



SharePoint Security

Advanced SharePoint Security Tips and Tools

22 Feb 2012 – OWASP L.A. 2012 – Los Angeles, CA



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)





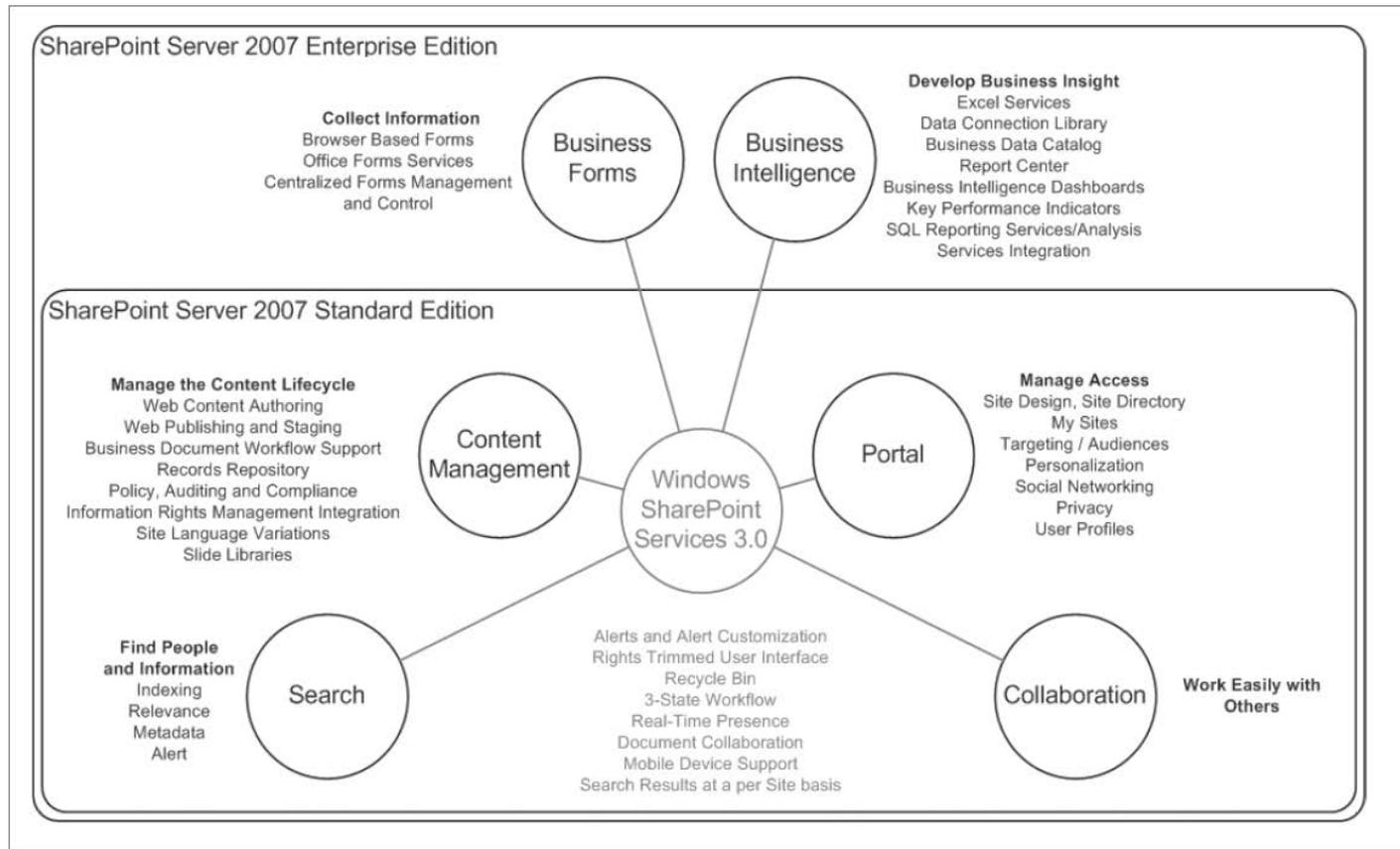
Core Components

MS SharePoint Products & Technologies



Core Components

MS SharePoint Products & Technologies



Core Components

MS SharePoint Products & Technologies

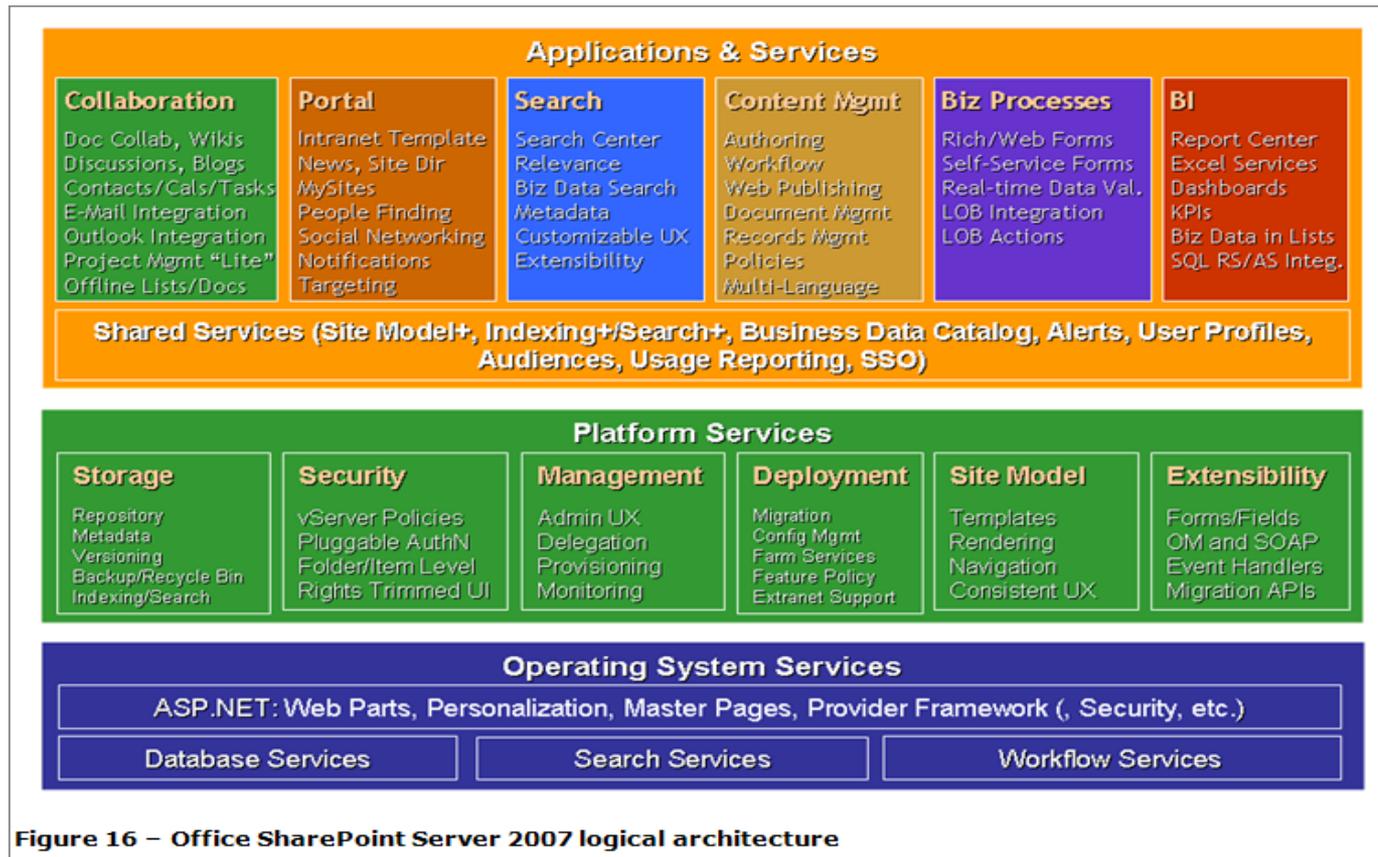


Figure 16 – Office SharePoint Server 2007 logical architecture

Centralized Portal

MS SharePoint Products & Technologies



Site Hierarchy

Intro to SharePoint

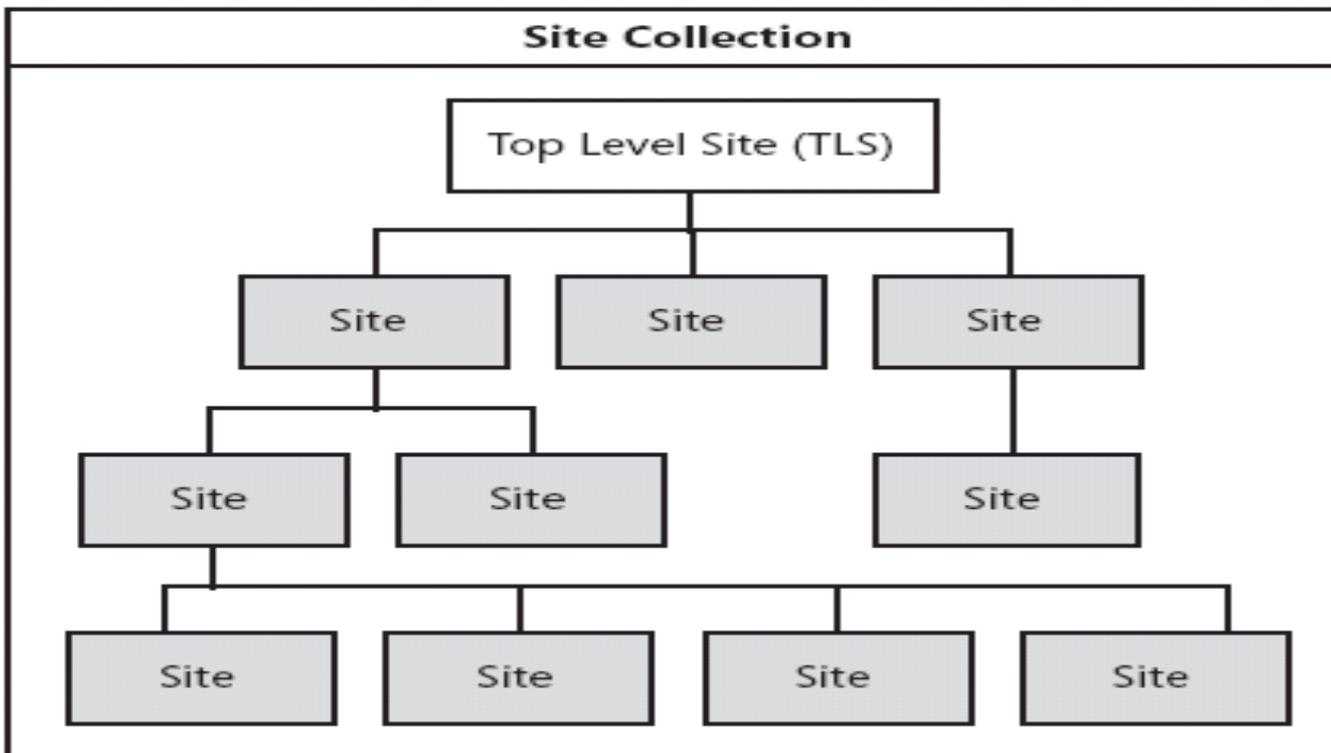


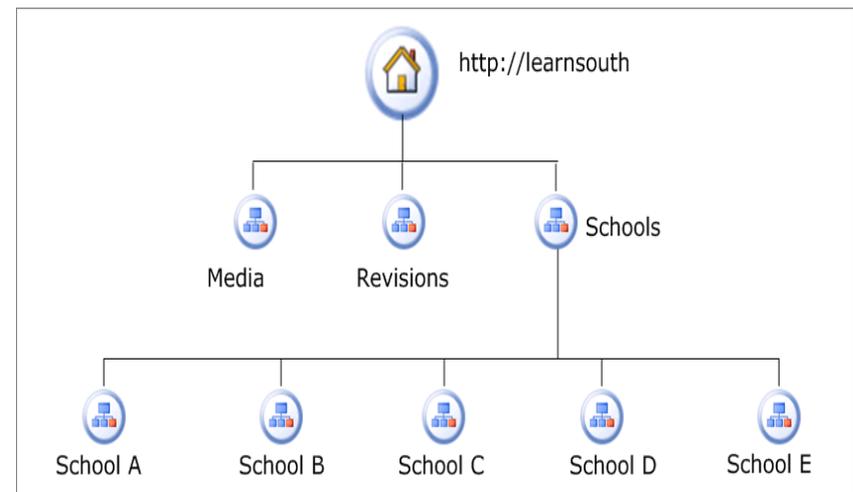
Figure 1-6 Site collections are a structured collection of sites.

SharePoint Site Hierarchy

Intro to SharePoint

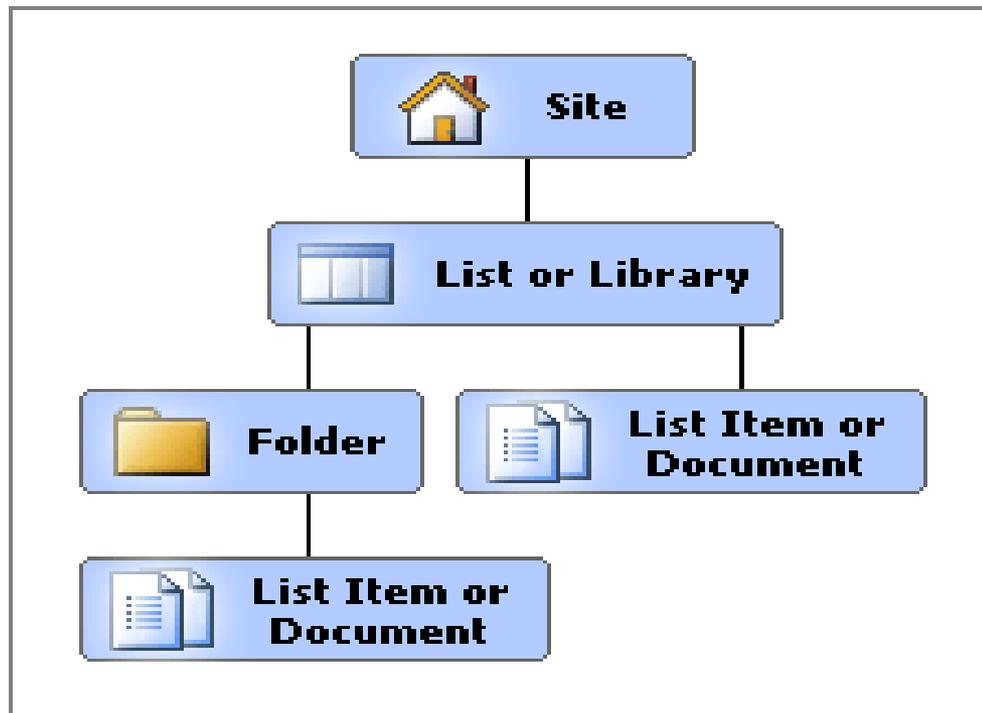
Base Site URLs:

- <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 left sidebar contains a "Site Hierarchy" tree view with categories like "Management", "Clients", "Resources", and "Site Directory". The main content area displays "All Site Content" with a list of libraries and lists. The right sidebar contains "Site Actions" and "Manage Content and Structure".

Key navigation elements highlighted in the image:

- Home
- Global Navigational Breadcrumb
- Top Link Bar
- Personalization - My Site
- Site Actions
- Content Navigational Breadcrumb
- All Site Content
- Site Actions
- Site Settings
- Manage Content and Structure
- Quick Launch Bar
- 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 collection.	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



WikiLeaks and SharePoint

RISK OF EXPOSURE

- Wget scripts targeting SharePoint downloads
- 250,000 government cables sent to WikiLeaks



InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

10 SharePoint Security Mistakes You Probably Make

Bradley Manning allegedly stole sensitive government cables destined for WikiLeaks from a SharePoint server. Are your information security controls tighter than the Army's were?

