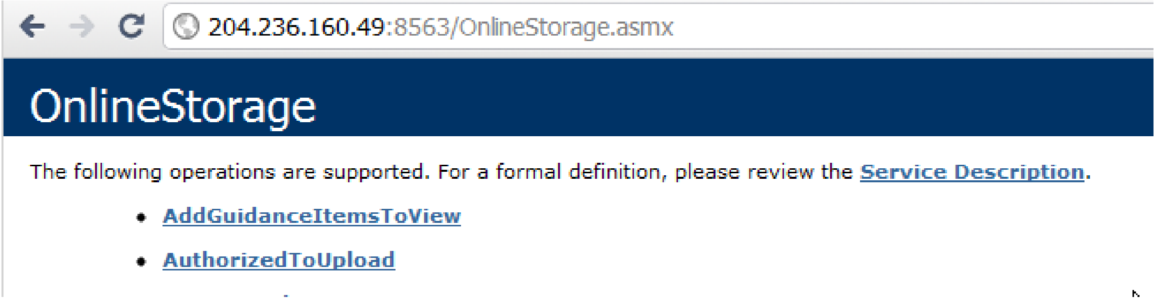
Use Case: Using TeamMentorAuthor to edit and create online content (with RBAC)

using the http://204.236.160.49:8563/OnlineStorage.asmx webservice



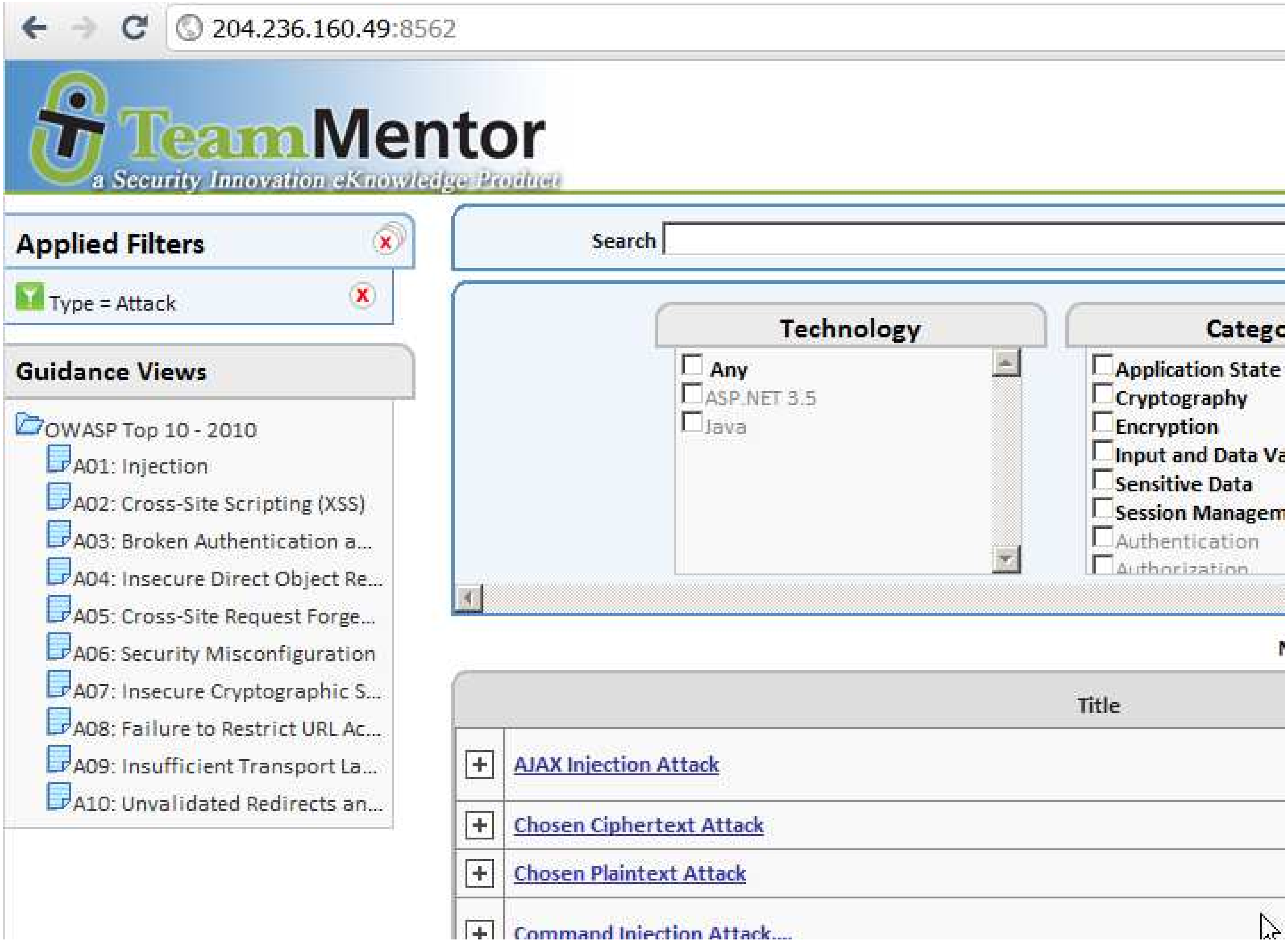
204.236.160.49:8563/OnlineStorage.asmx

OnlineStorage

The following operations are supported. For a formal definition, please review the Service Description.

- AddGuidanceItemsToView
- AuthorizedToUpload

which supports the website with the OWASP content database:



204.236.160.49:8562

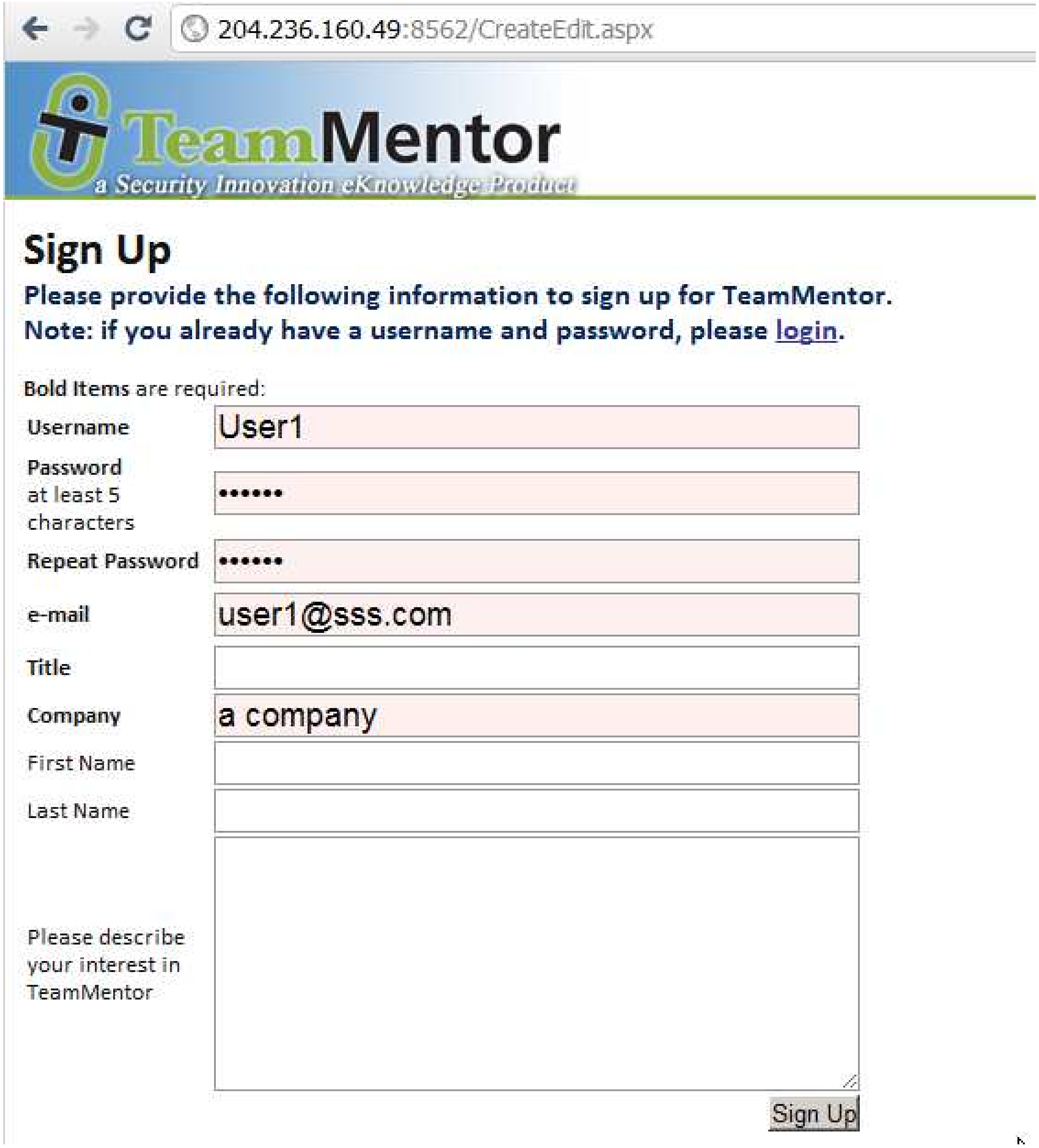
Applied Filters

Type = Attack

TeamMentor
a Security Innovation eKnowledge Product
Guidance Views
OWASP Top 10 - 2010
A01: Injection
A02: Cross-Site Scripting (XSS)
A03: Broken Authentication a...
A04: Insecure Direct Object Re...
A05: Cross-Site Request Forge...
A06: Security Misconfiguration
A07: Insecure Cryptographic S...
A08: Failure to Restrict URL Ac...
A09: Insufficient Transport La...
A10: Unvalidated Redirects an...
Search
Technology
Any
ASP.NET 3.5
Java
Catego
Application State
Cryptography
Encryption
Input and Data Va
Sensitive Data
Session Managem
Authentication
Authorization
Title
AJAX Injection Attack
Chosen Ciphertext Attack
Chosen Plaintext Attack
Command Injection Attack...

Create User

Create a normal user account (with read priviledges on the database)



204.236.160.49:8562/CreateEdit.aspx
TeamMentor
a Security Innovation eKnowledge Product

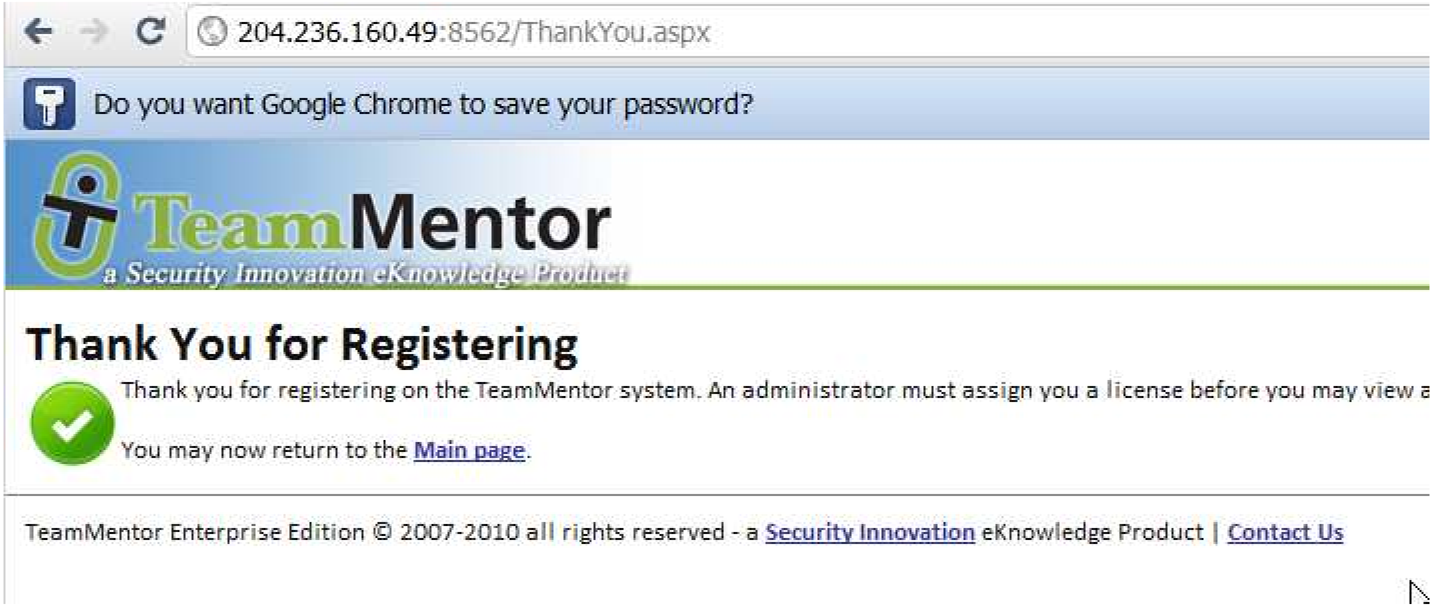
Sign Up

Please provide the following information to sign up for TeamMentor.
Note: if you already have a username and password, please login.

