OWASP
Open Web Application Security Project

OWASP Stammtisch #12

Frankfurt, 29.01.2014

Jan Philipp
Manager, Cyber Risk Services

Getting a handle on SharePoint Security

(SharePoint Sicherheit im “schlüpfrigen” Griff)

Purpose today

Introduction

- » Who I am (http://archimatrix.com/jphilipp)
- » Why this topic: SharePoint security
- » Goals and agenda of this presentation
- » What is SharePoint what can it do
- » What SharePoint security information already exists

Purpose today

Agenda

- » Introducing the SharePoint security model
  The company-defender/admin/architect view
- » Applying the SharePoint security model
  The vendor/default configuration reality
- » So how does this security hold up?
  The pen-tester/auditor/attacker view
- » Extending SharePoint
  The features that can kill you

Microsoft SharePoint

So what is this SharePoint?

» SharePoint is a Platform with many Web-parts to rapidly share data and create work-flows for teams on Web-Sites

» According to the vendor: **It does everything!**

Communities
Composites
Content
Search
Insights

Sites
Composites
Communities
Microsoft SharePoint
Insights
Content
Search

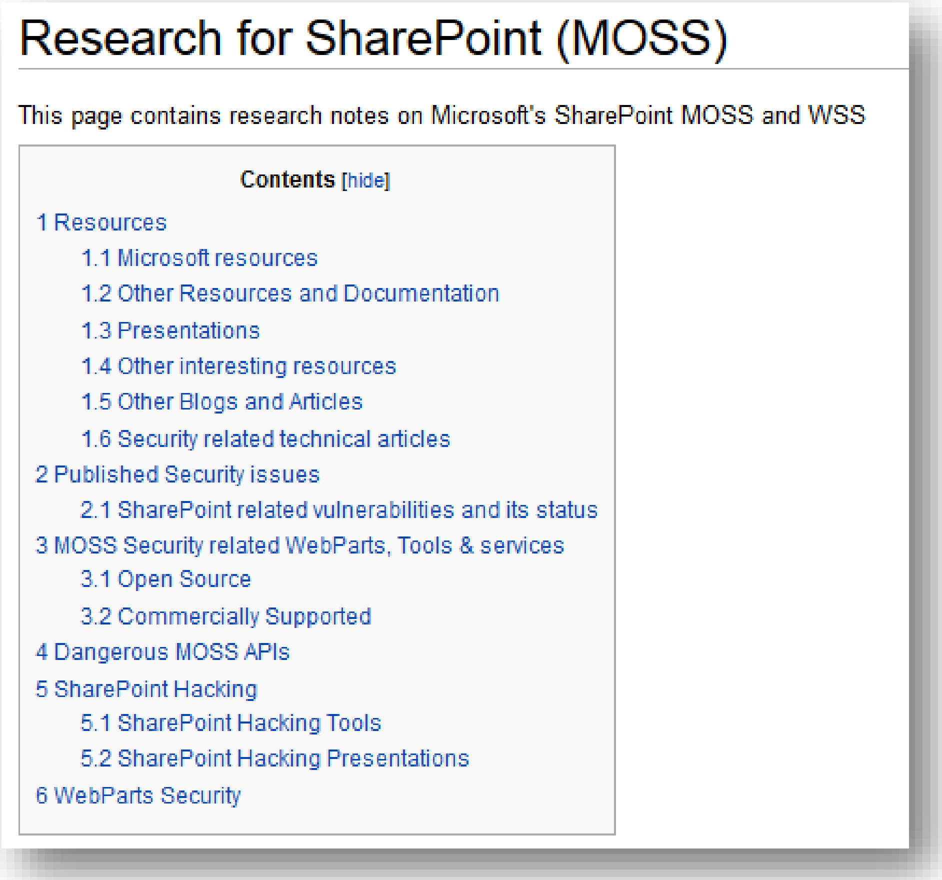
Business Intelligence
Office Services
(Social) mySites
SharePoint Designer
SharePoint 2013 Store

http://sharepoint.microsoft.com/de-de/product/capabilities/Seiten/default.aspx

Existing attacking knowledge

What SharePoint security information already exists

- » Technet & **OWASP**
- » A link collection, not more
- » Many gaps
- » Based on SP 2003/2007 (Many vulnerabilities are fixed in SP 2010/2013)
- » Missing presentations



Research for SharePoint (MOSS)

This page contains research notes on Microsoft's SharePoint MOSS and WSS

Contents [hide]

1 Resources
  1.1 Microsoft resources
  1.2 Other Resources and Documentation
  1.3 Presentations
  1.4 Other interesting resources
  1.5 Other Blogs and Articles
  1.6 Security related technical articles
2 Published Security issues
  2.1 SharePoint related vulnerabilities and its status
3 MOSS Security related WebParts, Tools & services
  3.1 Open Source
  3.2 Commercially Supported
4 Dangerous MOSS APIs
5 SharePoint Hacking
  5.1 SharePoint Hacking Tools
  5.2 SharePoint Hacking Presentations
6 WebParts Security

Source: https://www.owasp.org/index.php/Research_for_SharePoint_%28MOSS%29

The SP Security Model

Security Building Blocks

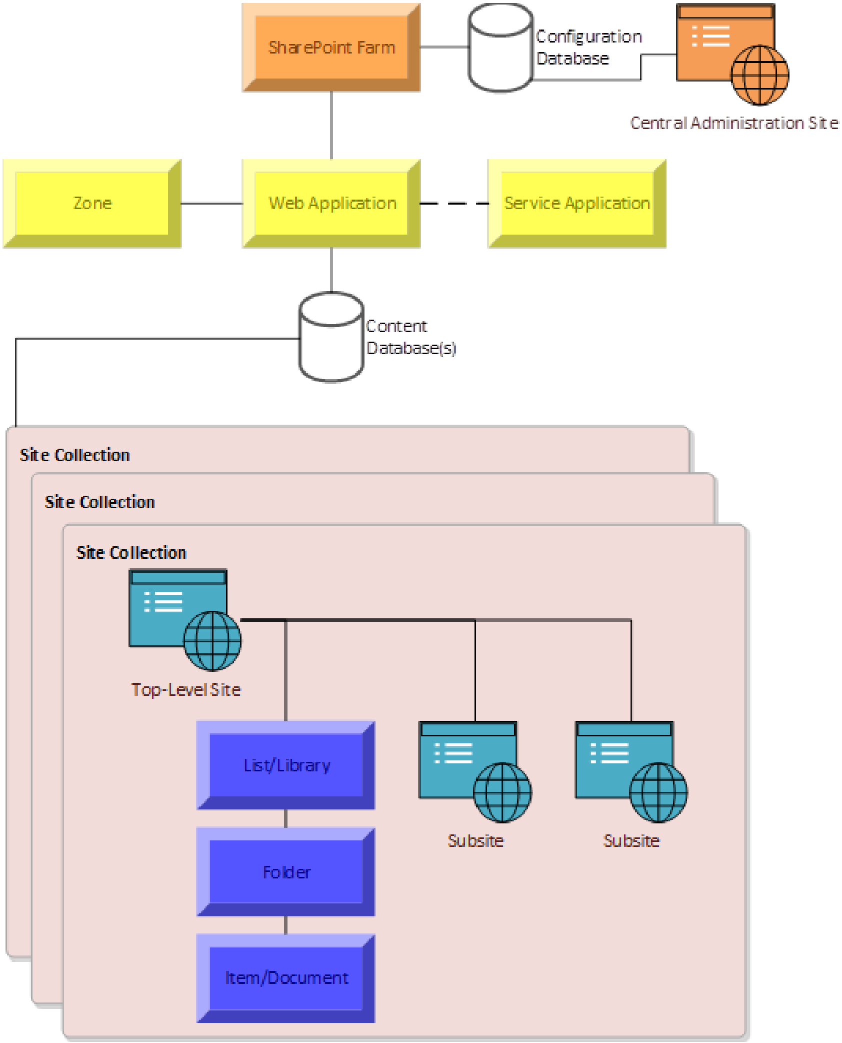
Classic Security

SharePoint Specifics

SharePoint security elements

SharePoint hierarchy of objects

- » Central Administration Site
- » Web/Service applications
  (Zones, if multiple URLs)
- » Site Collections
- » Sites
- » Site components



SharePoint separation of duties

Separate administration (for humans) should be set at:

- Central Administration site (IT: farm admins)
- Web-application level (IT: application owners & dev)
- Site-collection level (Business: site-collection owners)
- Site-level (Business: site-owners)

Separate (technical) accounts must be used for:

- The systems farm management
- Key farm services (crawl, search, timer, …)
- Cross system authentication (IIS app-pools, WOPI, …)

Avoid breaking inheritance !

The classic security model

The “A - G, (U), L ← P" security model

- **Accounts** in the Domain, organized
  by Domain Admins
  into **Global Groups**
- **Global Groups** organized
  by Enterprise Admins
  into **Universal Groups**
- **U**niversal Groups or **Global Groups** organized
  by Resource Admins
  into **Local Groups** (Resource Groups)
- The Local Groups are added to ACLs
  and **Permissions** are assigned by the resource admins

SP security best-practices

Applying the classic user access model to SharePoint

» SharePoint Groups = the locale Resource Groups
  Define these at the site-collection

» SharePoint is an RBAC (role based) model:
  Define the permissions per SharePoint group

Don’t put users in SharePoint groups!

Don’t assign permissions to AD Groups or users!

Service & connection accounts

» Have them! – before you start installing!

SP security best-practices

Easy on paper but…

- Farm Application access is often overlooked:

  Farm Admin, Server Admin, AD Domain Admins (CA Site)

- Service account/managed accounts issues

  Windows managed ≠ SharePoint managed

  They don’ t work everywhere

- Different authentication methods:

  Windows Native authentication

  Claims Based authentication ← The Best

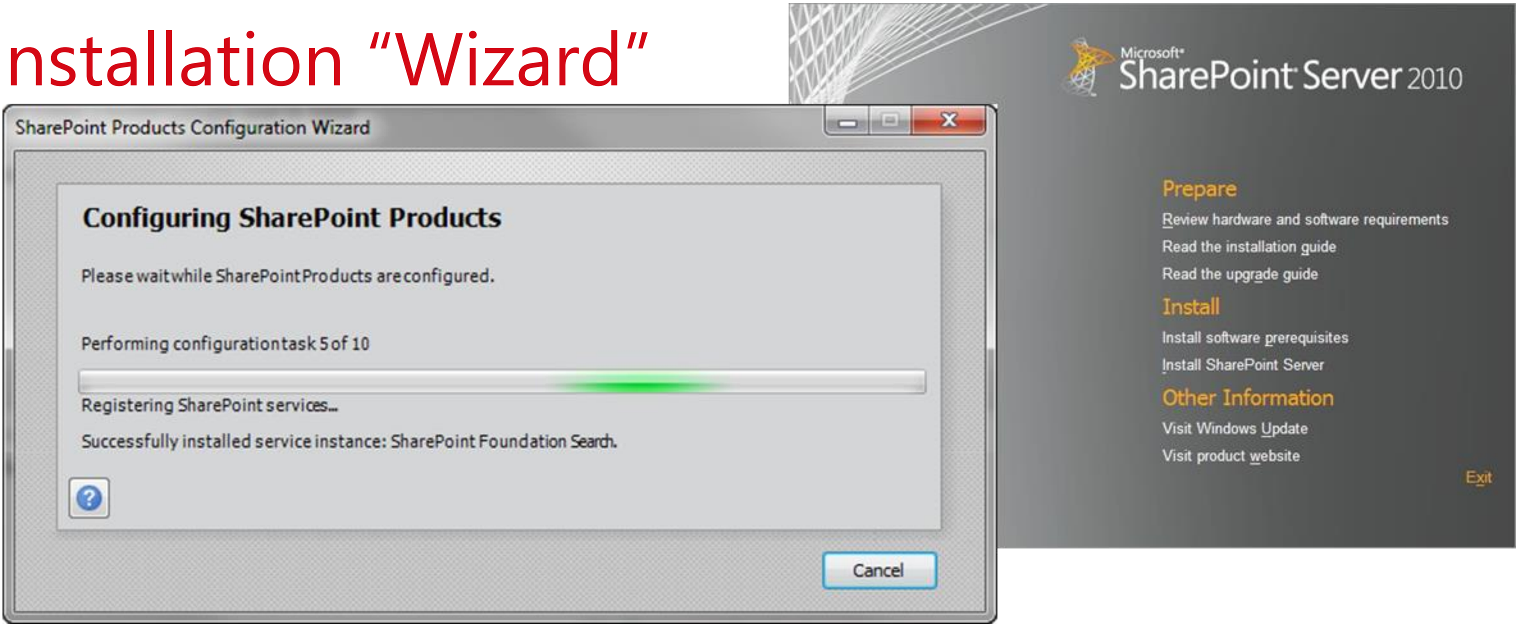
  Federated authentication

Applying the Model

Only easy in theory

So what happens in reality

Default installation "Wizard"



SharePoint Products Configuration Wizard

Configuring SharePoint Products

Please wait while SharePoint Products are configured.