By Mathew J. Schwartz, [InformationWeek](#)

January 31, 2012

URL: <http://www.informationweek.com/news/security/app-security/232500768>

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 3 rd 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 – 121 queries
4. Coming Soon: SharePoint Bing Dictionary
5. SHODAN searching for SharePoint servers
6. SharePoint Hacking Alerts

2. SharePoint URL Brute-forcing

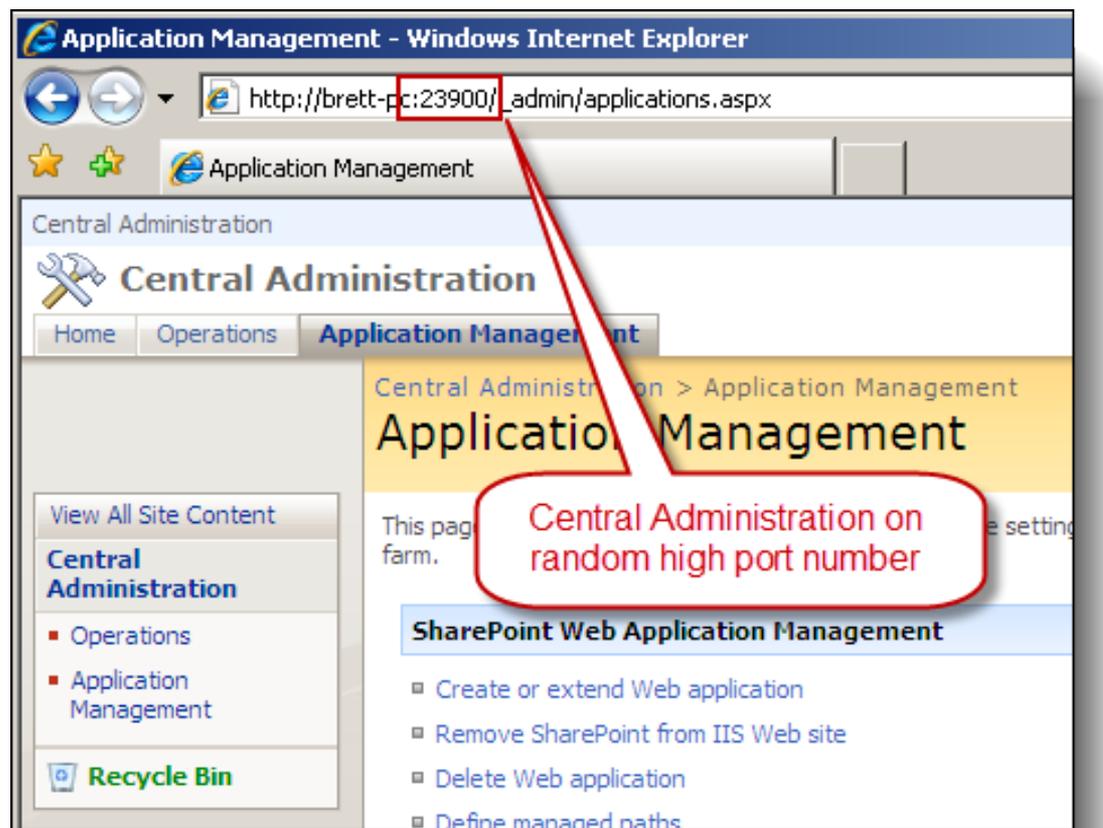
1. Forceful browse to common SharePoint extensions to test access
2. **NEW**: Tool to bruteforce SharePoint URLs – 101 known extensions

3. Nmap for other SharePoint administrative apps

1. E.g. Central Administration, Shared Service Providers (SSP)

External Exposure

SHAREPOINT ADMIN WEB APPS





External Exposure

GOOGLE HACKING SHAREPOINT

Google

"all site content" site:.com filetype:aspx Instant is on ▾

About 215,000 results (0.16 seconds) [Advanced search](#)

Everything

- Images
- Videos
- News
- Shopping
- More

Tempe, AZ
[Change location](#)

All Site Content 🔍
Home > All Site Content. All Site Content. Quick Launch. View All Site Content ... View: All Site Content Use SHIFT+ENTER to open the menu (new window). ...
[www.ppg.com](#) > Home - Cached - Similar

All Site Content 🔍
All Site Content. Quick Launch. View All Site Content ... View: All Site Content Use SHIFT+ENTER to open the menu (new window). ...
[research.datcommunity.com/exchange_login/.../viewlists.aspx](#) - Cached

All Site Content 🔍
State of Vermont Judiciary > All Site Content ... View: All Site Content Use SHIFT+ENTER to open the menu (new window). ...
[iweb.synecology.com/layouts/viewlists.aspx](#) - Cached - Similar

215,000 "All Site Content" SharePoint pages



External Exposure

GOOGLE HACKING SHAREPOINT

Google

"/_vti_bin/lists.aspx" filetype:asmx Instant is on ▾

About 98,300 results (0.21 seconds) [Advanced search](#)

Everything
Images
Videos
News
Shopping
More

Tempe, AZ
[Change location](#)

Lists Web Service

POST /_vti_bin/lists.aspx HTTP/1.1 Host: www.wssdemo.com Content-Type: text/xml; charset=utf-8 Content-Length: length SOAPAction: ...
www.wssdemo.com/_vti_bin/lists.aspx?op=GetListItems - [Cached](#) - [Similar](#)

Lists Web Service

POST /_vti_bin/lists.aspx HTTP/1.1 Host: jubileeminneapolis.org Content-Type: text/xml; charset=utf-8 Content-Length: length SOAPAction: ...
https://jubileeminneapolis.org/_vti_bin/lists.aspx

Lists Web Service

POST /_vti_bin/lists.aspx HTTP/1.1 Host: www.votorantim.com Content-Type: text/xml; charset=utf-8 Content-Length: length SOAPAction: ...
www.votorantim.com/_vti_bin/lists.aspx?op=GetListItems - [Cached](#)

98,000 exposed SharePoint "Lists Web Service"



External Exposure

GOOGLE HACKING SHAREPOINT

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

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

» inurl: "/_catalogs/wt/"

[www.orwelltourstravel.com - /_catalogs/wt/Forms/](http://www.orwelltourstravel.com/_catalogs/wt/Forms/)
www.orwelltourstravel.com - /_catalogs/wt/Forms/. [To Parent Directory] 4/30/ 2007 1:17 PM 6994 AllItems.aspx ...
[www.orwelltourstravel.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](#)
_lcid="1033" _version="11.0.5510" _dal="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...&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.



External Exposure

BING HACKING SHAREPOINT

bing instreamset:url:"layouts/viewlists.aspx"

Web **Web** More ▾

RELATED SEARCHES

- [SharePoint Quick Launch Bar](#)
- [Full Speed Ahead Fly aspx Layout Downloads](#)
- [Facebook Layouts](#)
- [New Facebook Layout Profile Layouts](#)
- [MySpace Layouts](#)
- [Hot Layouts](#)
- [Girly MySpace Layouts](#)

SEARCH HISTORY

Turn on search history to start remembering your searches.

[Turn history on](#)

ALL RESULTS 1-50 of 709 results · [Advanced](#)

[All Site Content - FH Paschen: Construction Company: General ...](#)
This page shows all the libraries, lists, discussion boards, and surveys in this Web site. Click the name of a library or list to view its contents.
https://extranet.fhpaschen.com/_layouts/viewlists.aspx

[All Site Content](#)
McAdory ES > All Site Content All Site Content ... View All Site Content
mcadoryel.jefcoed.com/_layouts/viewlists.aspx?BaseType=1&List... · [Cached page](#)

Related Searches for instreamset:url:"layouts/viewlists.aspx"

- [SharePoint Quick Launch Bar](#)
- [Facebook Layouts](#)
- [Profile Layouts](#)
- [Full Speed Ahead Fly aspx Lay...](#)
- [New Facebook Layout](#)
- [MySpace Layouts](#)

[All Site Content - Home - Deerlake Middle School](#)
This page shows all the libraries, lists, discussion boards, and surveys in this Web site. Click the name of a library or list to view its contents.
www.deerlake.leon.k12.fl.us/_layouts/viewlists.aspx

[All Site Content - Home - CCM Ministry Home](#)
Name Description Items Last Modified; Sites and Workspaces There are no subsites or workspaces.
ministries.calvarymelbourne.org/_layouts/viewlists.aspx?ShowSites=1

[All Site Content - Home - Williamson County Schools](#)
Name Description Items Last Modified; Sites and Workspaces Angie Prosize Email:

COMING SOON



External Exposure

SHODAN FOR SHAREPOINT

The screenshot shows a web browser window with the URL `www.shodanhq.com/search?q=WWW-authenticate+MicrosoftSharePointTeamServices`. The page features a navigation bar with links for Main, Exploits, Research, Videos, and Anniversary Promotion. The search bar contains the query `WWW-authenticate MicrosoftSharePointTeamServices`. Below the search bar, a table lists the top countries matching the search:

Country	Count
United States	19,490
United Kingdom	2,620
Germany	1,994
Canada	1,800
Australia	1,435

Below the table, a specific search result is displayed for IP address `88.39.32.133`, added on `08.02.2012` from `Arezzo`. The associated host is `host133-32-static.39-88-b.business.telecomitalia.it`. The response headers include:

- `HTTP/1.0 401 Unauthorized`
- `Content-Length: 1656`
- `Content-Type: text/html`
- `Server: Microsoft-IIS/6.0`
- `WWW-Authenticate: Negotiate`
- `WWW-Authenticate: NTLM`
- `MicrosoftSharePointTeamServices: 12.0.0.6219`
- `X-Powered-By: ASP.NET`
- `Date: Wed, 08 Feb 2012 11:09:58 GMT`

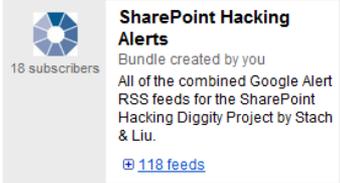
A red speech bubble annotation points to the `MicrosoftSharePointTeamServices: 12.0.0.6219` header, stating: "Using SHODAN to find SharePoint deployments".