Bold Items are required:

Username	User1
Password at least 5 characters	••••••
Repeat Password	••••••
e-mail	user1@sss.com
Title	
Company	a company
First Name	
Last Name	
Please describe your interest in TeamMentor	

the user created


204.236.160.49:8562/ThankYou.aspx
Do you want Google Chrome to save your password?
TeamMentor
a Security Innovation eKnowledge Product

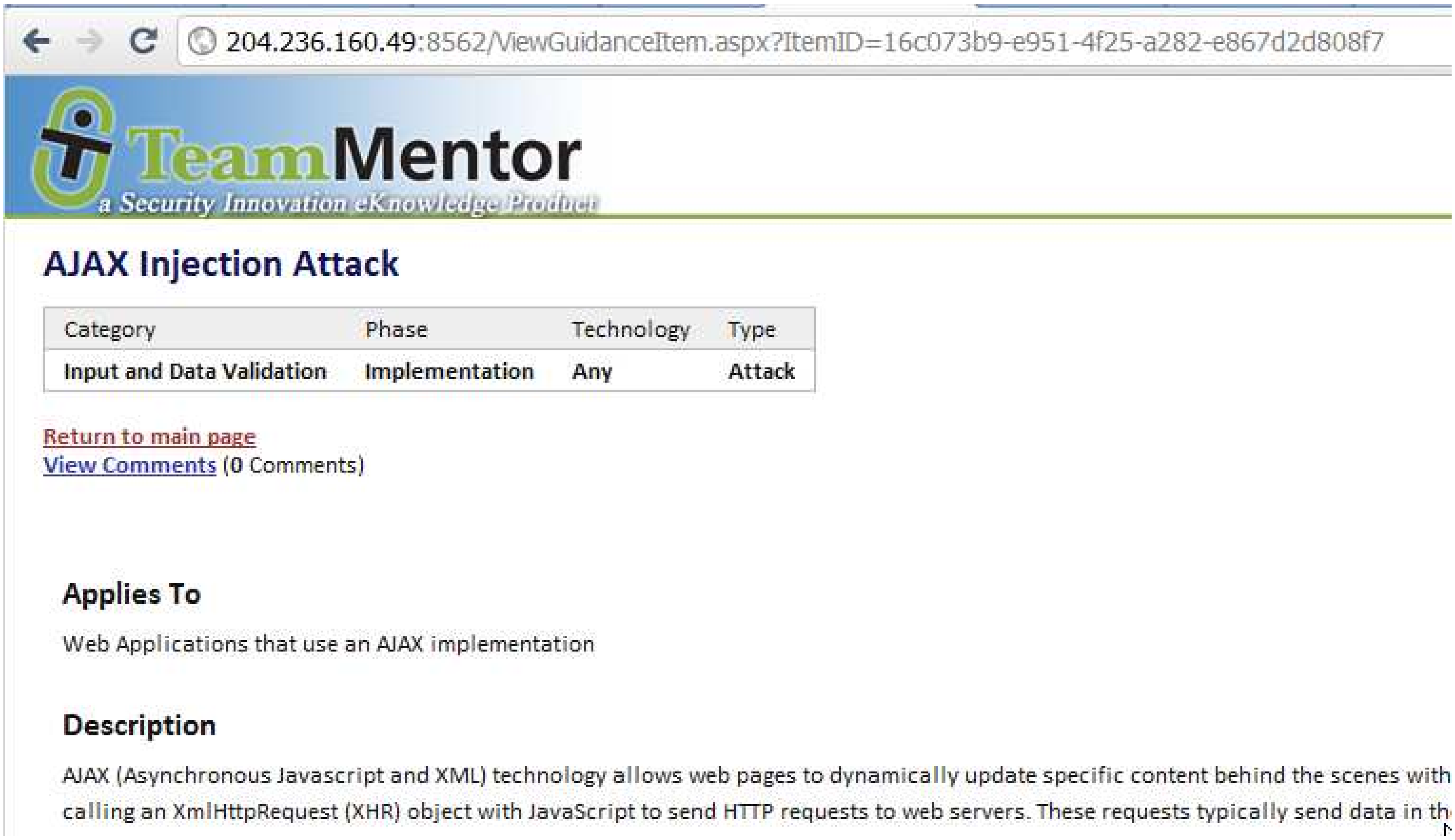
Thank You for Registering

Thank you for registering on the TeamMentor system. An administrator must assign you a license before you may view a

You may now return to the Main page.

TeamMentor Enterprise Edition © 2007-2010 all rights reserved - a Security Innovation eKnowledge Product | Contact Us

will have read access to the website


204.236.160.49:8562/ViewGuidanceItem.aspx?ItemID=16c073b9-e951-4f25-a282-e867d2d808f7
TeamMentor
a Security Innovation eKnowledge Product

AJAX Injection Attack

Category	Phase	Technology	Type
Input and Data Validation	Implementation	Any	Attack

Return to main page
View Comments (0 Comments)

Applies To

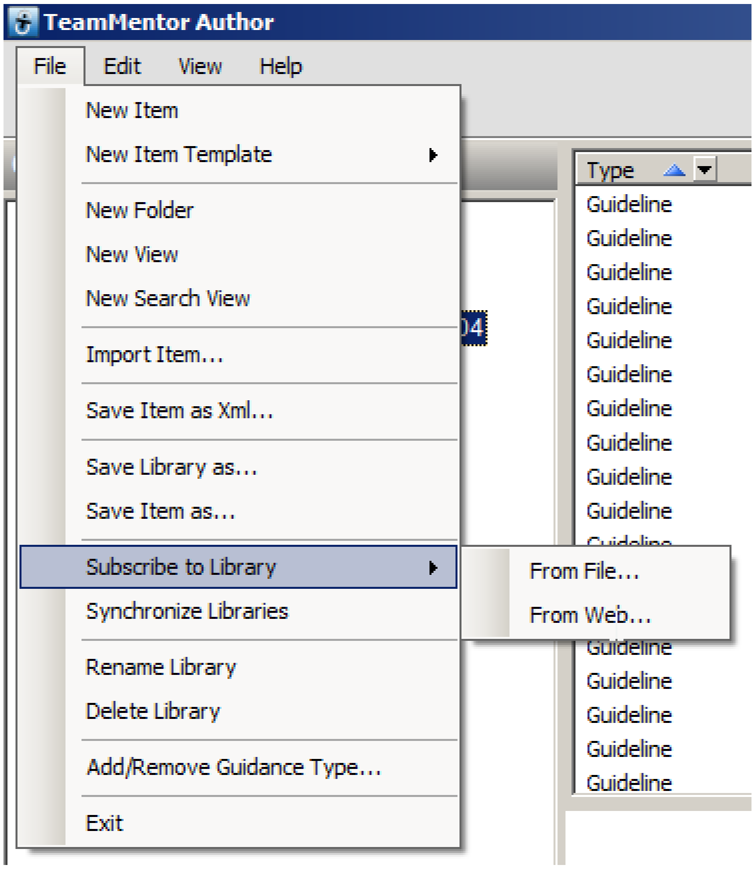
Web Applications that use an AJAX implementation

Description

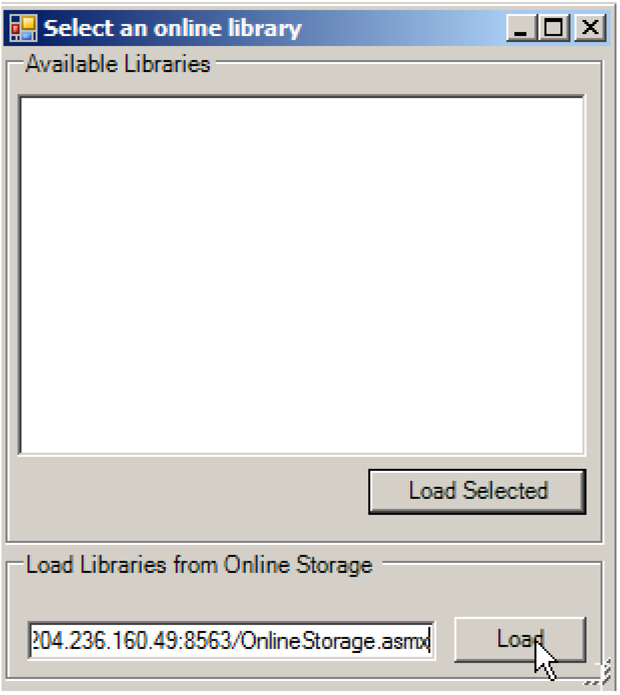
AJAX (Asynchronous Javascript and XML) technology allows web pages to dynamically update specific content behind the scenes with calling an XmlHttpRequest (XHR) object with JavaScript to send HTTP requests to web servers. These requests typically send data in th

Subscribing to library as a User

On the TeamMentorAuthor application, select the menu option to Syncronize a Library from the Web

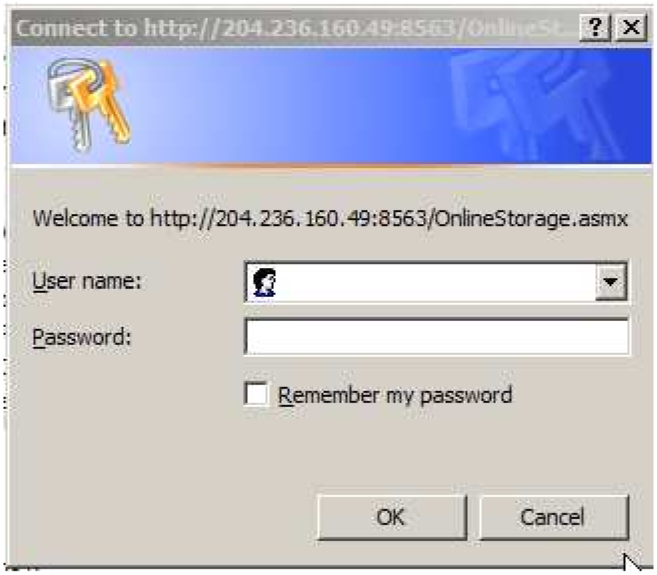


and enter the details of the webservice (http://204.236.160.49:8563/OnlineStorage.asmx) in new section called ***'Load Libraries from Online Storage'*** of the ***'Select an online Library'*** view:



204.236.160.49:8563/OnlineStorage.asmx

If this is the first time that you connect with this server, you will be promted for the login details:


Connect to http://204.236.160.49:8563/OnlineSt...

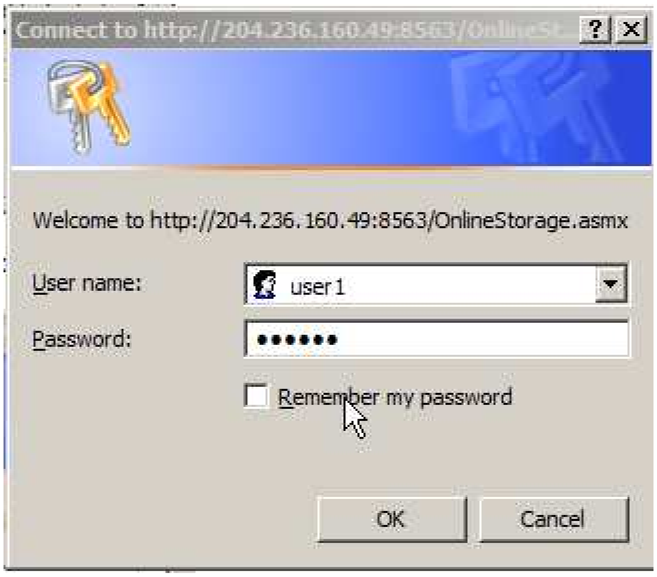
Welcome to http://204.236.160.49:8563/OnlineStorage.asmx

User name:

Password:

□ Remember my password

Use the details from the account previously created:


Connect to http://204.236.160.49:8563/OnlineSt...