Performing configuration task 5 of 10

Registering SharePoint services...

Successfully installed service instance: SharePoint Foundation Search.

Cancel
Microsoft® SharePoint Server 2010
Prepare
Review hardware and software requirements
Read the installation guide
Read the upgrade guide
Install
Install software prerequisites
Install SharePoint Server
Other Information
Visit Windows Update
Visit product website
Exit

- What happened in the background:
  - The powerful farm account is used for everything
  - MySites with auto creation and search is installed
  - Standard search and crawl is installed and configured
  - The SharePoint Designer is enabled
  - Legacy protocols (CGI, ISAPI, ...) are turned on

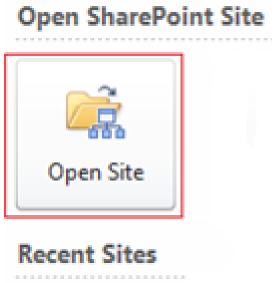
Common permission pitfalls

Default installation “Wizard” worked like a charm

- So how have we exploited this:

  Compromising one site can be used to gain access to all other sites in the farm because of the farmAdmin account

  The SharePoint Designer (FrontPage) is enabled http://www.microsoft.com/de-de/download/details.aspx?id=16573 free download and free access as authenticated users



Common permission pitfalls

Default installation "Wizard" worked like a charm

» But wait, you also get these attack surfaces:

Legacy features can be exploited:

- Did you know that if ISAPI can't process a request it passes it to the host Windows machine with built-in SYSTEM credentials ☺

Passwords are also passed in clear text (HTTP) from the Central Administration-site, when configuring services (Hey they put a warning on it)

Creepy crawlies – default search

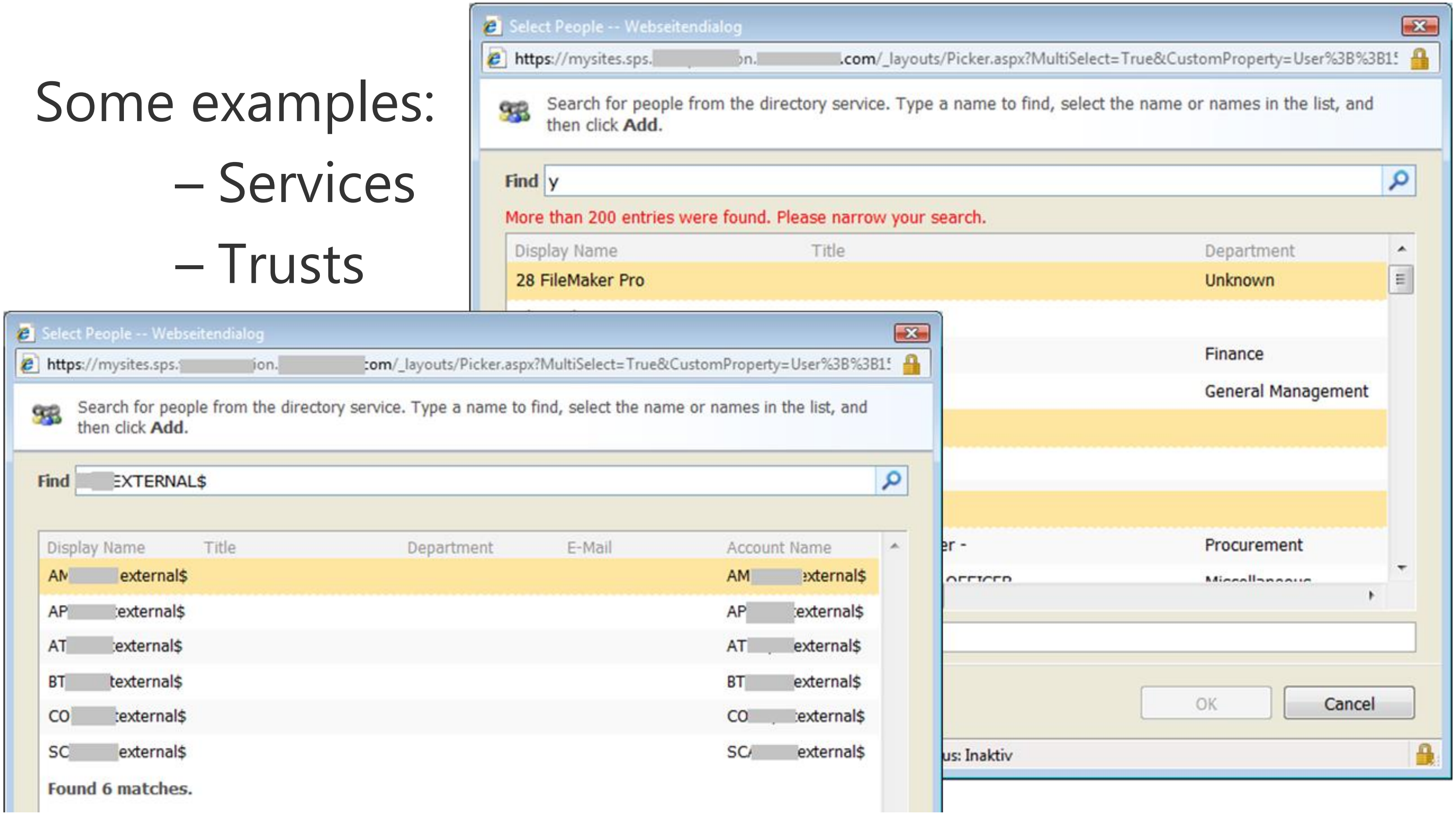
Enumerating your entire Active Directory

- You can read trusts, domains and accounts with the powerful built in search features!
- So you 'scoped' your People-Picker control – there are many URL's that get to one of the nine search components!
- So what, here's what it means:
  - We found the RID-500 built-in administrator, used for about 82% of all AD attacks
  - We found blank template accounts with default accounts that allowed us to gain access to systems
  - We found forest trust to test domains with weak security and could gain access to production AD

Creepy crawlies – default search

SharePoint search: What it shouldn't look like

- » Finding hidden accounts ($) – Yes you can!
- » Some examples:
  - – Services
  - – Trusts



Select People -- Webseitendialog

https://mysites.sps.[redacted]n.[redacted].com/_layouts/Picker.aspx?MultiSelect=True&CustomProperty=User%3B%3B15

Search for people from the directory service. Type a name to find, select the name or names in the list, and then click **Add**.

Find y

More than 200 entries were found. Please narrow your search.

Display Name	Title	Department
28 FileMaker Pro		Unknown
		Finance
		General Management
	er -	Procurement
	OFFICER	Miscellaneous

us: Inaktiv

Select People -- Webseitendialog

https://mysites.sps.[redacted]ion.[redacted]com/_layouts/Picker.aspx?MultiSelect=True&CustomProperty=User%3B%3B15

Search for people from the directory service. Type a name to find, select the name or names in the list, and then click **Add**.

Find [redacted]EXTERNAL$

Display Name	Title	Department	E-Mail	Account Name
AM[redacted]external$				AM[redacted]external$
AP[redacted]external$				AP[redacted]external$
AT[redacted]external$				AT[redacted]external$
BT[redacted]texternal$				BT[redacted]external$
CO[redacted]external$				CO[redacted]external$
SC[redacted]external$				SC[redacted]external$

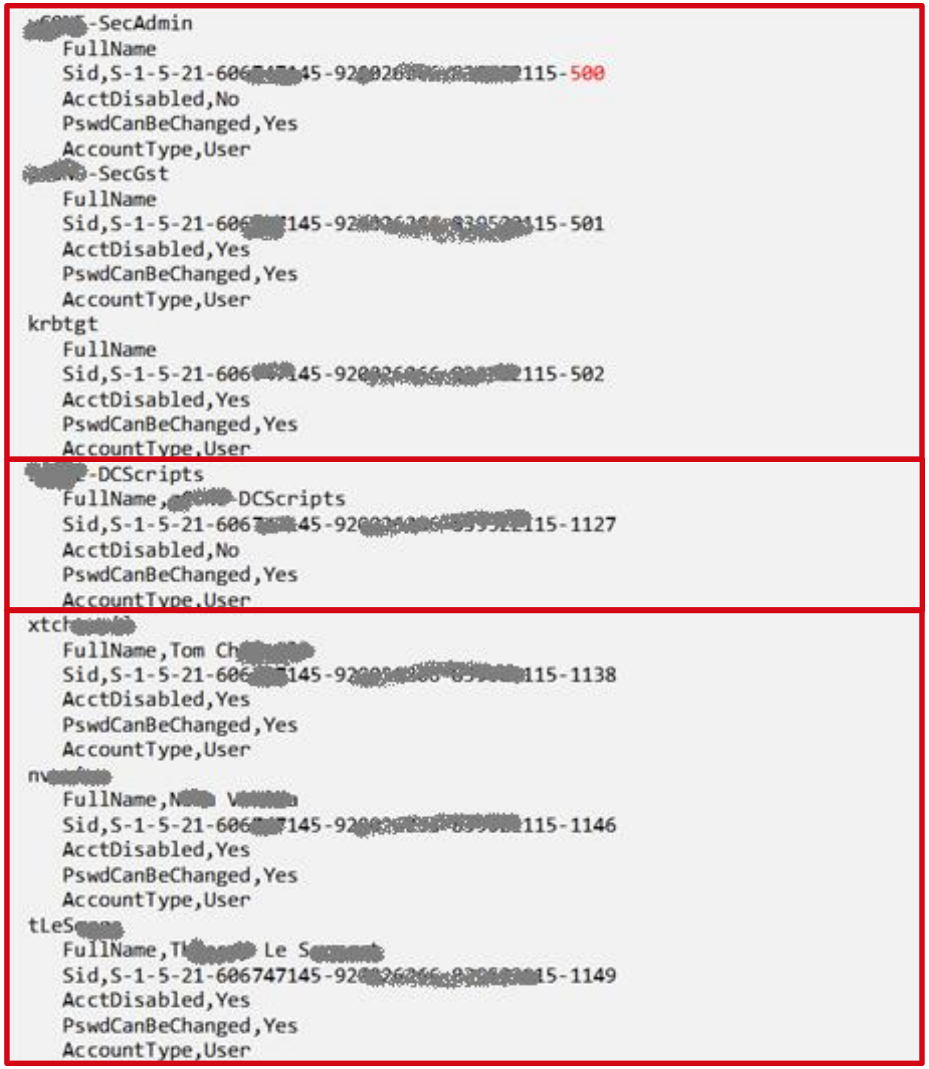
Found 6 matches.

Creepy crawlies – default search

SharePoint search:

What it shouldn’t look like

- Even more details are possible:
  - Built-in accounts
  - Service accounts
  - User accounts



```
[redacted]-SecAdmin
    FullName
    Sid,S-1-5-21-606[redacted]45-92[redacted]115-500
    AcctDisabled,No
    PswdCanBeChanged,Yes
    AccountType,User
[redacted]-SecGst
    FullName
    Sid,S-1-5-21-606[redacted]145-92[redacted]115-501
    AcctDisabled,Yes
    PswdCanBeChanged,Yes
    AccountType,User
krbtgt
    FullName
    Sid,S-1-5-21-606[redacted]145-92[redacted]115-502
    AcctDisabled,Yes
    PswdCanBeChanged,Yes
    AccountType,User
[redacted]-DCScripts
    FullName,[redacted]-DCScripts
    Sid,S-1-5-21-606[redacted]45-92[redacted]115-1127
    AcctDisabled,No
    PswdCanBeChanged,Yes
    AccountType,User
xtch[redacted]
    FullName,Tom Ch[redacted]
    Sid,S-1-5-21-606[redacted]145-92[redacted]115-1138
    AcctDisabled,Yes
    PswdCanBeChanged,Yes
    AccountType,User
nv[redacted]
    FullName,N[redacted] V[redacted]
    Sid,S-1-5-21-606[redacted]145-92[redacted]115-1146
    AcctDisabled,Yes
    PswdCanBeChanged,Yes
    AccountType,User
tLeS[redacted]
    FullName,Th[redacted] Le S[redacted]
    Sid,S-1-5-21-606747145-92[redacted]15-1149
    AcctDisabled,Yes
    PswdCanBeChanged,Yes
    AccountType,User
```

The trouble with marketing

Default features are also on

- SharePoint Social
  - Share and Follow
  - MySites auto-creation
  - Like (even on the Central Administration)

- SharePoint Designer Access
  - Yes it’s FrontPage IIS-Server extensions again

Turn them off – and not just at the GUI layer!

How does it hold up?

