

SharePoint Security

Advanced SharePoint Security Tips and Tools

05 Oct 2010



Presented by:
Francis Brown
Stach & Liu, LLC
www.stachliu.com

Agenda

OVERVIEW

- Brief Intro to SharePoint
 - Overview of Major Components
- SharePoint Security
 - Security Tips and Tools

Background

GETTING UP TO SPEED

Background

MS SharePoint Products & Technologies



- Windows SharePoint Services (WSS)
- Office SharePoint Server 2007/2010 (MOSS)
- SharePoint Designer 2007/2010 (SPD)



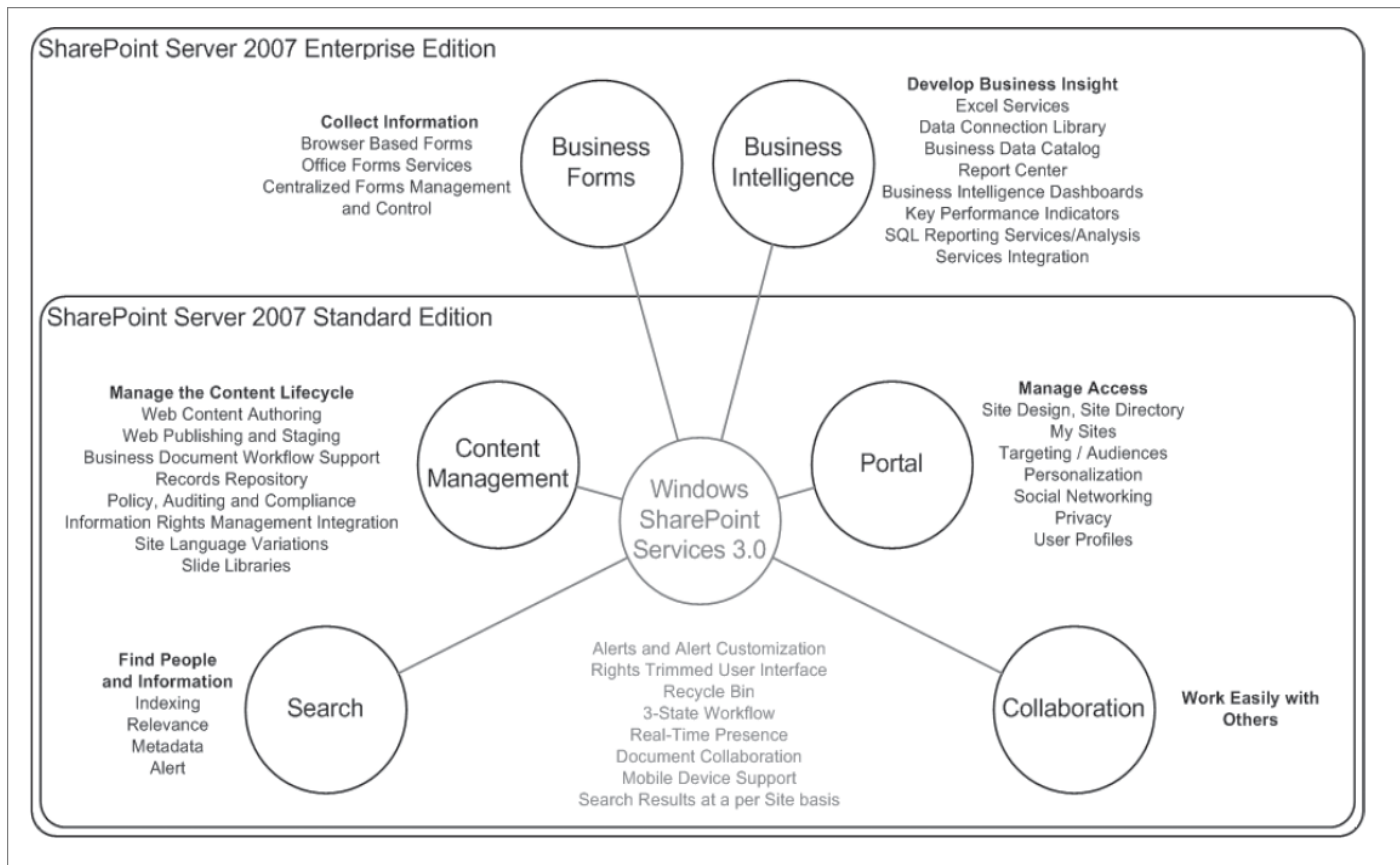
Background

MS SharePoint Products & Technologies



Background

MS SharePoint Products & Technologies



Background

MS SharePoint Products & Technologies

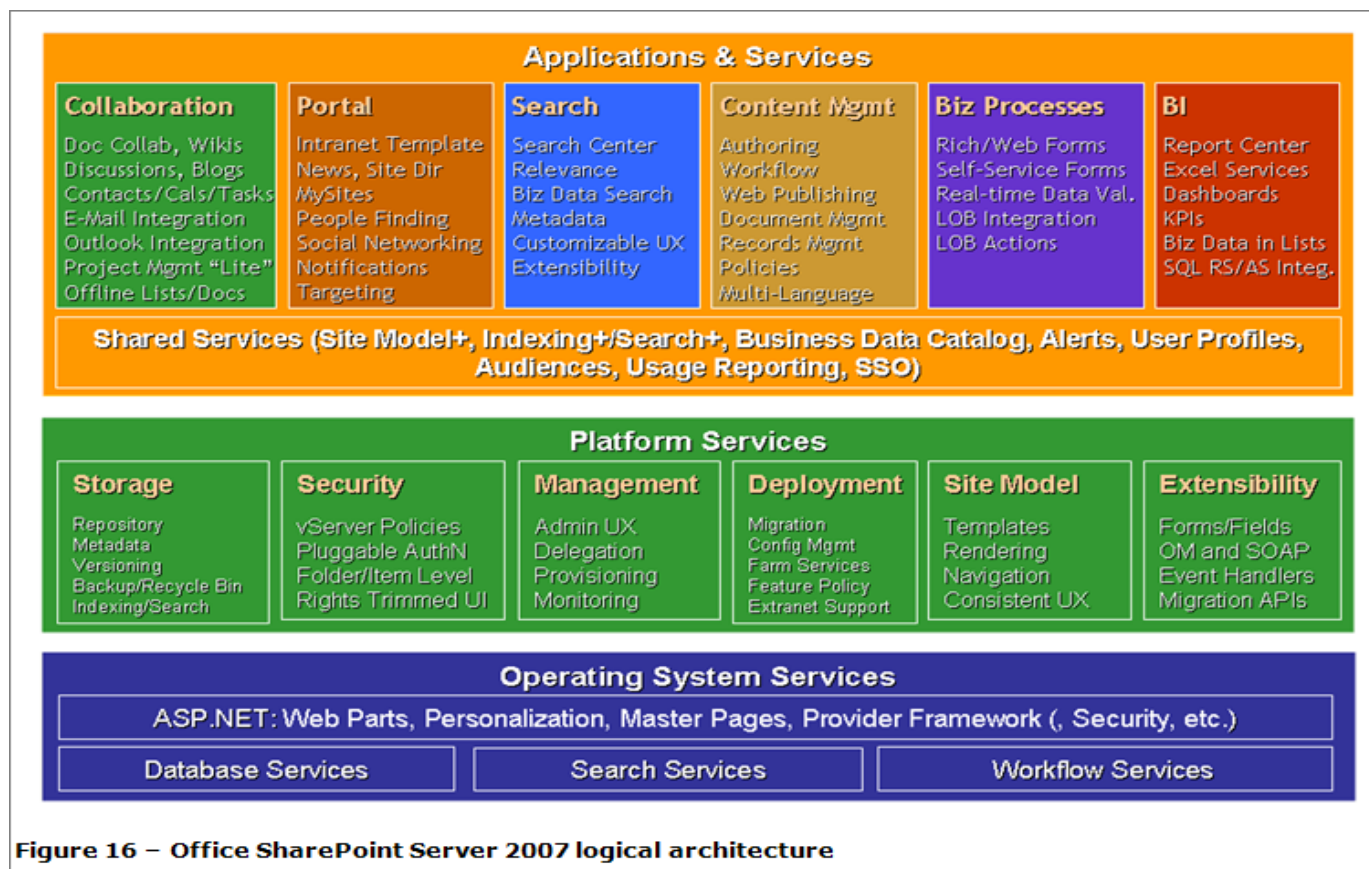


Figure 16 – Office SharePoint Server 2007 logical architecture

Background

MS SharePoint Products & Technologies



Site Hierarchy

Intro to SharePoint

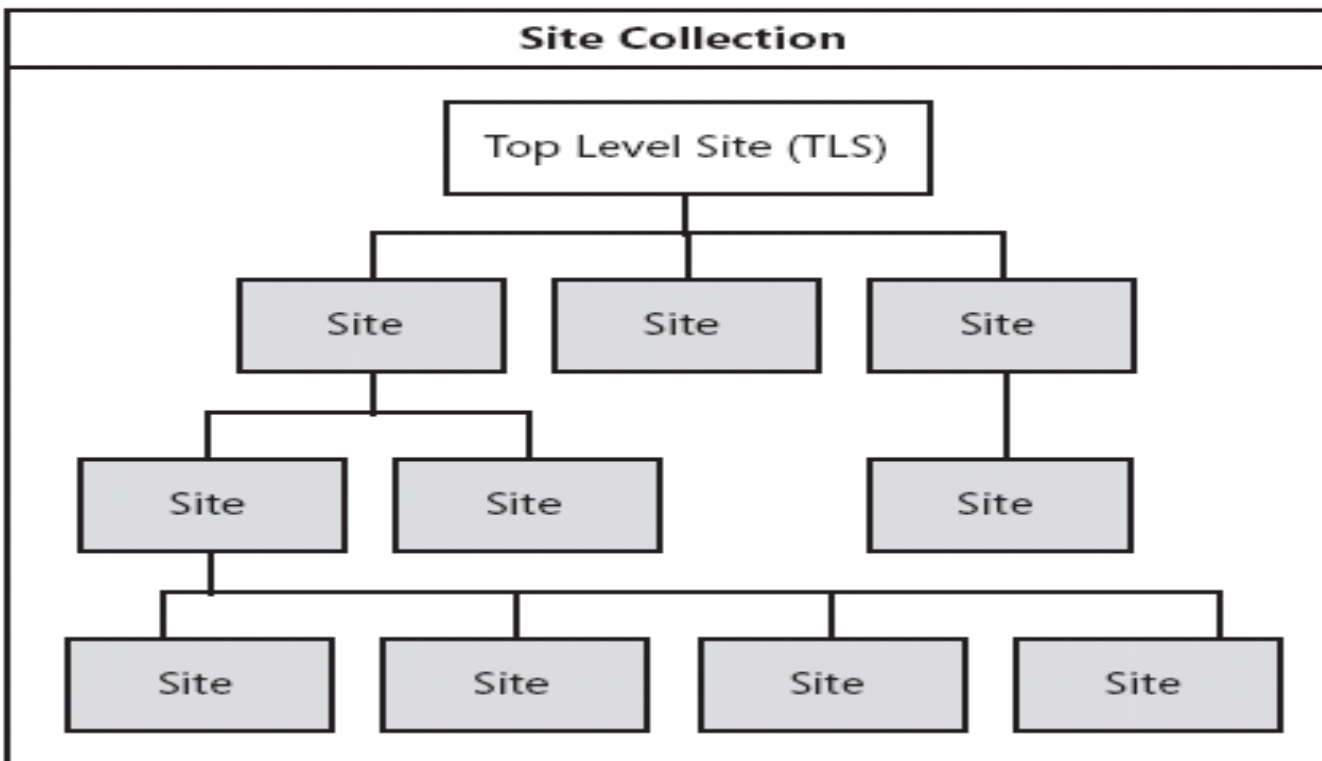


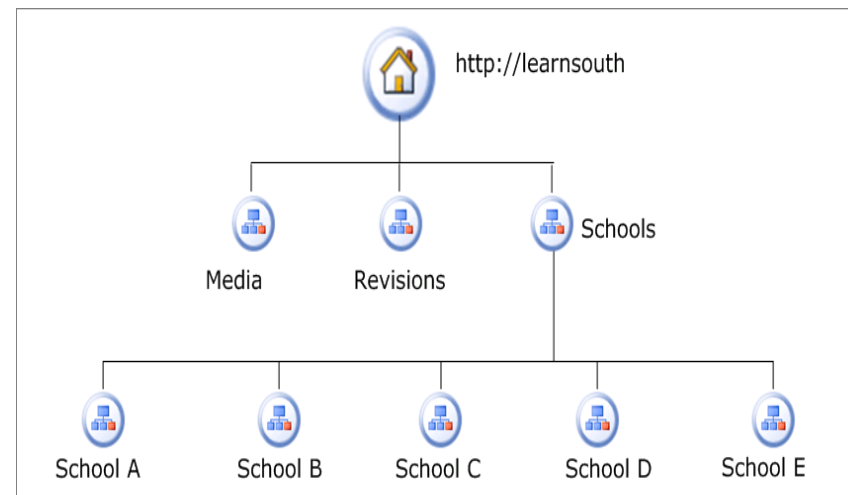
Figure 1-6 Site collections are a structured collection of sites.