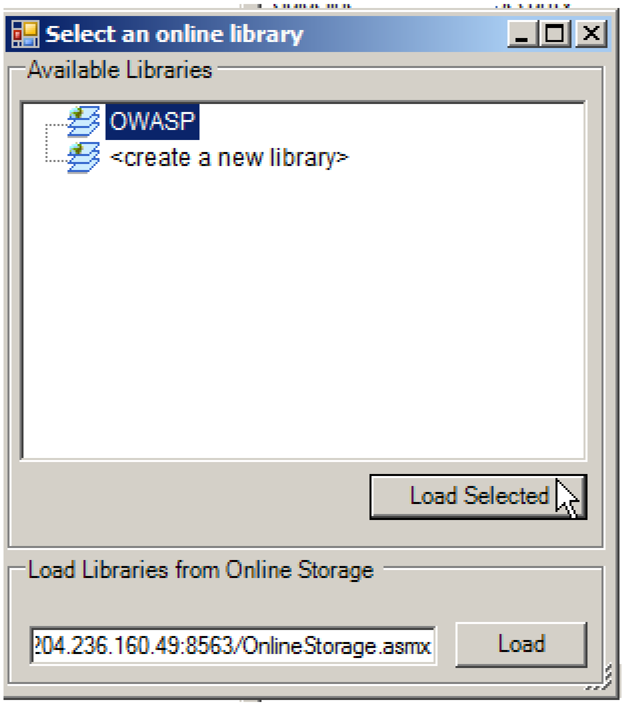
Welcome to http://204.236.160.49:8563/OnlineStorage.asmx

User name: user1

Password: ••••••

□ Remember my password

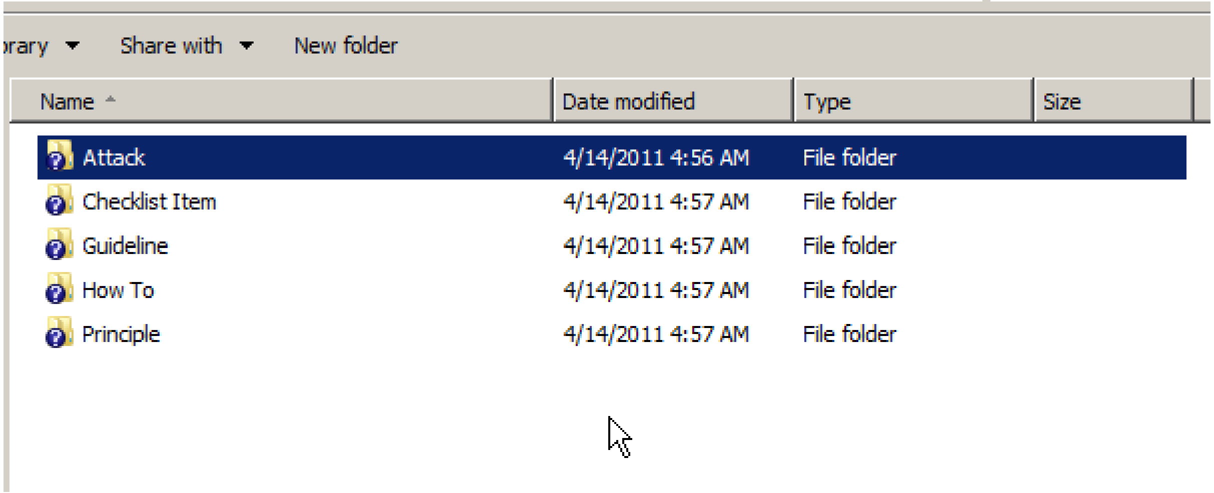
which will log the user to this site and retrieve the list of available databases



204.236.160.49:8563/OnlineStorage.asmx

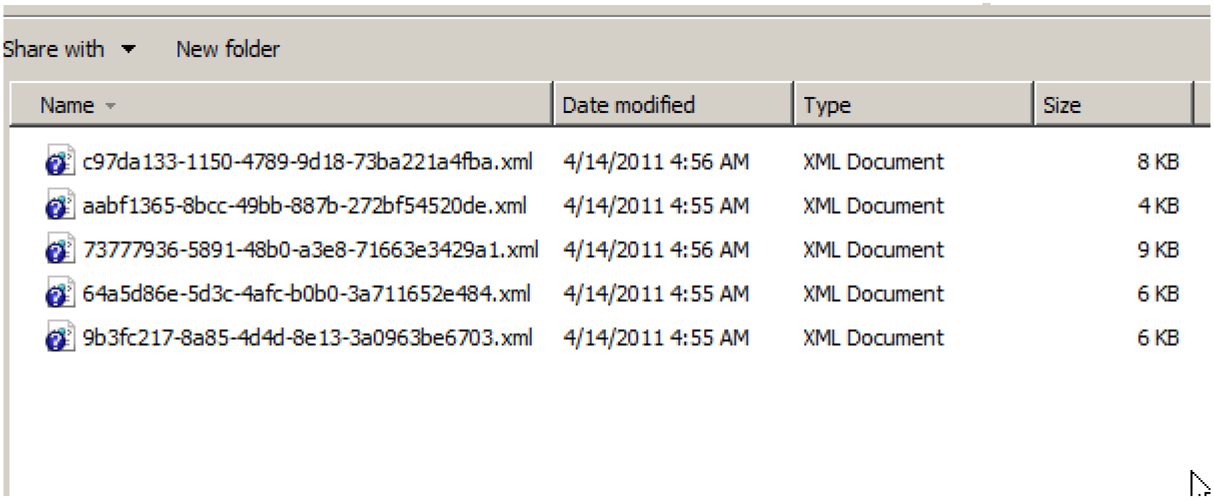
Select ***OWASP*** and click on ***'Load Selected'*** to will trigger the download of this library data (the process is quite slow so it will take a couple minutes):

If you open the Libraries folder, you will notice a new OWASP folder with several subfolders



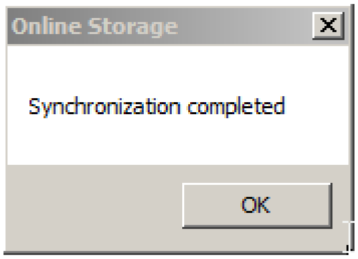
Name	Date modified	Type	Size
Attack	4/14/2011 4:56 AM	File folder	
Checklist Item	4/14/2011 4:57 AM	File folder	
Guideline	4/14/2011 4:57 AM	File folder	
How To	4/14/2011 4:57 AM	File folder	
Principle	4/14/2011 4:57 AM	File folder	

which will be populated as the files are downloaded from the server



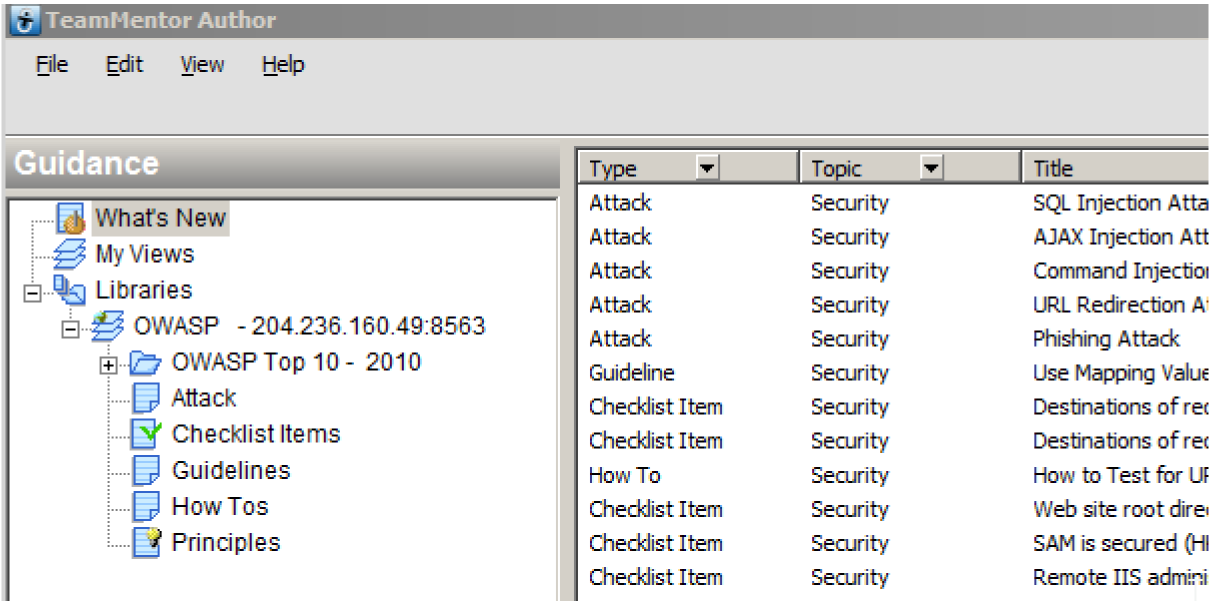
Name	Date modified	Type	Size
c97da133-1150-4789-9d18-73ba221a4fba.xml	4/14/2011 4:56 AM	XML Document	8 KB
aabf1365-8bcc-49bb-887b-272bf54520de.xml	4/14/2011 4:55 AM	XML Document	4 KB
73777936-5891-48b0-a3e8-71663e3429a1.xml	4/14/2011 4:56 AM	XML Document	9 KB
64a5d86e-5d3c-4afc-b0b0-3a711652e484.xml	4/14/2011 4:55 AM	XML Document	6 KB
9b3fc217-8a85-4d4d-8e13-3a0963be6703.xml	4/14/2011 4:55 AM	XML Document	6 KB

Once the sync is completed



Synchronization completed

you will get an replica of the content that is on the http://204.236.160.49:8562/Default.aspx website

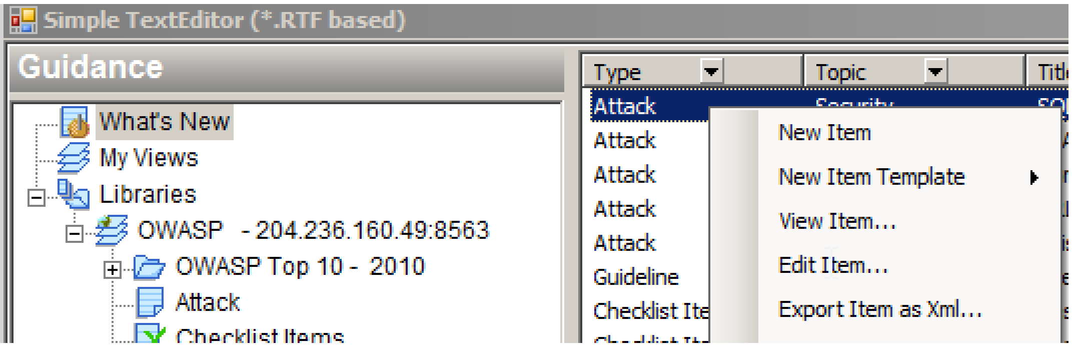


Type	Topic	Title
Attack	Security	SQL Injection Atta
Attack	Security	AJAX Injection Att
Attack	Security	Command Injectio
Attack	Security	URL Redirection A
Attack	Security	Phishing Attack
Guideline	Security	Use Mapping Value
Checklist Item	Security	Destinations of re
Checklist Item	Security	Destinations of re
How To	Security	How to Test for UI
Checklist Item	Security	Web site root dire
Checklist Item	Security	SAM is secured (H
Checklist Item	Security	Remote IIS admini

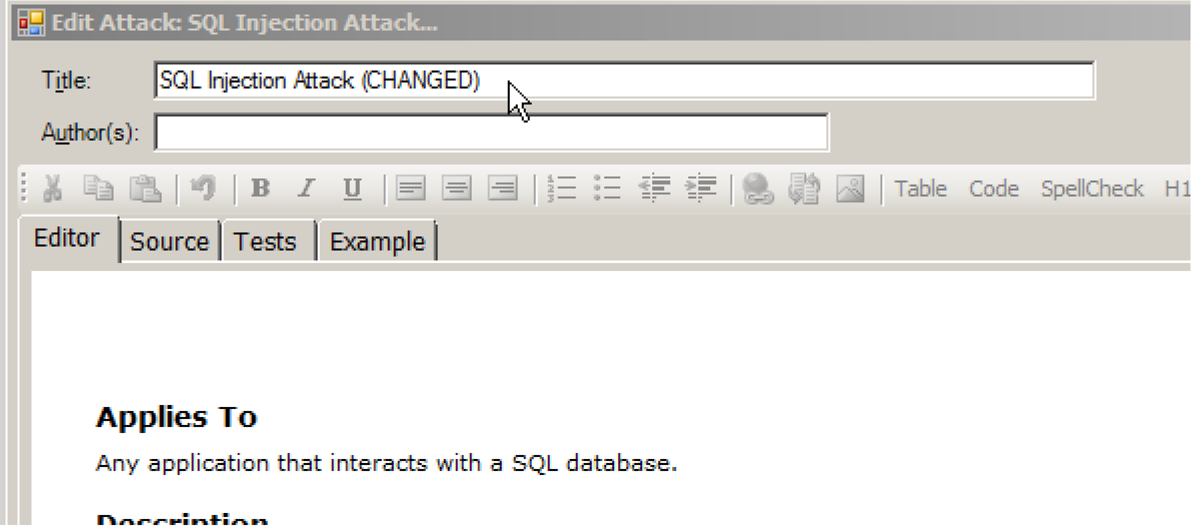
Trying to publish a local change to the server (as 'Reader' user)

To test the editing capabilities, let's make a change in one of the articles.