Tools

Webservices

WebDAV, CAML, …

Let’s test SharePoint…

Tools

- Predicable resources and information leaks

  Use your favourite Proxy (BurpSuite/Zap …) with fuzzdb

Other tools do not work well

or are they just

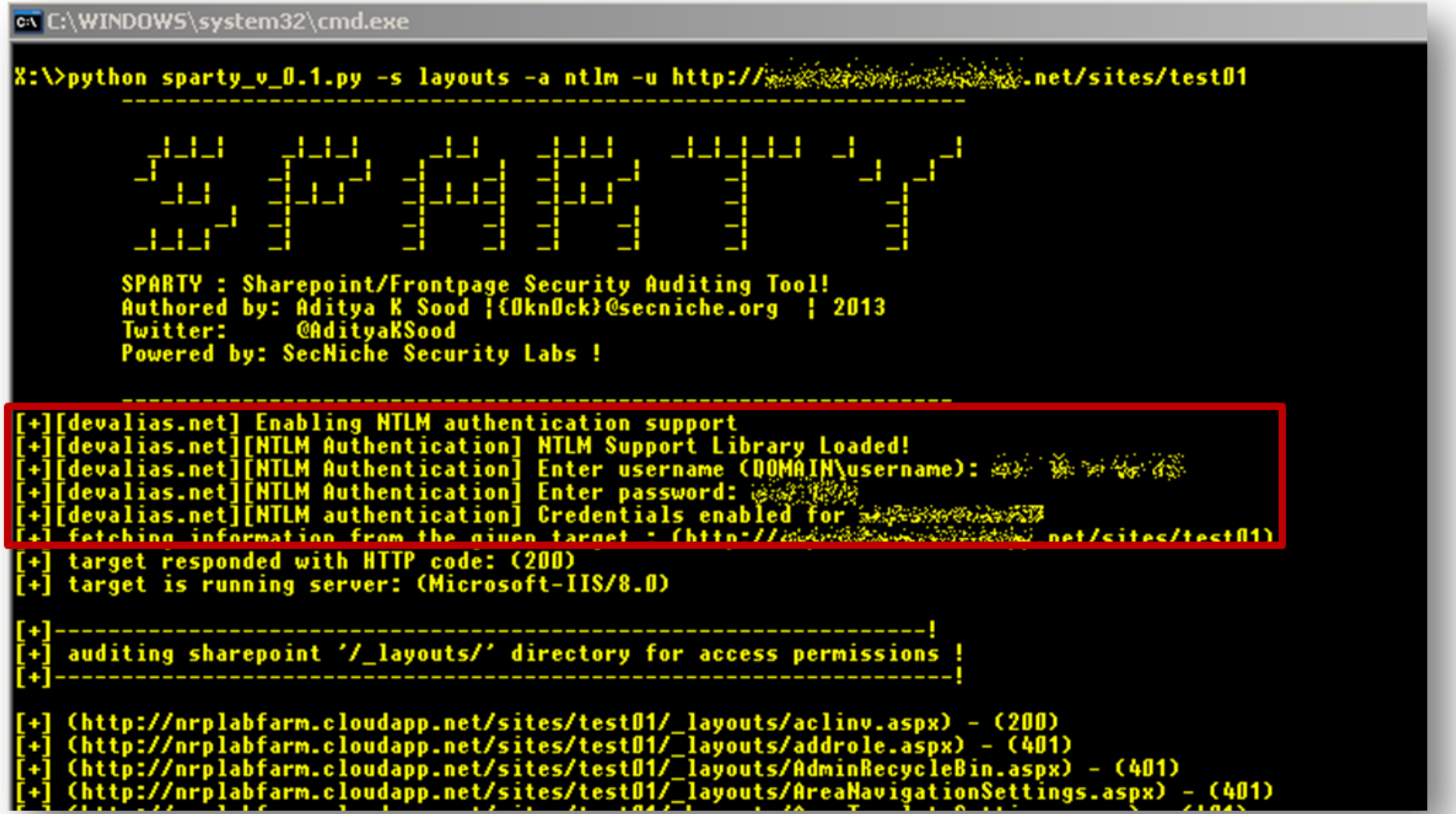
script-kiddie safe?

Tools for testing SharePoint

Audit Tool

» **Sparty** – MS SharePoint and FrontPage auditing tool

For NTLM support use unofficial patch https://github.com/alias1/sparty



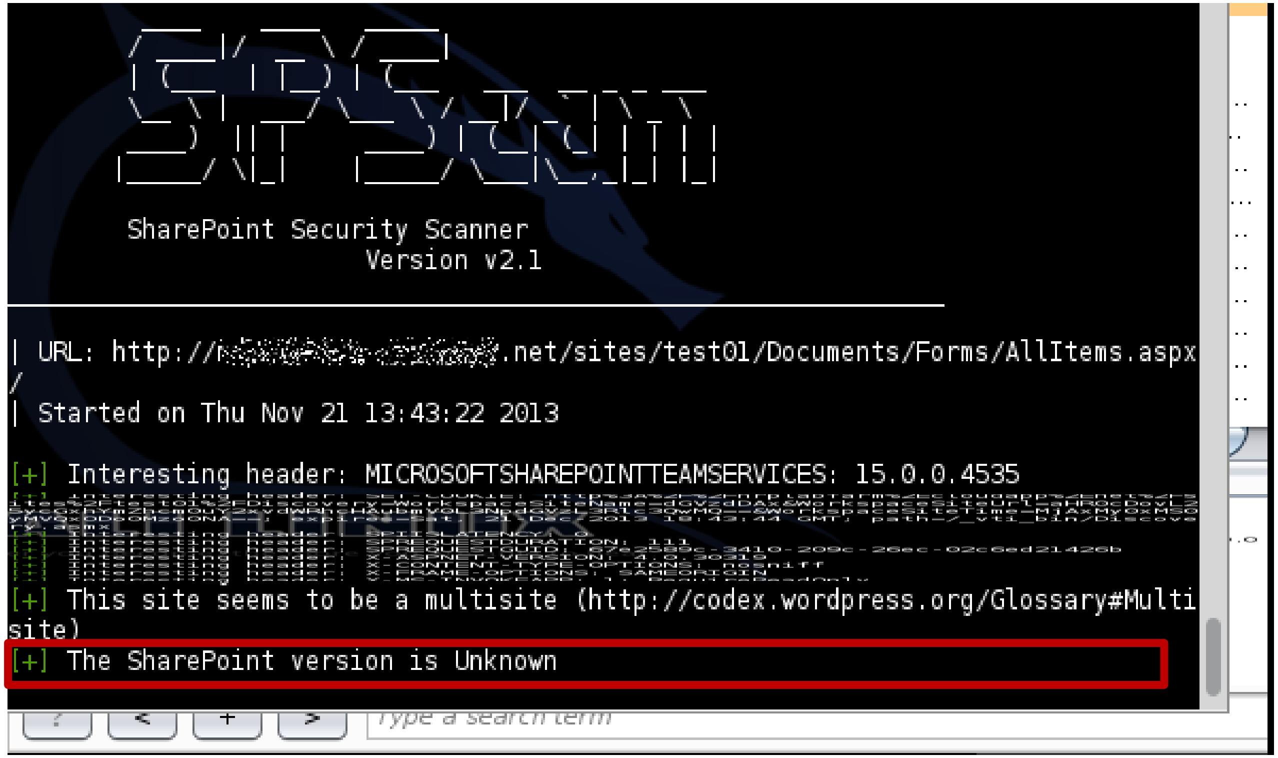
```
X:\>python sparty_v_0.1.py -s layouts -a ntlm -u http://[redacted].net/sites/test01
        ---------------------------------------------------------------

        SPARTY : Sharepoint/Frontpage Security Auditing Tool!
        Authored by: Aditya K Sood |{0kn0ck}@secniche.org  | 2013
        Twitter:     @AdityaKSood
        Powered by: SecNiche Security Labs !

        ---------------------------------------------------------------
[+][devalias.net] Enabling NTLM authentication support
[+][devalias.net][NTLM Authentication] NTLM Support Library Loaded!
[+][devalias.net][NTLM Authentication] Enter username (DOMAIN\username): [redacted]
[+][devalias.net][NTLM Authentication] Enter password: [redacted]
[+][devalias.net][NTLM authentication] Credentials enabled for [redacted]
[+] fetching information from the given target : (http://[redacted].net/sites/test01)
[+] target responded with HTTP code: (200)
[+] target is running server: (Microsoft-IIS/8.0)

[+]----------------------------------------------------------------!
[+] auditing sharepoint '/_layouts/' directory for access permissions !
[+]----------------------------------------------------------------!

[+] (http://nrplabfarm.cloudapp.net/sites/test01/_layouts/aclinv.aspx) - (200)
[+] (http://nrplabfarm.cloudapp.net/sites/test01/_layouts/addrole.aspx) - (401)
[+] (http://nrplabfarm.cloudapp.net/sites/test01/_layouts/AdminRecycleBin.aspx) - (401)
[+] (http://nrplabfarm.cloudapp.net/sites/test01/_layouts/AreaNavigationSettings.aspx) - (401)
```

Tools for testing SharePoint

Another audit Tool

- » **spscan** (https://github.com/toddsiegel/spscan)

  Fork of wpscan tool with SharePoint related data; for NTLM authentication use your favorite proxy

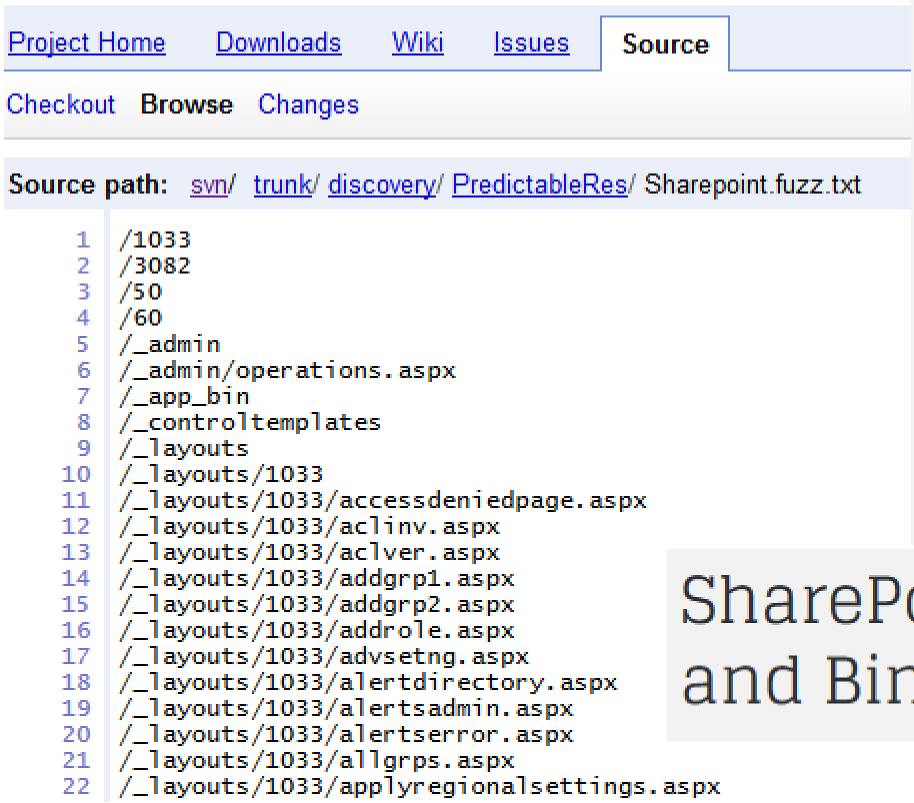


```
        SharePoint Security Scanner
                        Version v2.1

| URL: http://[redacted].net/sites/test01/Documents/Forms/AllItems.aspx
/
| Started on Thu Nov 21 13:43:22 2013

[+] Interesting header: MICROSOFTSHAREPOINTTEAMSERVICES: 15.0.0.4535
[+] Interesting header: SET-COOKIE: [illegible]
[illegible] expires=Sat, 21 Dec 2013 18:43:44 GMT; path=/_vti_bin/Discove
ry.asmx
[+] Interesting header: SPIISLATENCY: 0
[+] Interesting header: SPREQUESTDURATION: 111
[+] Interesting header: SPREQUESTGUID: 87e2589c-3410-209c-26ec-02c6ed21426b
[+] Interesting header: X-ASPNET-VERSION: 4.0.30319
[+] Interesting header: X-CONTENT-TYPE-OPTIONS: nosniff
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] This site seems to be a multisite (http://codex.wordpress.org/Glossary#Multi
site)
[+] The SharePoint version is Unknown
```

Spotting SharePoint services

fuzzdb

Attack and Discovery Pattern Database for Application Fuzzing



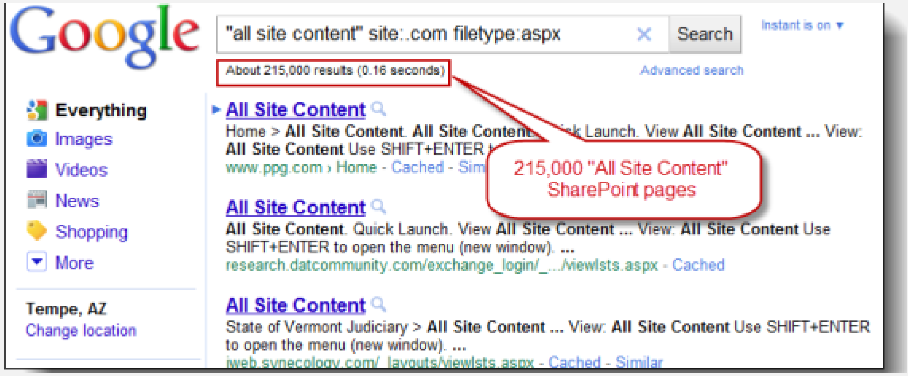
Source path: svn/ trunk/ discovery/ PredictableRes/ Sharepoint.fuzz.txt

```
/1033
/3082
/50
/60
/_admin
/_admin/operations.aspx
/_app_bin
/_controltemplates
/_layouts
/_layouts/1033
/_layouts/1033/accessdeniedpage.aspx
/_layouts/1033/aclinv.aspx
/_layouts/1033/aclver.aspx
/_layouts/1033/addgrp1.aspx
/_layouts/1033/addgrp2.aspx
/_layouts/1033/addrole.aspx
/_layouts/1033/advsetng.aspx
/_layouts/1033/alertdirectory.aspx
/_layouts/1033/alertsadmin.aspx
/_layouts/1033/alertserror.aspx
/_layouts/1033/allgrps.aspx
/_layouts/1033/applyregionalsettings.aspx
```

http://code.google.com/p/fuzzdb/source/browse/trunk/discovery/PredictableRes/Sharepoint.fuzz.txt

Google and Bing Hacking Dictionary Files

New **GoogleDiggity input dictionary** file contains **121 queries** that allow users to uncover SharePoint specific vulnerabilities exposed via the Google search engine. This dictionary helps assessors locate exposures of common SharePoint administrative pages, web services, and site galleries that an organization typically would not want to be made available to the public, let alone indexed by Google.



