Getting a handle on SharePoint security complexity
Purpose today

Introduction

» Who we are

» 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
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

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

http://sharepoint.microsoft.com/de-de/product/capabilities/Seiten/default.aspx
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](https://www.owasp.org/index.php/Research_for_SharePoint_%28MOSS%29)
The SP Security Model

Security Building Blocks
Classic Security
SharePoint Specifics
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 organized
- Global Groups organized by Enterprise Admins into Universal Groups organized
- Universal 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!
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
Default installation “Wizard”

» 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
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
free download and free access as authenticated users
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)
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
Creepy crawlies – default search

SharePoint search:
What it shouldn’t look like

» Even more details are possible:
  – Built-in accounts
  – Service accounts
  – User accounts
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 testing 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?
Audit Tool

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

For NTLM support use unofficial patch [https://github.com/alias1/sparty](https://github.com/alias1/sparty)
Another audit Tool

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

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

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.

SharePoint Hacking Alerts for Google and Bing

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

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

### Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>16,391</td>
</tr>
<tr>
<td>HTTP Alternate</td>
<td>394</td>
</tr>
<tr>
<td>HTTPS</td>
<td>125</td>
</tr>
<tr>
<td>HTTPS Alternate</td>
<td>23</td>
</tr>
<tr>
<td>Oracle iSQL Plus</td>
<td>10</td>
</tr>
</tbody>
</table>

### Top Countries

<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>7,638</td>
</tr>
<tr>
<td>Canada</td>
<td>925</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>810</td>
</tr>
<tr>
<td>Germany</td>
<td>699</td>
</tr>
<tr>
<td>China</td>
<td>434</td>
</tr>
</tbody>
</table>

### Top Organizations

<table>
<thead>
<tr>
<th>Organization</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Hosting</td>
<td>280</td>
</tr>
<tr>
<td>Comcast Business Communica</td>
<td>252</td>
</tr>
<tr>
<td>Amazon.com</td>
<td>189</td>
</tr>
<tr>
<td>Amp Technology, LLC</td>
<td>127</td>
</tr>
<tr>
<td>Deutsche Telekom AG</td>
<td>124</td>
</tr>
</tbody>
</table>

### Top Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>comcastbusiness.net</td>
<td>297</td>
</tr>
<tr>
<td>verizon.net</td>
<td>129</td>
</tr>
<tr>
<td>tierzero.net</td>
<td>118</td>
</tr>
<tr>
<td>t-ipconnect.de</td>
<td>108</td>
</tr>
<tr>
<td>cox.net</td>
<td>71</td>
</tr>
</tbody>
</table>
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
They like to talk...
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: 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: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:Body>
    <SearchPrincipalsResponse xmlns="http://schemas.microsoft.com/sharepoint/soap/">
      <SearchPrincipalsResults>
        <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"/>
          </MoreMatches>
        </PrincipalInfo>
      </SearchPrincipalsResults>
    </SearchPrincipalsResponse>
</soap:Body>
```

Nice conversation

Just be a member of a SharePoint site

» And you can:

<table>
<thead>
<tr>
<th>Request</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host:</td>
<td><code>&lt;SearchPrincipals xmlns=&quot;http://schemas.microsoft.com/sharepoint/soap/&quot;&gt;</code></td>
</tr>
<tr>
<td>Content-Type: application/soap+xml; charset=utf-8</td>
<td><code>&lt;maxResults&gt;</code>100<code>/maxResults&gt; </code>&lt;/searchPrincipals&gt;`</td>
</tr>
<tr>
<td>Content-Length: 481</td>
<td><code>&lt;principalType&gt;</code>All<code>/principalType&gt; </code>&lt;/SearchPrincipals&gt;`</td>
</tr>
<tr>
<td></td>
<td><code>&lt;soap2:Body&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;searchText&gt;</code>t<code>/searchText&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;principalType&gt;</code>All<code>/principalType&gt; </code>&lt;/SearchPrincipals&gt;`</td>
</tr>
</tbody>
</table>
I like WebDAV...

» And so should you
Mapped network drive
Introduction to Collaborative Application Markup Language (CAML)

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](http://msdn.microsoft.com/en-us/library/office/ms462365.aspx) and [HTML-Rendering Elements](http://msdn.microsoft.com/en-us/library/office/ms462365.aspx).

Using SPQuery and CAML (Collaborative Application Markup Language) is an efficient way to retrieve data in SharePoint list. It helps 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.

```csharp
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’s are smart!

Just do it on the client side...

» Do you like HTML5?

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 A rounds
Using some of the many SharePoint features

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

» 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>
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">
§A§</Execute>
</soap:Body></soap:Envelope>
What’s Next …

More Security Challenges ahead
There are many more security issues to talk about:

» Office caching of secured documents (encrypted but...)

» The SharePoint App-Store challenge

» SharePoint Social: Attackers are already following you

» The crawler service “creepy crawlies”
  Scoping search is harder than it looks
Thanks for coming out!

Jan Philipp
Solutions Consultant
Security

mobile: +49 171 740 6153
jan.philipp@nruns.com

Alexios Fakos
Principal Security Consultant

mobile: +49 151 5 500 2778
alexios.fakos@nruns.com

n.runs professionals GmbH
Nassauer Straße 60
D-61440 Oberursel

phone: +49 6171 699-370
fax: +49 6171 699-199

www.nruns.com

it. consulting . infrastructure . security . business