Click on the first article ('SQL Injection Attacks') and select 'Edit Item' from the context menu



make a change on the title:



Title: SQL Injection Attack (CHANGED)

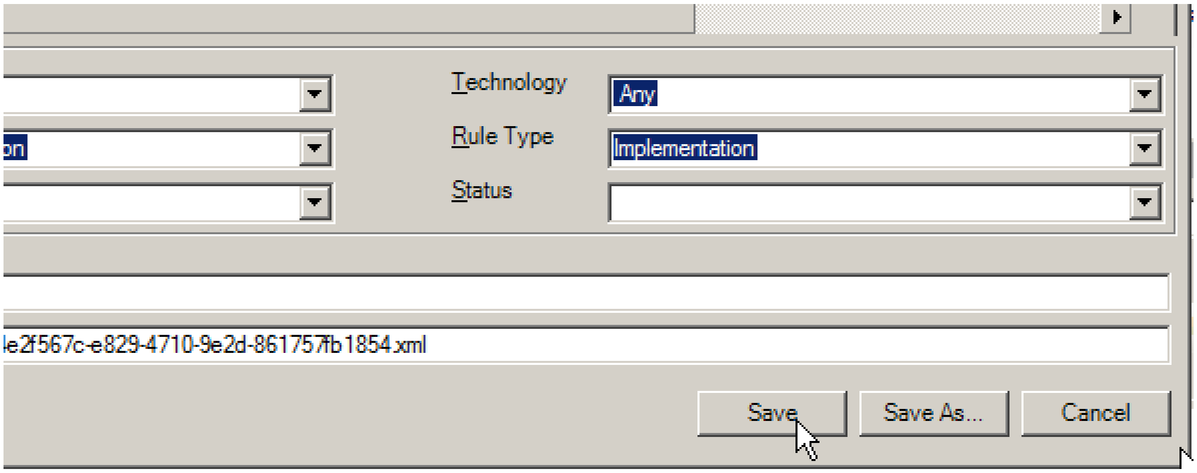
Author(s):

Applies To

Any application that interacts with a SQL database.

Description

Save it locally



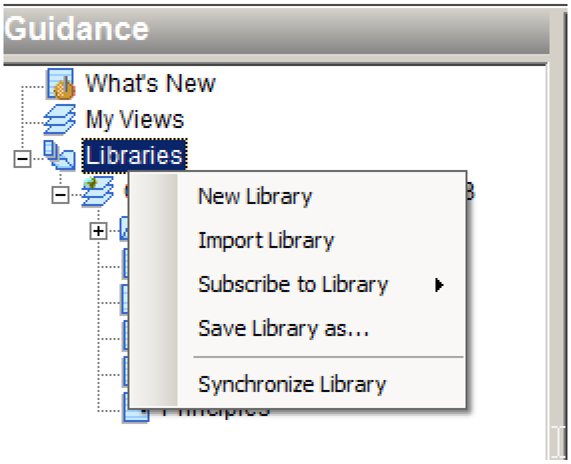
Technology: Any

Rule Type: Implementation

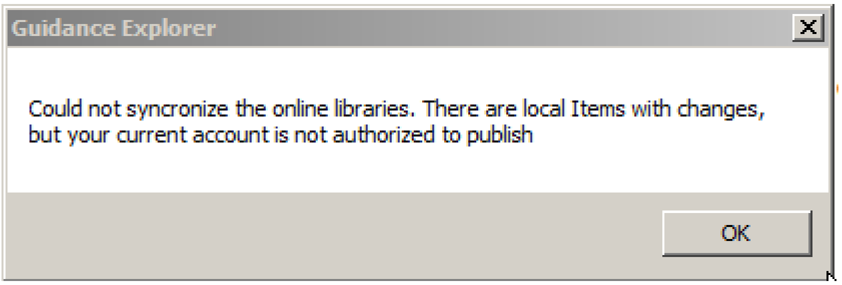
Status:

e2f567c-e829-4710-9e2d-861757fb1854.xml

Select ***'Synchronize Library'*** to Trigger an Library Synchorization process:

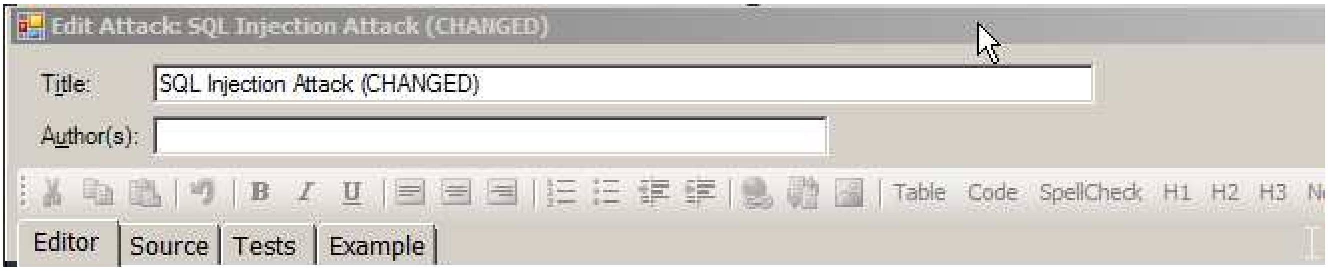


and note that because the current user doesn't have admin privileges, the synchronization is not going to work, and the following error message will be shown:



Could not syncronize the online libraries. There are local Items with changes, but your current account is not authorized to publish

To double-check, a view of the article locally changed,

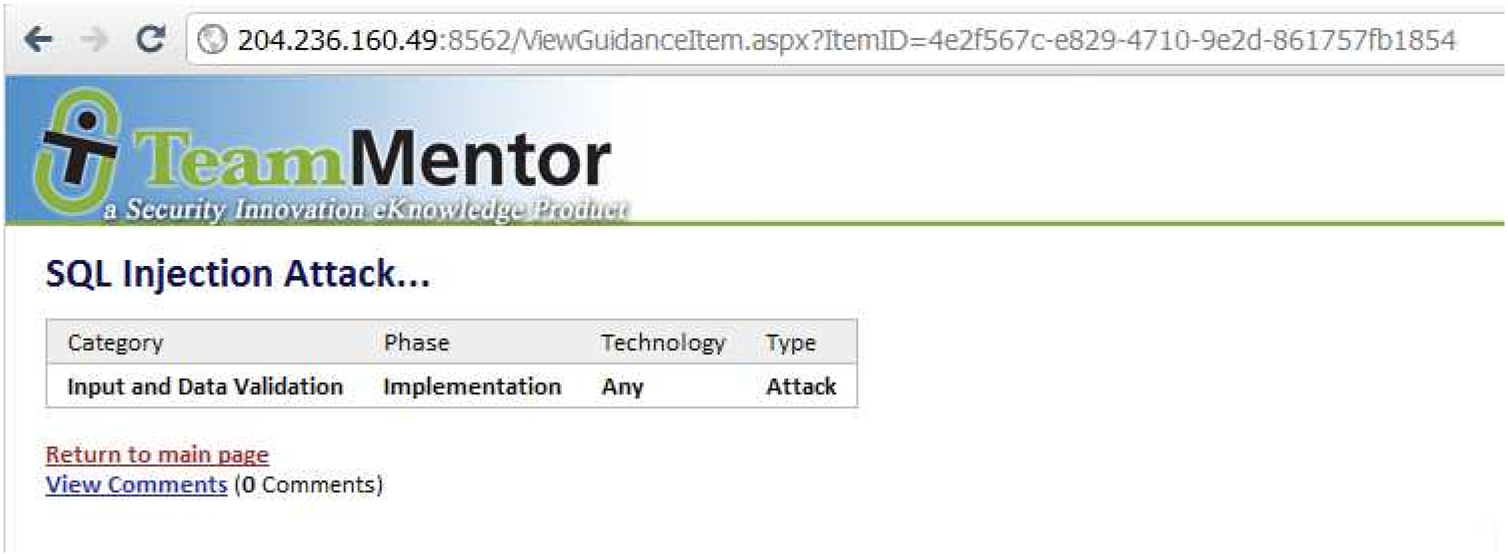


Edit Attack: SQL Injection Attack (CHANGED)

Title: SQL Injection Attack (CHANGED)

Author(s):

shows is still in its original format online



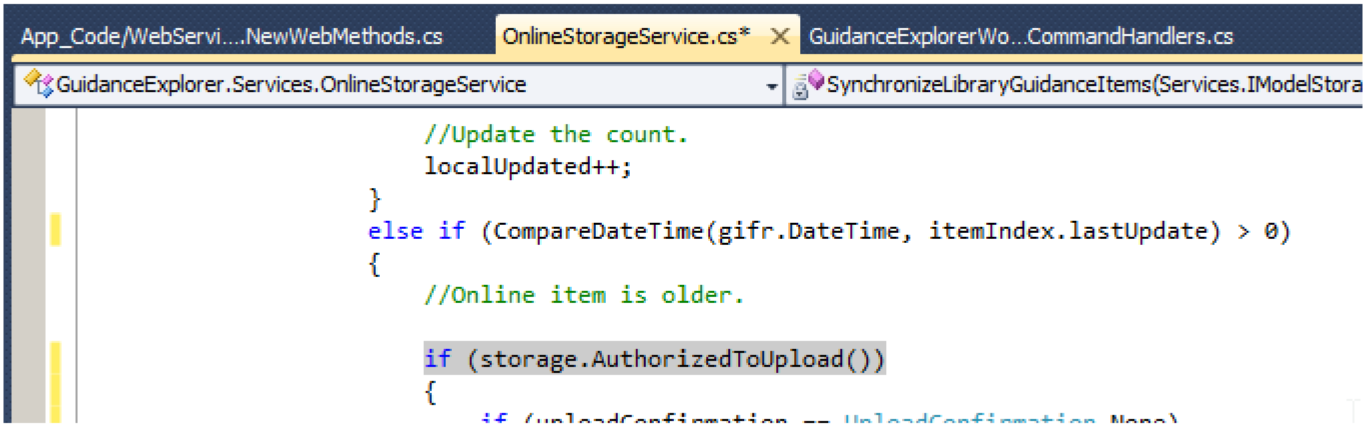
204.236.160.49:8562/ViewGuidanceItem.aspx?ItemID=4e2f567c-e829-4710-9e2d-861757fb1854

SQL Injection Attack...