About 215,000 results (0.16 seconds)

All Site Content
Home > All Site Content. All Site Content ... Quick Launch. View All Site Content ... View: All Site Content Use SHIFT+ENTER ...
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/_.../viewlsts.aspx - Cached

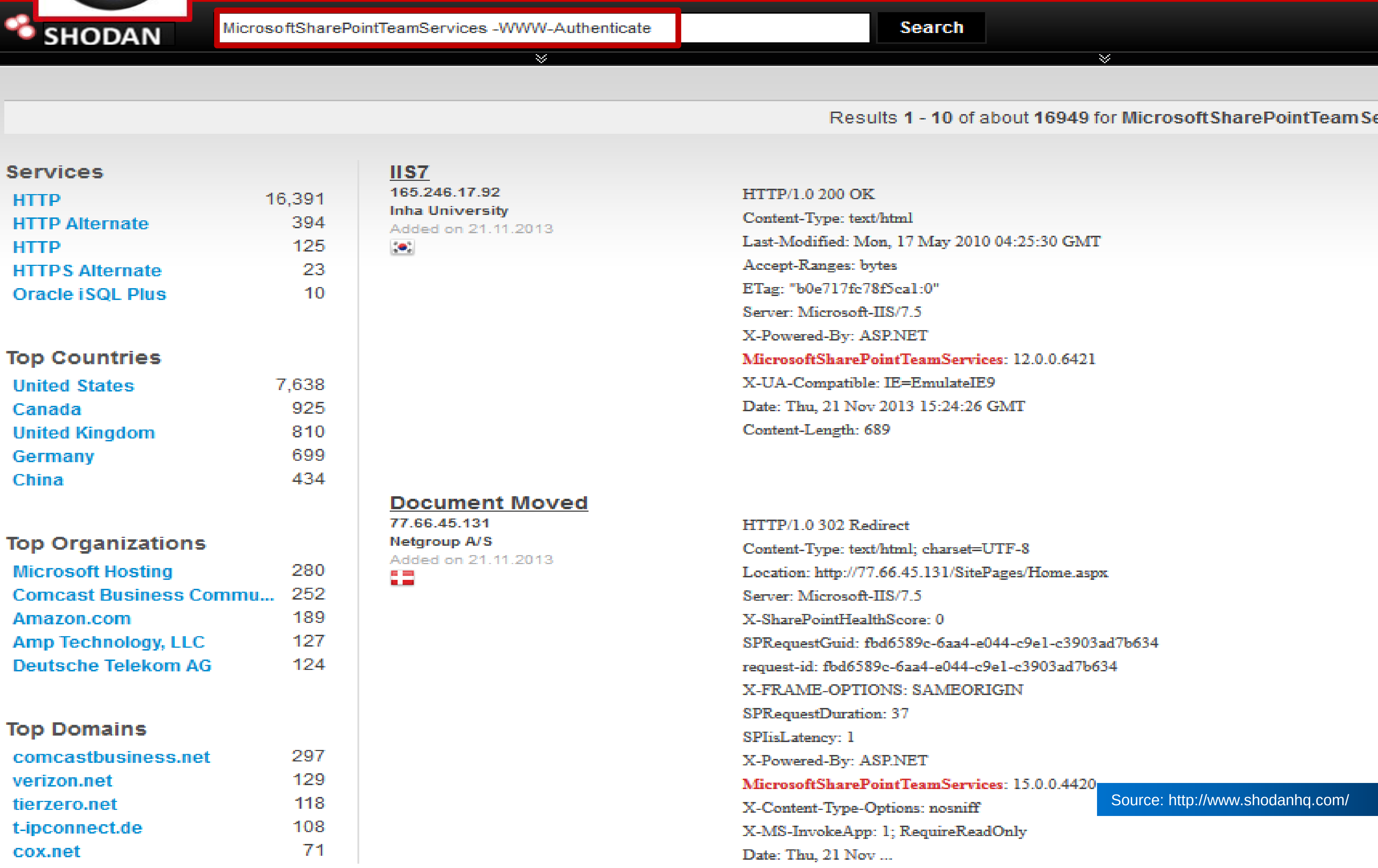
All Site Content
State of Vermont Judiciary > All Site Content ... View: All Site Content Use SHIFT+ENTER to open the menu (new window). ...
iweb.synecology.com/_layouts/viewlsts.aspx - Cached - Similar

215,000 "All Site Content" SharePoint pages

SharePoint Hacking Alerts for Google and Bing

Source: http://www.bishopfox.com/resources/tools/sharepoint-hacking-diggity/attack-tools/

Spotting SharePoint services …



Results **1** - **10** of about **16949** for **MicrosoftSharePointTeamSe**

Services

HTTP	16,391
HTTP Alternate	394
HTTP	125
HTTPS Alternate	23
Oracle iSQL Plus	10

Top Countries

United States	7,638
Canada	925
United Kingdom	810
Germany	699
China	434

Top Organizations

Microsoft Hosting	280
Comcast Business Commu...	252
Amazon.com	189
Amp Technology, LLC	127
Deutsche Telekom AG	124

Top Domains

comcastbusiness.net	297
verizon.net	129
tierzero.net	118
t-ipconnect.de	108
cox.net	71

IIS7
165.246.17.92
Inha University
Added on 21.11.2013

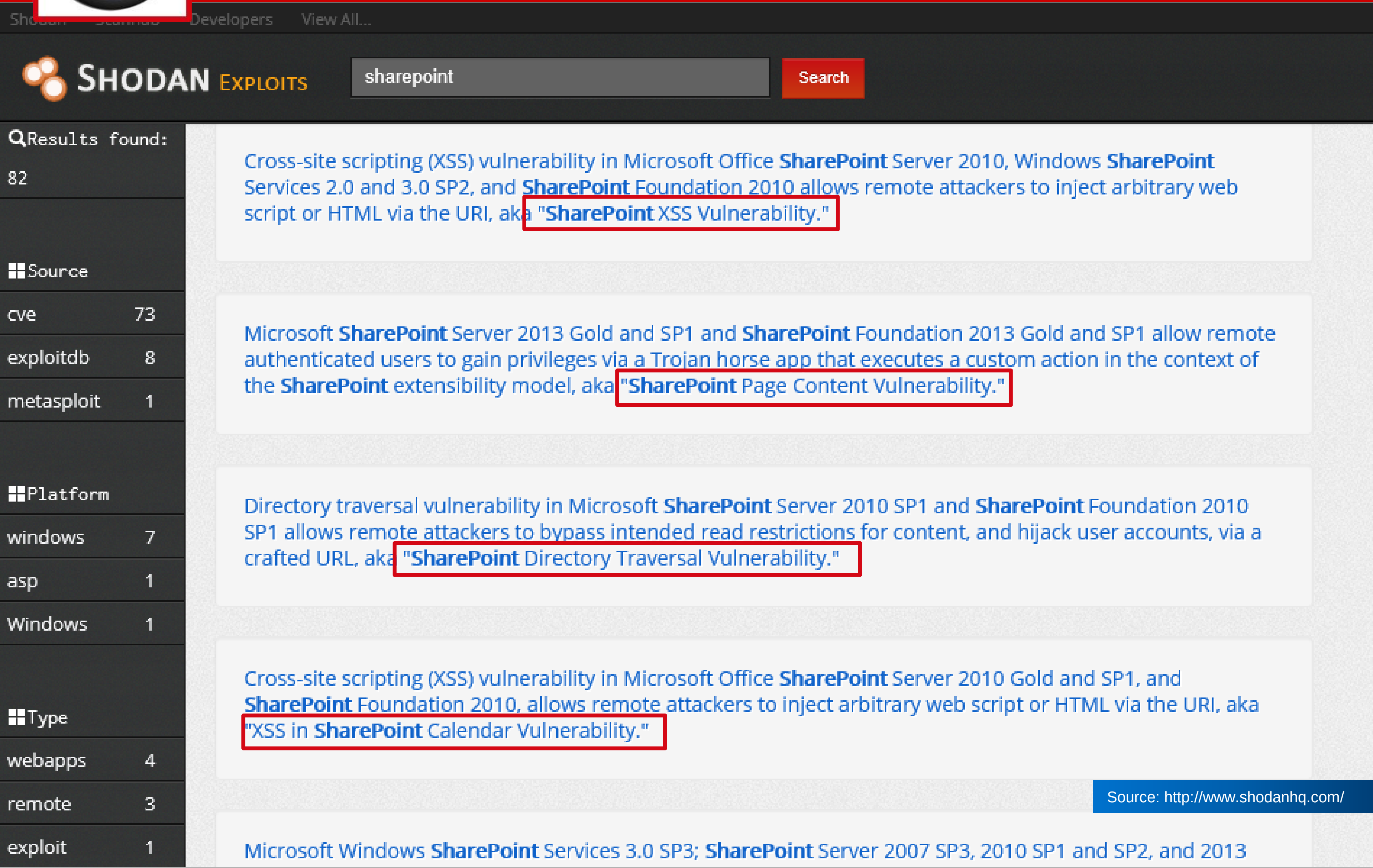
```
HTTP/1.0 200 OK
Content-Type: text/html
Last-Modified: Mon, 17 May 2010 04:25:30 GMT
Accept-Ranges: bytes
ETag: "b0e717fc78f5ca1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 12.0.0.6421
X-UA-Compatible: IE=EmulateIE9
Date: Thu, 21 Nov 2013 15:24:26 GMT
Content-Length: 689
```

Document Moved
77.66.45.131
Netgroup A/S
Added on 21.11.2013

```
HTTP/1.0 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: http://77.66.45.131/SitePages/Home.aspx
Server: Microsoft-IIS/7.5
X-SharePointHealthScore: 0
SPRequestGuid: fbd6589c-6aa4-e044-c9e1-c3903ad7b634
request-id: fbd6589c-6aa4-e044-c9e1-c3903ad7b634
X-FRAME-OPTIONS: SAMEORIGIN
SPRequestDuration: 37
SPIisLatency: 1
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 15.0.0.4420
X-Content-Type-Options: nosniff
X-MS-InvokeApp: 1; RequireReadOnly
Date: Thu, 21 Nov ...
```

Source: http://www.shodanhq.com/

… and SharePoint known issues



cve	73
exploitdb	8
metasploit	1

windows	7
asp	1
Windows	1

webapps	4
remote	3
exploit	1

Cross-site scripting (XSS) vulnerability in Microsoft Office **SharePoint** Server 2010, Windows **SharePoint** Services 2.0 and 3.0 SP2, and **SharePoint** Foundation 2010 allows remote attackers to inject arbitrary web script or HTML via the URI, aka "**SharePoint** XSS Vulnerability."

Microsoft **SharePoint** Server 2013 Gold and SP1 and **SharePoint** Foundation 2013 Gold and SP1 allow remote authenticated users to gain privileges via a Trojan horse app that executes a custom action in the context of the **SharePoint** extensibility model, aka "**SharePoint** Page Content Vulnerability."

Directory traversal vulnerability in Microsoft **SharePoint** Server 2010 SP1 and **SharePoint** Foundation 2010 SP1 allows remote attackers to bypass intended read restrictions for content, and hijack user accounts, via a crafted URL, aka "**SharePoint** Directory Traversal Vulnerability."