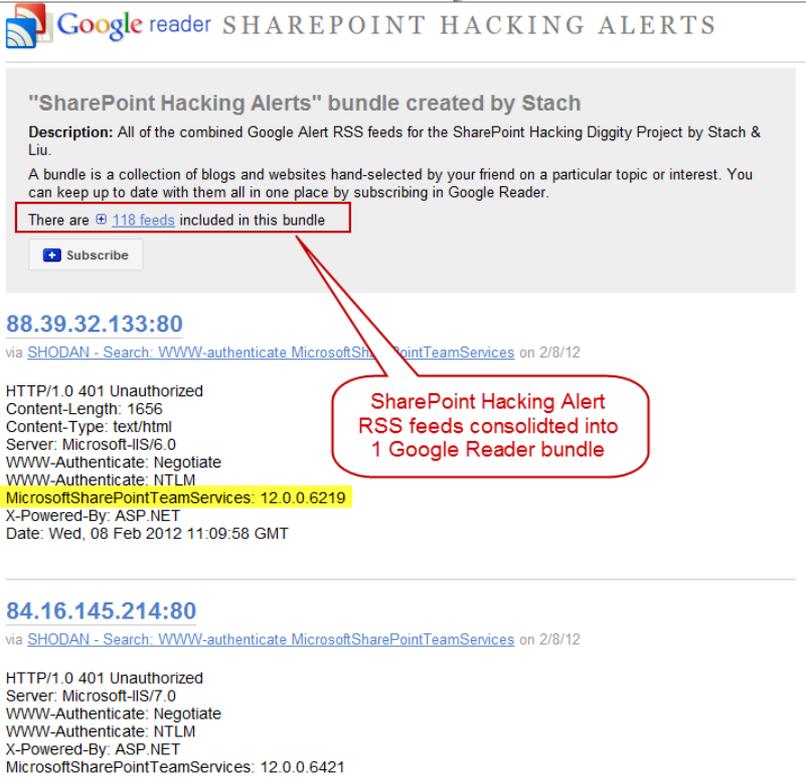
External Exposure



SHAREPOINT HACKING ALERTS



SharePoint Hacking Alerts
Bundle created by you
18 subscribers
All of the combined Google Alert RSS feeds for the SharePoint Hacking Diggity Project by Stach & Liu.
[118 feeds](#)



Google reader SHAREPOINT HACKING ALERTS

"SharePoint Hacking Alerts" bundle created by Stach

Description: All of the combined Google Alert RSS feeds for the SharePoint Hacking Diggity Project by Stach & Liu.
A bundle is a collection of blogs and websites hand-selected by your friend on a particular topic or interest. You can keep up to date with them all in one place by subscribing in Google Reader.

There are [118 feeds](#) included in this bundle

[Subscribe](#)

88.39.32.133:80
via SHODAN - Search: WWW-authenticate MicrosoftSharePointTeamServices on 2/8/12

HTTP/1.0 401 Unauthorized
Content-Length: 1656
Content-Type: text/html
Server: Microsoft-IIS/6.0
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
MicrosoftSharePointTeamServices: 12.0.0.6219
X-Powered-By: ASP.NET
Date: Wed, 08 Feb 2012 11:09:58 GMT

84.16.145.214:80
via SHODAN - Search: WWW-authenticate MicrosoftSharePointTeamServices on 2/8/12

HTTP/1.0 401 Unauthorized
Server: Microsoft-IIS/7.0
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 12.0.0.6421

SharePoint Hacking Alert RSS feeds consolidated into 1 Google Reader bundle

SHAREPOINT HACKING TOOLS

DEMO

External Exposure

SHAREPOINT URL BRUTEFORCING

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\GH\>perl "SharePointURLBrute.pl" TestApps.txt SharePoint-UrlExtensionsv4.txt

Starting search for common SharePoint Pages

FOUND: http://www.example.com/_catalogs/wp/Forms/AllItems.aspx
FOUND: http://www.example.com/_catalogs/wt/Forms/Common.aspx
FOUND: http://www.example.com/_layouts/listedit.aspx
FOUND: http://www.example.com/_layouts/MyInfo.aspx
FOUND: http://www.example.com/_layouts/MyPage.aspx
FOUND: http://www.example.com/_layouts/MvTasks.aspx
FOUND: http://www.example.com/_layouts/picker.aspx
FOUND: http://www.example.com/_layouts/policyconfig.aspx
FOUND: http://www.example.com/_layouts/Policylist.aspx
FOUND: http://www.example.com/_layouts/useredit.aspx
FOUND: http://www.example.com/_layouts/viewgrouppermissions.aspx
FOUND: http://www.example.com/default.aspx
FOUND: http://www.example.com/Pages/Forms/AllItems.aspx