Category	Phase	Technology	Type
Input and Data Validation	Implementation	Any	Attack

Return to main page
View Comments (0 Comments)

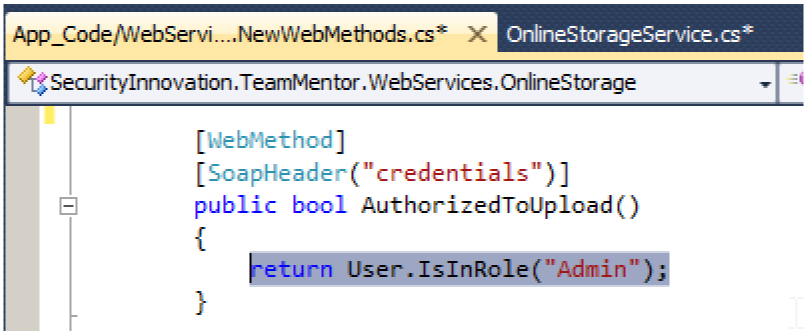
For reference, the security check on the client app was done here:


App_Code/WebServi....NewWebMethods.cs
OnlineStorageService.cs*
GuidanceExplorerWo...CommandHandlers.cs
GuidanceExplorer.Services.OnlineStorageService
SynchronizeLibraryGuidanceItems(Services.IModelStora

```
                    //Update the count.
                    localUpdated++;
                }
                else if (CompareDateTime(gifr.DateTime, itemIndex.lastUpdate) > 0)
                {
                    //Online item is older.

                    if (storage.AuthorizedToUpload())
                    {
                        if (uploadConfirmation == UploadConfirmation.None)
```

that calls the AuthorizedToUpload WebMethod which performs a RBAC check on the current logged in user:

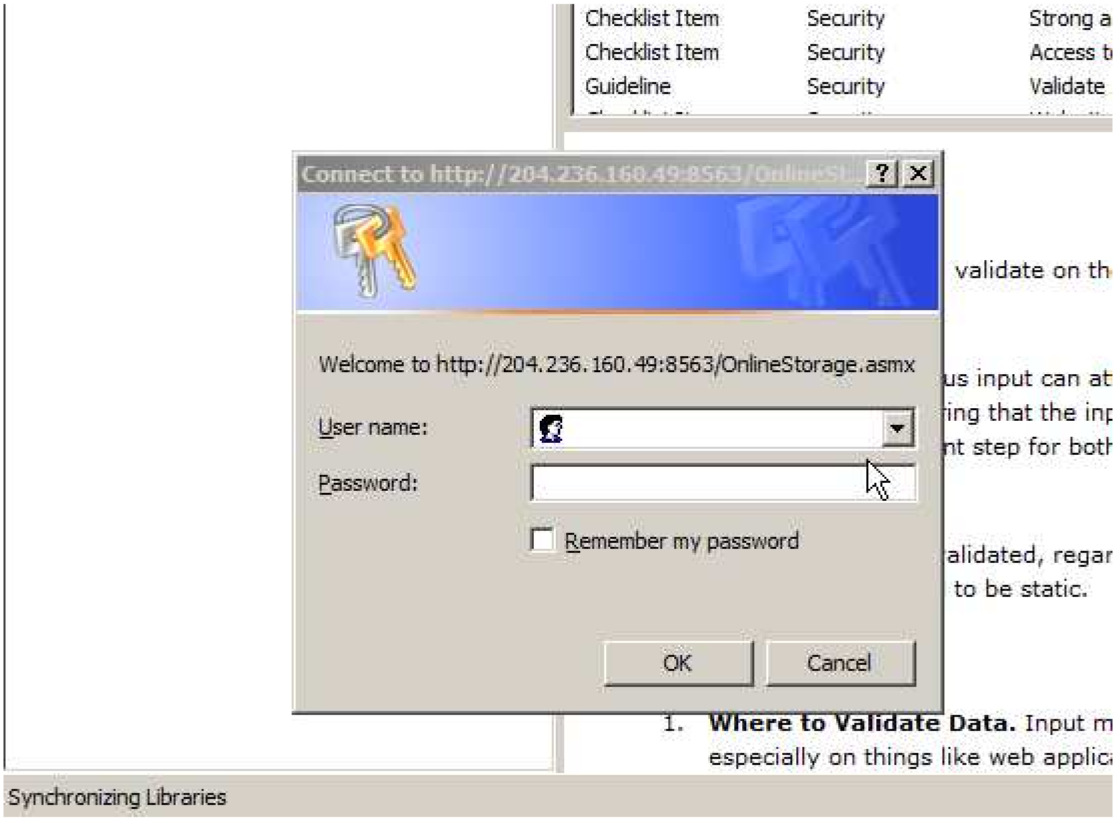

App_Code/WebServi....NewWebMethods.cs*
OnlineStorageService.cs*
SecurityInnovation.TeamMentor.WebServices.OnlineStorage

```
        [WebMethod]
        [SoapHeader("credentials")]
        public bool AuthorizedToUpload()
        {
            return User.IsInRole("Admin");
        }
```

Publish a local change to the server (as 'Admin' user)

Next step is to try the publish process when done by an account with admin privileges.

Restart TeamMentorAuthor application, and since there is an sychronization process trigerred on launch, if you haven't saved the previous credentials, you will be prompted for a username and password:



Checklist Item	Security	Strong a
Checklist Item	Security	Access t
Guideline	Security	Validate

Connect to http://204.236.160.49:8563/OnlineSt...

Welcome to http://204.236.160.49:8563/OnlineStorage.asmx

User name:

Password:

☐ Remember my password

validate on th

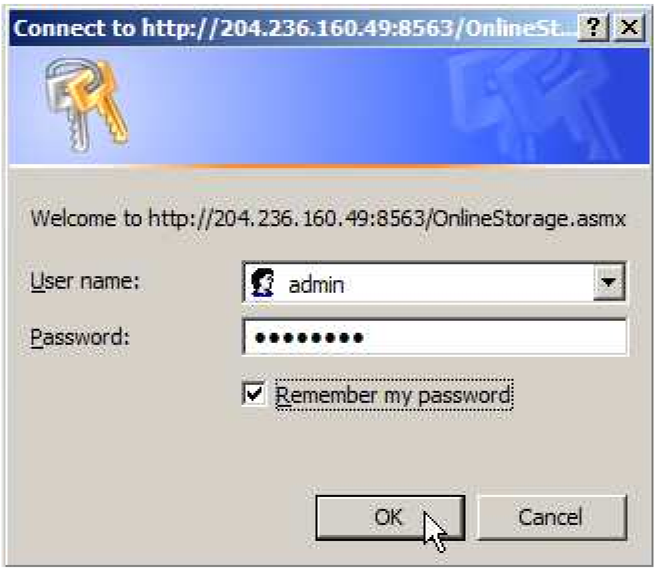
us input can at
ing that the inp
nt step for both

alidated, regar
to be static.

1. **Where to Validate Data.** Input m
especially on things like web applic

Synchronizing Libraries

For this test to work, enter an account with admin privileges



Connect to http://204.236.160.49:8563/OnlineSt...

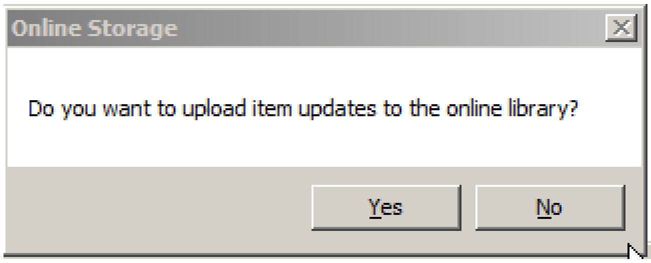
Welcome to http://204.236.160.49:8563/OnlineStorage.asmx

User name: admin

Password: ••••••••

☑ Remember my password

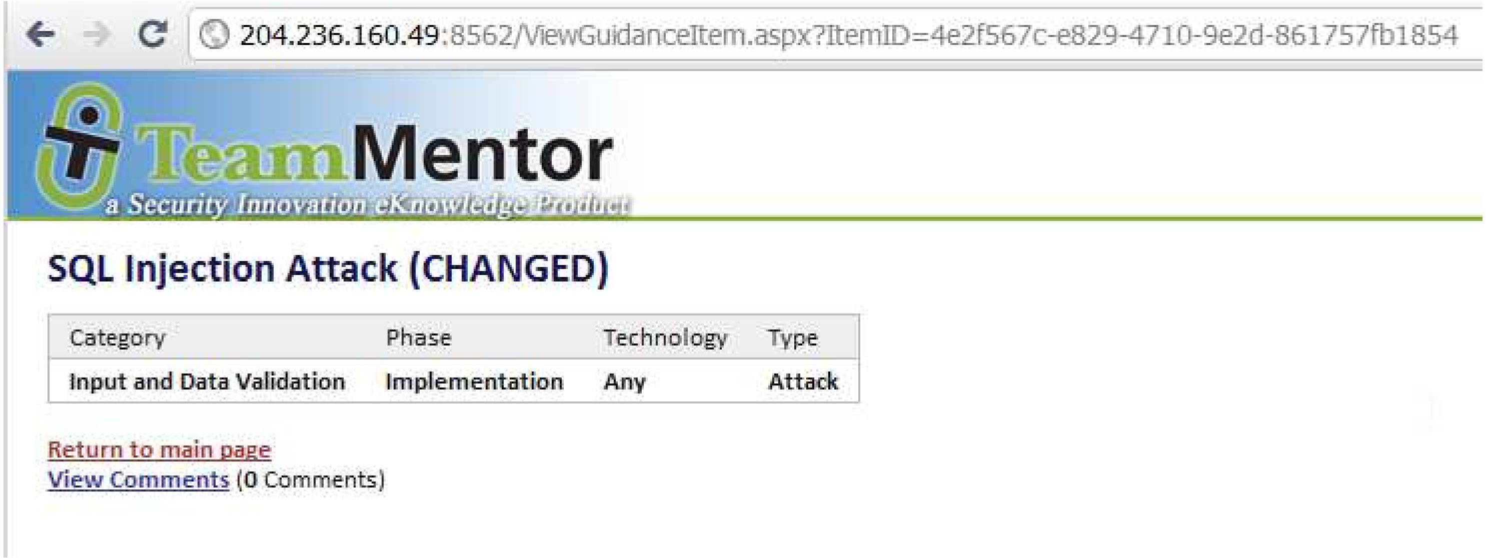
and because we have priviledges, we will be prompted if we want to upload the online storage



Online Storage

Do you want to upload item updates to the online library?

and once the synchronization completes one can see the new change reflected on the website:


204.236.160.49:8562/ViewGuidanceItem.aspx?ItemID=4e2f567c-e829-4710-9e2d-861757fb1854

TeamMentor
a Security Innovation eKnowledge Product

SQL Injection Attack (CHANGED)

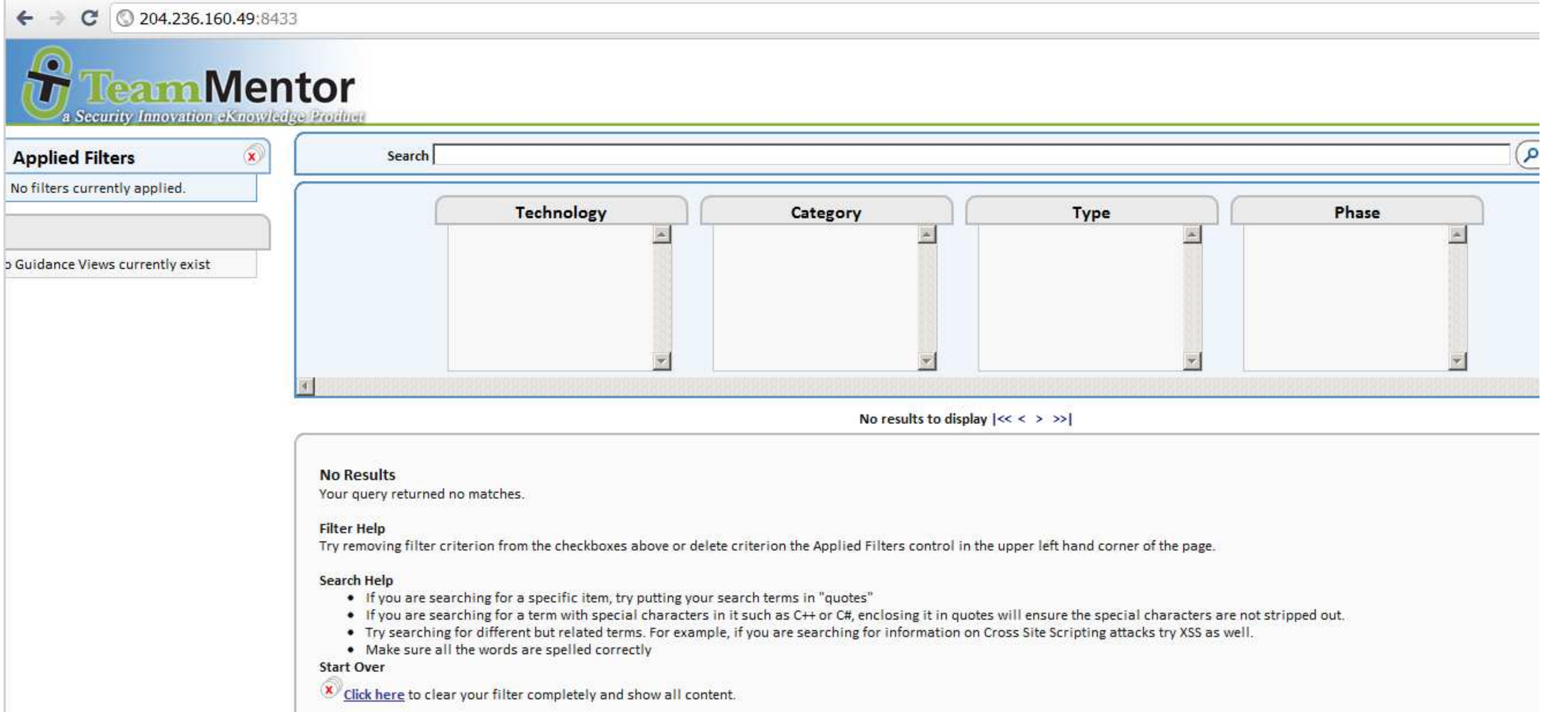
Category	Phase	Technology	Type
Input and Data Validation	Implementation	Any	Attack

Creating and populating new Libraries (as 'Admin' user)

It is also possible to create libraries , on remote servers.