SharePoint Site Hierarchy

Intro to SharePoint

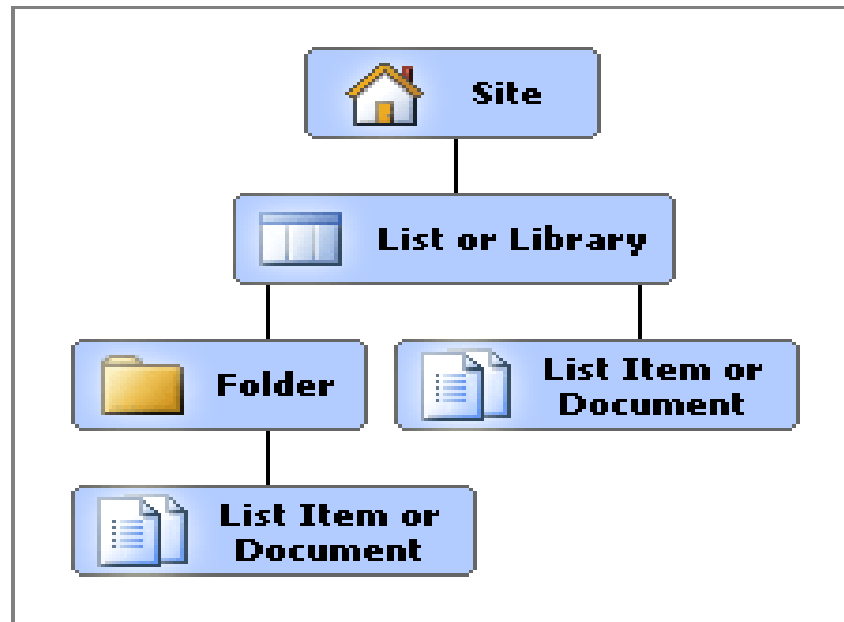
Base Site URLs:

- <http://learnsouth/>
- <http://learnsouth/Media/>
- <http://learnsouth/Revisions/>
- <http://learnsouth/Schools/>
- <http://learnsouth/Schools/SchoolA/>
- <http://learnsouth/Schools/SchoolB/>
- <http://learnsouth/Schools/SchoolC/>



Site Structure

Intro to SharePoint



Site Navigation

Intro to SharePoint

The screenshot shows a SharePoint site titled "STACH&LIU Home". The interface includes a top navigation bar with "Home", "Management", "Clients", "Resources", and "Site Index". A breadcrumb trail shows "Home > All Site Content". The main content area displays "All Site Content" with a list of libraries and lists. A left-hand navigation pane shows "Management", "Clients", "Resources", "Site Directory", and "Site Hierarchy". A right-hand sidebar contains "Site Actions", "Create Page", "Create Site", "View All Site Content", "View Reports", "Site Settings", and "Manage Content and Structure".