Search Complete

C:\GH\>
```

picker.aspx is the
Active Directory
lookup tool

Security Tip #2

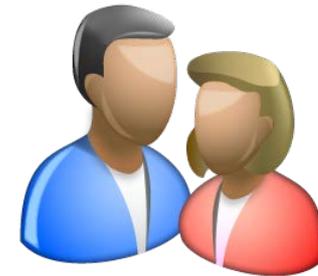
BEWARE USERS WITH EXCESSIVE ACCESS



Excessive User Access

MORE THAN YOU BARGAINED FOR...

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



CONTINUED SHAREPOINT HACKING
DEMO



Excessive User Access



SHAREPOINT WEB SERVICES

Permissions

The following operations are supported. For a formal de

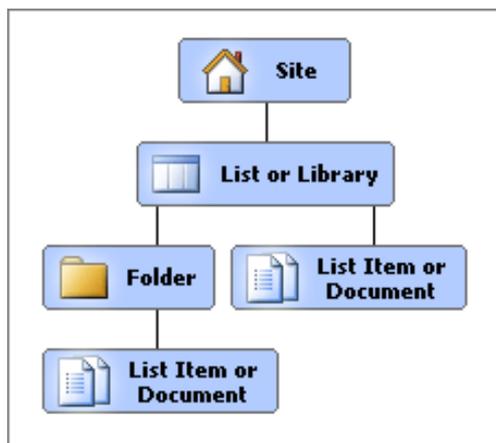
- [AddPermission](#)
- [AddPermissionCollection](#)
- [GetPermissionCollection](#)
- [RemovePermission](#)
- [RemovePermissionCollection](#)
- [UpdatePermission](#)

Security Tip #3

CHECK PERMISSIONS AND INHERITANCE

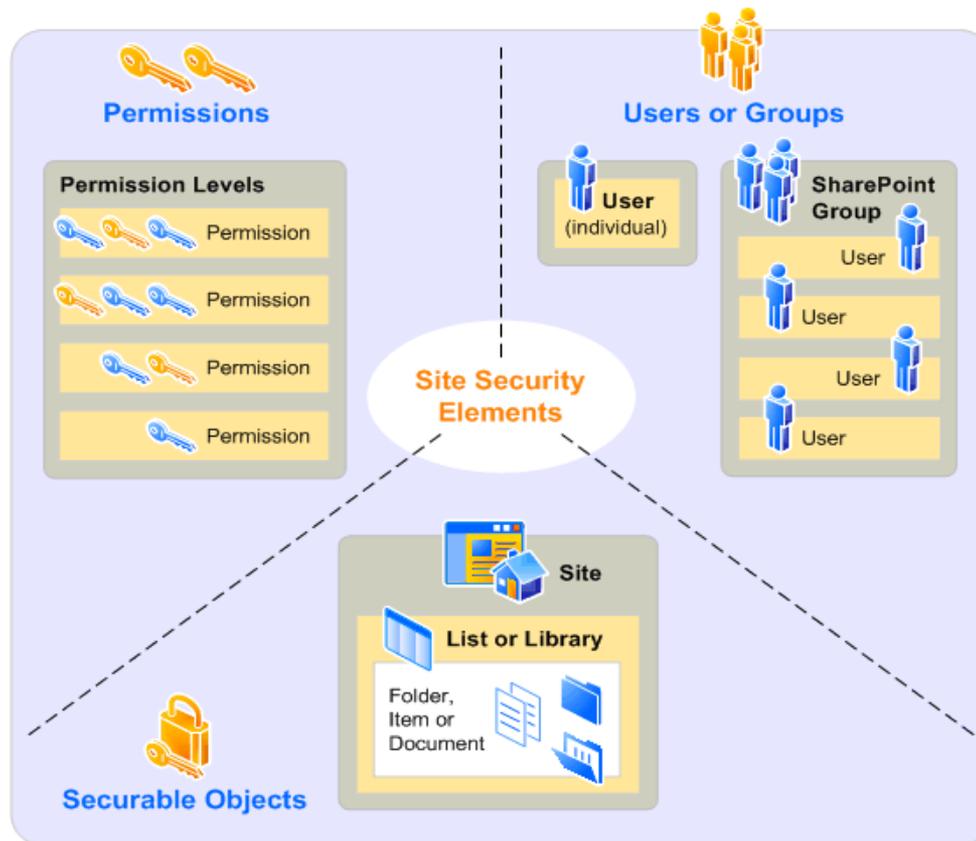
User Permissions

SECURITY TIPS



User Permissions

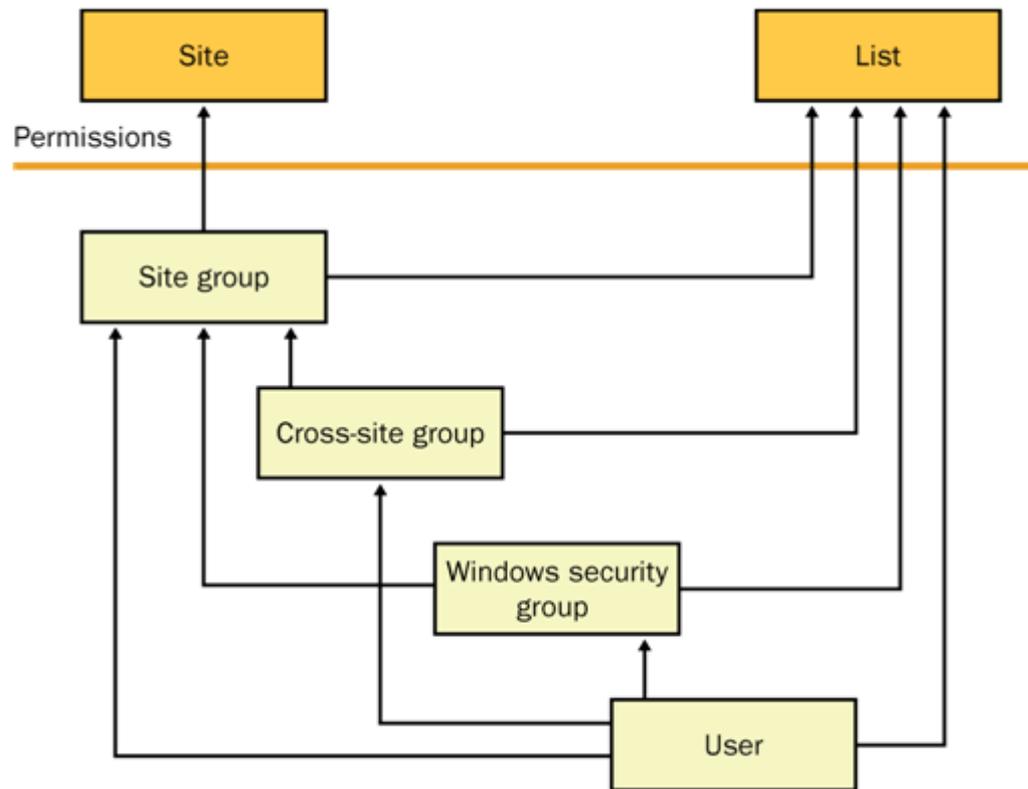
SECURITY TIPS





User Permissions

SECURITY TIPS



Security Tools

USER PERMISSIONS

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 -

	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

Site Security Management

- Manage Site Security
- Set Site Security
- Restore Default 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: Tom Shirley

Access: Contribute

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

Permissions Manager

This page provides groups permissions management on lists/libraries/pages. V0.1 updated on 01 feb. 2010

Inheritance preserved
 Inheritance broken

Copy list permissions

Source list: Target list:

Permissions on Lists/Libraries

Groups	Group Owner	Default permission	Contacts	Content and Structure Reports	Documents	Events	Form Templates	FRANCE	Images
Home Members	Home Owners	Contribute	Contribute	Contribute	Read	Contribute	Contribute	Contribute	Contribute
Home Owners	Home Owners	Full Control	Full Control	Full Control	Read	Full Control	Full Control	Full Control	Full Control
Home Visitors	Home Owners	Read	Read	Read	Read	Read	Read	Read	Read
Style Resource Readers	Home Owners			Read				Read	

Copy page permissions

Source page: Target page:

Permissions on Pages

Groups	Pages	Default.aspx	Demo.aspx	France.aspx
Home Members	Contribute	Contribute	Contribute	Contribute
Home Owners	Full Control	Contribute	Full Control	Full Control
Home Visitors	Read	Read	Read	Read

Set permissions

- Full Control
- Design
- Manage Hierarchy
- Approve
- Contribute
- Read
- Restricted Read
- Limited Access
- View Only
- Edit Personal User Information

Clear Cancel OK

Security Tools

USER PERMISSIONS

The screenshot shows the SUSI 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", "List Group Membership for User" (selected), and "Find All P...". 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 display area shows the results for "Group Membership for User TEST-A4Q50UI8ZQ\admini" for the site collection "http://test-a4q5oui8zq". The results are categorized into Site Collection Administrators, SharePoint Groups, and Active Directory Groups.

SUSI

Security Reports