This is quite interresting on the case of an TeamMentor online database which is delivered to a customer (or tool) in an empty state.

Lets use for example the http://204.236.160.49:8433 server which has an empty database:


204.236.160.49:8433

TeamMentor
a Security Innovation eKnowledge Product

Applied Filters
No filters currently applied.
o Guidance Views currently exist
Search
Technology
Category
Type
Phase
No results to display |<< < > >>|

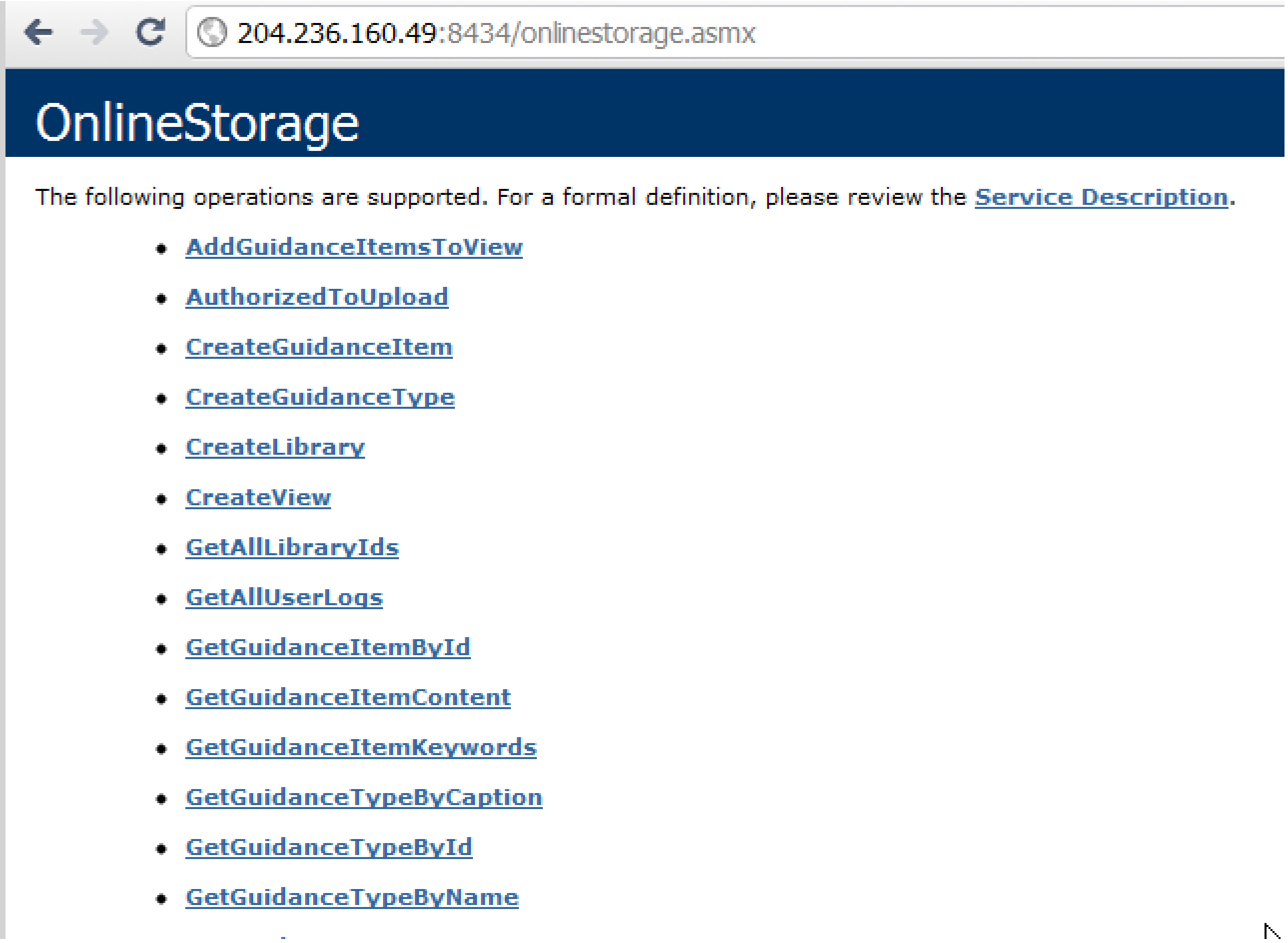
No Results
Your query returned no matches.

Filter Help
Try removing filter criterion from the checkboxes above or delete criterion the Applied Filters control in the upper left hand corner of the page.

Search Help
- If you are searching for a specific item, try putting your search terms in "quotes"
- If you are searching for a term with special characters in it such as C++ or C#, enclosing it in quotes will ensure the special characters are not stripped out.
- Try searching for different but related terms. For example, if you are searching for information on Cross Site Scripting attacks try XSS as well.
- Make sure all the words are spelled correctly

Start Over
Click here to clear your filter completely and show all content.

this website is supported by the OnlineStorage.asmx webservice located at http://204.236.160.49:8434/onlinestorage.asmx



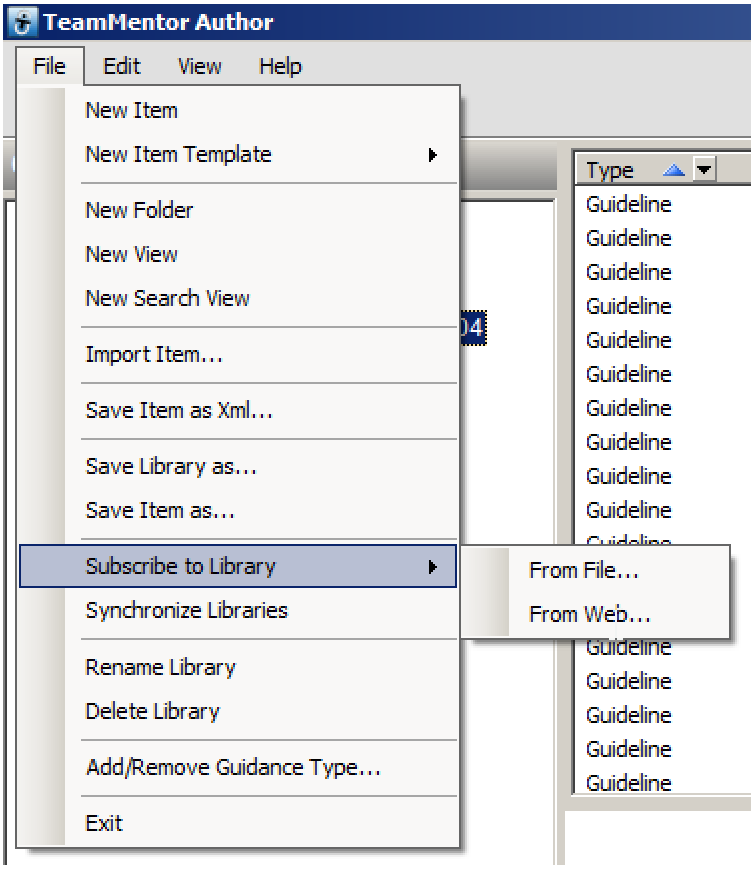
204.236.160.49:8434/onlinestorage.asmx

OnlineStorage

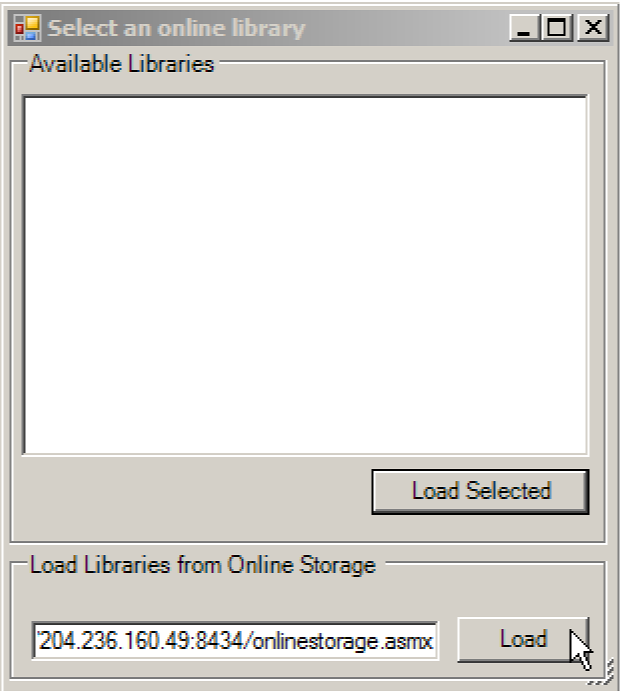
The following operations are supported. For a formal definition, please review the Service Description.

- AddGuidanceItemsToView
- AuthorizedToUpload
- CreateGuidanceItem
- CreateGuidanceType
- CreateLibrary
- CreateView
- GetAllLibraryIds
- GetAllUserLogs
- GetGuidanceItemById
- GetGuidanceItemContent
- GetGuidanceItemKeywords
- GetGuidanceTypeByCaption
- GetGuidanceTypeById
- GetGuidanceTypeByName

As before select the menu option to Syncronize a Library from the Web

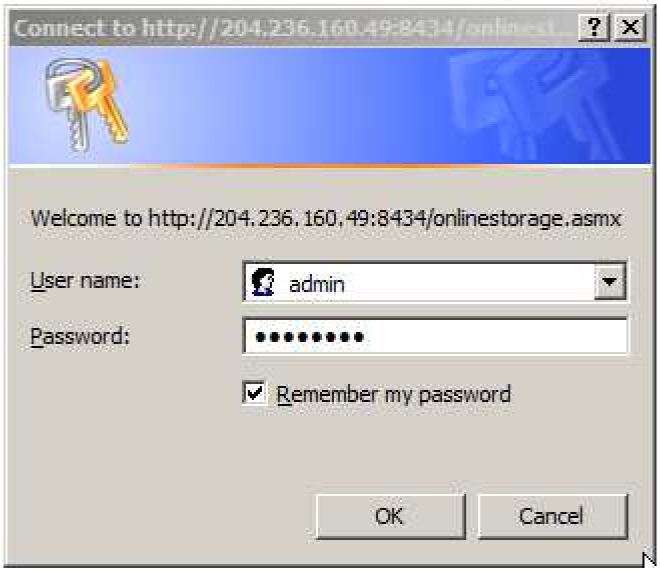


Enter the url http://204.236.160.49:8434/onlinestorage.asmx in the ***'Load Libraries from Online Storage'*** section



204.236.160.49:8434/onlinestorage.asmx

Login with an account with admin priviledges


Connect to http://204.236.160.49:8434/onlinest...

