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

![Diagram of SharePoint architecture](https://via.placeholder.com/150)

**Applications & Services**
- Collaboration
  - Doc Collab, Wikis
  - Discussions, blogs
  - Contacts/Cals/Tasks
  - E-mail integration
  - Outlook integration
  - Project mgmt. "Lite"
  - Offline lists/docs
- Portal
  - Intranet template
  - News, site dir
  - My sites
  - People finding
  - Social networking
  - Notifications
  - Targeting
- Search
  - Search center
  - Relevance
  - Biz data search
  - Metadata
  - Customizable UX
  - Extensibility
- Content Mgmt
  - Authoring
  - Workflow
  - Web publishing
  - Document mgmt
  - Records mgmt
  - Policies
  - Multi-language
- Biz Processes
  - Rich/WEB forms
  - Self-service forms
  - Real-time data val.
  - LOB integration
  - LOB actions
- BI
  - Report center
  - Excel services
  - Dashboards
  - KPIs
  - Biz data in lists
  - SQL/RS/AS Integ.

**Shared Services**
- Site model+
- Indexing+/Search+
- Business data catalog, alerts, user profiles,
  audiences, usage reporting, SSO

**Platform Services**
- Storage
  - Repository
  - Metadata
  - Versioning
  - Backup/Recycle bin
  - Indexing/search
- Security
  - Server policies
  - Pluggable auth
  - Folder/iam level
  - Rights trimmed UI
- Management
  - Admin UX
  - Delegation
  - Provisioning
  - Monitoring
- Deployment
  - Migration
  - Config mgmt
  - Farm services
  - Feature policy
  - Extranet support
- Site model
  - Templates
  - Rendering
  - Navigation
  - Consistent UX
- Extensibility
  - Forms/fields
  - OM and SOAP
  - Event handlers
  - Migration APIs

**Operating System Services**
- ASP.NET: Web parts, personalization, master pages, provider framework, (security, etc.)
  - Database services
  - Search services
  - Workflow services

*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
Security Tips
WHAT YOU SHOULD KNOW
WikiLeaks and SharePoint

RISK OF EXPOSURE

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

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
## Security Tips

### ONE POINT SECURITY

<table>
<thead>
<tr>
<th>#</th>
<th>Security Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Know your external exposure…</td>
</tr>
<tr>
<td>2</td>
<td>Beware of normal users with excessive access…</td>
</tr>
<tr>
<td>3</td>
<td>Spot check user permissions and inheritance…</td>
</tr>
<tr>
<td>4</td>
<td>Beware 3rd party plugins/code…BUT not too much…</td>
</tr>
<tr>
<td>5</td>
<td>Backup every which way from Sunday…</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>…</td>
</tr>
</tbody>
</table>
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

Central Administration on random high port number
External Exposure

GOOGLE HACKING SHAREPOINT

Google search results showing about 215,000 results for "all site content site:.com filetype:aspx". The search query is highlighted, and the search results are displayed, indicating the existence of many SharePoint pages.

215,000 "All Site Content" SharePoint pages
External Exposure

GOOGLE HACKING SHAREPOINT

About 98,300 results (0.21 seconds)

98,000 exposed SharePoint "Lists Web Service"
External Exposure

GOOGLE HACKING SHAREPOINT

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

BING HACKING SHAREPOINT

COMING SOON
External Exposure

SHODAN FOR SHAREPOINT

Using SHODAN to find SharePoint deployments

88.39.32.133

HTTP/1.0 401 Unauthorized
Content-Length: 1636
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
External Exposure

SHAREPOINT HACKING ALERTS

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/lt/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/MyTasks.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\>
Security Tip #2

BEWARE USERS WITH EXCESSIVE ACCESS
Excessive User Access

MORE THAN YOU BARGAINED FOR . . .

• Web Services examples
  • Admin.asmx
  • Permissions.asmx

• 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 description:

- 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

Site Security Management
- Manage Site Security
- Set Site Security
- Restore Default 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.

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

- 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:
- User: Test

<table>
<thead>
<tr>
<th>Users/Groups</th>
<th>Type</th>
<th>User Name</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove</td>
<td>VSS/Development</td>
<td>Administrator</td>
<td>Full Control</td>
</tr>
<tr>
<td>Remove</td>
<td>VSS/Development</td>
<td>Domain Admin</td>
<td>Full Control</td>
</tr>
<tr>
<td>Remove</td>
<td>Test Members</td>
<td>SharePoint Group</td>
<td>Contribute</td>
</tr>
<tr>
<td>Remove</td>
<td>User, Test</td>
<td>VSS/Development</td>
<td>Restricted Read</td>
</tr>
<tr>
<td>Add to List</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Set Security
Security Tools