Select a site site found: <http://test-a4q5oui8zq> ✓

SharePoint Site:

Choose A Security Report

Show Permissions Inheritance For Site Collection List Group Membership for User Find All P...

Get Users User:

Group Membership for User TEST-A4Q50UI8ZQ\admini
For the site collection <http://test-a4q5oui8zq>

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

Active Directory Groups:

Security Tools

USER PERMISSIONS

Quest®
Site Administrator
for SharePoint

Grant SharePoint Permissions

Set Reset

Shared Documents

List Names From: Current object permissions Show Users Refresh

Type	Name	Permission
Allow	Main Owners	Full Control
Allow	Main Visitors	Read
Allow	Main Members	Contribute
Allow	Doug	Full Control

Group/User: QUESTLOCAL\alex Advanced User Selection

Permission: Design Allow Advanced Permission Selection

Applies To:

Note: Please select only a single account in the Group/User field above before clicking 'Add' below.

List of users and groups to grant:

Type	Name	Permission
Allow	QUESTLOCAL\alex	Design

Add -->

<-- Remove

Reload Status: Ready

Help OK Cancel

Security Tip #4

BEWARE 3RD PARTY CODE...NOT TOO MUCH

3RD Party Plugins

NECESSARY EVIL

- SharePoint without 3rd party plugins is like an iPhone with no apps
 - Solutions, Features
 - Web Parts, Templates
- If too strict, people will circumvent you
 - Leads to **rogue SharePoint deployments**

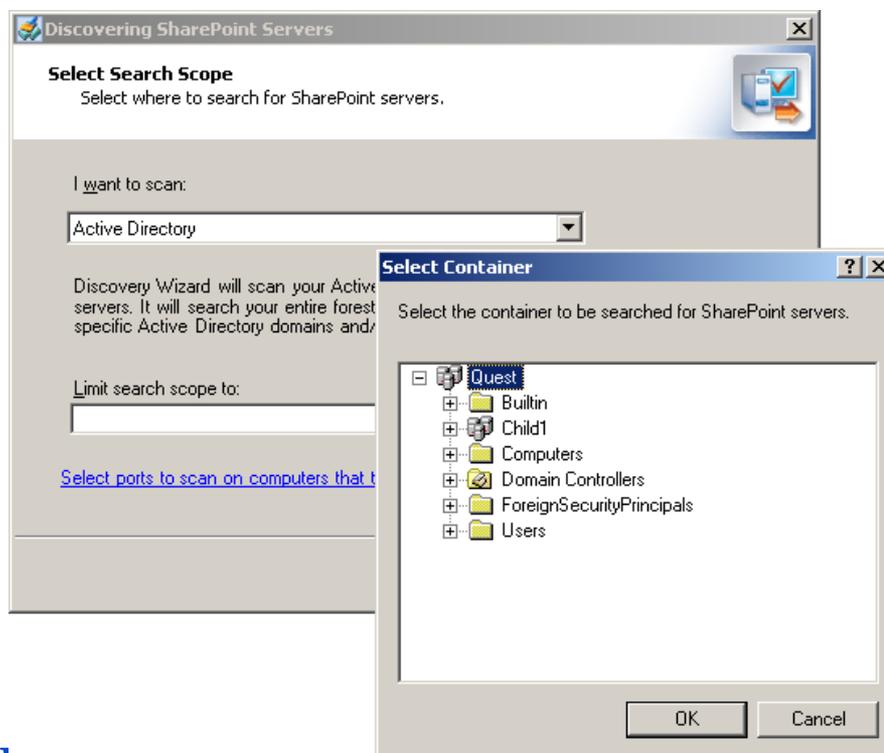




Detect Rogue SharePoint

ROGUE DEPLOYMENTS

Quest Software - Server Administrator for SharePoint



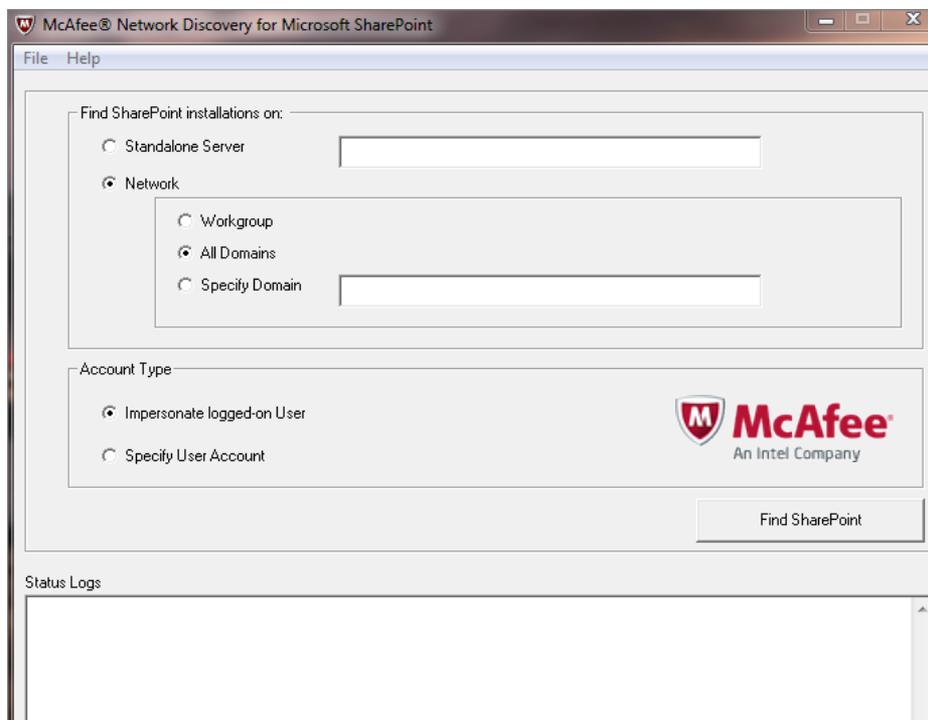
Quest[®]
Server Administrator
for SharePoint



Detect Rogue SharePoint

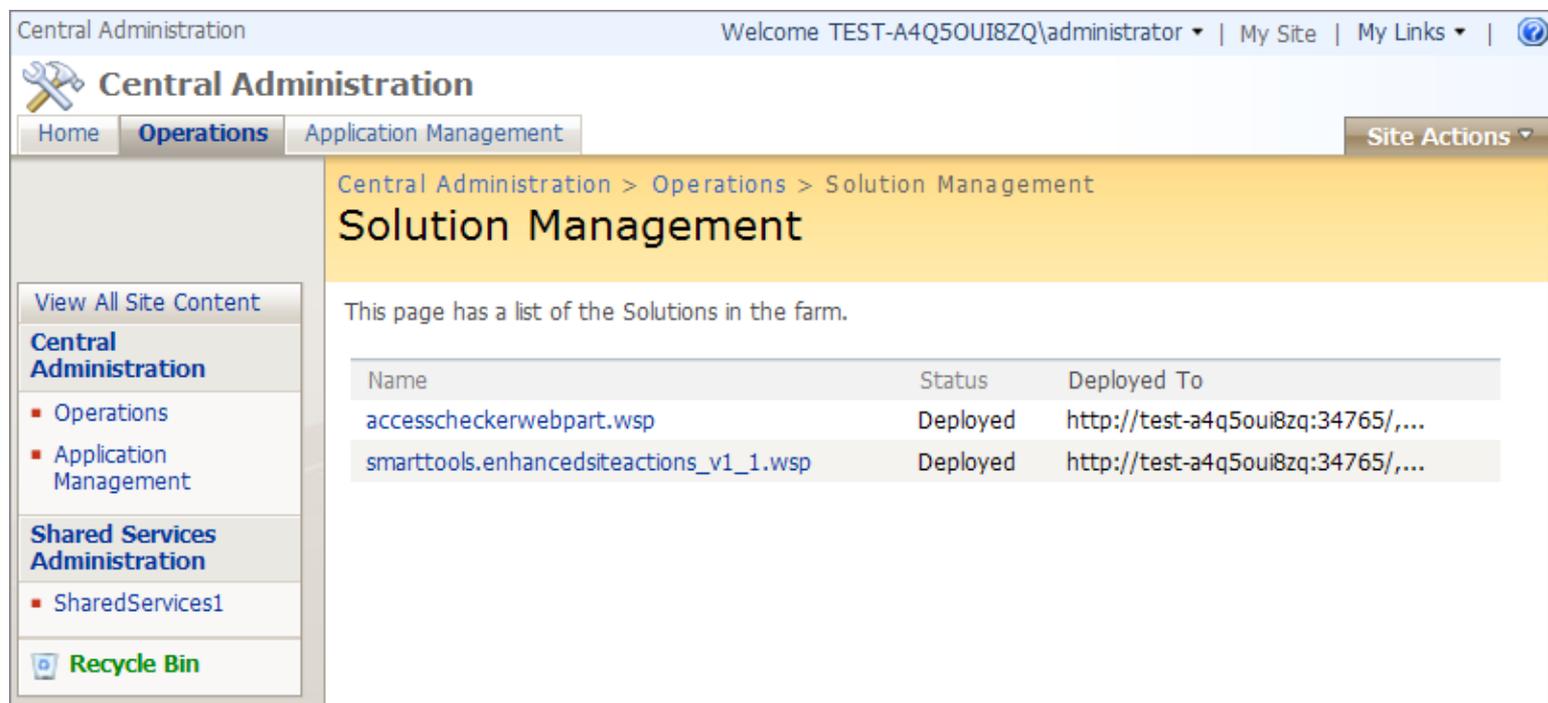
ROGUE DEPLOYMENTS

McAfee - Network Discovery for Microsoft SharePoint



3RD 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'.

3RD Party Plugins

SOLUTIONS

The image shows a Windows file explorer window with the following files:

Name	Size	Type	Date Modified	Attributes
EULA.rtf	1 KB	Rich Text Document	7/7/2009 10:12 AM	A
readme.html				
Setup.exe				
Setup.exe.config				
TheExpertCalendar.wsp				

A red circle highlights the file **TheExpertCalendar.wsp**. A red arrow points from this file to the **The Expert Calendar System Check** dialog box. A red callout box points to the file with the text: ***.wsp SharePoint solution file**.

The **The Expert Calendar System Check** dialog box displays the following status:

- ✓ Windows SharePoint Service 3.0 is installed.
- ✓ You have permission to install and deploy SharePoint solutions.
- ✓ The Windows SharePoint Services Administration service is started.
- ✓ The Windows SharePoint Services Timer service is started.
- ✓ Solution file found.
- ✓ The Expert Calendar is not installed.

Below the list, it states: "All checks succeeded. Please click Next to continue." The URL www.codeplex.com/sharepointin is visible at the bottom.

The **The Expert Calendar Installation Successfully Completed** dialog box is overlaid on top. It displays the following details:

```
***** SOLUTION DEPLOYMENT *****
TEST-A4Q50UI8ZQ : http://test-a4q5oui8zq:34765/ : The solution was successfully deployed.
TEST-A4Q50UI8ZQ : http://test-a4q5oui8zq:25321/ : The solution was successfully deployed.
TEST-A4Q50UI8ZQ : http://test-a4q5oui8zq/ : The solution was successfully deployed.
```

Buttons for **Previous**, **Next**, and **Close** are visible at the bottom. The URL www.codeplex.com/sharepointinstaller is visible at the bottom left.

3RD Party Plugins

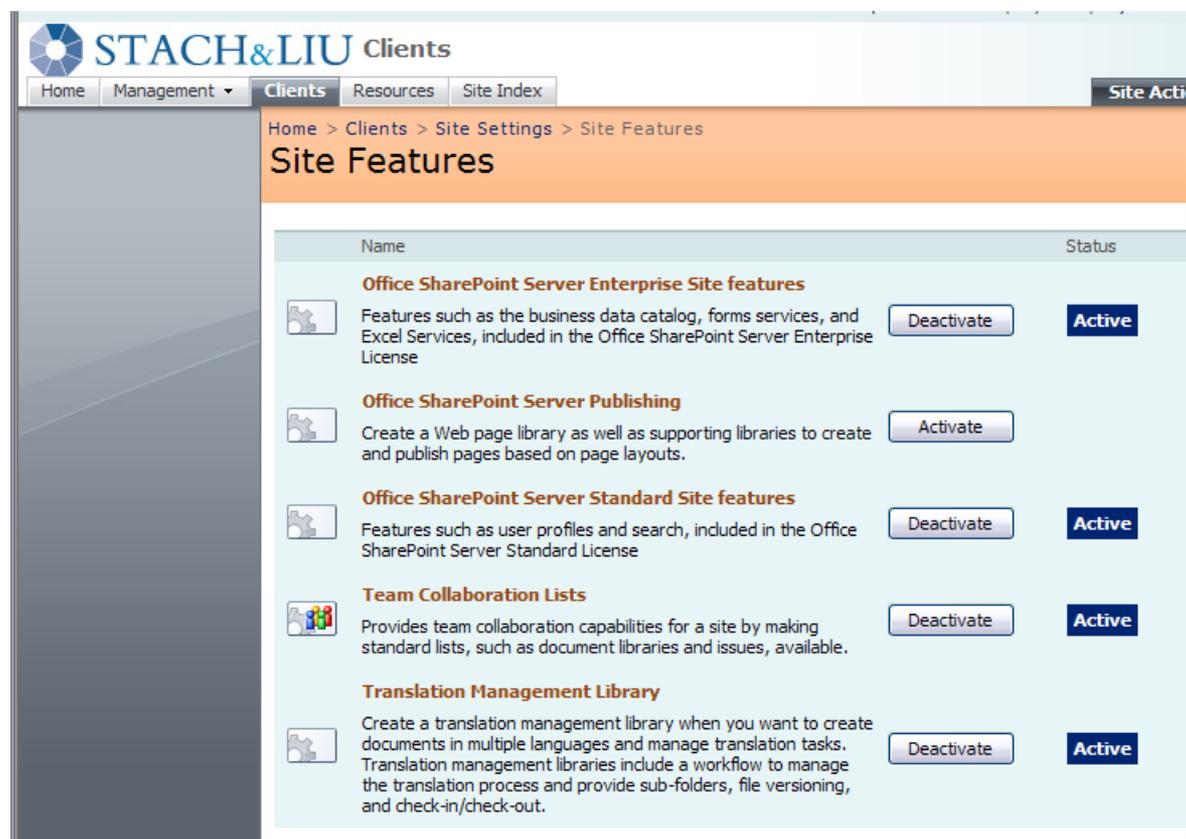
FEATURES

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 third-party plugins, each with a description, a 'Deactivate' button, and a status indicator (Active).

Name	Status
Access Checker Web Part Quickly check what objects within a Sharepoint site hierarchy a user has access to.	Deactivate Active
Bamboo Calendar Plus Web Part Add advanced calendaring display capabilities to a site with the Bamboo Calendar Plus Web Part.	Deactivate Active
Bamboo ListRollup WebPart Bamboo ListRollup WebPart	Deactivate Active
Bamboo World Clock And Weather Web Part Bamboo World Clock And Weather Web Part	Deactivate Active
Collect Signatures Workflow Gathers signatures needed to complete a Microsoft Office document.	Deactivate 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'.	Deactivate Active
Disposition Approval Workflow Manages document expiration and retention by allowing participants to decide whether to retain or delete expired documents.	Deactivate 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.	Deactivate Active

3RD Party Plugins

FEATURES



STACH&LIU Clients

Home Management Clients Resources Site Index Site Activ

Home > Clients > Site Settings > Site Features

Site Features

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

3RD Party Plugins

FUTURE SECURITY

- SharePoint 2010 has sandboxed solutions
- Minimize risk of running untrusted 3rd party plugins



SharePoint Customization Wizard

Specify the site and security level for debugging

What local site do you want to use for debugging?

What is the trust level for this SharePoint solution?

Deploy as a sandboxed solution