Red callout boxes highlight the following elements:

- Home
- Global Navigational Breadcrumb
- Top Link Bar
- Personalization - My Site
- Site Actions
- Content Navigational Breadcrumb
- View All Site Content
- Management
- Accounting
- Client Relationship Mgmt (CRM)
- Exec Dash
- Clients
- Resources
- Site Directory
- Site Hierarchy
- Quick Launch Bar
- All Site Content
- Site Actions
- Site Settings
- Manage Content and Structure
- Tree View

Name	Description	Created	Modified
Document Libraries			
Documents	This library was created by the Publishing feature to store documents that are used on pages in this site.	0	4 months ago
Form Templates	This library contains administrative forms that were activated to this site collection.	0	4 months ago
Images	This system library was created by the Publishing feature to store images that are used on pages in this site.	0	4 months ago
Pages	This system library was created by the Publishing feature to store pages that are created in this site collection.	0	4 months ago
Site Collection Documents	This system library was created by the Publishing feature to store documents that are used throughout the site collection.	0	4 months ago
Site Collection Images	This system library was created by the Publishing Resources feature to store images that are used throughout the site collection.	0	4 months ago
Style Library	This system list was created by the Publishing feature to store custom XSL styles and stylesheets used in this site.	63	4 months ago
Picture Libraries			
There are no picture libraries. To create one, click Create above.			
Lists			
Contacts	Create a contacts list when you want to manage information about people that your team works with such as customers or partners. You can share information between your contacts list and Windows SharePoint Services-compatible contacts programs.	0	4 months ago
Content and Structure Reports	Use the reports list to customize the queries that appear in the Content and Structure Tool views	7	4 months ago
Events	Use the Events list to post information about meetings, deadlines, and other events related to this area.	1	4 months ago
Links	Create a links list when you have links to Web pages or other resources that you want to share.	0	4 months ago

Security Tips

WHAT YOU SHOULD KNOW

Security Tips

SHAREPOINTSECURITY

#	Security Tip
1	Know your external exposure...
2	Beware of normal users with excessive access...
3	Spot check user permissions and inheritance...
4	Beware third-party plugins/code...BUT not too much...
5	Backup every which way from Sunday...
	...

Security Tip #1

KNOW YOUR EXTERNAL EXPOSURE

External Exposure

FINDING HOLES

1. "Google Hack yourself"
 1. Search Google for exposed SharePoint admin pages
 2. E.g. `inurl:"/_catalogs/wt/"`
 3. **NEW**: SharePoint Google Regexs for S&L SearchDiggity – 109 queries
2. SharePoint URL Brute-forcing
 1. Forceful browse to common SharePoint extensions to test access
 2. **NEW**: Tool to bruteforce SharePoint URLs – 89 known extensions
3. Nmap for other SharePoint administrative apps
 1. E.g. Central Administration, Shared Service Providers (SSP)

External Exposure

GOOGLE HACKING SHAREPOINT

The screenshot shows a Google search interface with the query 'inurl:/_catalogs/wt/'. The search results list several pages, including 'www.orelltourstravel.com', 'Index of /_catalogs/wt/Forms', 'Upload.aspx - Hostmonster.com', 'SPChart configurator', 'Site Template Gallery', and 'ISACA.org'. A red callout box points to the ISACA.org result, stating: 'ISACA.org exposes SharePoint "Site Template Gallery" via Google.' The ISACA.org result is also circled in red.

inurl:/_catalogs/wt/" - Goo... x

www.google.com/m/search?q=inurl:/_catalogs/wt/"

inurl:/_catalogs/wt/"

[www.orelltourstravel.com - /_catalogs/wt/Forms/](#)
www.orelltourstravel.com - /_catalogs/wt/Forms/. [To Parent Directory] 4/30/2007 1:17 PM 6994 AllItems.aspx ...
www.orelltourstravel.com/_cata... - Options ▾

[Index of /_catalogs/wt/Forms](#)
Index of /_catalogs/wt/Forms. Parent Directory · AllItems.aspx · Common.aspx · DispForm.aspx · EditForm.aspx · Upload.aspx ...
fptest.manzanaresfamily.net/_ca... - Options ▾

[Upload.aspx - Hostmonster.com | Welcome](#)
_licid="1033" _version="11.0.5510" _da="1" --> <!-- _LocalBinding --> <%@ F...rePoint. ...
fptest.manzanaresfamily.net/_ca... - Options ▾
[More from manzanaresfamily.net >](#)

[SPChart configurator](#)
usmc-sharepoint.securespsites.c... - Options ▾

[Site Template Gallery](#)
Edit in Browser, /_layouts/images/icxddoc.gif, /_layouts/formserver.aspx? XsnLocation={ite...Orl}&OpenIn=Browser, 0x0, 0x1, FileType ...
www.afei.org/./Common.aspx - Options ▾

[Site Template Gallery](#)
HelpSite, M2M Help Site, 10/19/2009 11:31 AM, English. ISACA_Chapter, ISACA Chapter Site, 3/19/2010 3:50 PM, English ...
www.isaca.org/./Common.aspx - Options ▾

[Site Template Gallery](#)
Make a template available for use in Web site creation by adding it to this gallery. The templates in this gallery are available to ...
www.brickschools.org/staff/nobr... - Options ▾

ISACA.org exposes SharePoint "Site Template Gallery" via Google.

SHAREPOINT HACKING TOOLS

DEMO

Security Tip #2

BEWARE USERS WITH EXCESSIVE ACCESS

CONTINUED SHAREPOINT HACKING
DEMO

Excessive User Access

MORE THAN YOU BARGAINED FOR...

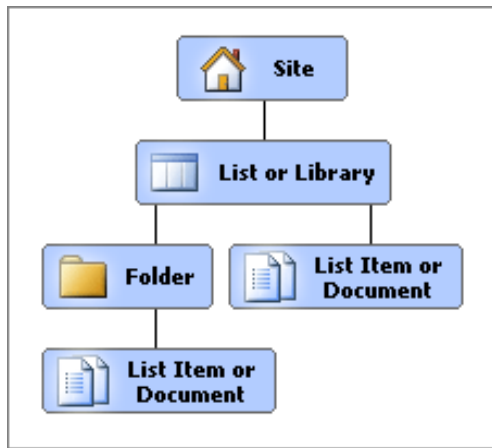
- Web Services examples
 - Admin.aspx
 - Permissions.aspx
- User Administration examples
 - "People and Groups"
 - "Add Users"
 - "PeoplePicker"