Cross-site scripting (XSS) vulnerability in Microsoft Office **SharePoint** Server 2010 Gold and SP1, and **SharePoint** Foundation 2010, allows remote attackers to inject arbitrary web script or HTML via the URI, aka "XSS in **SharePoint** Calendar Vulnerability."

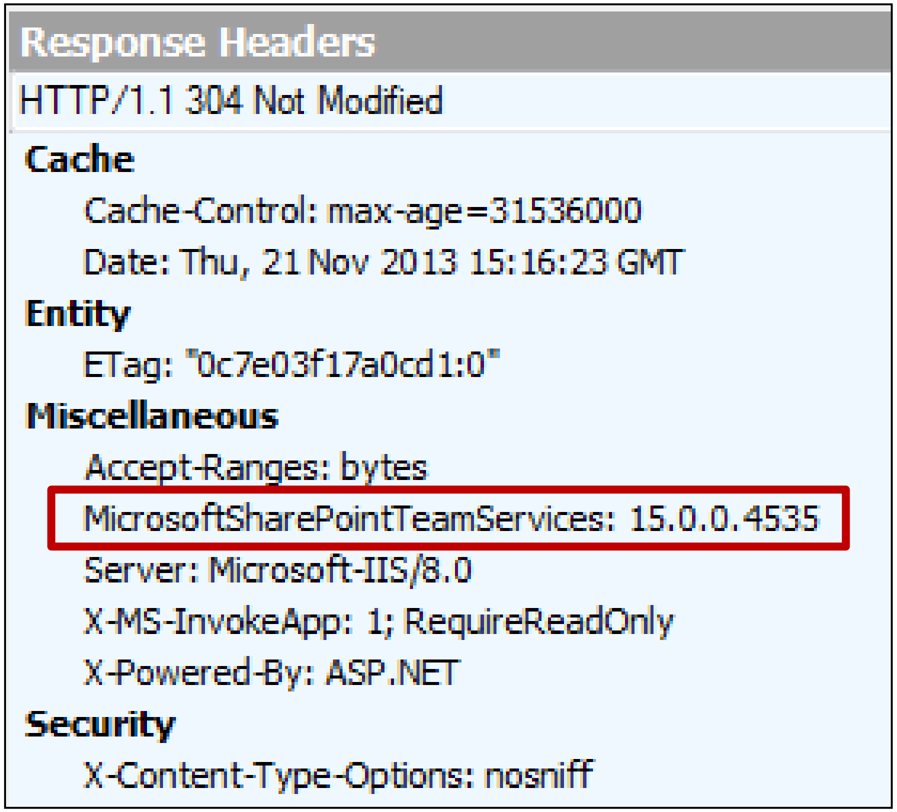
Microsoft Windows **SharePoint** Services 3.0 SP3; **SharePoint** Server 2007 SP3, 2010 SP1 and SP2, and 2013

Source: http://www.shodanhq.com/

Attacking surface

SharePoint Build Numbers and Cumulative Updates

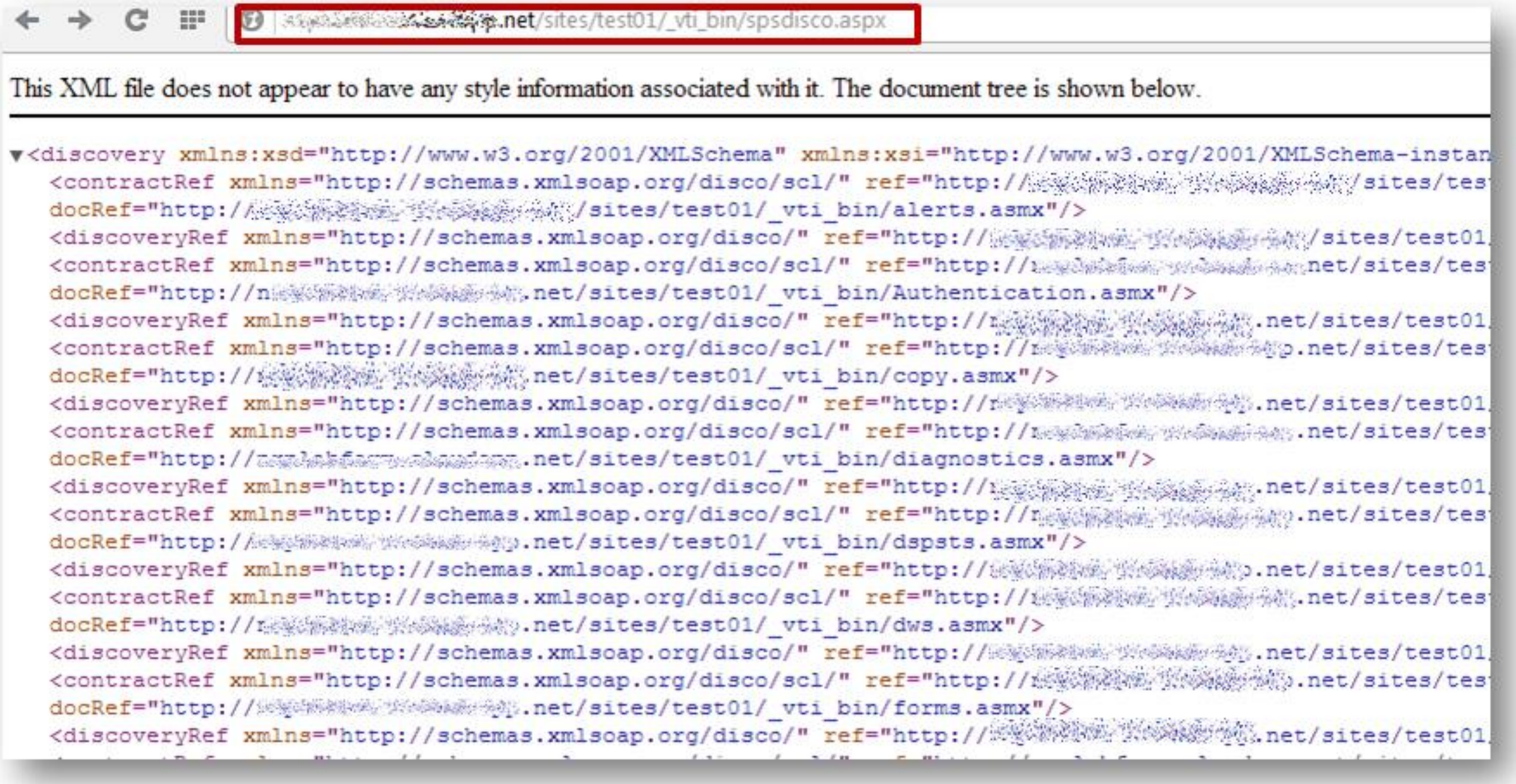
- SharePoint 2003/2007
  http://blogs.technet.com/b/steve_chen/archive/2012/03/14/3486623.aspx
- SharePoint 2010
  http://www.toddklindt.com/sp2010builds
- SharePoint 2013
  http://www.toddklindt.com/sp2013builds



```
Response Headers
HTTP/1.1 304 Not Modified
Cache
    Cache-Control: max-age=31536000
    Date: Thu, 21 Nov 2013 15:16:23 GMT
Entity
    ETag: "0c7e03f17a0cd1:0"
Miscellaneous
    Accept-Ranges: bytes
    MicrosoftSharePointTeamServices: 15.0.0.4535
    Server: Microsoft-IIS/8.0
    X-MS-InvokeApp: 1; RequireReadOnly
    X-Powered-By: ASP.NET
Security
    X-Content-Type-Options: nosniff
```