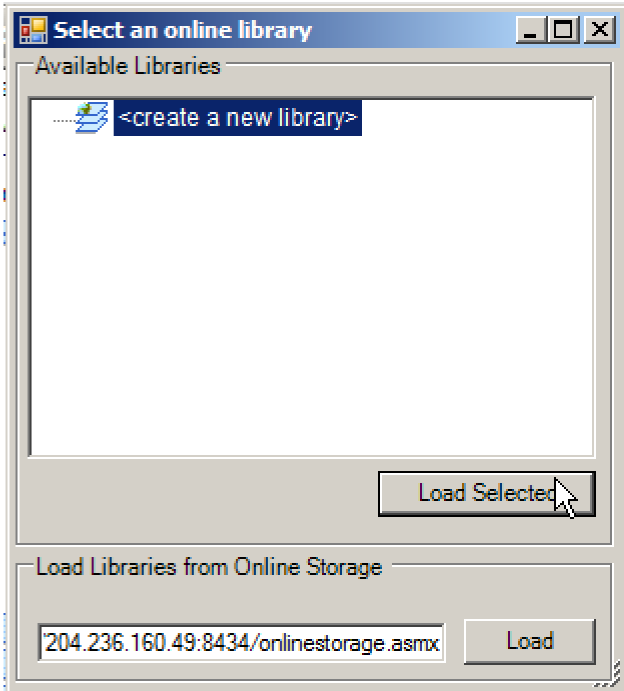
Welcome to http://204.236.160.49:8434/onlinestorage.asmx

User name: admin

Password: ●●●●●●●●●

☑ Remember my password

and select the ***<create a new library>*** option


Select an online library

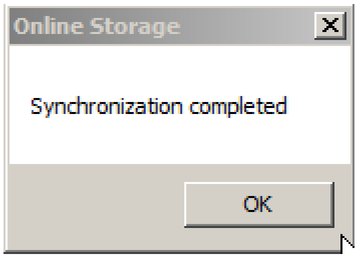
Available Libraries

<create a new library>

Load Libraries from Online Storage

204.236.160.49:8434/onlinestorage.asmx

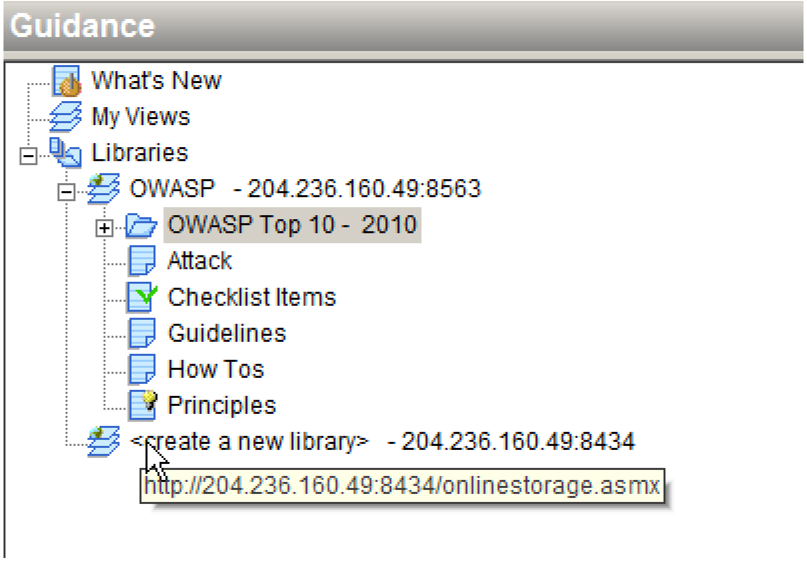
Once the Sync process completes:


Online Storage

Synchronization completed

The new Library will be on the Libraries list.

Note how there is a reference to the server:port that this library is in, and whem the mouse overs on top of the library node, the actually web address of the webservice is shown

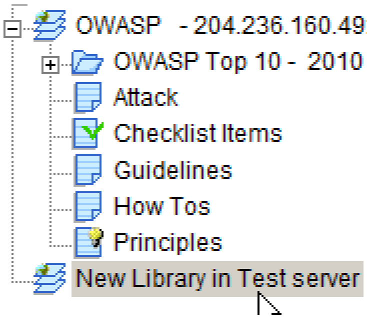


Guidance

- What's New
- My Views
- Libraries
  - OWASP - 204.236.160.49:8563
    - OWASP Top 10 - 2010
    - Attack
    - Checklist Items
    - Guidelines
    - How Tos
    - Principles
  - <create a new library> - 204.236.160.49:8434

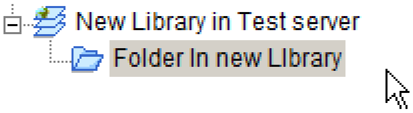
http://204.236.160.49:8434/onlinestorage.asmx

Now, rename the new Library



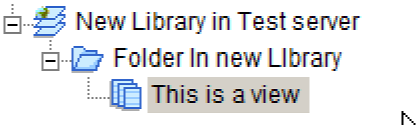
- OWASP - 204.236.160.49:8563
  - OWASP Top 10 - 2010
  - Attack
  - Checklist Items
  - Guidelines
  - How Tos
  - Principles
- New Library in Test server

... add a folder



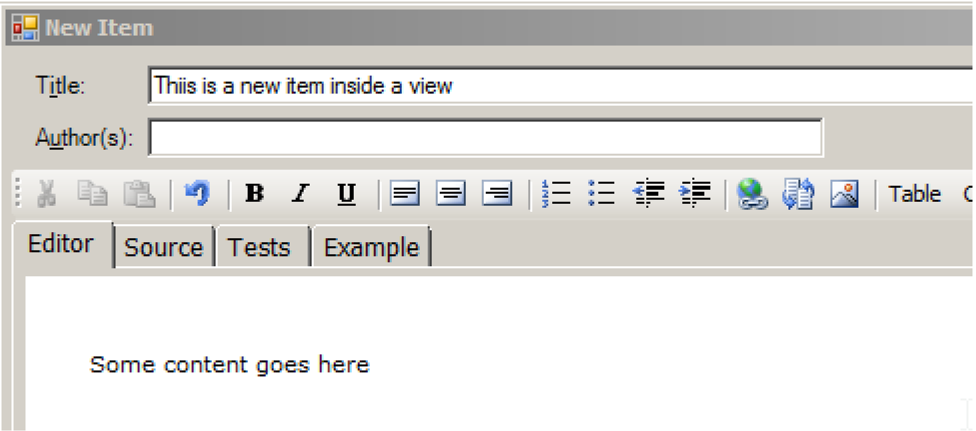
- New Library in Test server
  - Folder In new LIbrary

... add a view



- New Library in Test server
  - Folder In new LIbrary
    - This is a view

... create a couple new Items



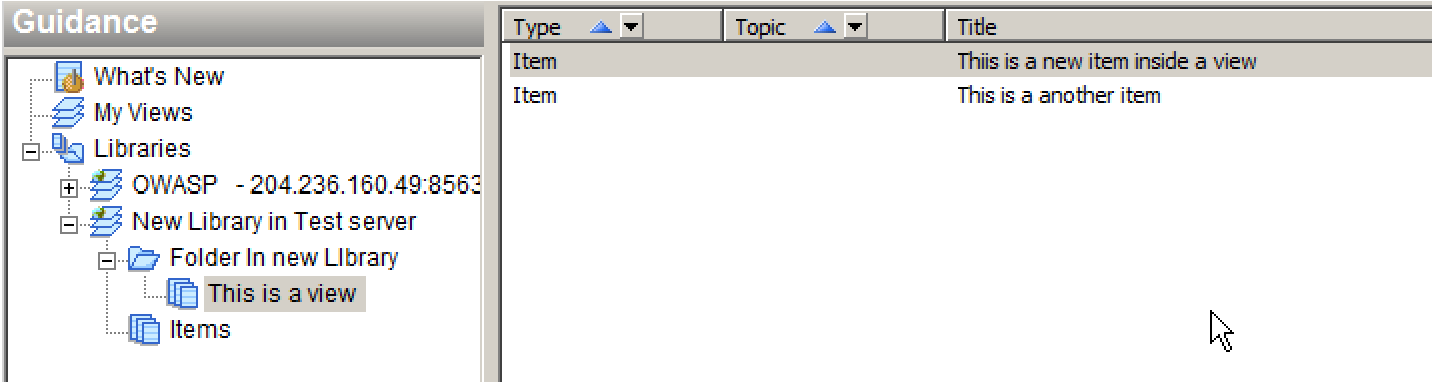
New Item

Title: Thiis is a new item inside a view

Author(s):

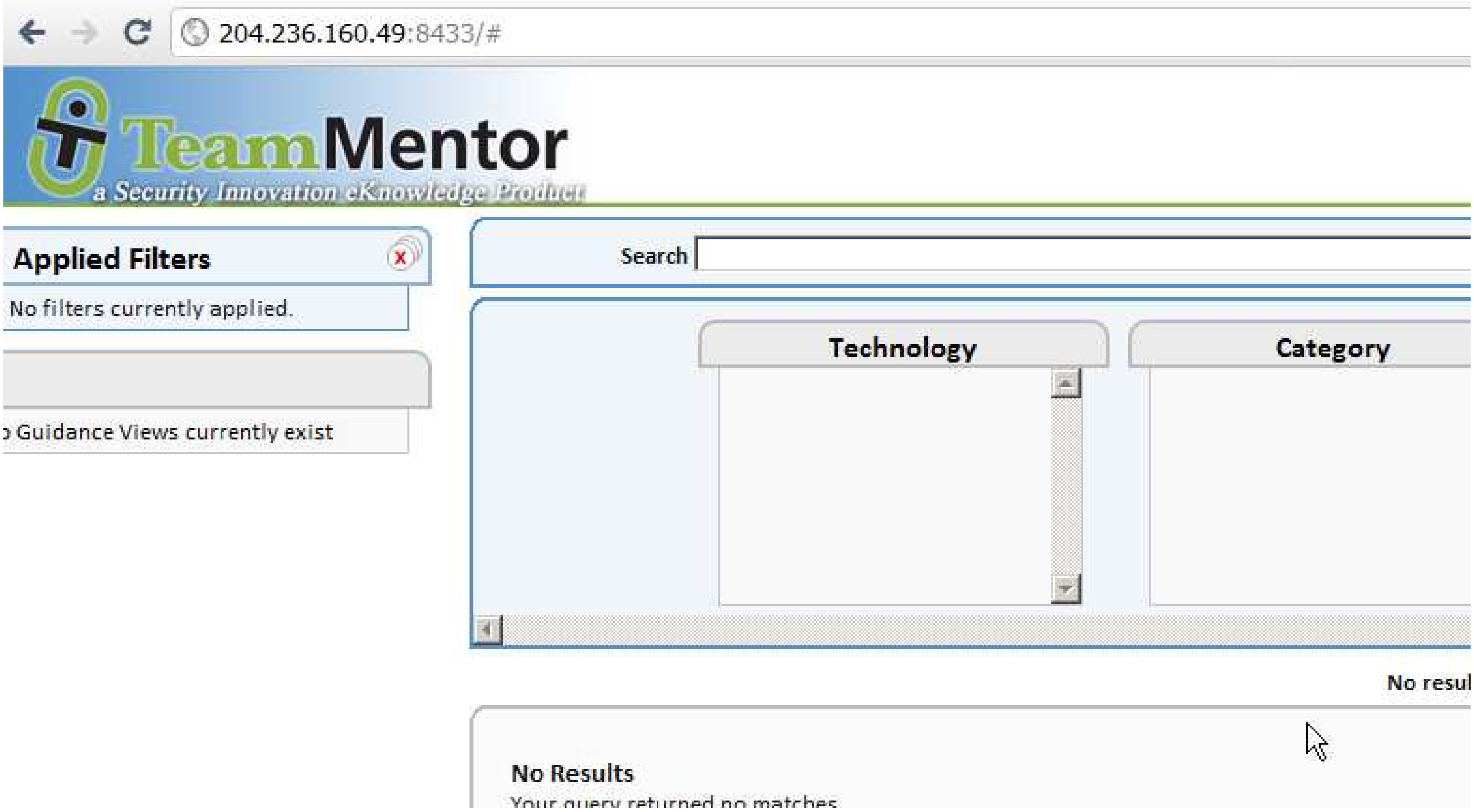
Some content goes here

... and at the moment ... locally ... the new library should look like this



Type	Topic	Title
Item		Thiis is a new item inside a view
Item		This is a another item

... and online (before sync) should look like this:



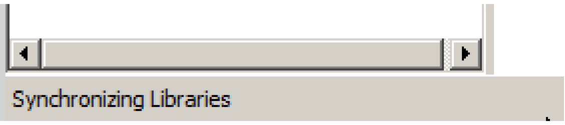
No filters currently applied.

› Guidance Views currently exist

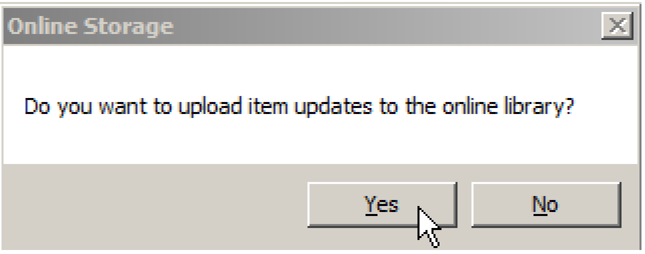
No Results

Your query returned no matches

The final step is to Sychronize this Library (available on the context and main menu)



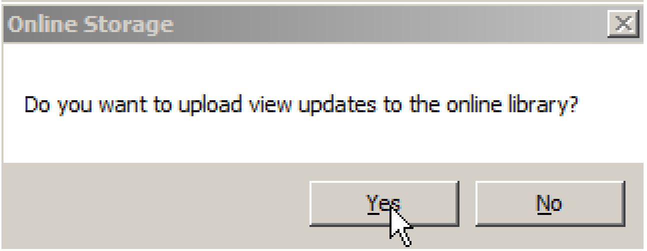
... which will ask to update the item updates



Online Storage

Do you want to upload item updates to the online library?

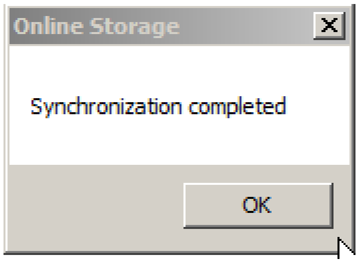
... and the view updates



Online Storage

Do you want to upload view updates to the online library?

