SharePoint Security

Advanced SharePoint Security Tips and Tools

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

OWASP
The Open Web Application Security Project

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

STACH&LIU

Agenda

- Brief Intro to SharePoint
  - Overview of Major Components

- SharePoint Security
  - Security Tips and Tools

STACH&LIU

Background

GETTING UP TO SPEED

STACH&LIU

Background

MS SharePoint Products & Technologies

- Windows SharePoint Services (WSS)

- Office SharePoint Server 2007/2010 (MOSS)
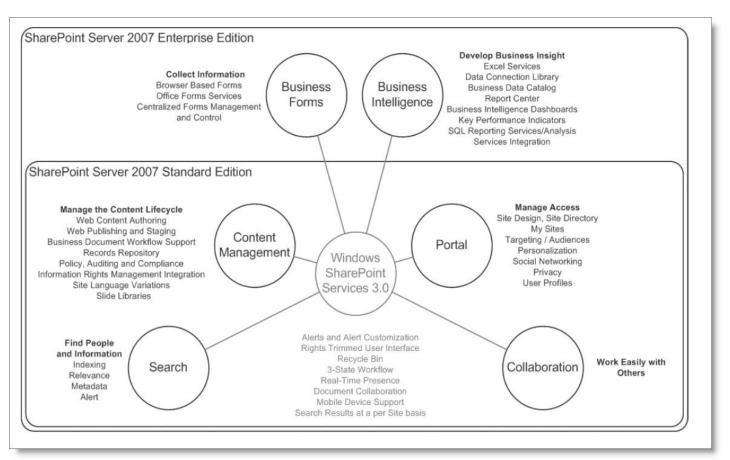
- SharePoint Designer 2007/2010 (SPD)
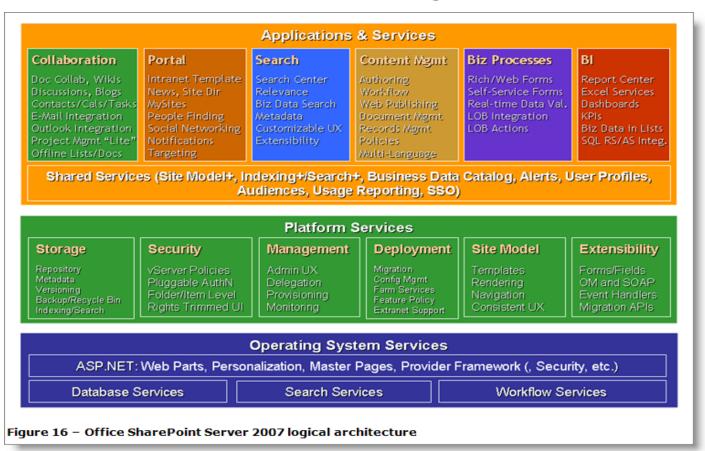
STACH&LIU

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

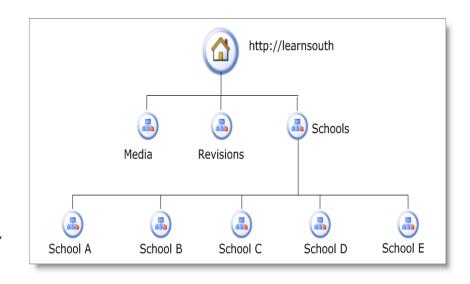**Figure 1-6**   Site collections are a structured collection of sites.

STACH&LIU

SharePoint Site Hierarchy

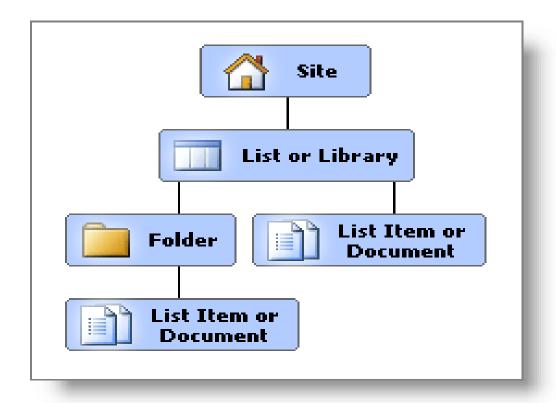Intro to SharePoint

Base Site URLs:

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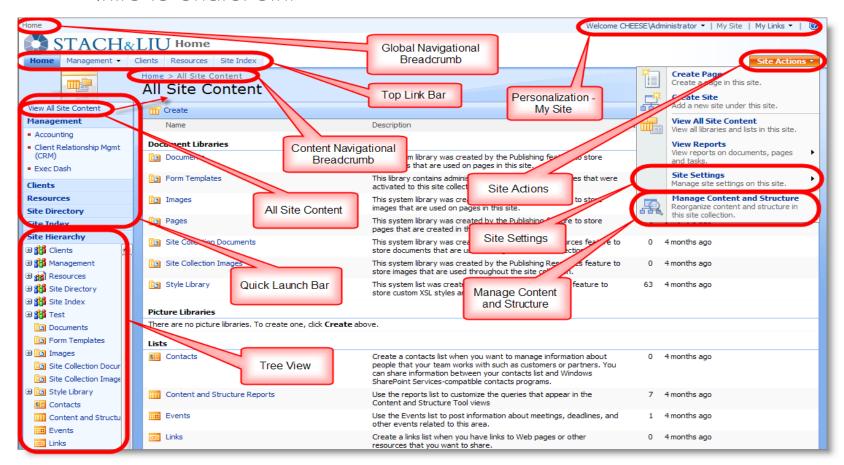- http://learnsouth/Schools/SchoolC/

Site Structure

Intro to SharePoint

Site Navigation

Intro to SharePoint

Security Tips

WHAT YOU SHOULD KNOW

STACH&LIU

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

STACH&**LIU**

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 3rd party plugins/code…BUT not too much…
5	Backup every which way from Sunday…
	…

STACH&LIU

Security Tip #1

KNOW YOUR EXTERNAL EXPOSURE

STACH&LIU

External Exposure

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)

STACH&LIU

External Exposure

SHAREPOINT ADMIN WEB APPS

External Exposure

GOOGLE HACKING SHAREPOINT

215,000 "All Site Content" SharePoint pages

STACH&LIU

External Exposure

GOOGLE HACKING SHAREPOINT

External Exposure

External Exposure

BING HACKING SHAREPOINT

External Exposure

SHODAN FOR SHAREPOINT

External Exposure

SHAREPOINT HACKING ALERTS

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

STACH&LIU

Security Tip #2

BEWARE USERS WITH EXCESSIVE ACCESS

STACH&LIU

Excessive User Access

- Web Services examples
  - Admin.asmx
  - Permissions.asmx

- User Administration examples
  - "People and Groups"
  - "Add Users"
  - "PeoplePicker"

STACH&LIU

CONTINUED SHAREPOINT HACKING

DEMO

Excessive User Access

SHAREPOINT WEB SERVICES

Security Tip #3

CHECK PERMISSIONS AND INHERITANCE

STACH&LIU

User Permissions

User Permissions

User Permissions

SECURITY TIPS

Security Tools

USER PERMISSIONS

Security Tools

USER PERMISSIONS

Security Tools

USER PERMISSIONS

Security Tools

USER PERMISSIONS

Security Tools

USER PERMISSIONS

Security Tip #4

BEWARE 3RD PARTY CODE...NOT TOO MUCH

STACH&LIU

3RD Party Plugins

NECESSARY EVIL

- SharePoint without 3rd party plugins is like an iPhone with no apps
  - Solutions, Features
  - Web Parts, Templates

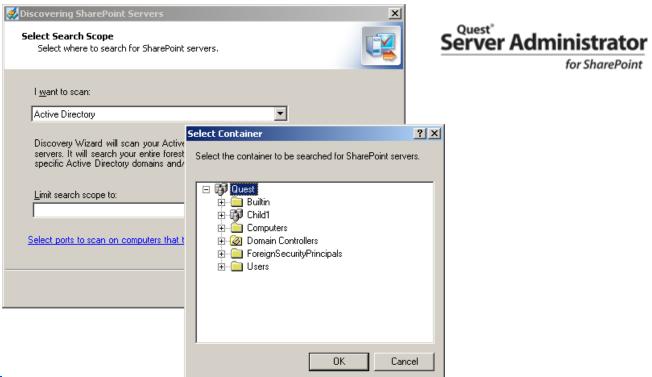- If too strict, people will circumvent you
  - Leads to rogue SharePoint deployments