SharePoint Webservices

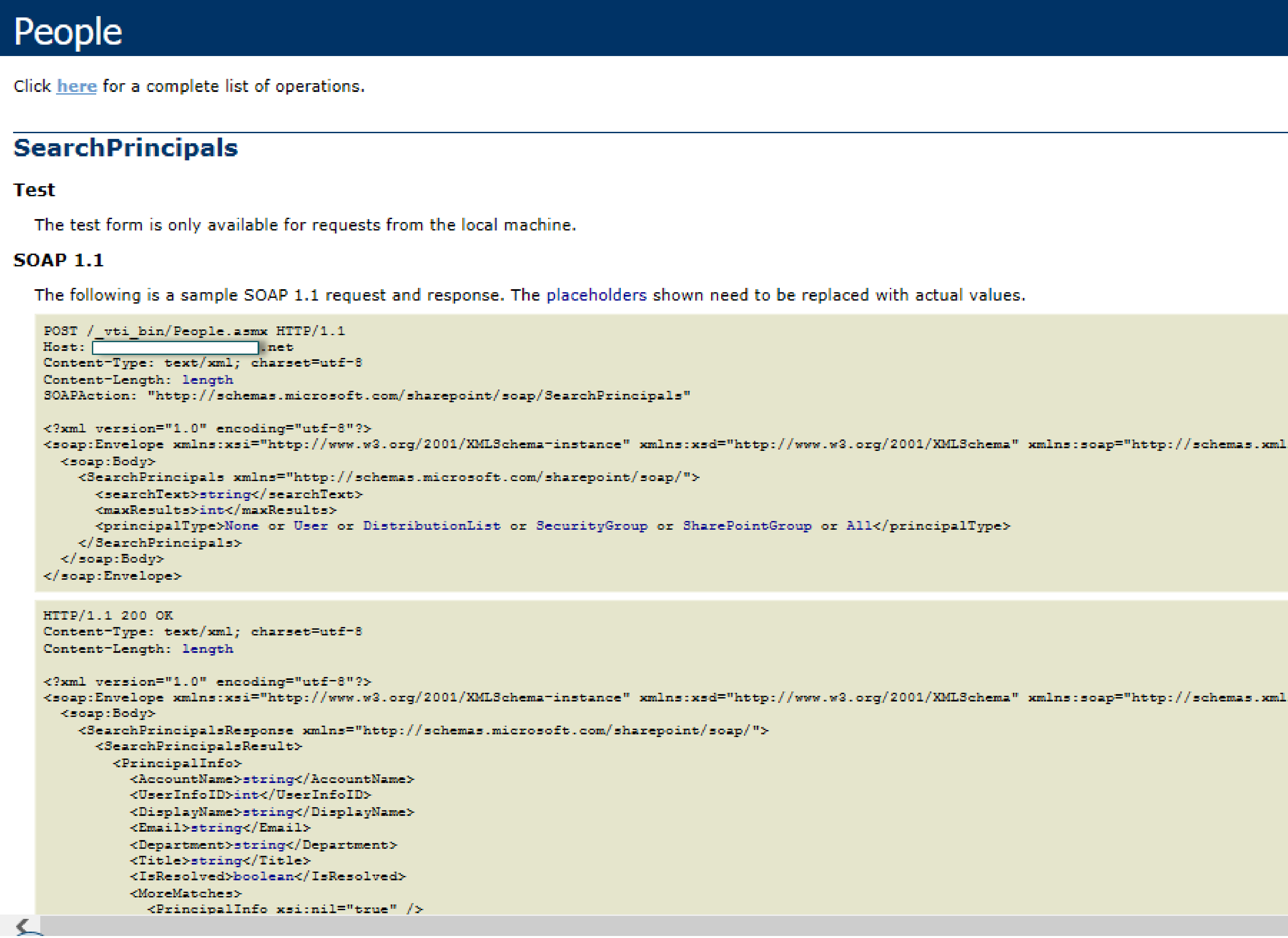
SPSDisco, They like to talk…



[redacted].net/sites/test01/_vti_bin/spsdisco.aspx

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<discovery xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instan
   <contractRef xmlns="http://schemas.xmlsoap.org/disco/scl/" ref="http://[redacted]/sites/tes
   docRef="http://[redacted]/sites/test01/_vti_bin/alerts.asmx"/>
   <discoveryRef xmlns="http://schemas.xmlsoap.org/disco/" ref="http://[redacted]/sites/test01
   <contractRef xmlns="http://schemas.xmlsoap.org/disco/scl/" ref="http://[redacted].net/sites/tes
   docRef="http://[redacted].net/sites/test01/_vti_bin/Authentication.asmx"/>
   <discoveryRef xmlns="http://schemas.xmlsoap.org/disco/" ref="http://[redacted].net/sites/test01
   <contractRef xmlns="http://schemas.xmlsoap.org/disco/scl/" ref="http://[redacted].net/sites/tes
   docRef="http://[redacted].net/sites/test01/_vti_bin/copy.asmx"/>
   <discoveryRef xmlns="http://schemas.xmlsoap.org/disco/" ref="http://[redacted].net/sites/test01
   <contractRef xmlns="http://schemas.xmlsoap.org/disco/scl/" ref="http://[redacted].net/sites/tes
   docRef="http://[redacted].net/sites/test01/_vti_bin/diagnostics.asmx"/>
   <discoveryRef xmlns="http://schemas.xmlsoap.org/disco/" ref="http://[redacted].net/sites/test01
   <contractRef xmlns="http://schemas.xmlsoap.org/disco/scl/" ref="http://[redacted].net/sites/tes
   docRef="http://[redacted].net/sites/test01/_vti_bin/dspsts.asmx"/>
   <discoveryRef xmlns="http://schemas.xmlsoap.org/disco/" ref="http://[redacted].net/sites/test01
   <contractRef xmlns="http://schemas.xmlsoap.org/disco/scl/" ref="http://[redacted].net/sites/tes
   docRef="http://[redacted].net/sites/test01/_vti_bin/dws.asmx"/>
   <discoveryRef xmlns="http://schemas.xmlsoap.org/disco/" ref="http://[redacted].net/sites/test01
   <contractRef xmlns="http://schemas.xmlsoap.org/disco/scl/" ref="http://[redacted].net/sites/tes
   docRef="http://[redacted].net/sites/test01/_vti_bin/forms.asmx"/>
   <discoveryRef xmlns="http://schemas.xmlsoap.org/disco/" ref="http://[redacted].net/sites/test01
```



People

Click here for a complete list of operations.

SearchPrincipals

Test

The test form is only available for requests from the local machine.

SOAP 1.1

The following is a sample SOAP 1.1 request and response. The placeholders shown need to be replaced with actual values.

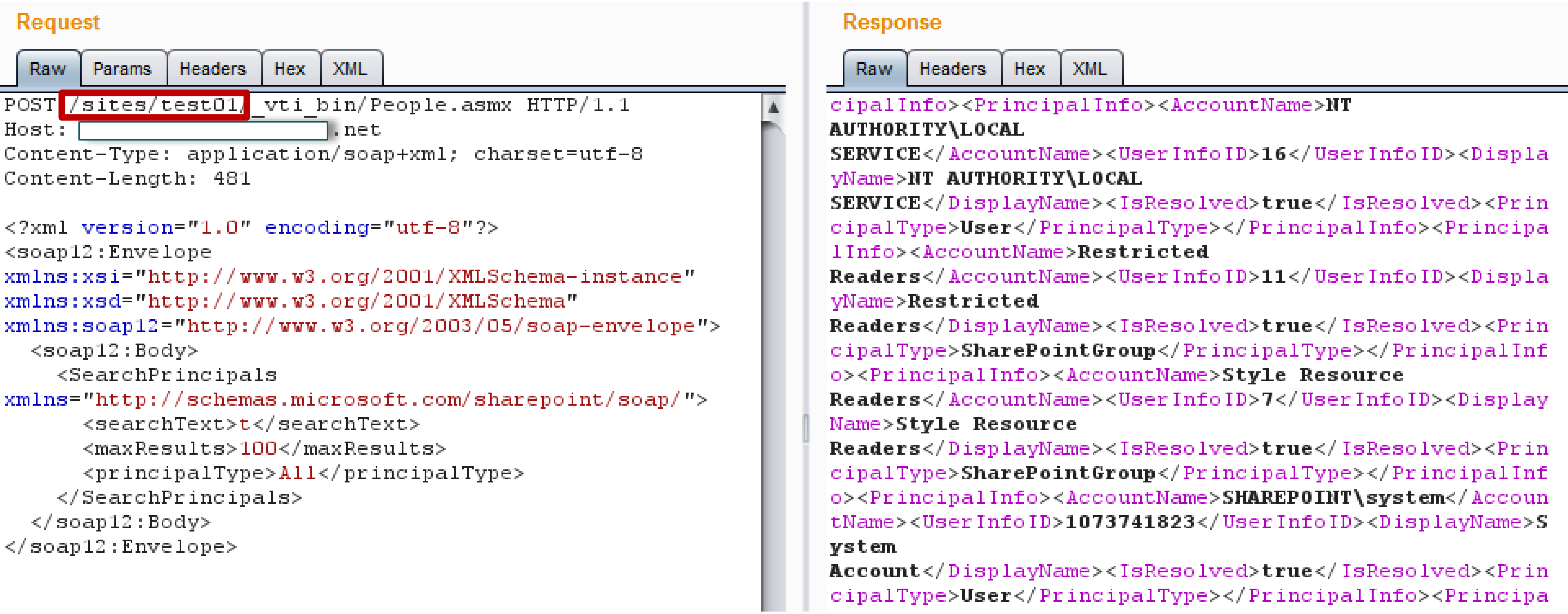
```
POST /_vti_bin/People.asmx HTTP/1.1
Host: [redacted].net
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://schemas.microsoft.com/sharepoint/soap/SearchPrincipals"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xml
  <soap:Body>
    <SearchPrincipals xmlns="http://schemas.microsoft.com/sharepoint/soap/">
      <searchText>string</searchText>
      <maxResults>int</maxResults>
      <principalType>None or User or DistributionList or SecurityGroup or SharePointGroup or All</principalType>
    </SearchPrincipals>
  </soap:Body>
</soap:Envelope>
```

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xml
  <soap:Body>
    <SearchPrincipalsResponse xmlns="http://schemas.microsoft.com/sharepoint/soap/">
      <SearchPrincipalsResult>
        <PrincipalInfo>
          <AccountName>string</AccountName>
          <UserInfoID>int</UserInfoID>
          <DisplayName>string</DisplayName>
          <Email>string</Email>
          <Department>string</Department>
          <Title>string</Title>
          <IsResolved>boolean</IsResolved>
          <MoreMatches>
            <PrincipalInfo xsi:nil="true" />
```

Nice conversation

Just be a member of a SharePoint site

- » And you can:



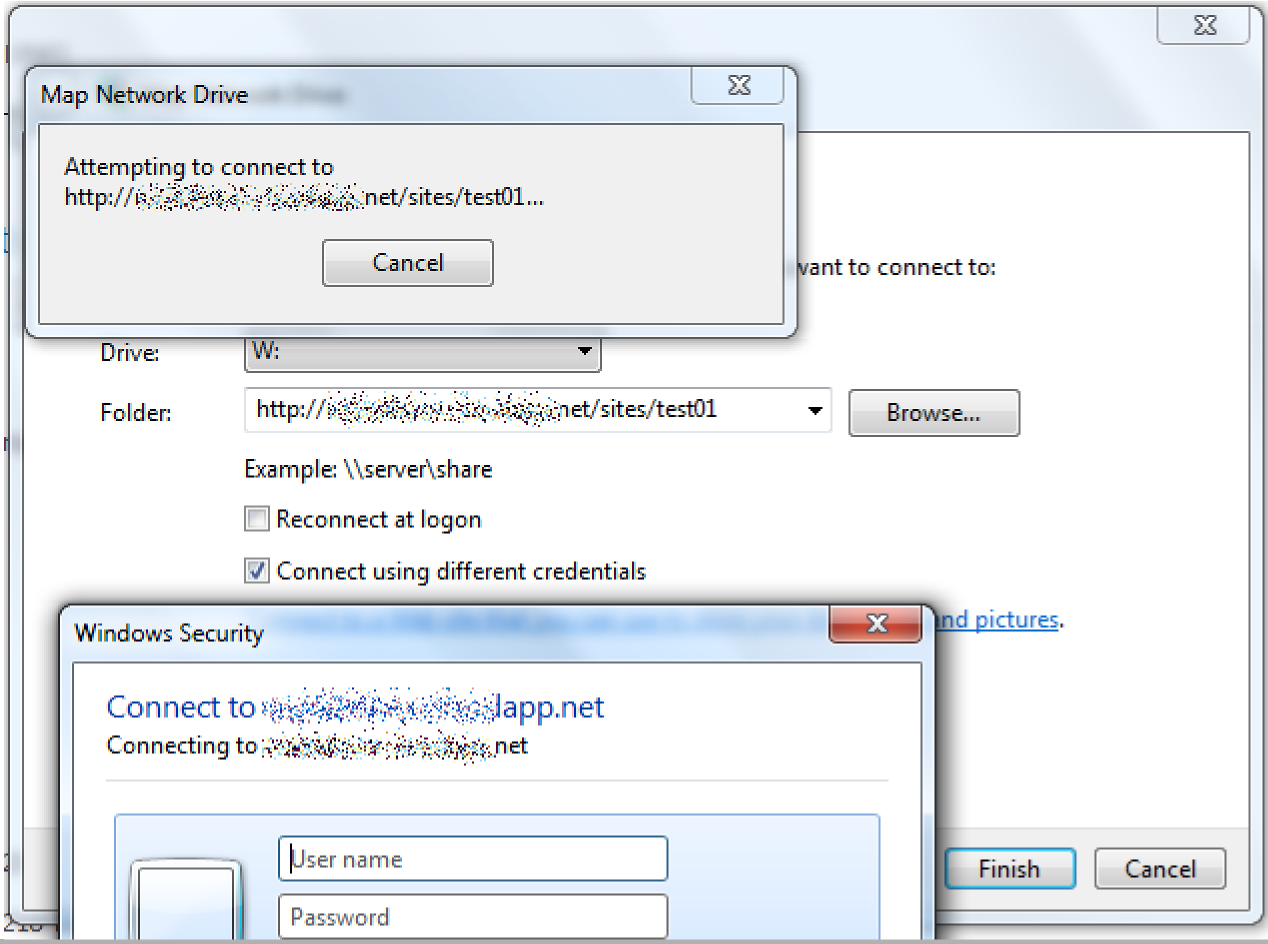
```
POST /sites/test01/_vti_bin/People.asmx HTTP/1.1
Host: [redacted].net
Content-Type: application/soap+xml; charset=utf-8
Content-Length: 481

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <SearchPrincipals
xmlns="http://schemas.microsoft.com/sharepoint/soap/">
      <searchText>t</searchText>
      <maxResults>100</maxResults>
      <principalType>All</principalType>
    </SearchPrincipals>
  </soap12:Body>
</soap12:Envelope>
```

```
cipalInfo><PrincipalInfo><AccountName>NT
AUTHORITY\LOCAL
SERVICE</AccountName><UserInfoID>16</UserInfoID><Displa
yName>NT AUTHORITY\LOCAL
SERVICE</DisplayName><IsResolved>true</IsResolved><Prin
cipalType>User</PrincipalType></PrincipalInfo><Principa
lInfo><AccountName>Restricted
Readers</AccountName><UserInfoID>11</UserInfoID><Displa
yName>Restricted
Readers</DisplayName><IsResolved>true</IsResolved><Prin
cipalType>SharePointGroup</PrincipalType></PrincipalInf
o><PrincipalInfo><AccountName>Style Resource
Readers</AccountName><UserInfoID>7</UserInfoID><Display
Name>Style Resource
Readers</DisplayName><IsResolved>true</IsResolved><Prin
cipalType>SharePointGroup</PrincipalType></PrincipalInf
o><PrincipalInfo><AccountName>SHAREPOINT\system</Accoun
tName><UserInfoID>1073741823</UserInfoID><DisplayName>S
ystem
Account</DisplayName><IsResolved>true</IsResolved><Prin
cipalType>User</PrincipalType></PrincipalInfo><Principa
```

We can talk even better together

I like WebDAV…

- » And so should you



Map Network Drive

Attempting to connect to
http://[redacted]net/sites/test01...

vant to connect to:

Drive: W:

Folder: http://[redacted]net/sites/test01

Example: \\server\share

☐ Reconnect at logon

☑ Connect using different credentials

nd pictures.