Security Tip #3

CHECK PERMISSIONS AND INHERITANCE

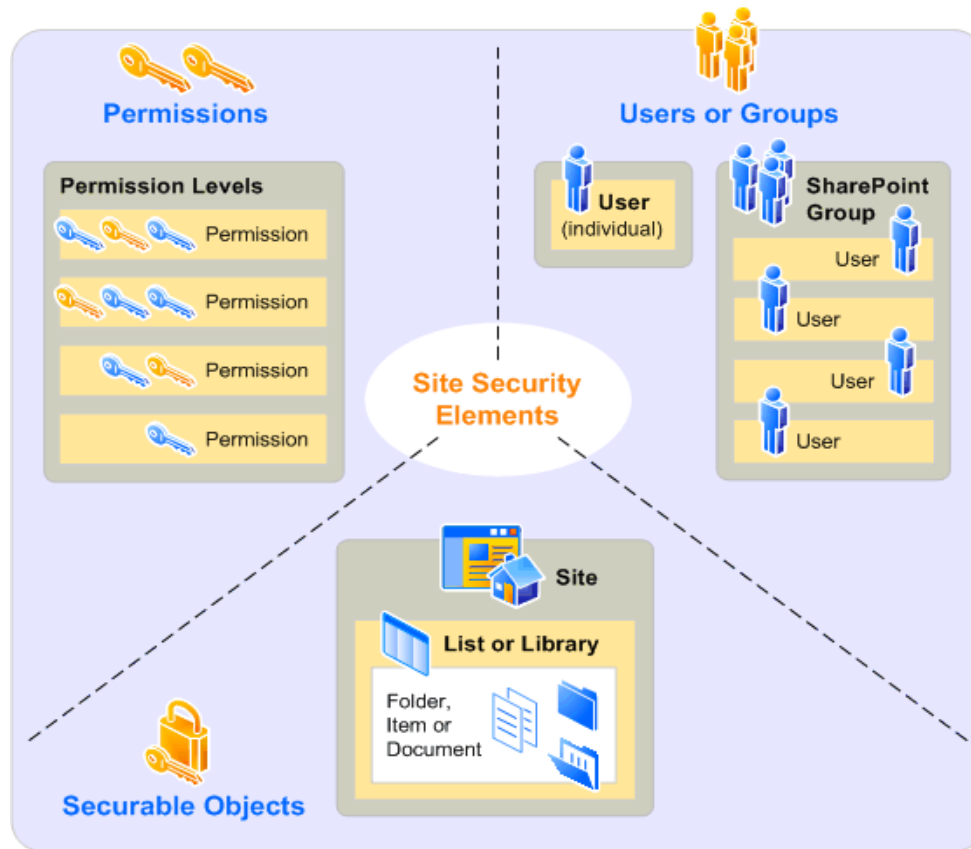
User Permissions

SECURITY TIPS



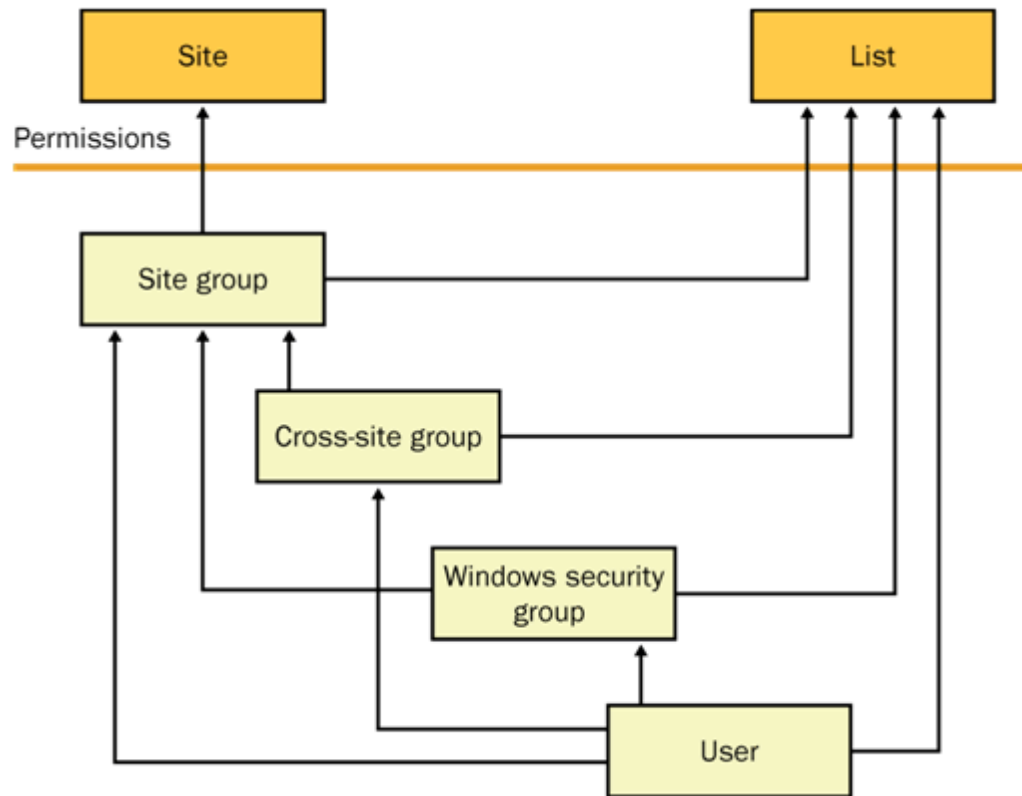
User Permissions

SECURITY TIPS



User Permissions

SECURITY TIPS



Security Tools

USER PERMISSIONS

Site Security Management

- ▣ Manage Site Security
- ▣ Set Site Security
- ▣ Restore Default Security

Team Site > Site Settings > Set Site Security

Set Site Security

Use this page to give new permissions.

NOTE: This will clear all selected items of their inherited AND custom security and replace it with the security specified on this page.

Add Users

You can enter user names, group names, or e-mail addresses. Separate them with semicolons.

Users/Groups:

Give Permission

Choose the permissions you want these users or groups to have.

Give Permission

- Full Control - Has full control.
- Design - Can view, add, update, delete, approve, and customize.
- Contribute - Can view, add, update, and delete.
- Read - Can view only.
- Restricted Read -

[Add to List](#)

	Users/Groups	Type	User Name	Permissions
Remove	WSSDEVELOPMENT\administrator	User	WSSDEVELOPMENT\administrator	Full Control
Remove	WSSDEVELOPMENT\domain admins	Domain Group	WSSDEVELOPMENT\domain admins	Full Control
Remove	Test Members	SharePoint Group	Test Members	Contribute
Remove	User, Test	User	WSSDEVELOPMENT\testuser	Restricted Read

[Set Security](#)

Security Tools

USER PERMISSIONS

Users and Permissions



- ▣ People and groups
- ▣ Site collection administrators
- ▣ Advanced permissions
- ▣ **Check User Access**
- ▣ View Permission Inheritance

Check User Access

IT > Site Settings > Check User Access

This page allows you to check a users access to sites and lists.

Download Report Check Access




















Login Name:  

Access: ▾

Filter Options

- Show All
- Only show items where the user does not have access
- Only show items where the user has access

Green - Tom Shirley has Contribute or greater access.
Red - Tom Shirley does not have Contribute or greater access.