Detect Rogue SharePoint

ROGUE DEPLOYMENTS

Quest Software - Server Administrator for SharePoint
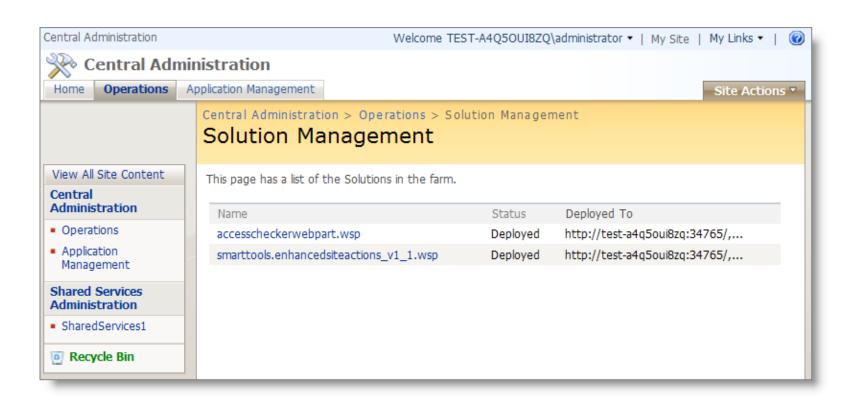
Detect Rogue SharePoint

ROGUE DEPLOYMENTS

McAfee - Network Discovery for Microsoft SharePoint

3RD Party Plugins

SOLUTIONS

3RD Party Plugins

SOLUTIONS
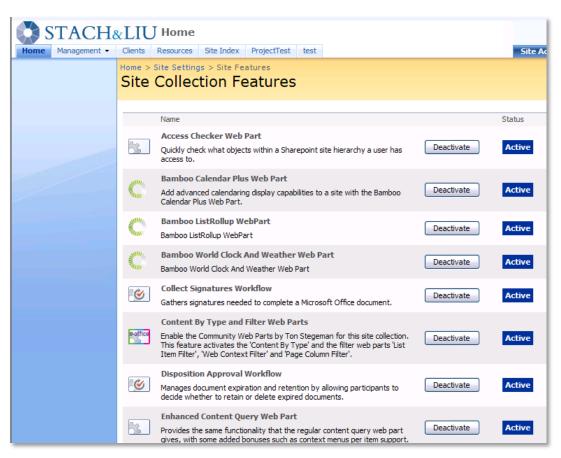
3RD Party Plugins

FEATURES

3RD Party Plugins

FEATURES

3RD Party Plugins
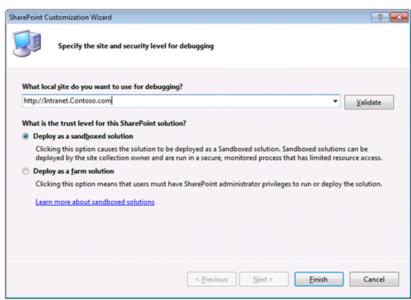
FUTURE SECURITY

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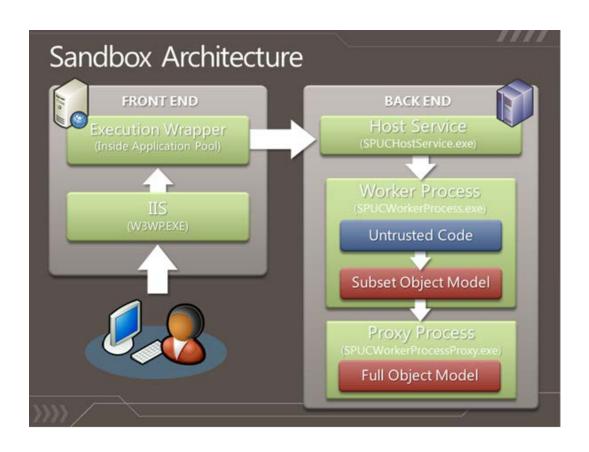
- Minimize risk of running untrusted 3rd party plugins