User Permissions

Check User Access

Download Report

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. Updated on 01 Feb, 2019

Copy list permissions

Source list

Target list

Contacts

Copy ->

Contacts

Permissions on Lists/Libraries

<table>
<thead>
<tr>
<th>Groups</th>
<th>Group Owner</th>
<th>Default permission</th>
<th>Contacts</th>
<th>Content and Structure Reports</th>
<th>Documents</th>
<th>Events</th>
<th>Form Templates</th>
<th>FRANCE</th>
<th>Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Members</td>
<td>Home Members</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Read</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
</tr>
<tr>
<td>Home Owners</td>
<td>Home Owners</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Read</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
</tr>
<tr>
<td>Home Owners</td>
<td>Home Owners</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Read</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
</tr>
<tr>
<td>Home Owners</td>
<td>Home Owners</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
</tr>
</tbody>
</table>

Copy page permissions

Source page

Default.aspx

Copy ->

Default.aspx

Permissions on Pages

<table>
<thead>
<tr>
<th>Groups</th>
<th>Pages</th>
<th>Themes</th>
<th>News</th>
<th>Resources</th>
<th>Finance</th>
<th>Site</th>
<th>User Information</th>
<th>Site Administration</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Members</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
<td>Contribute</td>
</tr>
<tr>
<td>Home Owners</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
<td>Full Control</td>
</tr>
<tr>
<td>Home Visitors</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
</tr>
</tbody>
</table>

Set permissions

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

USER PERMISSIONS

Security Reports

Group Membership for User TEST-A4Q50UI8ZQ\admin

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
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
Detect Rogue SharePoint

ROGUE DEPLOYMENTS

McAfee - Network Discovery for Microsoft SharePoint
### 3RD Party Plugins

#### Solution Management

This page has a list of the Solutions in the farm.

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Deployed To</th>
</tr>
</thead>
<tbody>
<tr>
<td>accesscheckerwebpart.wsp</td>
<td>Deployed</td>
<td><a href="http://test-a4q5oui8zq:34765/">http://test-a4q5oui8zq:34765/</a>,...</td>
</tr>
<tr>
<td>smarttools.enhancedsiteactions_v1_1.wsp</td>
<td>Deployed</td>
<td><a href="http://test-a4q5oui8zq:34765/">http://test-a4q5oui8zq:34765/</a>,...</td>
</tr>
</tbody>
</table>
3RD Party Plugins

SOLUTIONS

The Expert Calendar

System Check
Checking if The Expert Calendar can be installed from this machine

- 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.

Installation Successfully Completed

Details:

All checks succeeded. Please continue with installation.

www.codeplex.com/sharepointinstaller
3\textsuperscript{rd} Party Plugins

### Site Collection Features

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Checker Web Part</td>
<td>Active</td>
</tr>
<tr>
<td>Quickly check what objects within a Sharepoint site hierarchy a user has access to.</td>
<td></td>
</tr>
<tr>
<td>Bamboo Calendar Plus Web Part</td>
<td>Active</td>
</tr>
<tr>
<td>Add advanced calendaring display capabilities to a site with the Bamboo Calendar Plus Web Part.</td>
<td></td>
</tr>
<tr>
<td>Bamboo ListRollup WebPart</td>
<td>Active</td>
</tr>
<tr>
<td>Bamboo World Clock And Weather Web Part</td>
<td>Active</td>
</tr>
<tr>
<td>Bamboo World Clock And Weather Web Part</td>
<td>Active</td>
</tr>
<tr>
<td>Collect Signatures Workflow</td>
<td>Active</td>
</tr>
<tr>
<td>Gathers signatures needed to complete a Microsoft Office document.</td>
<td></td>
</tr>
<tr>
<td>Content by Type and Filter Web Parts</td>
<td>Active</td>
</tr>
<tr>
<td>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'.</td>
<td></td>
</tr>
<tr>
<td>Disposition Approval Workflow</td>
<td>Active</td>
</tr>
<tr>
<td>Manages document expiration and retention by allowing participants to decide whether to retain or delete expired documents.</td>
<td></td>
</tr>
<tr>
<td>Enhanced Content Query Web Part</td>
<td>Active</td>
</tr>
<tr>
<td>Provides the same functionality that the regular content query web part gives, with some added bonuses such as context menus per item support.</td>
<td></td>
</tr>
</tbody>
</table>
3rd Party Plugins

Features

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

Office SharePoint Server Publishing
Create a Web page library as well as supporting libraries to create and publish pages based on page layouts.

Office SharePoint Server Standard Site features
Features such as user profiles and search, included in the Office SharePoint Server Standard License

Team Collaboration Lists
Provides team collaboration capabilities for a site by making standard lists, such as document libraries and issues, available.

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 workflows to manage the translation process and provide sub-folders, file versioning, and check-in/check-out.
3\textsuperscript{RD} Party Plugins

**FUTURE SECURITY**

- SharePoint 2010 has sandboxed solutions
- Minimize risk of running untrusted 3\textsuperscript{rd} party plugins
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
Backups

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

SITE AND LIST TEMPLATES

Backup current site as a "site template"

Manage site and list templates
Backups

Save Site as Template

File Name
Enter the name for this template file.

Template Name:
Site Backup

Template Description:

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.

Saves as single *.stp file
Can opt to include content (e.g., files, list items, etc.)
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: