SharePoint Security Revealed

Thomas Röthlisberger – IT Security Analyst
thomas.roethlisberger@csnc.ch

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What is this talk about?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Agenda

What is SharePoint?

- Demo SharePoint

SharePoint Web Security

- Demo XSS and CSRF

Hardening Considerations

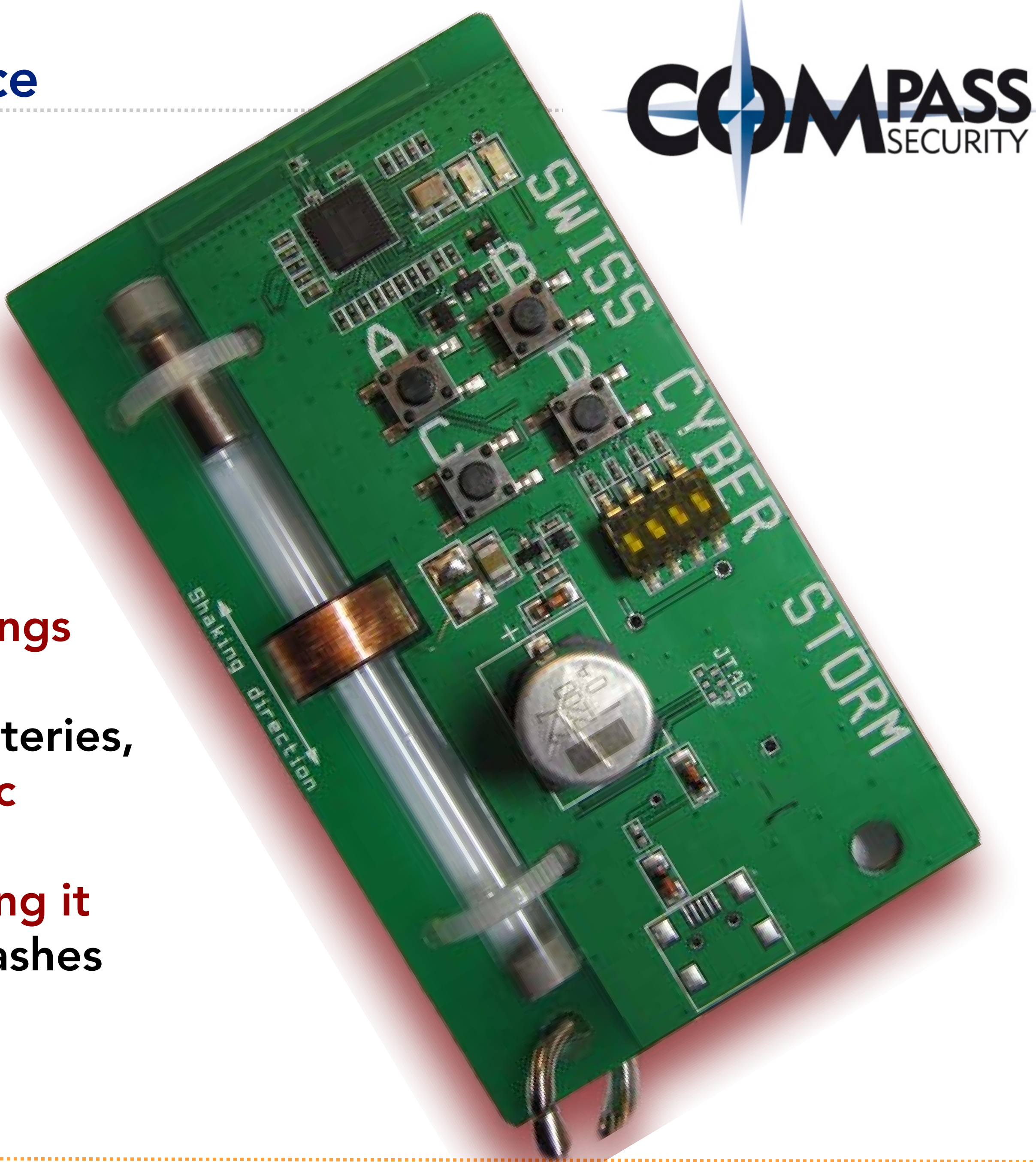
- Demo Hidden List and REST API

Conclusion

Quiz and Q&A

The Voting Device

The Voting Device



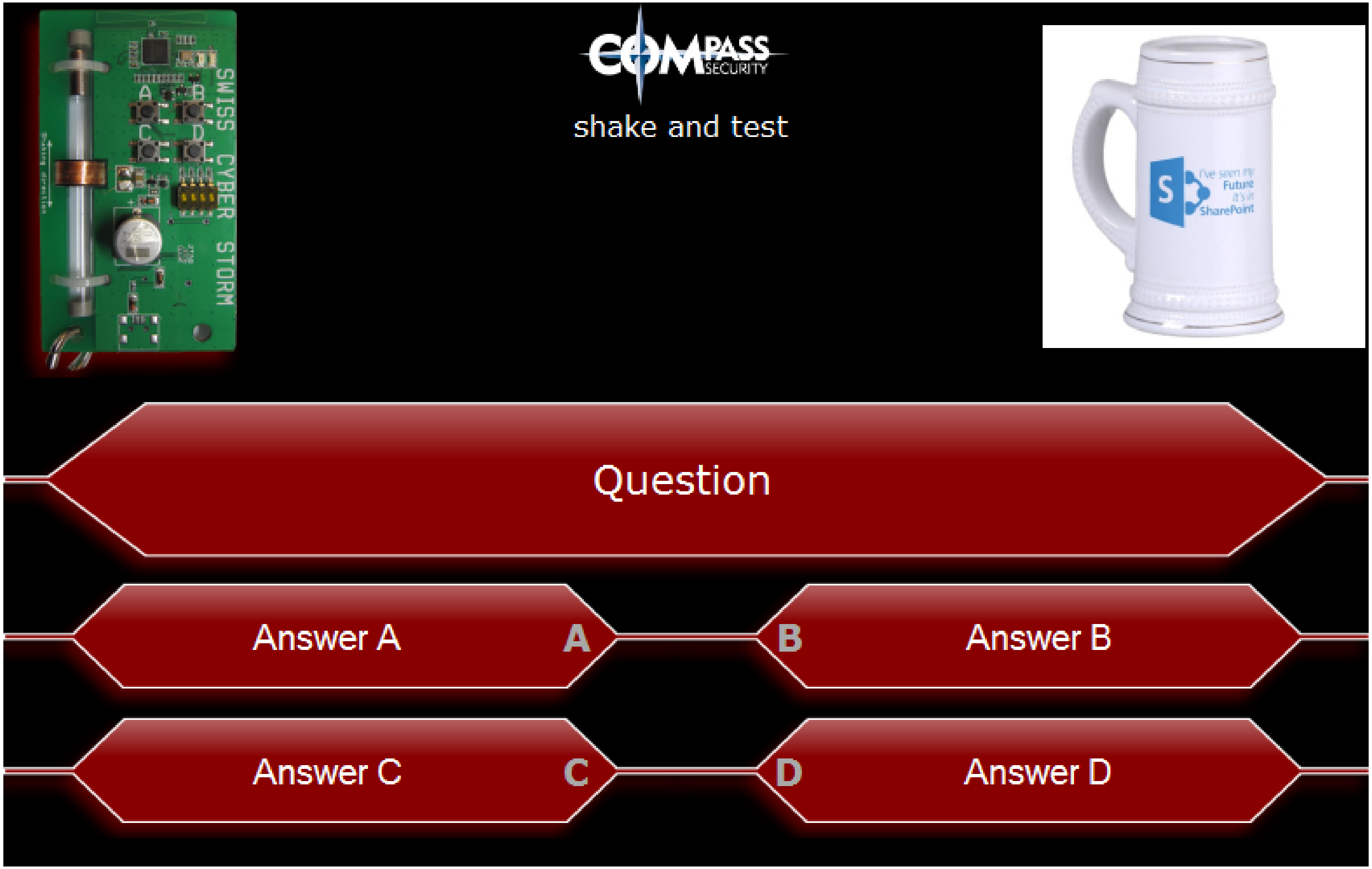
It enables you to
participate on votings

The device has no batteries,
so it works autarkic

You power it by shaking it
until green light flashes

The Voting

Let's give it a try…



What is SharePoint?