Clicking this option causes the solution to be deployed as a Sandboxed solution. Sandboxed solutions can be deployed by the site collection owner and are run in a secure, monitored process that has limited resource access.

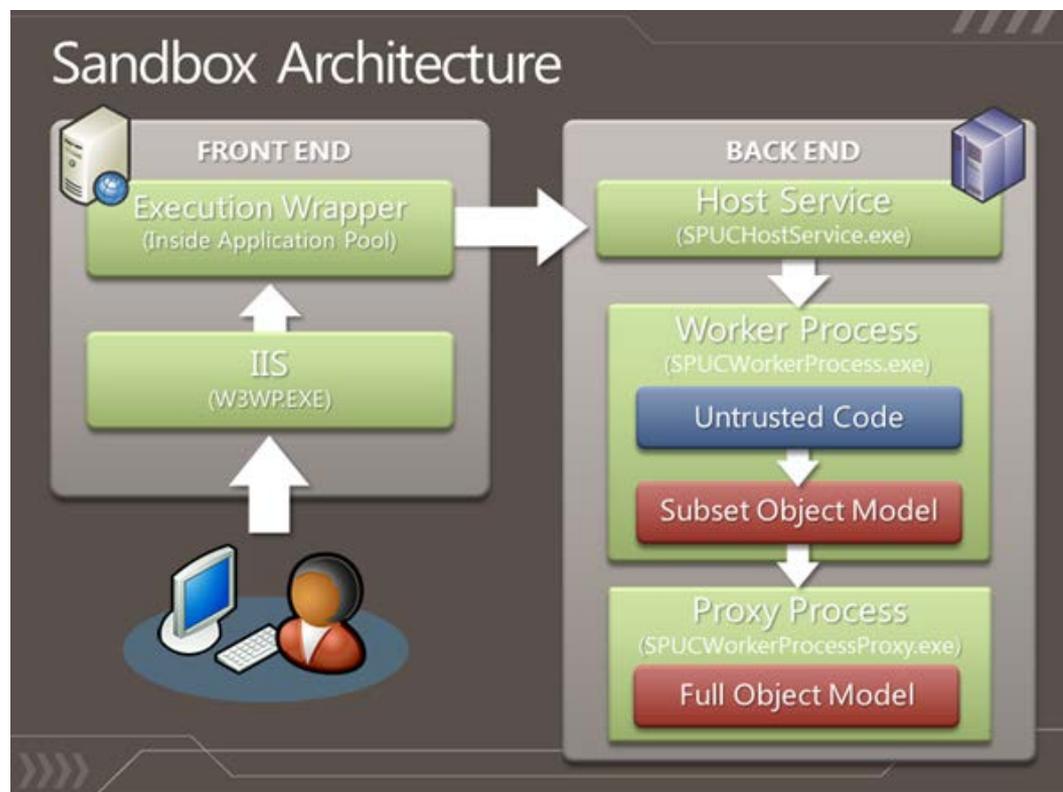
Deploy as a farm solution
Clicking this option means that users must have SharePoint administrator privileges to run or deploy the solution.

[Learn more about sandboxed solutions](#)

< Previous Next > **Finish** Cancel

3RD Party Plugins

SANDBOXED SOLUTIONS





Security Tip #5

BACKUP EVERY WHICH
WAY FROM SUNDAY



Backups

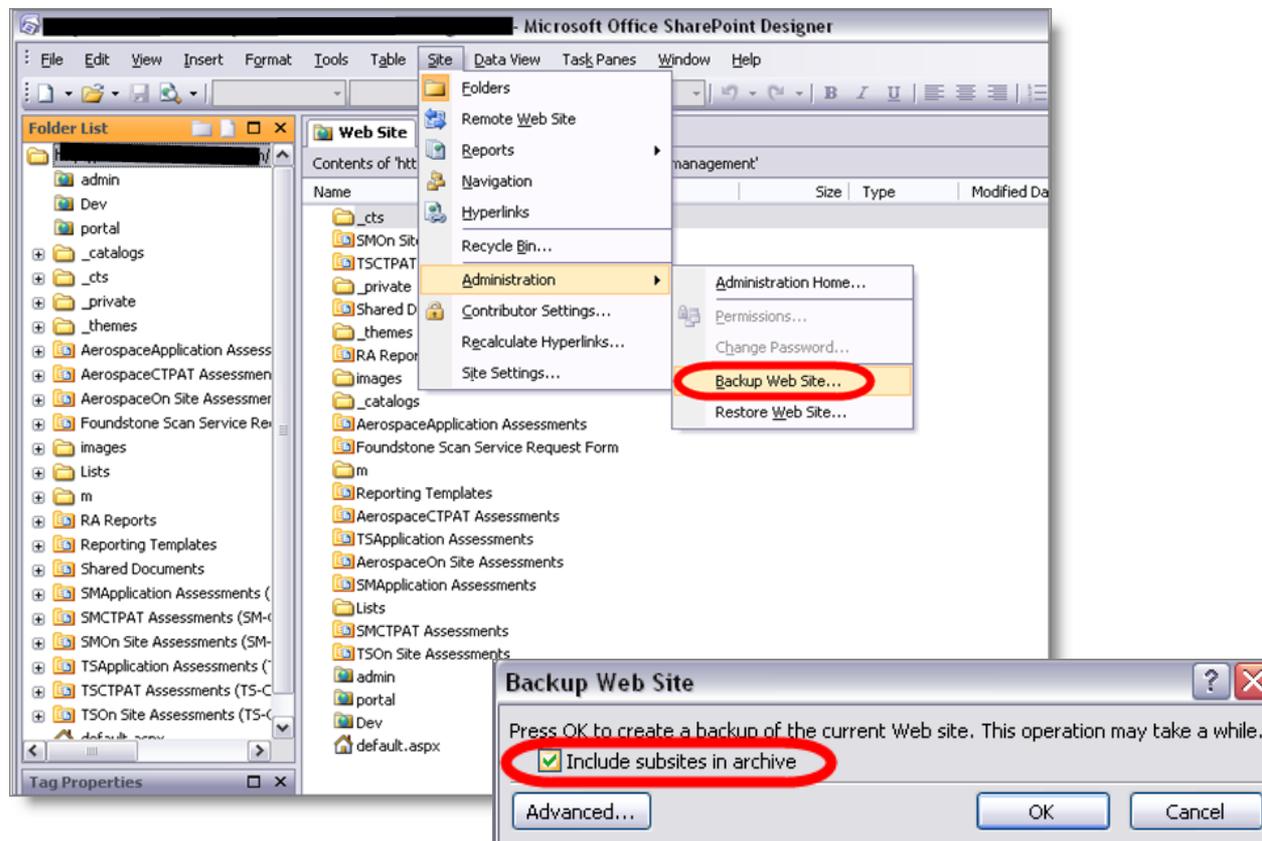
MANY METHODS ... MOST TERRIBLE

1. Microsoft System Center: Data Protection Manager
2. Windows 2003/2008 Server backups
3. Stsadm.exe cmdline tool backups
4. Central Administration v3 backups
5. SharePoint Designer backups
6. Site and List template backups
7. 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 displays the Central Administration web interface. The 'Operations' tab is selected and highlighted with a red circle. The main content area is titled 'Operations' and contains a list of links organized into 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

View All Site Content

Central Administration

- Operations
- Application Management

Shared Services Administration

- SharedServices1

Recycle Bin

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 number 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. The first, labeled 'Backup current site as a "site template"', points to the 'Save site as template' option in the 'Look and Feel' section. The second, labeled 'Manage site and list templates', points to the 'Site templates' and 'List templates' options in the 'Galleries' section.

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

- Site templates
- 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>

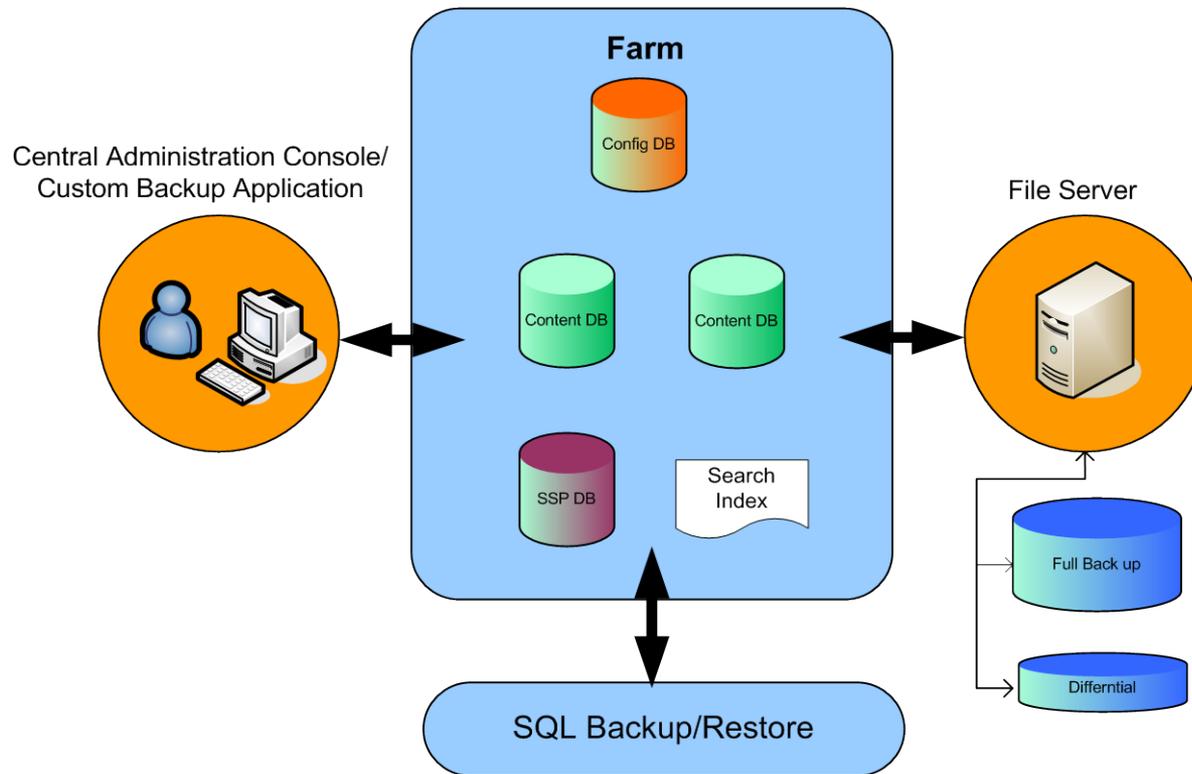
OK Cancel

Saves as single *.stp file

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

Backups

RAW SQL DATABASES



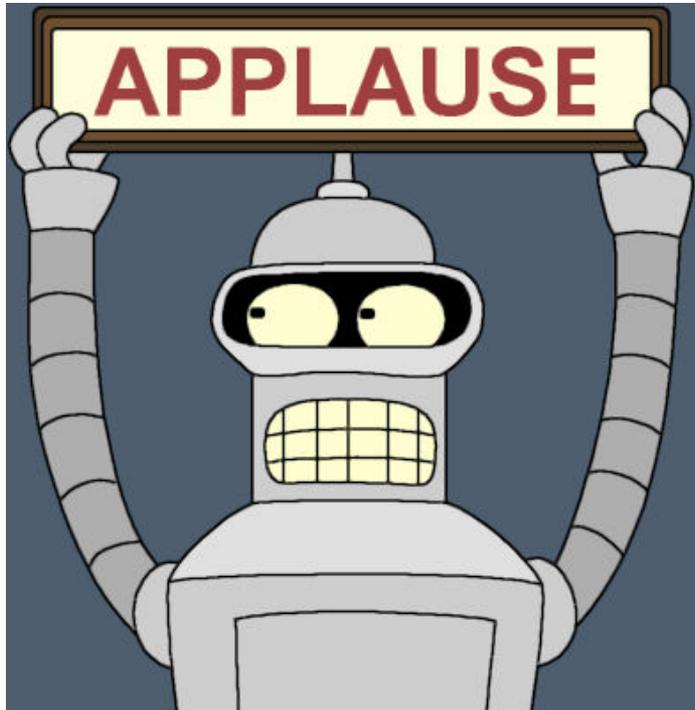


Questions?
Ask us something
We'll try to answer it.

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/>