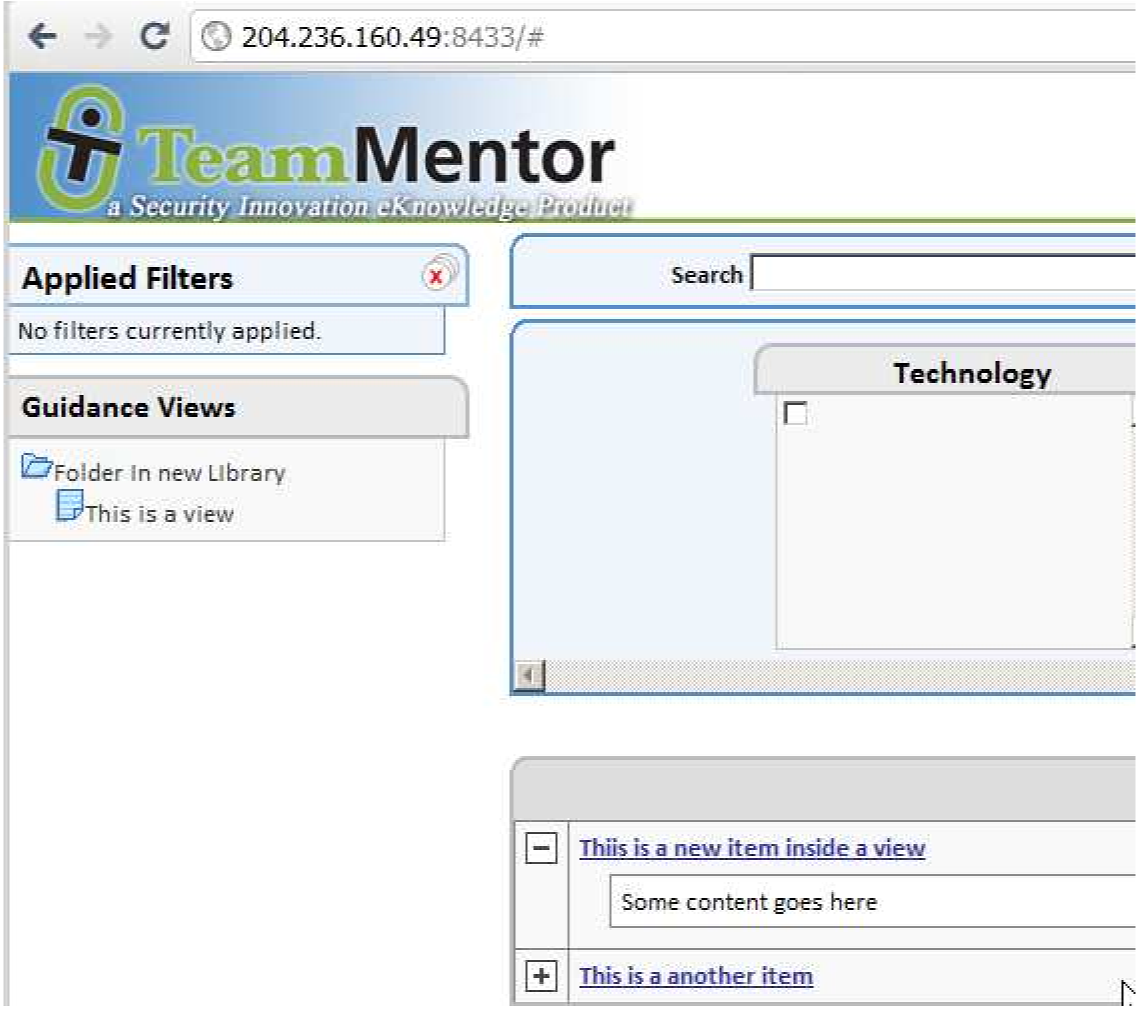
Once the synchronization completes:



Online Storage

Synchronization completed

..the newly created content and view will be online:



204.236.160.49:8433/#

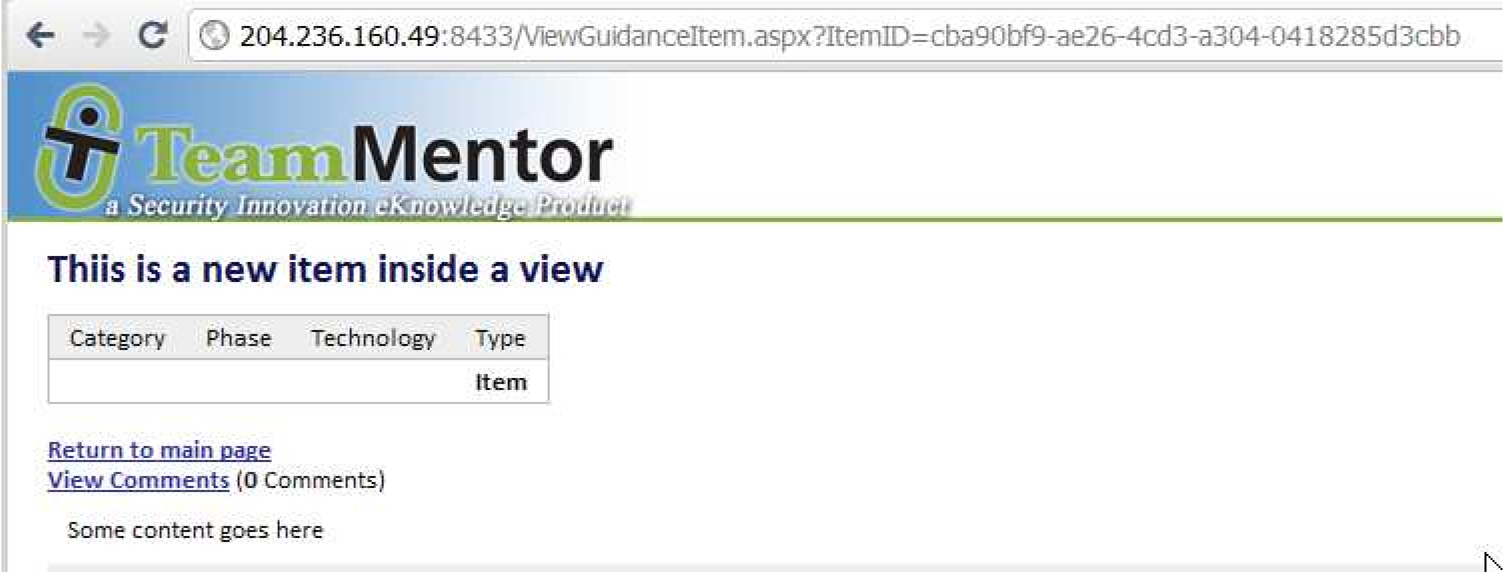
No filters currently applied.

Thiis is a new item inside a view

Some content goes here

This is a another item

logged in users, can see the article's content



204.236.160.49:8433/ViewGuidanceItem.aspx?ItemID=cba90bf9-ae26-4cd3-a304-0418285d3cbb

Thiis is a new item inside a view

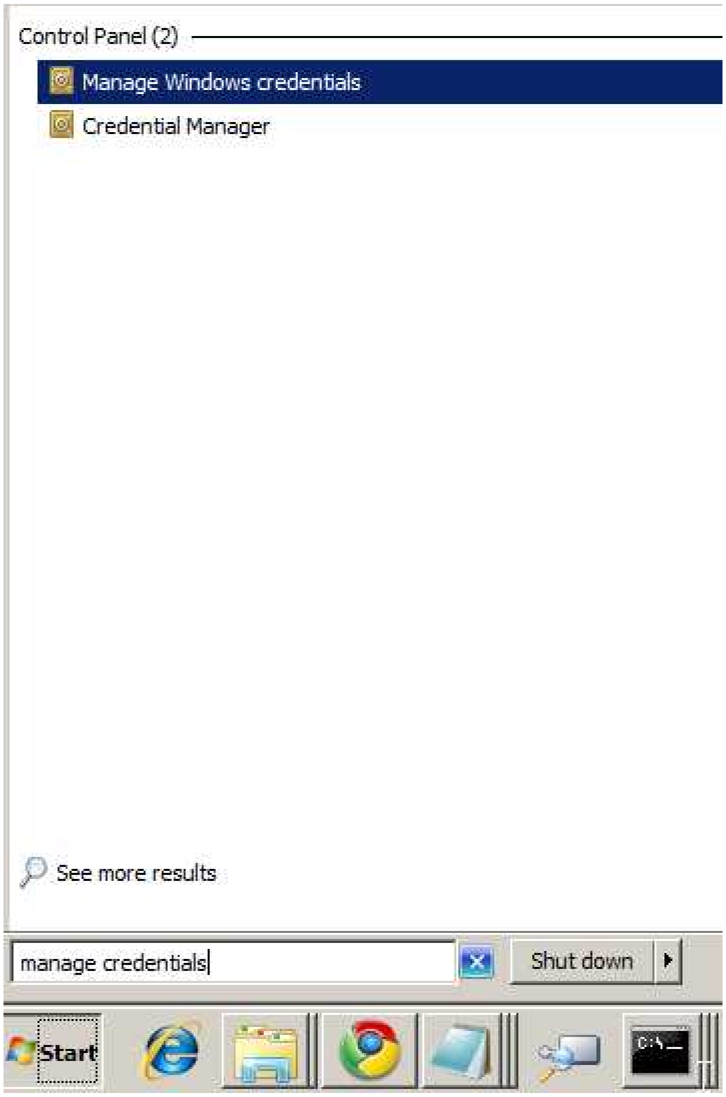
Category	Phase	Technology	Type
			Item

(0 Comments)

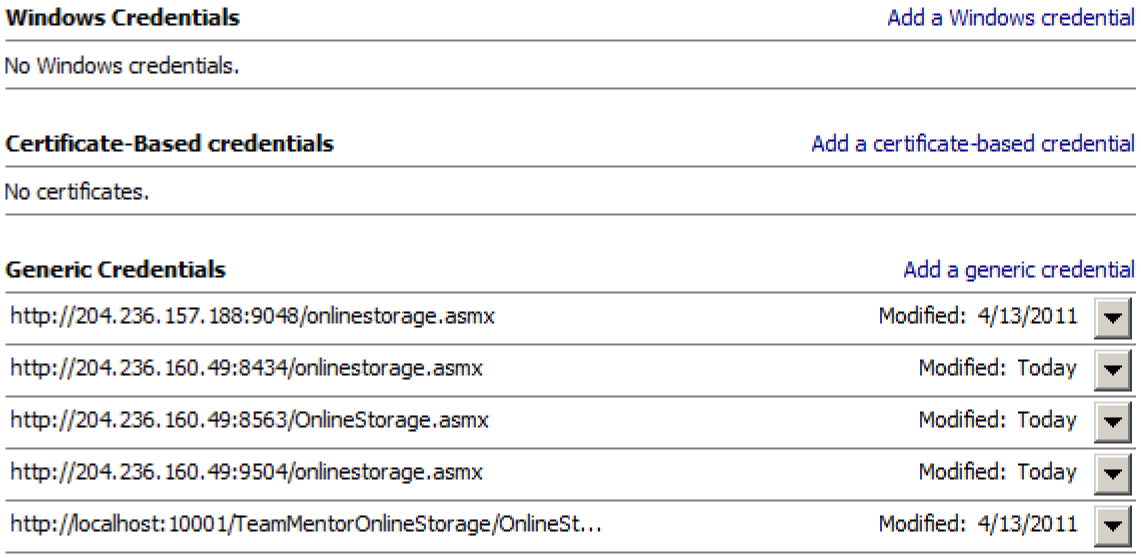
Some content goes here

Local Credential management process

When prompted for credentials, if you chose to save them locally, the username and password entred will be securely stored on the Windows Credentials Manager which can be accessed like this



with the accounts mapped to the actual WebService's URL that was used :



Windows Credentials Add a Windows credential

No Windows credentials.

Certificate-Based credentials Add a certificate-based credential

No certificates.

Generic Credentials Add a generic credential

http://204.236.157.188:9048/onlinestorage.asmx Modified: 4/13/2011 ▼

http://204.236.160.49:8434/onlinestorage.asmx Modified: Today ▼

http://204.236.160.49:8563/OnlineStorage.asmx Modified: Today ▼

http://204.236.160.49:9504/onlinestorage.asmx Modified: Today ▼

http://localhost:10001/TeamMentorOnlineStorage/OnlineSt... Modified: 4/13/2011 ▼