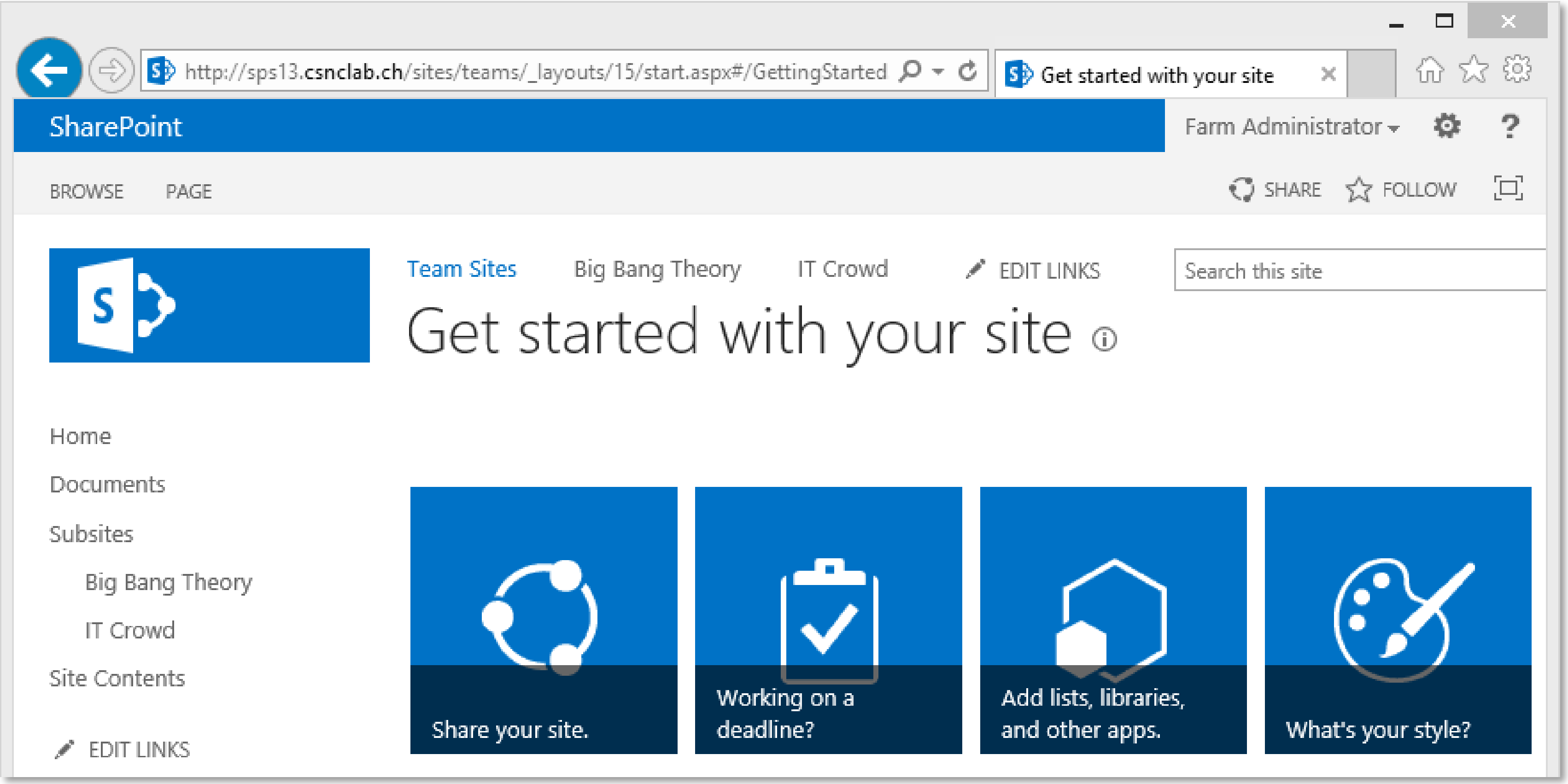
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What is SharePoint?