- [-]  /IT
 -  After Hours Contacts (2)
 -  Announcements (1)
 -  Calendar (0)
 -  Links (0)
 -  Policies and Procedures (4)
 -  Shared Documents (0)
 -  Site Contacts (1)
 -  Tasks (0)
 -  Team Discussion (0)
 -  Useful References (3)
- [-]  /IT/Management
 -  Announcements (1)
 -  Calendar (0)
 -  Links (0)
 -  Shared Documents (2)
 -  Site Contacts (1)
 -  Tasks (0)
 -  Team Discussion (0)

Security Tools

USER PERMISSIONS

The screenshot shows the SUSHI Security Reports tool interface. The left sidebar contains a navigation menu with categories: Administration (Security Reports, Profile Images Import, Backup, Restore, Email Test), Lists (Copy A View, Meta Data, Bulk List Creation, Bulk Site Columns, Import Documents, Delete Old Documents), Sites (Bulk Site Creation, Themes), and Help & Settings. The main content area is titled "Security Reports" and includes a "Select a site" dropdown showing "site found: http://test-a4q5oui8zq ✓". Below this, the "SharePoint Site:" field contains "http://test-a4q5oui8zq". The "Choose A Security Report" section has three radio buttons: "Show Permissions Inheritance For Site Collection" (unselected), "List Group Membership for User" (selected), and "Find All P..." (unselected). A "Get Users" button is next to a "User:" dropdown menu showing "TEST-A4Q50UI8ZQ\ad". A "Run Security Report" button is highlighted with a dashed border. The main report area displays "Group Membership for User TEST-A4Q50UI8ZQ\admin" and "For the site collection http://test-a4q5oui8zq". It lists "Site Collection Administrators" (user TEST-A4Q50UI8ZQ\administrator is a site collection admin), "SharePoint Groups" (Approvers, Designers, Hierarchy Managers, Home Owners, Quick Deploy Users, Restricted Readers, Style Resource Readers, Viewers), and "Active Directory Groups:".

Security Tip #4

BEWARE THIRD-PARTY CODE... NOT TOO MUCH

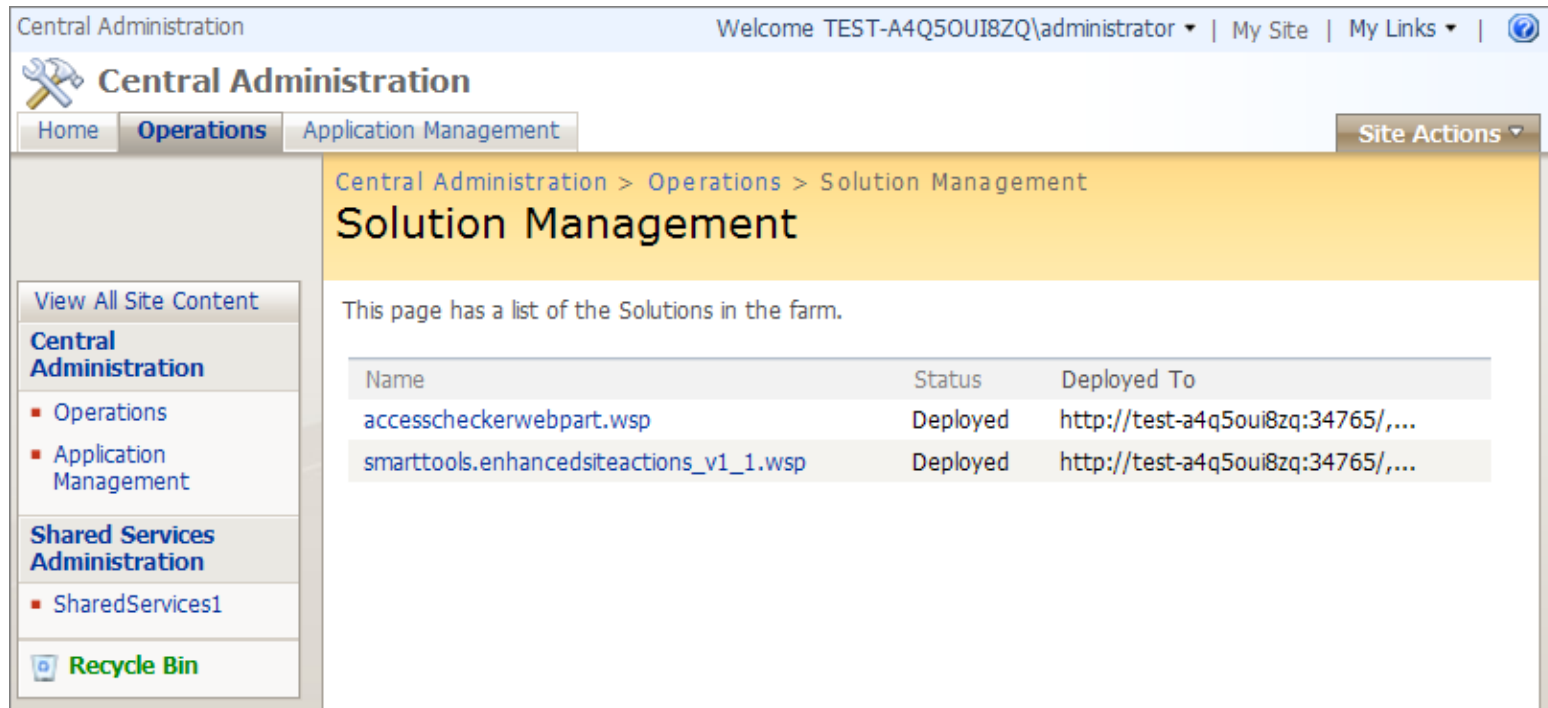
Third-Party Plugins

NECESSARY EVIL

- SharePoint without third-party plugins is like an iPhone with no apps
 - Solutions, Features
 - Web Parts, Templates
- If too strict, people will circumvent you

Third-Party Plugins

SOLUTIONS



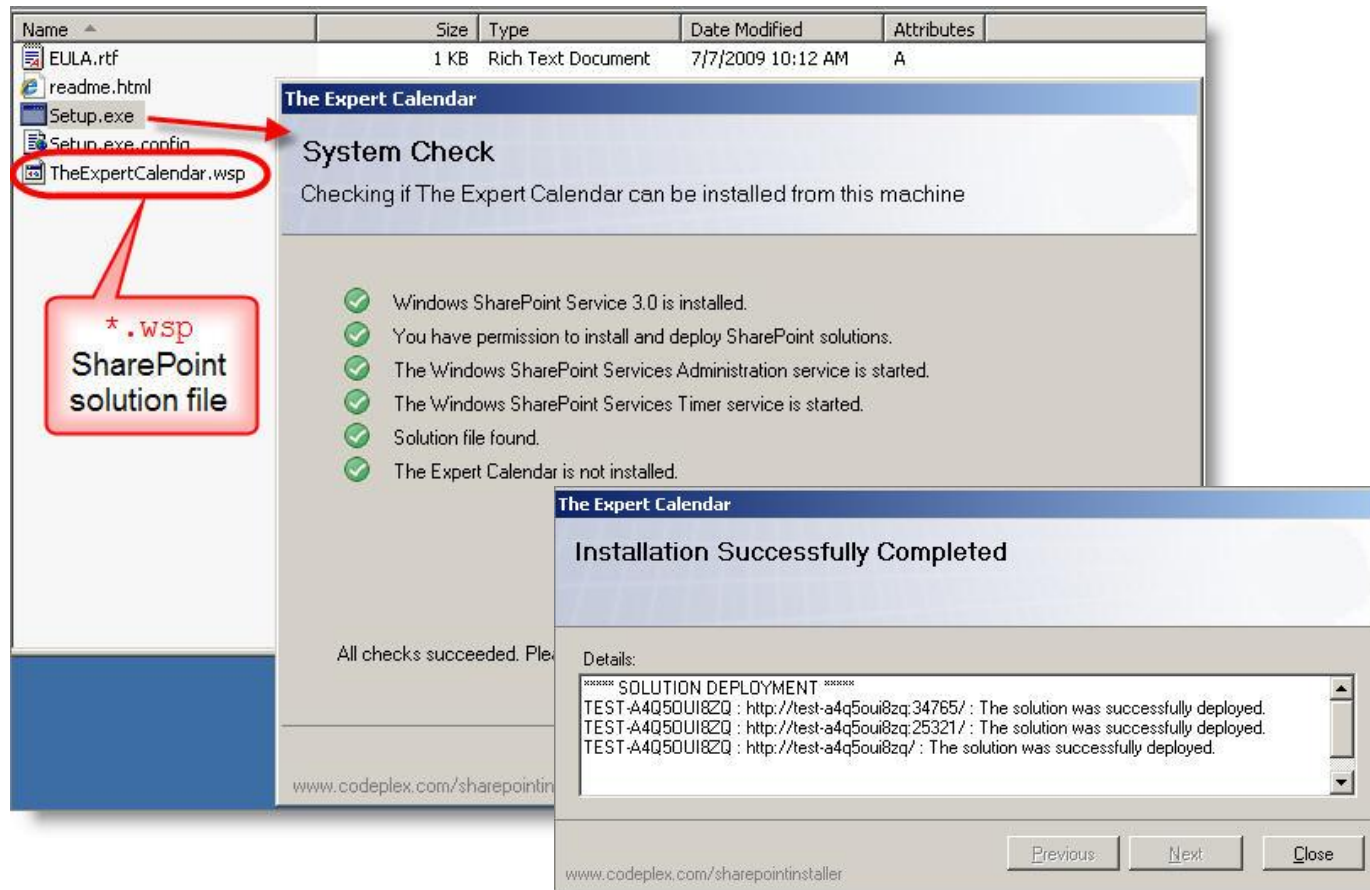
The screenshot shows the 'Central Administration' interface. The breadcrumb trail is 'Central Administration > Operations > Solution Management'. The page title is 'Solution Management'. Below the title, it states 'This page has a list of the Solutions in the farm.' A table lists the solutions:

Name	Status	Deployed To
accesscheckerwebpart.wsp	Deployed	http://test-a4q5oui8zq:34765/,...
smarttools.enhancedsiteactions_v1_1.wsp	Deployed	http://test-a4q5oui8zq:34765/,...

The left sidebar contains navigation links: 'View All Site Content', 'Central Administration' (with sub-links for 'Operations' and 'Application Management'), 'Shared Services Administration' (with sub-link for 'SharedServices1'), and 'Recycle Bin'.

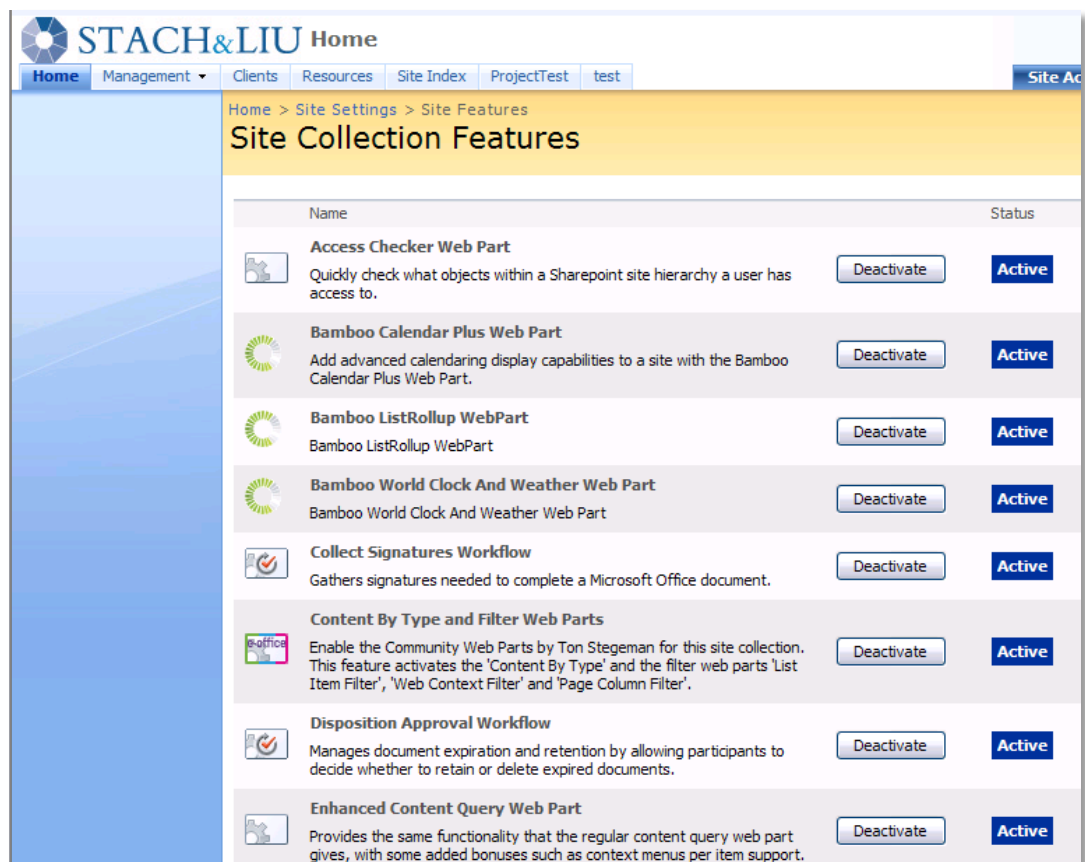
Third-Party Plugins

SOLUTIONS



Third-Party Plugins

FEATURES



The screenshot displays the 'Site Collection Features' page in a SharePoint environment. The page title is 'STACH&LIU Home' and the breadcrumb trail is 'Home > Site Settings > Site Features'. The page lists several features, each with a description, a 'Deactivate' button, and a status indicator (Active or Inactive).

Name	Status
Access Checker Web Part Quiddy check what objects within a Sharepoint site hierarchy a user has access to.	Active
Bamboo Calendar Plus Web Part Add advanced calendaring display capabilities to a site with the Bamboo Calendar Plus Web Part.	Active
Bamboo ListRollup WebPart Bamboo ListRollup WebPart	Active
Bamboo World Clock And Weather Web Part Bamboo World Clock And Weather Web Part	Active
Collect Signatures Workflow Gathers signatures needed to complete a Microsoft Office document.	Active
Content By Type and Filter Web Parts Enable the Community Web Parts by Ton Stegeman for this site collection. This feature activates the 'Content By Type' and the filter web parts 'List Item Filter', 'Web Context Filter' and 'Page Column Filter'.	Active
Disposition Approval Workflow Manages document expiration and retention by allowing participants to decide whether to retain or delete expired documents.	Active
Enhanced Content Query Web Part Provides the same functionality that the regular content query web part gives, with some added bonuses such as context menus per item support.	Active

Third-Party Plugins

FEATURES

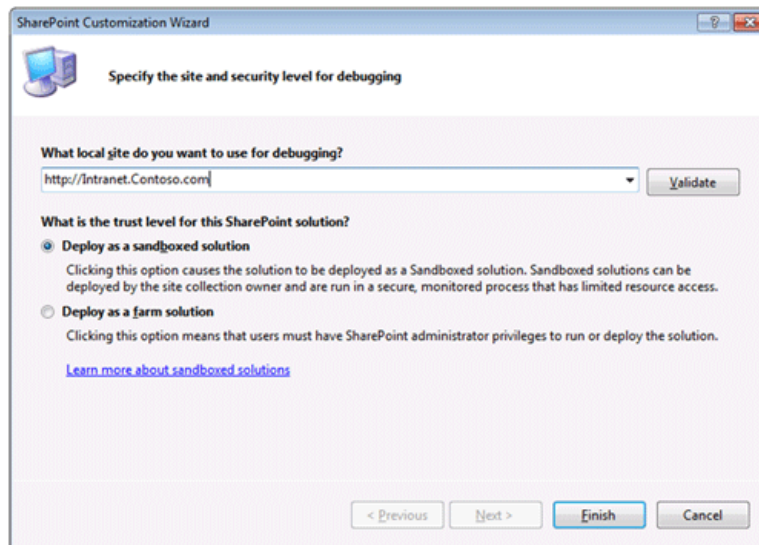
The screenshot displays the 'Site Features' page in the STACH&LIU Clients application. The page has a navigation bar with 'Home', 'Management', 'Clients', 'Resources', and 'Site Index'. The breadcrumb trail is 'Home > Clients > Site Settings > Site Features'. The main content area is titled 'Site Features' and contains a table with the following data:

Name	Status
Office SharePoint Server Enterprise Site features Features such as the business data catalog, forms services, and Excel Services, included in the Office SharePoint Server Enterprise License	Deactivate Active
Office SharePoint Server Publishing Create a Web page library as well as supporting libraries to create and publish pages based on page layouts.	Activate
Office SharePoint Server Standard Site features Features such as user profiles and search, included in the Office SharePoint Server Standard License	Deactivate Active
Team Collaboration Lists Provides team collaboration capabilities for a site by making standard lists, such as document libraries and issues, available.	Deactivate Active
Translation Management Library Create a translation management library when you want to create documents in multiple languages and manage translation tasks. Translation management libraries include a workflow to manage the translation process and provide sub-folders, file versioning, and check-in/check-out.	Deactivate Active

Third-Party Plugins

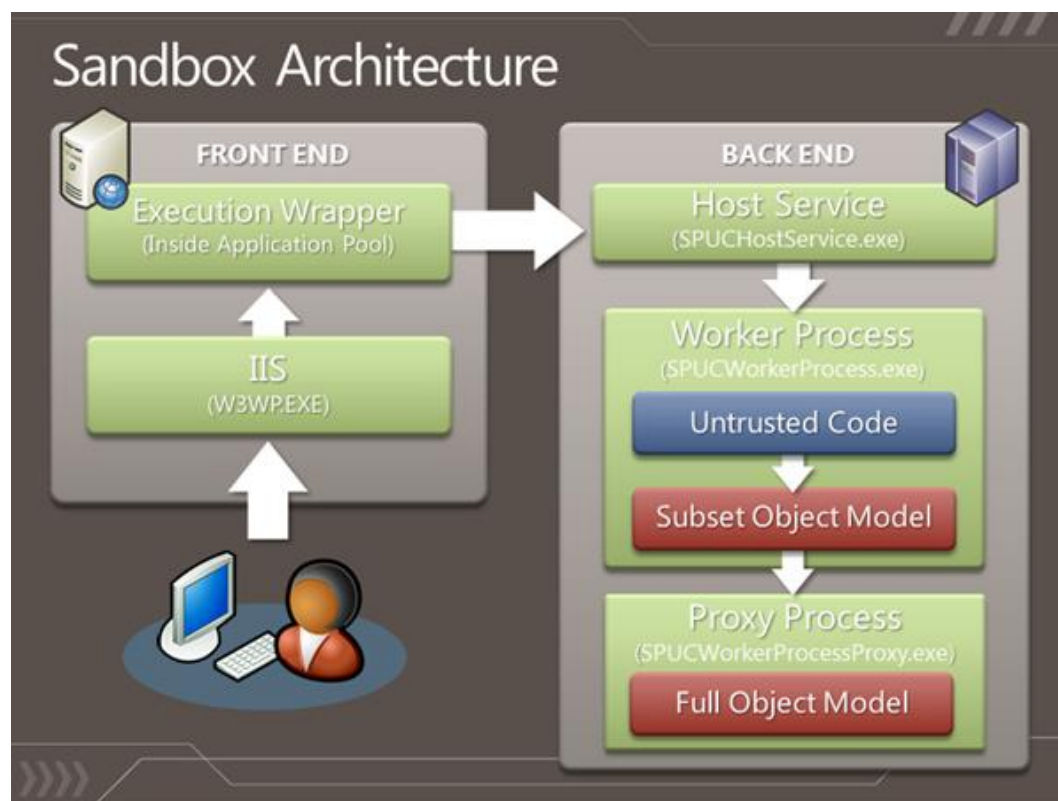
FUTURE SECURITY

- SharePoint 2010 has sandboxed solutions
- Minimize risk of running untrusted third-party plugins



Third-Party Plugins

SANDBOXED SOLUTIONS



Security Tip #5

BACKUP EVERY WHICH
WAY FROM SUNDAY

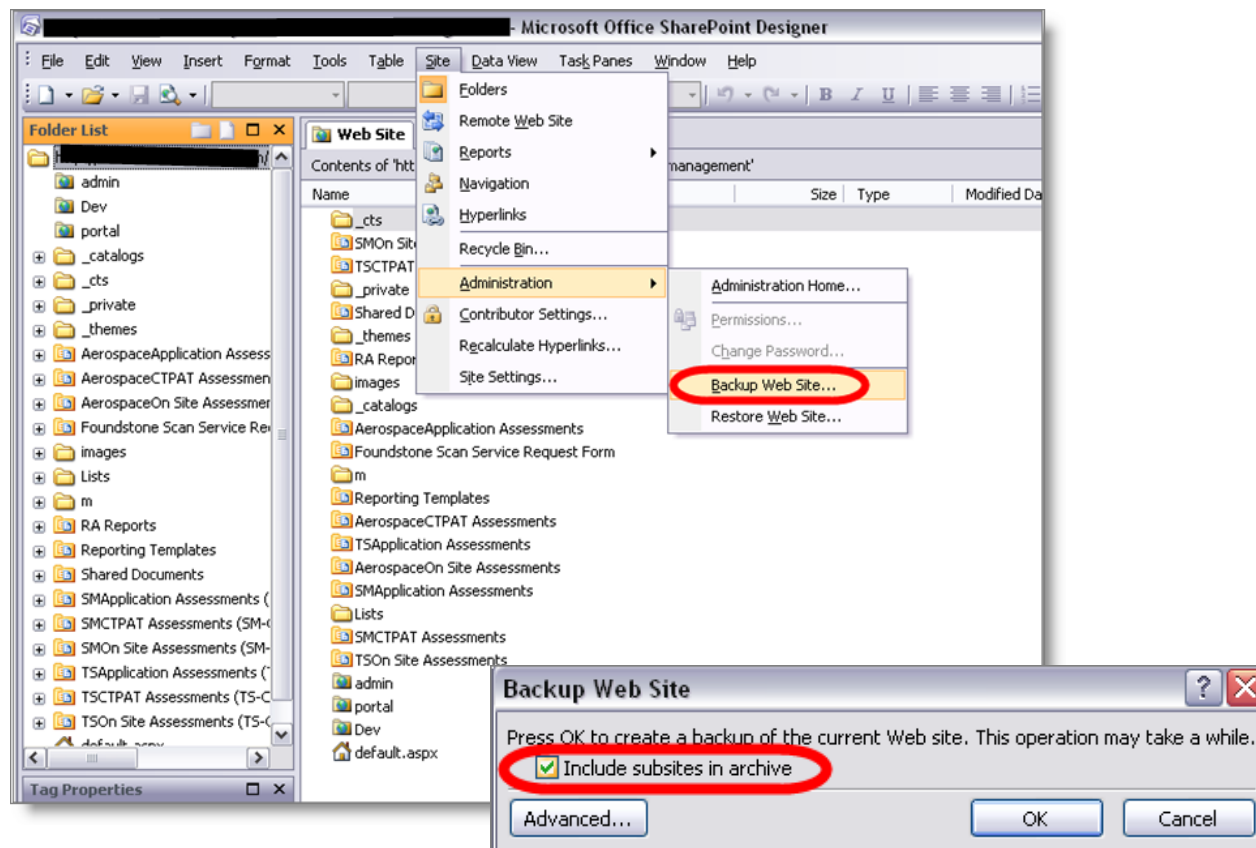
Backups

MANY METHODS ... ALL TERRIBLE

1. Windows 2003/2008 Server backups
2. Stsadm.exe cmdline tool backups
3. Central Administration v3 backups
4. SharePoint Designer backups
5. Site and List template backups
6. Raw MS SQL database backups

Backups

SHAREPOINT DESIGNER



Backups

STSADM / CENTRAL ADMINISTRATION

```
stsadm.exe -o backup -url <URL name> -filename <\\server.name\folder name\file name> [-overwrite]
```

The screenshot shows the Central Administration console interface. The 'Operations' tab is selected in the top navigation bar. The main content area is titled 'Operations' and contains a list of links organized into four sections: 'Topology and Services', 'Global Configuration', 'Security Configuration', and 'Backup and Restore'. The 'Backup and Restore' section is highlighted with a red circle and contains the following links: 'Perform a backup', 'Backup and restore history', 'Restore from backup', and 'Backup and restore job status'.