Windows Security

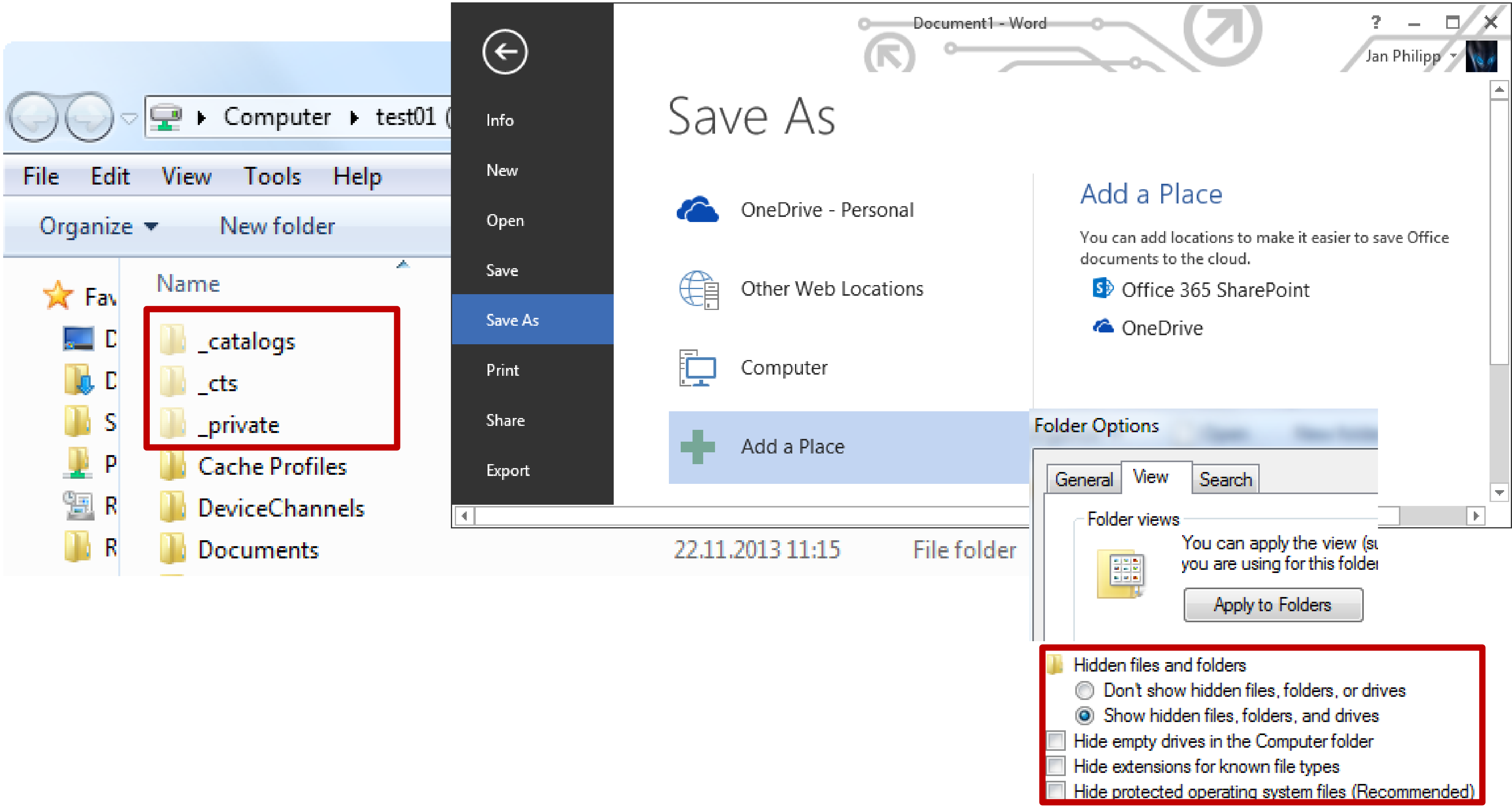
Connect to [redacted]lapp.net
Connecting to [redacted]net

User name

Password

WebDAV quirks

Mapped network drives

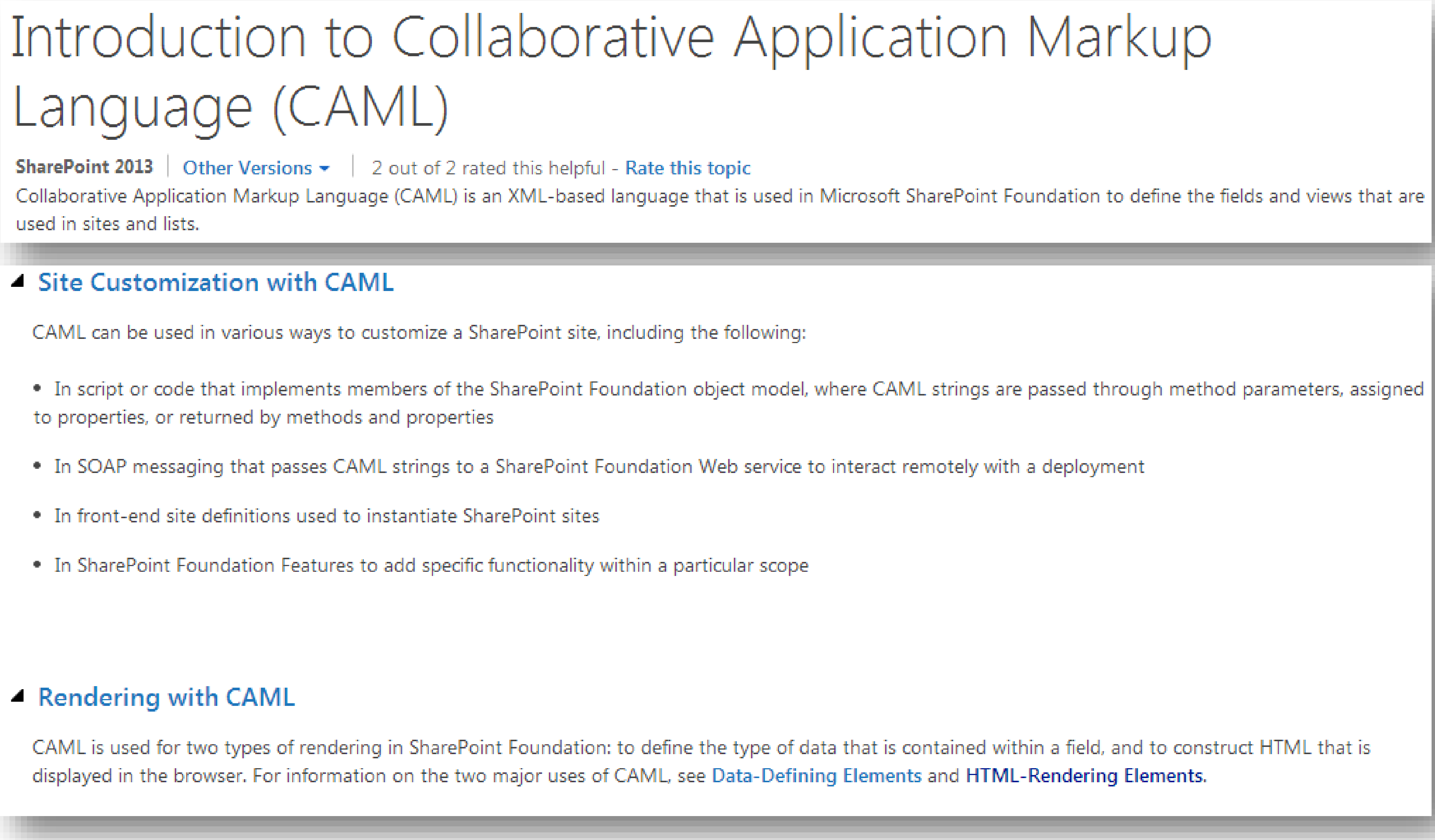


You can add locations to make it easier to save Office documents to the cloud.

You can apply the view (su you are using for this folde

Hidden files and folders
○ Don't show hidden files, folders, or drives
● Show hidden files, folders, and drives
□ Hide empty drives in the Computer folder
□ Hide extensions for known file types
□ Hide protected operating system files (Recommended)

SharePoint query language



Introduction to Collaborative Application Markup Language (CAML)

SharePoint 2013 | Other Versions ▾ | 2 out of 2 rated this helpful - Rate this topic

Collaborative Application Markup Language (CAML) is an XML-based language that is used in Microsoft SharePoint Foundation to define the fields and views that are used in sites and lists.

◢ Site Customization with CAML

CAML can be used in various ways to customize a SharePoint site, including the following:

- In script or code that implements members of the SharePoint Foundation object model, where CAML strings are passed through method parameters, assigned to properties, or returned by methods and properties
- In SOAP messaging that passes CAML strings to a SharePoint Foundation Web service to interact remotely with a deployment
- In front-end site definitions used to instantiate SharePoint sites
- In SharePoint Foundation Features to add specific functionality within a particular scope

◢ Rendering with CAML

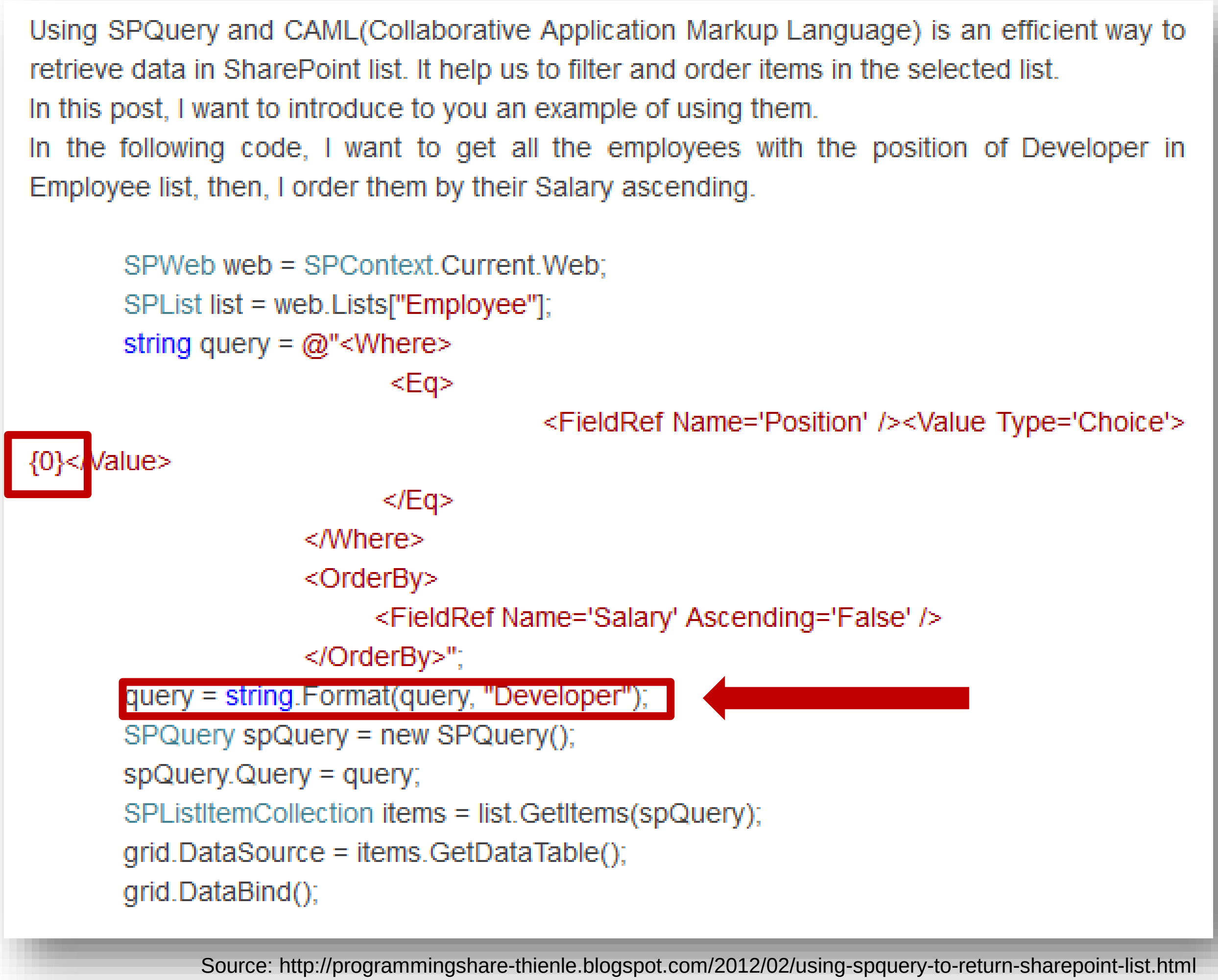
CAML is used for two types of rendering in SharePoint Foundation: to define the type of data that is contained within a field, and to construct HTML that is displayed in the browser. For information on the two major uses of CAML, see Data-Defining Elements and HTML-Rendering Elements.

Source: http://msdn.microsoft.com/en-us/library/office/ms462365.aspx

Developer insights

Using SPQUERY to return SharePoint list items

CAML INJECTION



Using SPQuery and CAML(Collaborative Application Markup Language) is an efficient way to retrieve data in SharePoint list. It help us to filter and order items in the selected list.