Browser-based collaboration and content management platform

The latest release of the product is SharePoint 2013



http://sps13.csnclab.ch/sites/teams/_layouts/15/start.aspx#/GettingStarted

Get started with your site

Terminology

Web Application

Site Collection

Site

Subsite

List

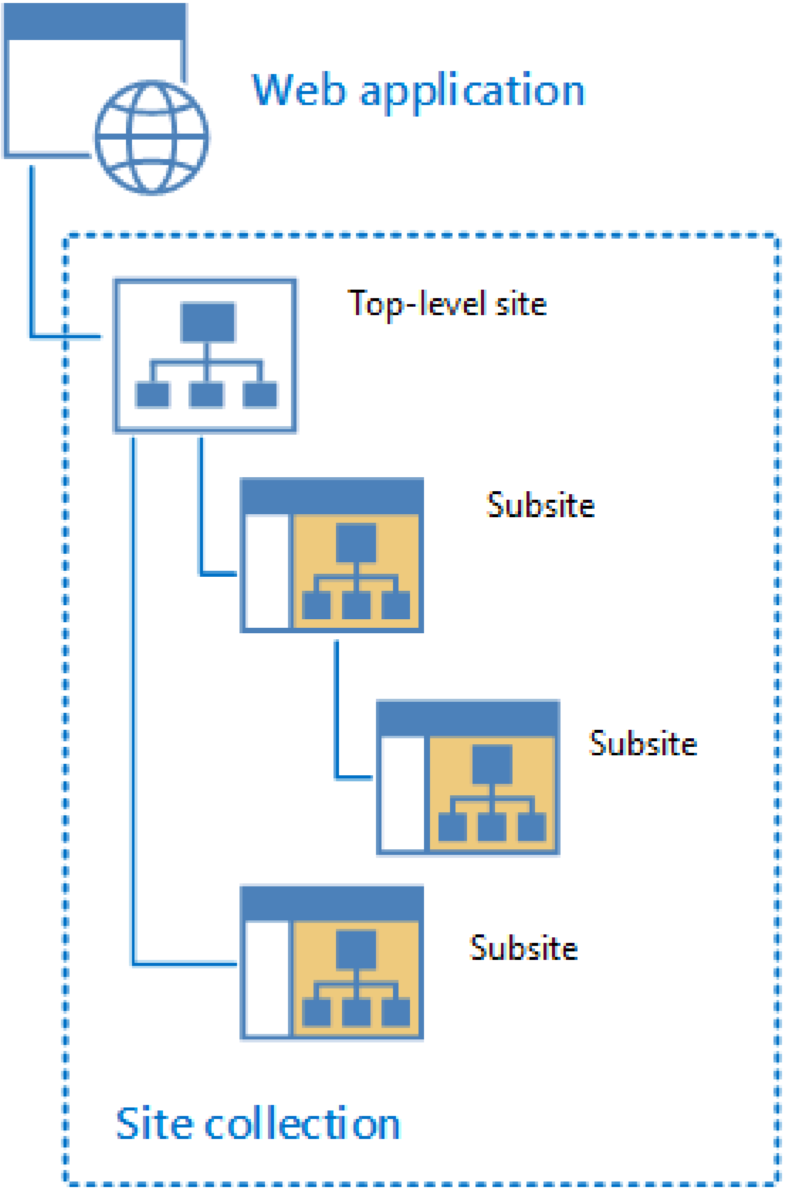
Custom List

Document Library

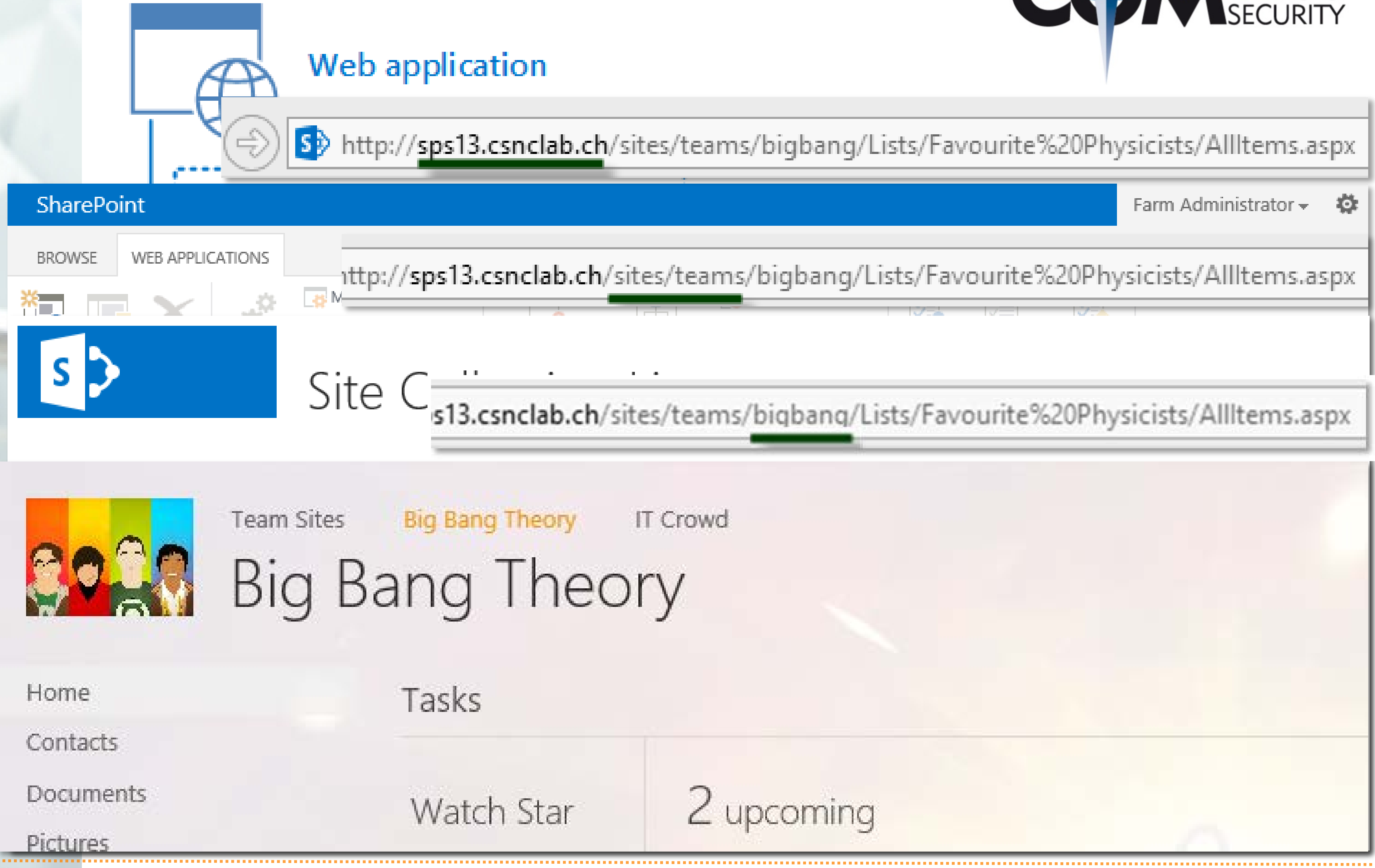
Web Parts

Apps

Web Application, Site Collection, Site



Web Application, Site Collection, Site



Web application

http://sps13.csnclab.ch/sites/teams/bigbang/Lists/Favourite%20Physicists/AllItems.aspx

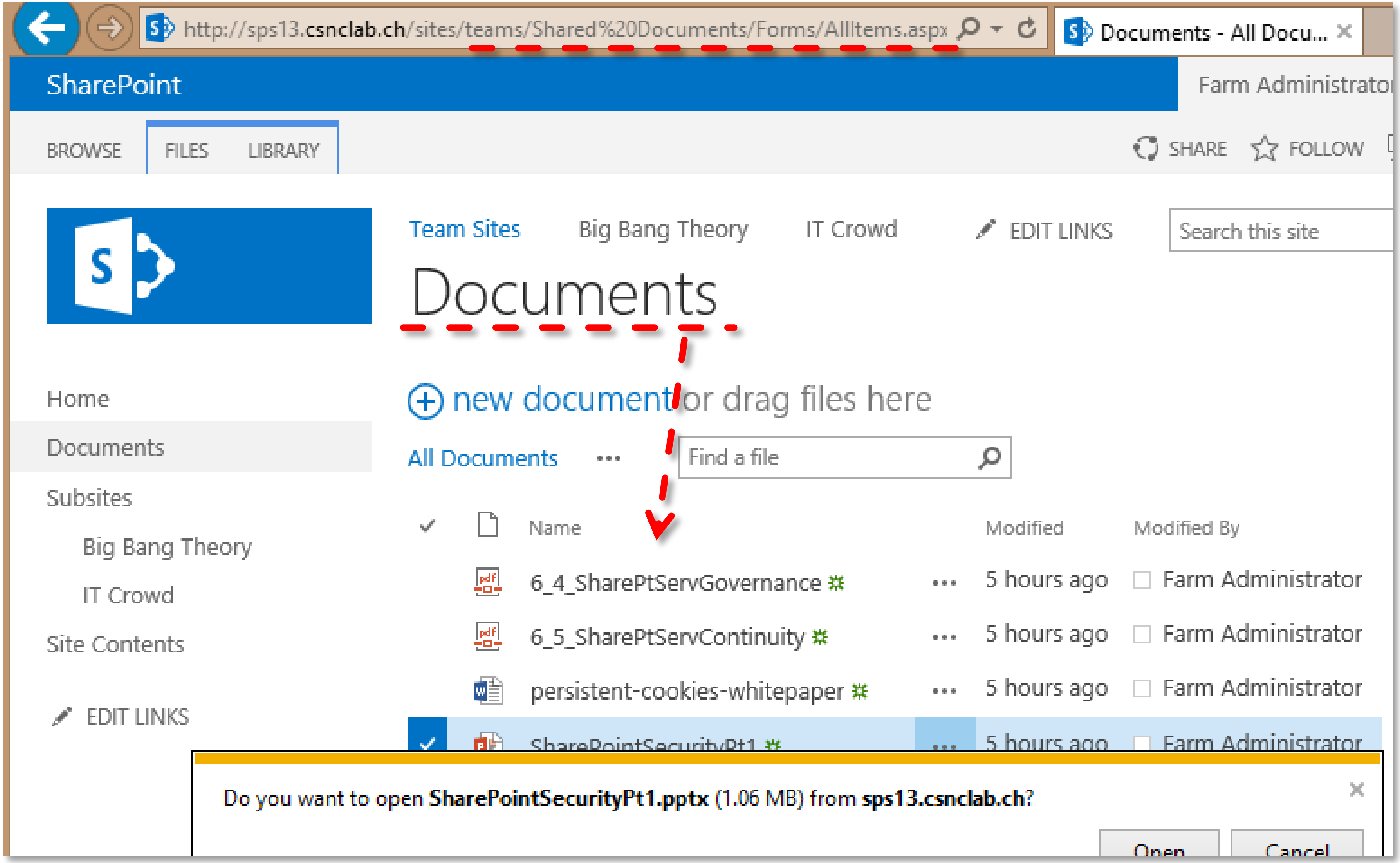
ttp://sps13.csnclab.ch/sites/teams/bigbang/Lists/Favourite%20Physicists/AllItems.aspx

Site C

s13.csnclab.ch/sites/teams/bigbang/Lists/Favourite%20Physicists/AllItems.aspx

Document Libraries

Document Libraries contain files:



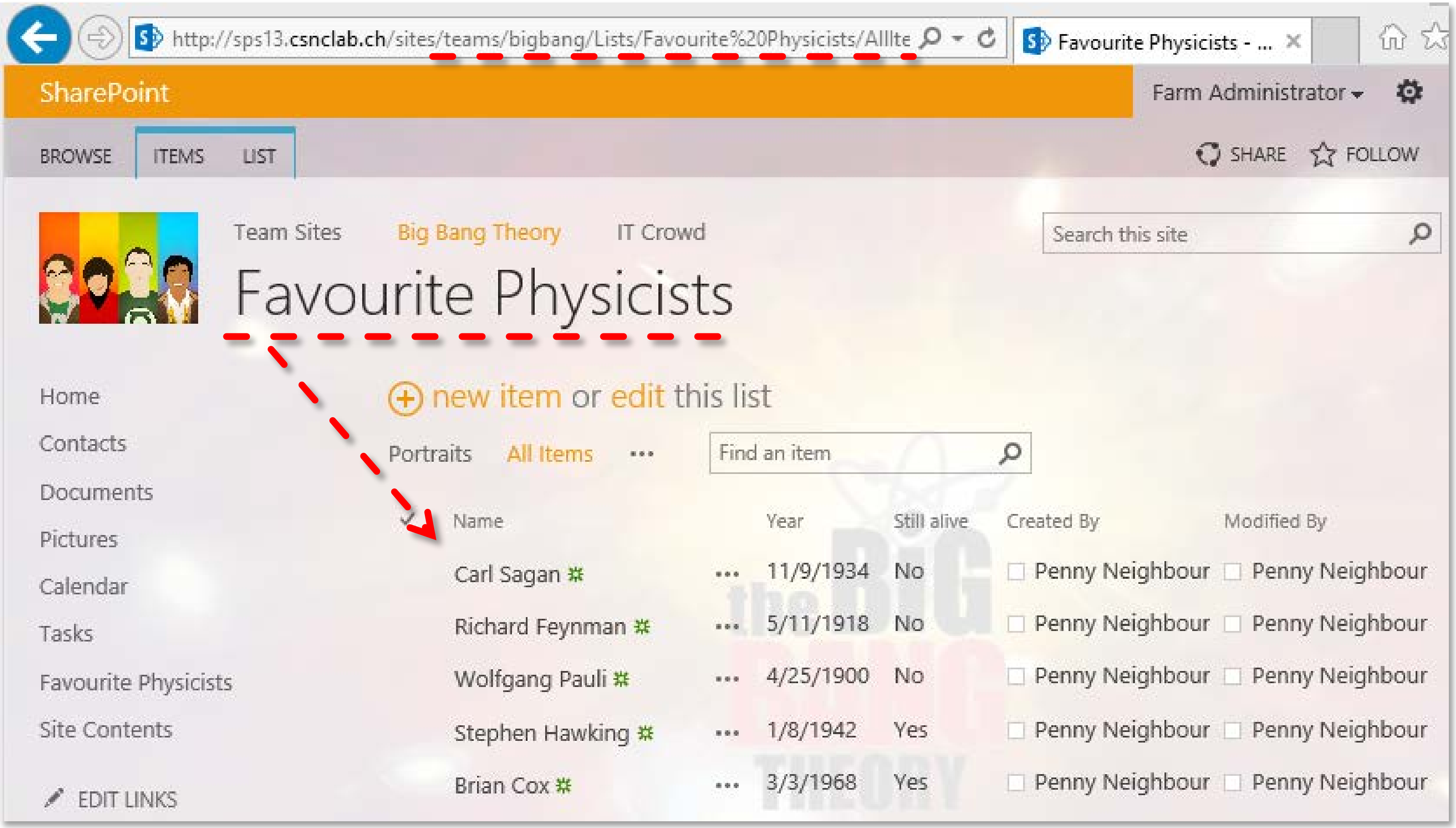
http://sps13.csnclab.ch/sites/teams/Shared%20Documents/Forms/AllItems.aspx

Do you want to open **SharePointSecurityPt1.pptx** (1.06 MB) from **sps13.csnclab.ch**?

	Name		Modified	Modified By
	6_4_SharePtServGovernance	•••	5 hours ago	Farm Administrator
	6_5_SharePtServContinuity	•••	5 hours ago	Farm Administrator
	persistent-cookies-whitepaper	•••	5 hours ago	Farm Administrator
✓	SharePointSecurityPt1	•••	5 hours ago	Farm Administrator

Lists and Custom Lists

Lists and Custom Lists contain structured information:



http://sps13.csnclab.ch/sites/teams/bigbang/Lists/Favourite%20Physicists/AllIte

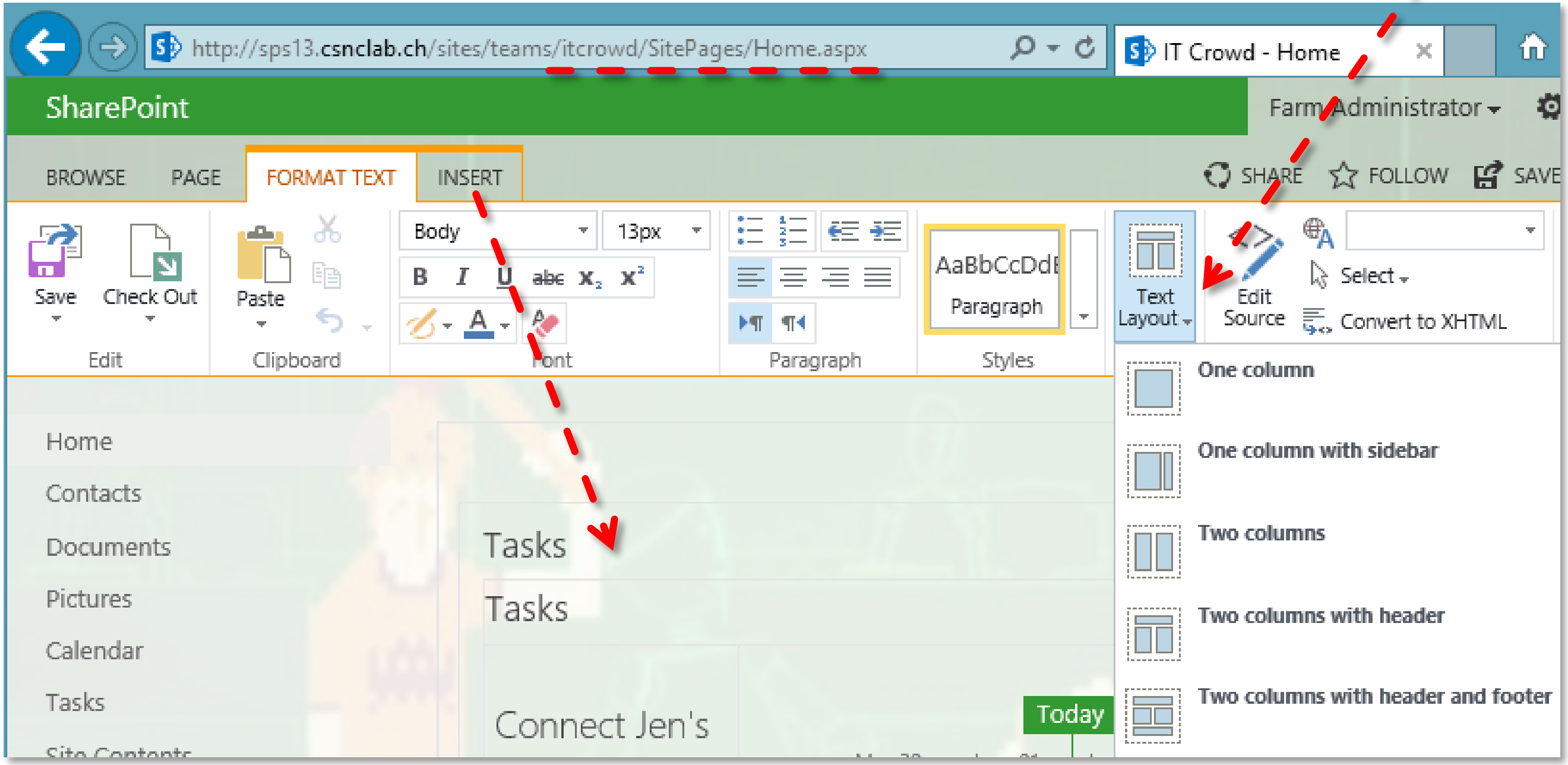
Favourite Physicists

Name		Year	Still alive	Created By	Modified By
Carl Sagan	...	11/9/1934	No	Penny Neighbour	Penny Neighbour
Richard Feynman	...	5/11/1918	No	Penny Neighbour	Penny Neighbour
Wolfgang Pauli	...	4/25/1900	No	Penny Neighbour	Penny Neighbour
Stephen Hawking	...	1/8/1942	Yes	Penny Neighbour	Penny Neighbour
Brian Cox	...	3/3/1968	Yes	Penny Neighbour	Penny Neighbour

Web Part Pages

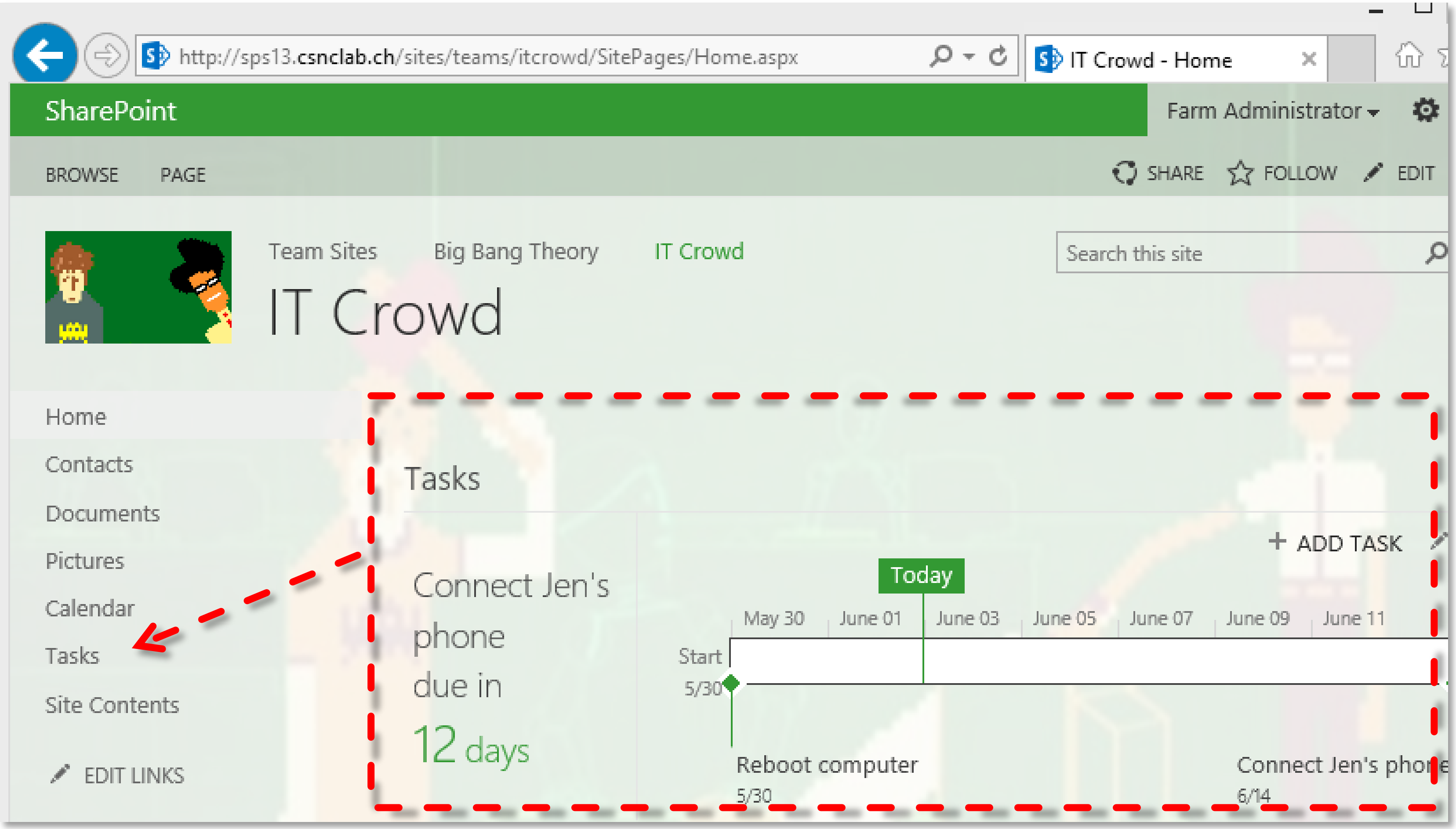
A web site in SharePoint is built with Web Part Pages

Web Part Pages host Web Parts and App Parts on a given layout


http://sps13.csnclab.ch/sites/teams/itcrowd/SitePages/Home.aspx

Web Parts

Web Parts render data from Doc. Libraries, Lists and other sources



http://sps13.csnclab.ch/sites/teams/itcrowd/SitePages/Home.aspx

IT Crowd - Home

SharePoint

Farm Administrator

BROWSE PAGE

SHARE FOLLOW EDIT

Team Sites Big Bang Theory IT Crowd

Search this site

IT Crowd

- Home
- Contacts
- Documents
- Pictures
- Calendar
- Tasks
- Site Contents

EDIT LINKS

Tasks

+ ADD TASK

Connect Jen's phone due in 12 days

Today

May 30 June 01 June 03 June 05 June 07 June 09 June 11

Start 5/30

Reboot computer 5/30

Connect Jen's phone 6/14

Apps

Apps do the same as Web Parts, but are much more limited.

Apps do not allow any code behind to access SharePoint server-side objects.

Apps can create Lists and Doc Libraries, but they are stored in a dedicated Site Collection on a different domain.

Apps are isolated on client side in iFrames (The Same Origin Policy prevents access to the data of your web site).

Apps

Apps do the same as Web Parts, but are much more limited.

Apps do not allow any code behind to access SharePoint server-side objects.

Apps can create Lists and Doc Libraries, but they are stored in a dedicated Site Collection on a different subdomain.

Apps are isolated on client side in iFrames (The Same Origin Policy prevents access to the data of your web site).

Everything is an App!

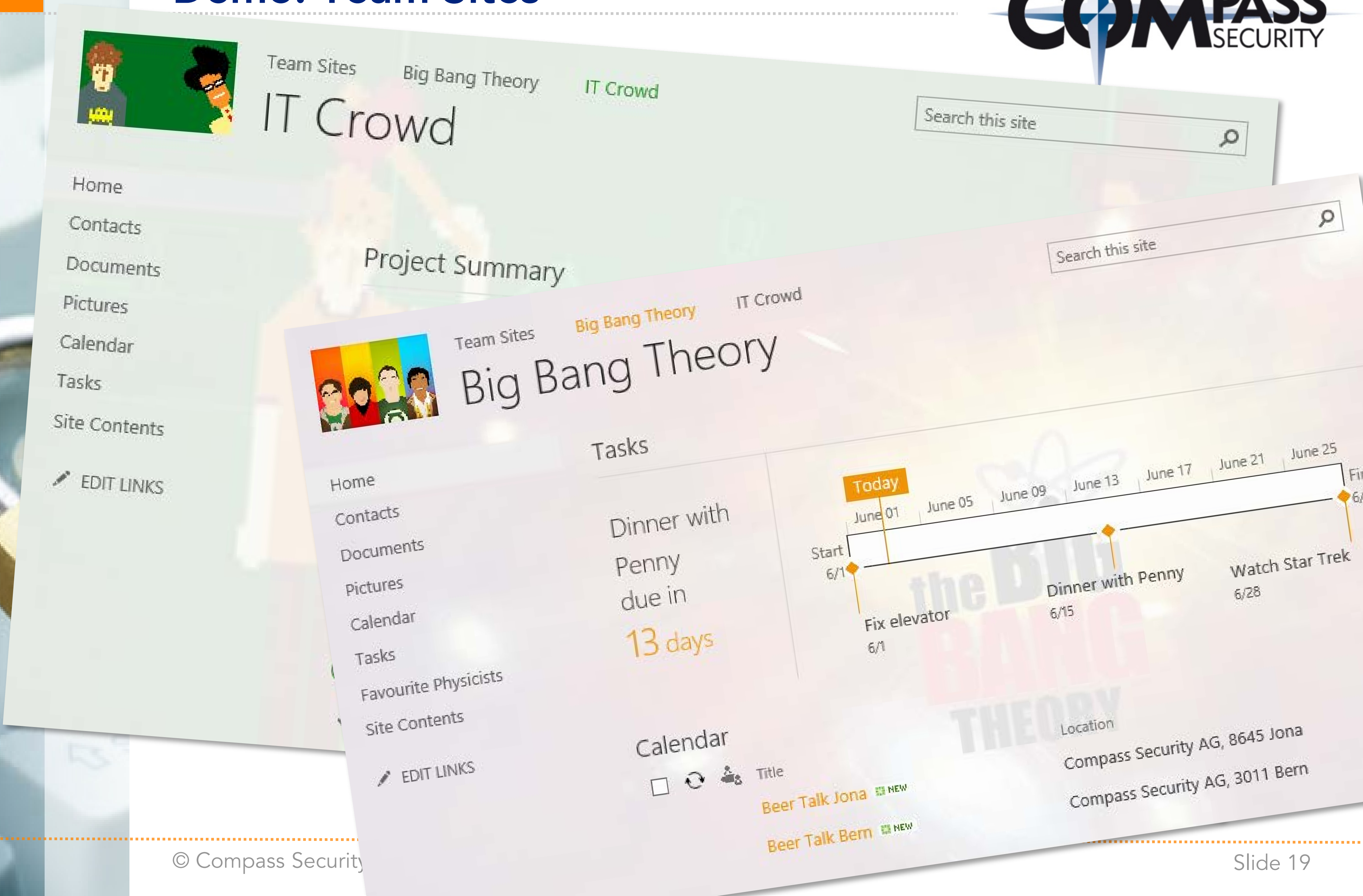
==> To make it easier for end-users, Microsoft now calls everything an app, but technically this is not true.