Central Administration

Welcome CHEESE\administrator

Central Administration

Home **Operations** Application Management

Central Administration > Operations

Operations

This page contains links to pages that help you manage your server or server farm, such as changing the server farm topology, specifying services running on each server, and changing settings that affect multiple servers or applications.

Topology and Services

- Servers in farm
- Services on server
- Outgoing e-mail settings
- Incoming e-mail settings
- Approve/reject distribution groups

Global Configuration

- Timer job status
- Timer job definitions
- Master site directory settings
- Site directory links scan
- Alternate access mappings
- Manage farm features
- Quiesce farm
- Solution management

Security Configuration

- Service accounts
- Information Rights Management
- Antivirus
- Blocked file types
- Update farm administrator's group
- Information management policy configuration
- Manage settings for single sign-on

Backup and Restore

- Perform a backup
- Backup and restore history
- Restore from backup
- Backup and restore job status

Backups

SITE AND LIST TEMPLATES

The screenshot shows the SharePoint 'Site Settings' page. The breadcrumb trail is 'Home > Site Settings'. The page title is 'Site Settings'. Under 'Site Information', the Site URL is 'http://test-a4q5oui8zq/' and the Mobile Site URL is 'http://test-a4q5oui8zq/m/'. The version is 12.0.0.6535. The page is divided into several sections: 'People and Permissions', 'Look and Feel', 'Galleries', and 'Site Templates'. The 'Look and Feel' section contains a list of options: 'Title, description, and icon', 'Tree view', 'Site theme', 'Top link bar', 'Quick Launch', 'Save site as template', and 'Reset to site definition'. The 'Galleries' section contains: 'Master pages', 'Site content types', 'Site columns', 'Site templates', 'List templates', 'Web Parts', and 'Workflows'. Two red callout boxes are present. One points to the 'Save site as template' option in the 'Look and Feel' section, with the text 'Backup current site as a "site template"'. The other points to the 'Site templates' and 'List templates' options in the 'Galleries' section, with the text 'Manage site and list templates'. Both 'Save site as template' and 'List templates' are circled in red.

Home > Site Settings
Site Settings

Site Information
Site URL: http://test-a4q5oui8zq/
Mobile Site URL: http://test-a4q5oui8zq/m/
Version: 12.0.0.6535

People and Permissions
People and groups
Collection
Administrators
Advanced permissions
Check User Access
View Permission Inheritance

Look and Feel
Title, description, and icon
Tree view
Site theme
Top link bar
Quick Launch
Save site as template
Reset to site definition

Galleries
Master pages
Site content types
Site columns
Site templates
List templates
Web Parts
Workflows

Site Templates

Backup current site as a "site template"

Manage site and list templates

Backups

SITE AND LIST TEMPLATES

Home > Site Settings > Save as Template

Save Site as Template

Use this page to save your Web site as a site template. Users can create new Web sites from this template.

File Name Enter the name for this template file.	File name: <input type="text" value="mysite"/> .stp
Name and Description The name and description of this template will be displayed on the Web site template picker page when users create new Web sites.	Template name: <input type="text" value="Site Backup"/> Template description: <input type="text"/>
Include Content Include content in your template if you want new Web sites created from this template to include the contents of all lists and document libraries in this Web site. Some customizations, such as custom workflows, are present in the template only if you choose to include content. Including content can increase the size of your template. Caution: Item security is not maintained in a template. If you have private content in this Web site, enabling this option is not recommended.	<input checked="" type="checkbox"/> <u>Include Content</u>

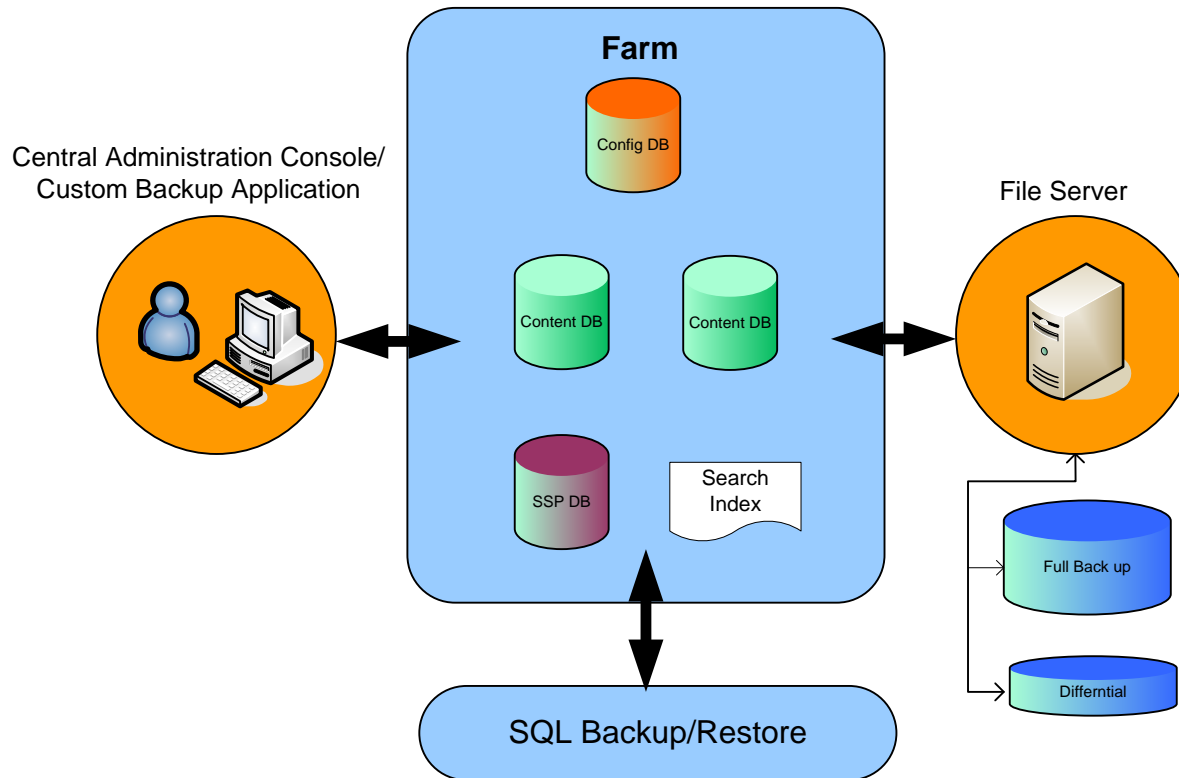
OK Cancel

Saves as single *.stp file

Can opt to include content (e.g. files, list items, etc.)

Backups

RAW SQL DATABASES



Questions?
Ask us something
We'll try to answer it.

For more info:
Email: contact@stachliu.com
Project: diggity@stachliu.com
Stach & Liu, LLC
www.stachliu.com

Thank You

Stach & Liu SharePoint Hacking Diggity Project info:

<http://www.stachliu.com/index.php/resources/tools/sharepoint-hacking-diggity-project/>