3RD Party Plugins

SANDBOXED SOLUTIONS

Security Tip #5
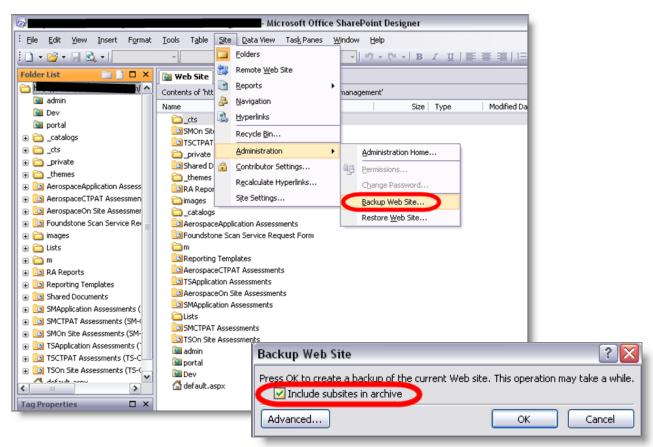
BACKUP EVERY WHICH
WAY FROMSUNDAY

STACH&LIU

Backups

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

STACH&LIU

Backups

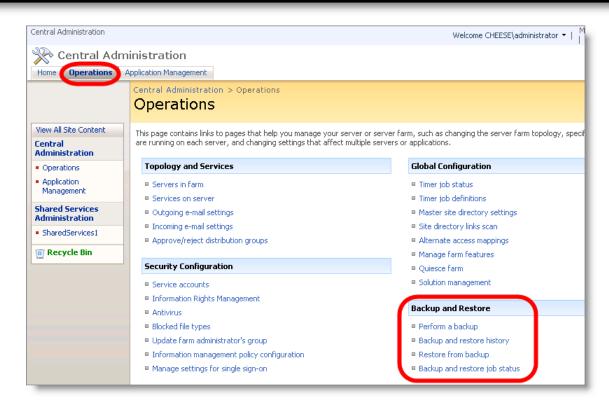## SHAREPOINT DESIGNER

Backups

STSADM / CENTRAL ADMINISTRATION

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

Backups

SITE AND LIST TEMPLATES

Backups

S I T E   A N D   L I S T   T E M P L A T E S

STACH&LIU
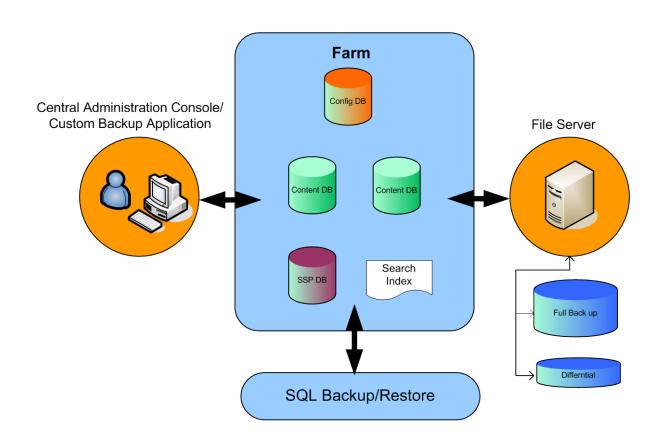
Backups

RAW SQL DATABASES

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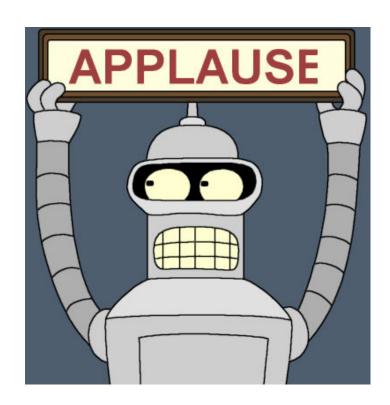# Ask us something
We'll try to answer it.

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

STACH&LIU

Thank You

Stach & Liu SharePoint Hacking Diggity Project info:
http://www.stachliu.com/index.php/resources/tools/sharepoint-hacking-diggity-project/

STACH&LIU