==> Built-in "apps" like Tasks, Contacts or Calendar are not isolated in a dedicated site collection.

Site Templates

Type	Name	Description
Collaboration	Team Site	A place to work together with a group of people.
	Project Site	A site for managing and collaborating on a project.
Publishing	Publishing Portal	A starter hierarchy for an Internet-facing site or a large intranet portal.
	Enterprise Wiki	A site for publishing knowledge that you capture and want to share.

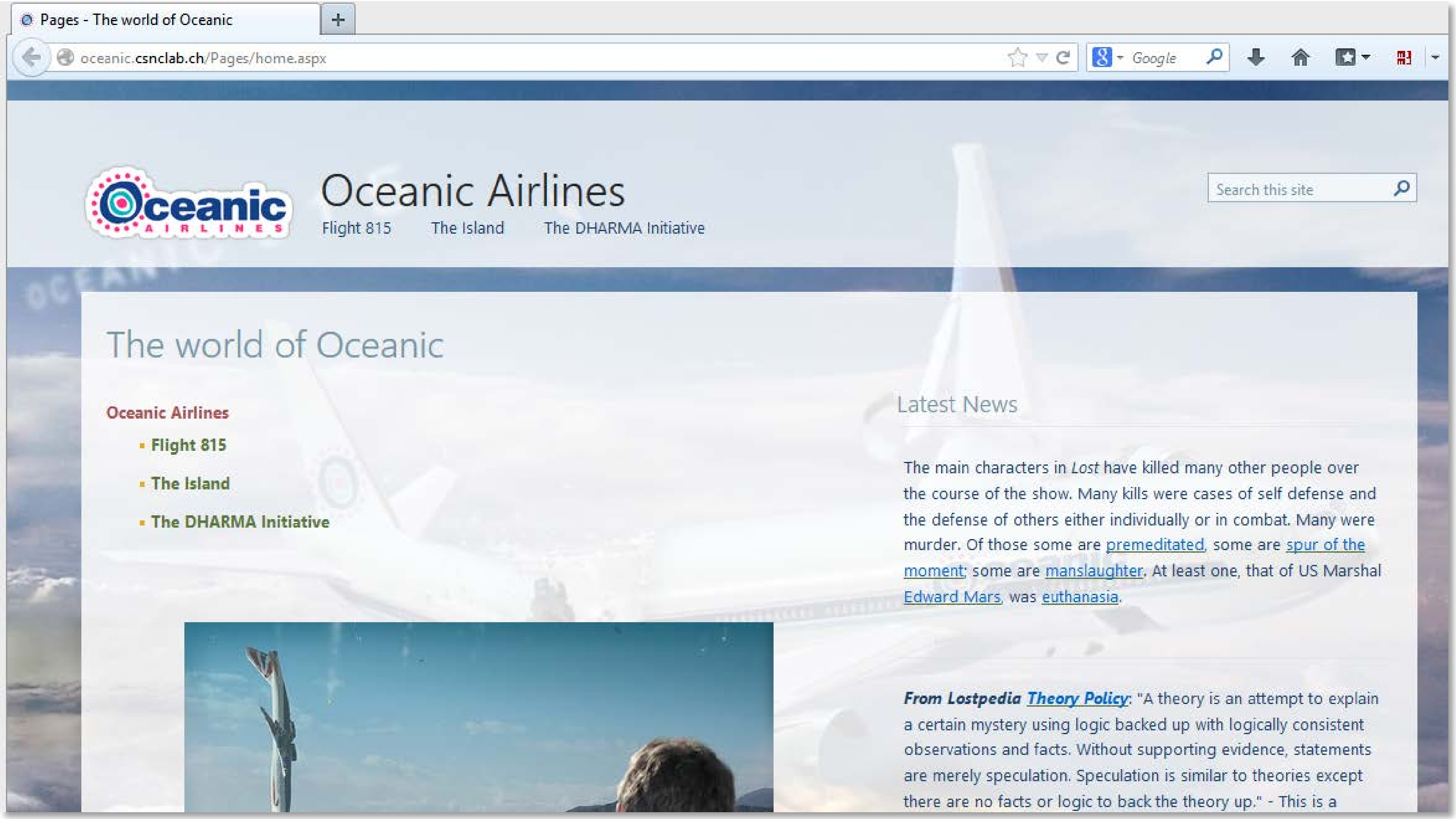
Demo: Team Sites



Dinner with Penny due in 13 days

Web Site (Publishing Portal)

Internet-facing Web Sites are published for Anonymous Users:



Pages - The world of Oceanic
oceanic.csnclab.ch/Pages/home.aspx
Google
Oceanic AIRLINES
Search this site