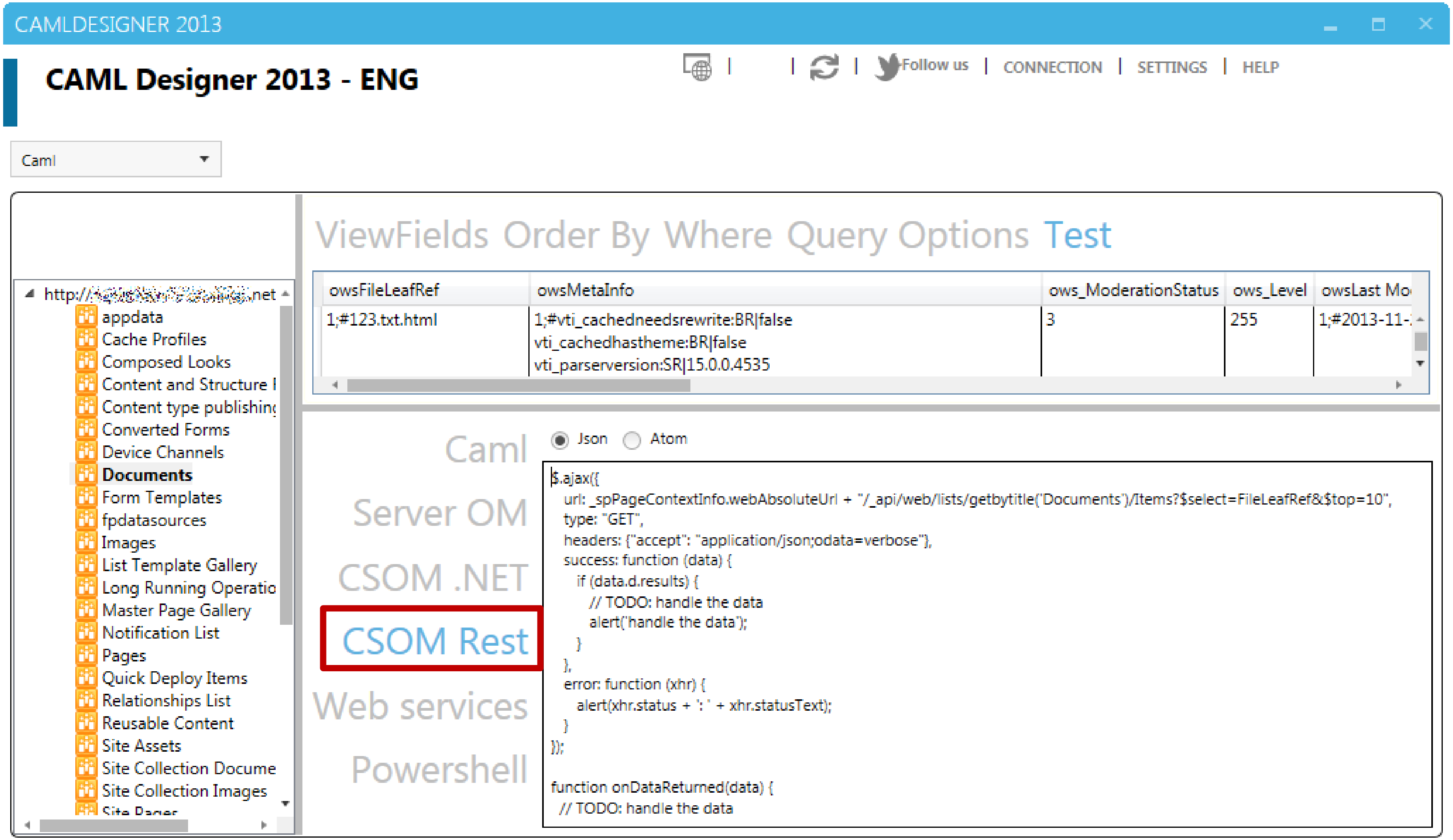
In this post, I want to introduce to you an example of using them.

In the following code, I want to get all the employees with the position of Developer in Employee list, then, I order them by their Salary ascending.

```
        SPWeb web = SPContext.Current.Web;
        SPList list = web.Lists["Employee"];
        string query = @"<Where>
                              <Eq>
                                           <FieldRef Name='Position' /><Value Type='Choice'>
{0}</Value>
                              </Eq>
                       </Where>
                       <OrderBy>
                             <FieldRef Name='Salary' Ascending='False' />
                       </OrderBy>";
        query = string.Format(query, "Developer");
        SPQuery spQuery = new SPQuery();
        spQuery.Query = query;
        SPListItemCollection items = list.GetItems(spQuery);
        grid.DataSource = items.GetDataTable();
        grid.DataBind();
```

Source: http://programmingshare-thienle.blogspot.com/2012/02/using-spquery-to-return-sharepoint-list.html

Developer tools



CAML Designer 2013 - ENG

- http://[redacted].net
  - appdata
  - Cache Profiles
  - Composed Looks
  - Content and Structure I
  - Content type publishing
  - Converted Forms
  - Device Channels
  - **Documents**
  - Form Templates
  - fpdatasources
  - Images
  - List Template Gallery
  - Long Running Operatio
  - Master Page Gallery
  - Notification List
  - Pages
  - Quick Deploy Items
  - Relationships List
  - Reusable Content
  - Site Assets
  - Site Collection Docume
  - Site Collection Images
  - Site Pages

owsFileLeafRef	owsMetaInfo	ows_ModerationStatus	ows_Level	owsLast Mo
1;#123.txt.html	1;#vti_cachedneedsrewrite:BR|false vti_cachedhastheme:BR|false vti_parserversion:SR|15.0.0.4535	3	255	1;#2013-11-:

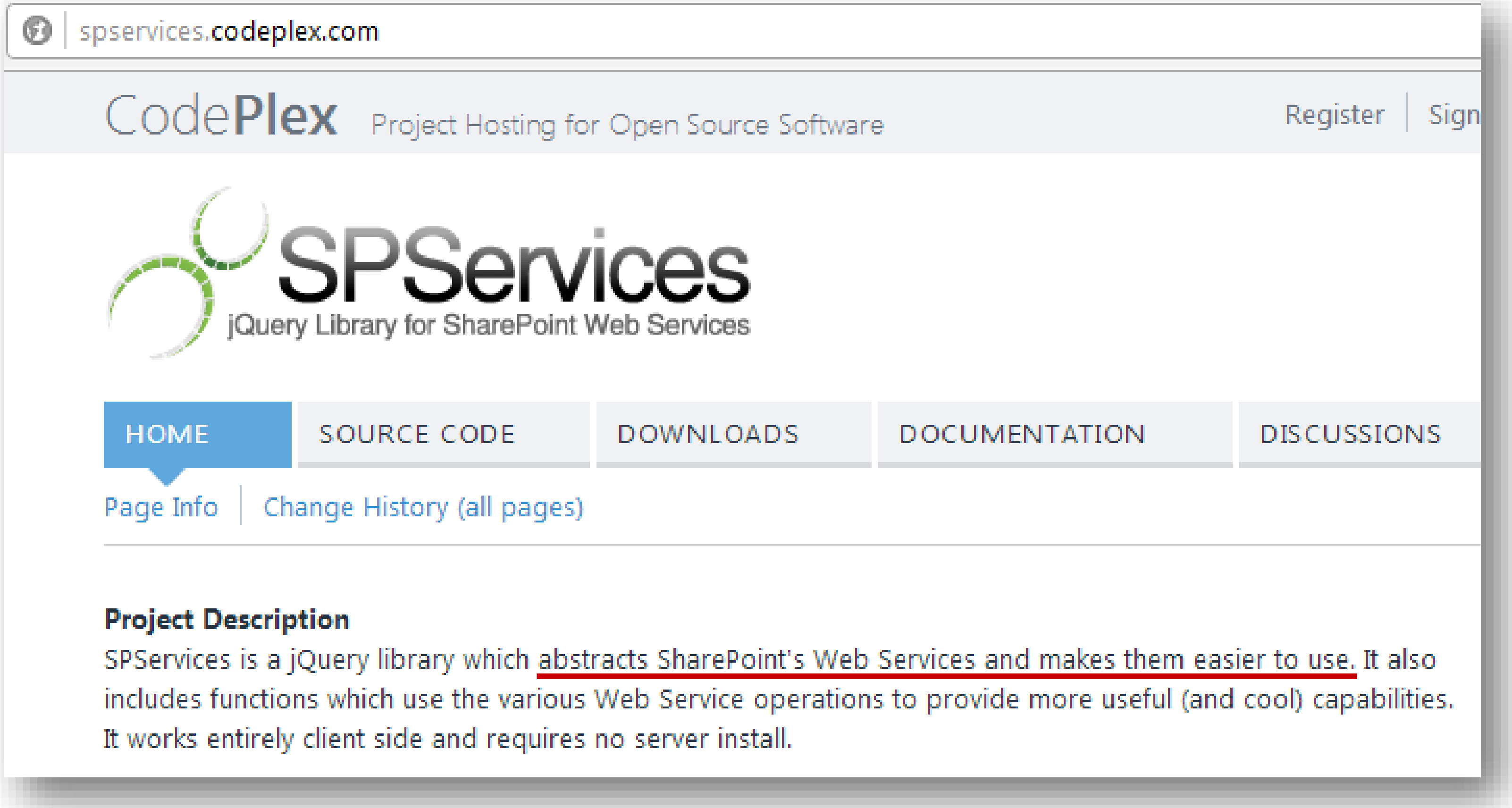
● Json ○ Atom

```
$.ajax({
  url: _spPageContextInfo.webAbsoluteUrl + "/_api/web/lists/getbytitle('Documents')/Items?$select=FileLeafRef&$top=10",
  type: "GET",
  headers: {"accept": "application/json;odata=verbose"},
  success: function (data) {
    if (data.d.results) {
      // TODO: handle the data
      alert('handle the data');
    }
  },
  error: function (xhr) {
    alert(xhr.status + ': ' + xhr.statusText);
  }
});

function onDataReturned(data) {
 // TODO: handle the data
```

Developer's are smart!

Just do it on the client side...

» Do you like HTML5?



spservices.codeplex.com
CodePlex Project Hosting for Open Source Software
Register | Sign
SPServices
jQuery Library for SharePoint Web Services
HOME
SOURCE CODE
DOWNLOADS
DOCUMENTATION
DISCUSSIONS
Page Info | Change History (all pages)

Project Description

SPServices is a jQuery library which abstracts SharePoint's Web Services and makes them easier to use. It also includes functions which use the various Web Service operations to provide more useful (and cool) capabilities. It works entirely client side and requires no server install.

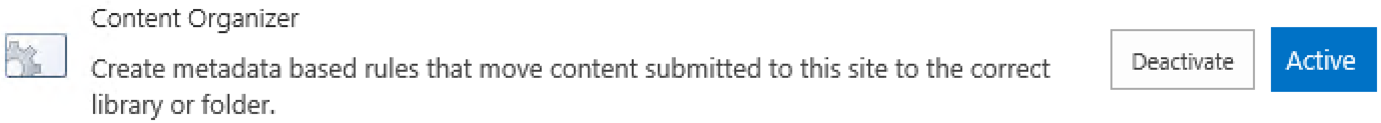
Extending SharePoint

Pitfalls
Challenges
Work Arounds

Content Organizer extension

Using some of the many SharePoint features

- » Your admins are comfortable with SharePoint
- » They enable the built-in document routing feature



Content Organizer

Create metadata based rules that move content submitted to this site to the correct library or folder.

- » Everything works automatically, that can’t be bad
  - Document Routing bypasses SharePoint security model!
  - Users can upload from one library to one where they don’t have permissions
  - Worse: SharePoint will give them an access denied but upload and route the documents anyway

Datapump extension

Backend impersonation

- You cannot pass Kerberos user credentials directly to the backend database but need the user credentials there
- You can use the Datapump Webservice to do this

- So what is the problem?!
  - Any user with any site permissions can cause a DoS of the Datapump and the back-end SQL Analysis Services
  - End user can pass different credentials from the logged on user to the Datapump, which retrieves the Kerberos ticket to pass to the back-end

Datapump extension

Backend impersonation – simple crash code

```
POST /olap/msmdpump.dll HTTP/1.1
Connection: close
Content-Type: text/xml
Content-Length: 572
Host: <obfuscated-enter your webserver FQDN>


<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Header><Session xmlns="urn:schemas-microsoft-com:xml-analysis" SessionId="B021E390-38B4-4822-86FD-49A096A4D9F1"/></soap:Header><soap:Body><Execute xmlns="urn:schemas-microsoft-com:xml-analysis"><Command><Statement>§A§</Statement></Command><Properties><PropertyList><Catalog></Catalog><Timeout>0</Timeout><Format>Tabular</Format><DbpropMsmdFlattened2>false</DbpropMsmdFlattened2><SafetyOptions>0</SafetyOptions><Dialect>SQL</Dialect></PropertyList></Properties></Execute></soap:Body></soap:Envelope>
```

What’s Next …

More Security
Challenges ahead

And there is more…

There are many more security issues to talk about:

- Office caching of secured documents (encrypted but…)
- The SharePoint App-Store challenge https://store.office.com/appshome.aspx?productgroup=SharePoint
- SharePoint Social:
  Attackers are already following you
- The crawler service “creepy crawlies”
  Scoping search is harder than it looks

JSOM Fiddle	Prototype JSOM, CAML, … quickly
Region Country City KWizCom	Cross-Site Cascading Lists
You Tube	Connect with Us – it‘s free!

Fragen, Sorgen, Nöte?

Thanks for coming out!

Jan Philipp

Manager, Cyber Risk Services

Und kennt sich etwas mit Microsoft aus

jphilipp@deloitte.de

Change Control Slide (1 of 1)

Track all changes here! (Always last Hidden Slides)

- 2013.11.10 – Jan Philipp, Alexios Fakos

  Creation of outline, timing, and frame work
- 2013.11.11 – Jan Philipp

  Adding of “Container Ship” theme
- 2013.11.11 – Alexios Fakos

  Adding of section 3 content
- 2013.11.26 – Jan Philipp

  Intro, Summary, and sections 1, 2, and 4 content added
- 2013.11.28 – Jan Philipp, Alexios Fakos

  Consistency check and dry-run. Finalized for OWASP AppSec BeNeLux release.
- 2015.01.28 – Jan Philipp

  Adapted for OWASP Frankfurt Stammtisch