Oceanic Airlines

Flight 815 The Island The DHARMA Initiative

The world of Oceanic

Oceanic Airlines

- Flight 815
- The Island
- The DHARMA Initiative

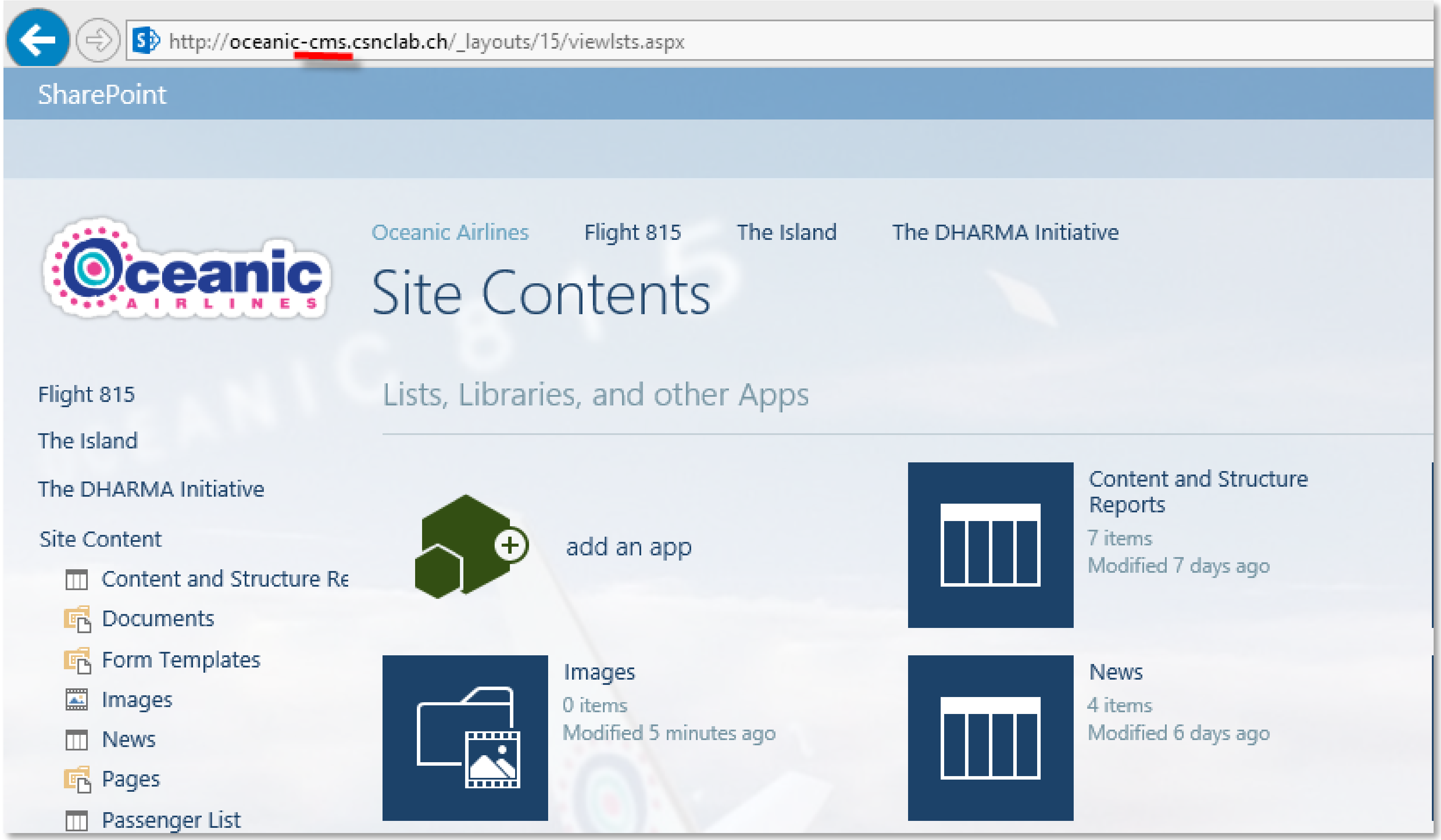
Latest News

The main characters in *Lost* have killed many other people over the course of the show. Many kills were cases of self defense and the defense of others either individually or in combat. Many were murder. Of those some are premeditated, some are spur of the moment; some are manslaughter. At least one, that of US Marshal Edward Mars, was euthanasia.

From Lostpedia Theory Policy: "A theory is an attempt to explain a certain mystery using logic backed up with logically consistent observations and facts. Without supporting evidence, statements are merely speculation. Speculation is similar to theories except there are no facts or logic to back the theory up." - This is a

Web Site (Publishing Portal)

Editors use an internal URL to author the content:



http://oceanic-cms.csnclab.ch/_layouts/15/viewlsts.aspx

SharePoint

Oceanic Airlines | Flight 815 | The Island | The DHARMA Initiative

Site Contents

Flight 815

The Island

The DHARMA Initiative

Site Content

- Content and Structure Re
- Documents
- Form Templates
- Images
- News
- Pages
- Passenger List

Lists, Libraries, and other Apps

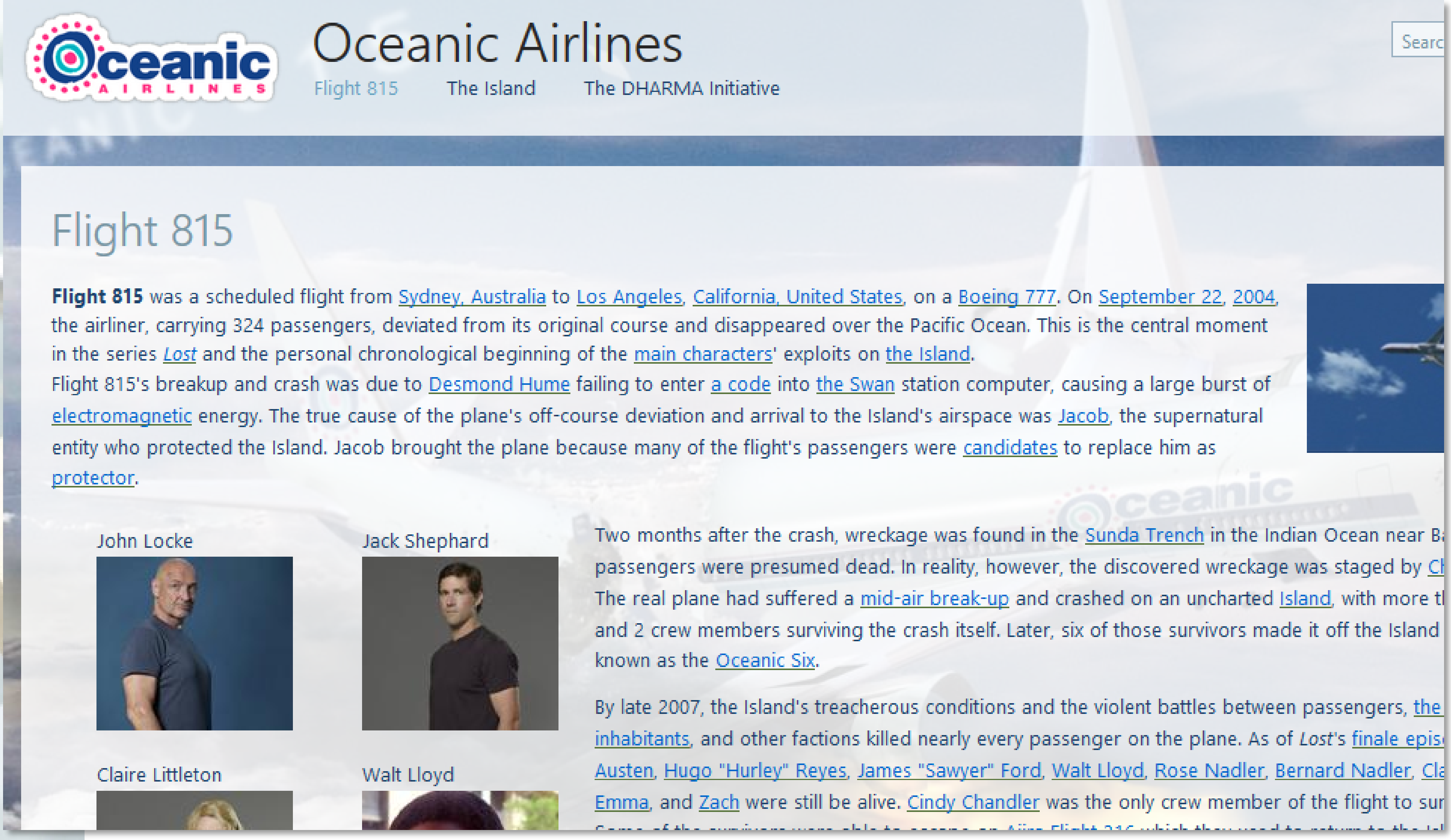
add an app

Content and Structure Reports
7 items
Modified 7 days ago

Images
0 items
Modified 5 minutes ago

News
4 items
Modified 6 days ago

Demo: Public Web Site



Oceanic Airlines

Flight 815 The Island The DHARMA Initiative

Flight 815

Flight 815 was a scheduled flight from Sydney, Australia to Los Angeles, California, United States, on a Boeing 777. On September 22, 2004, the airliner, carrying 324 passengers, deviated from its original course and disappeared over the Pacific Ocean. This is the central moment in the series *Lost* and the personal chronological beginning of the main characters' exploits on the Island.

Flight 815's breakup and crash was due to Desmond Hume failing to enter a code into the Swan station computer, causing a large burst of electromagnetic energy. The true cause of the plane's off-course deviation and arrival to the Island's airspace was Jacob, the supernatural entity who protected the Island. Jacob brought the plane because many of the flight's passengers were candidates to replace him as protector.

John Locke

Jack Shephard

Claire Littleton

Walt Lloyd

Two months after the crash, wreckage was found in the Sunda Trench in the Indian Ocean near Ba
passengers were presumed dead. In reality, however, the discovered wreckage was staged by Ch
The real plane had suffered a mid-air break-up and crashed on an uncharted Island, with more th
and 2 crew members surviving the crash itself. Later, six of those survivors made it off the Island
known as the Oceanic Six.

By late 2007, the Island's treacherous conditions and the violent battles between passengers, the
inhabitants, and other factions killed nearly every passenger on the plane. As of *Lost*'s finale epis
Austen, Hugo "Hurley" Reyes, James "Sawyer" Ford, Walt Lloyd, Rose Nadler, Bernard Nadler, Cla
Emma, and Zach were still be alive. Cindy Chandler was the only crew member of the flight to sur
Some of the survivors were able to escape on Ajira Flight 316 which they used to return to the Isl

SharePoint Web Security

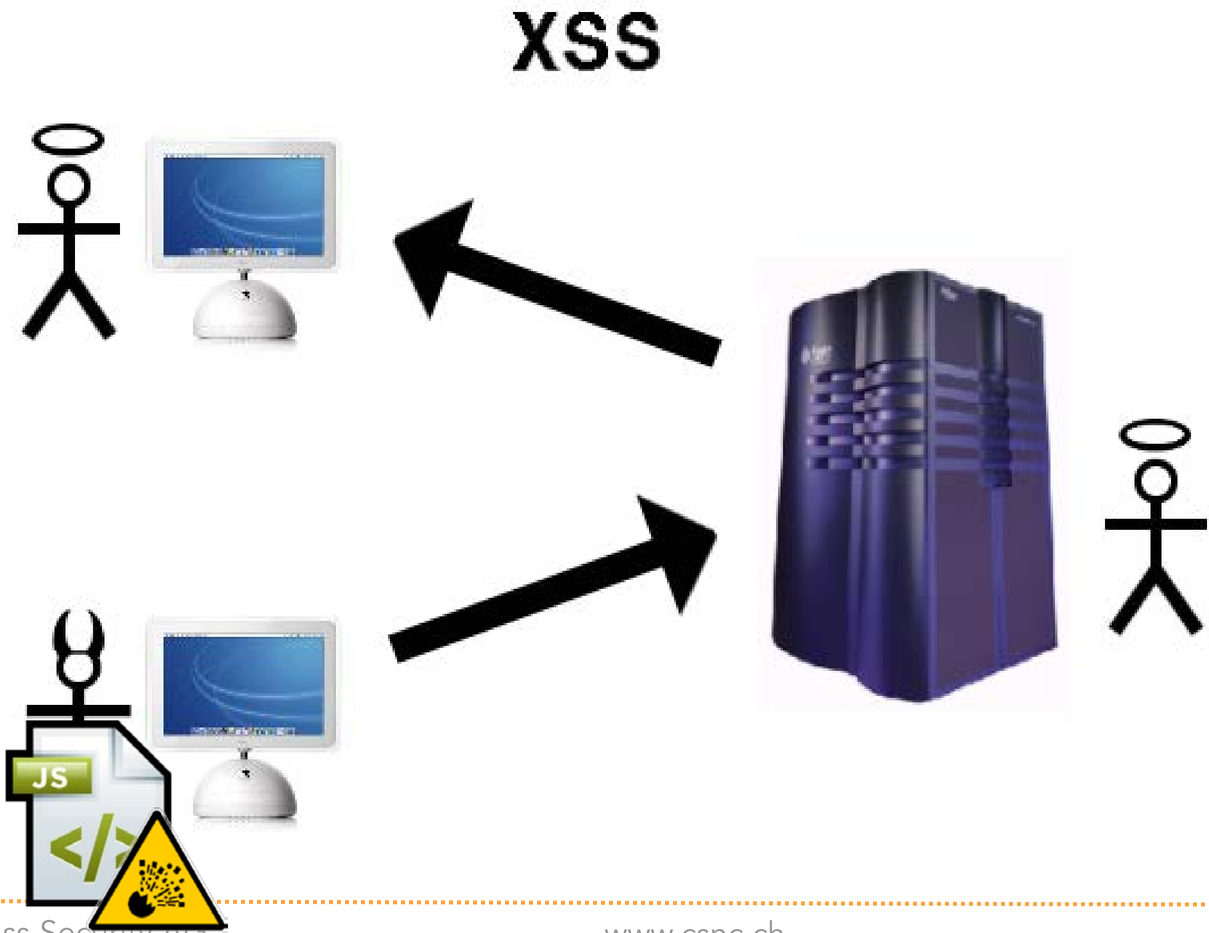
Cross-Site Scripting (XSS)

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Cross-Site Scripting

With Cross-Site Scripting vulnerabilities, attackers are able to execute JavaScript code in the users' context



Cross-Site Scripting – Threats

Stealing user sessions (cookie value) to gain access to the application.

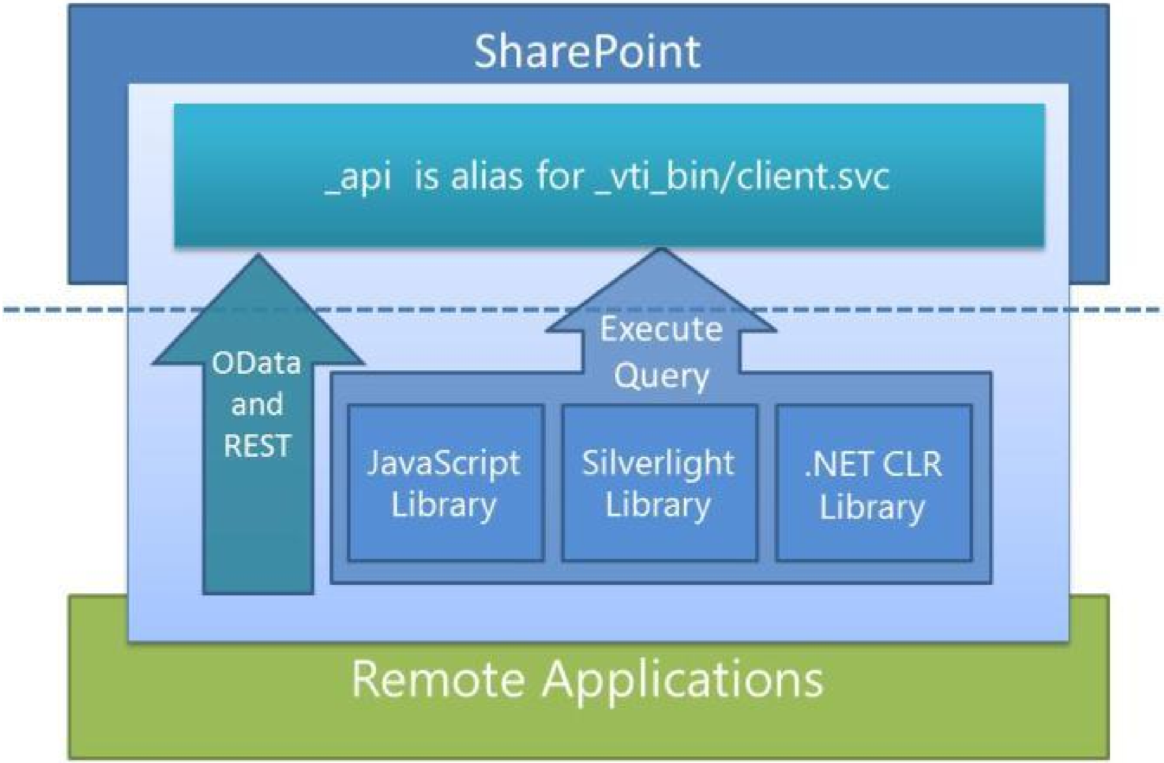
Usually not relevant on SharePoint Web Applications (Windows Integrated Authentication or HttpOnly Flag set).

However, cookies of other applications on the same domain can be stolen.

Cross-Site Scripting – Threats

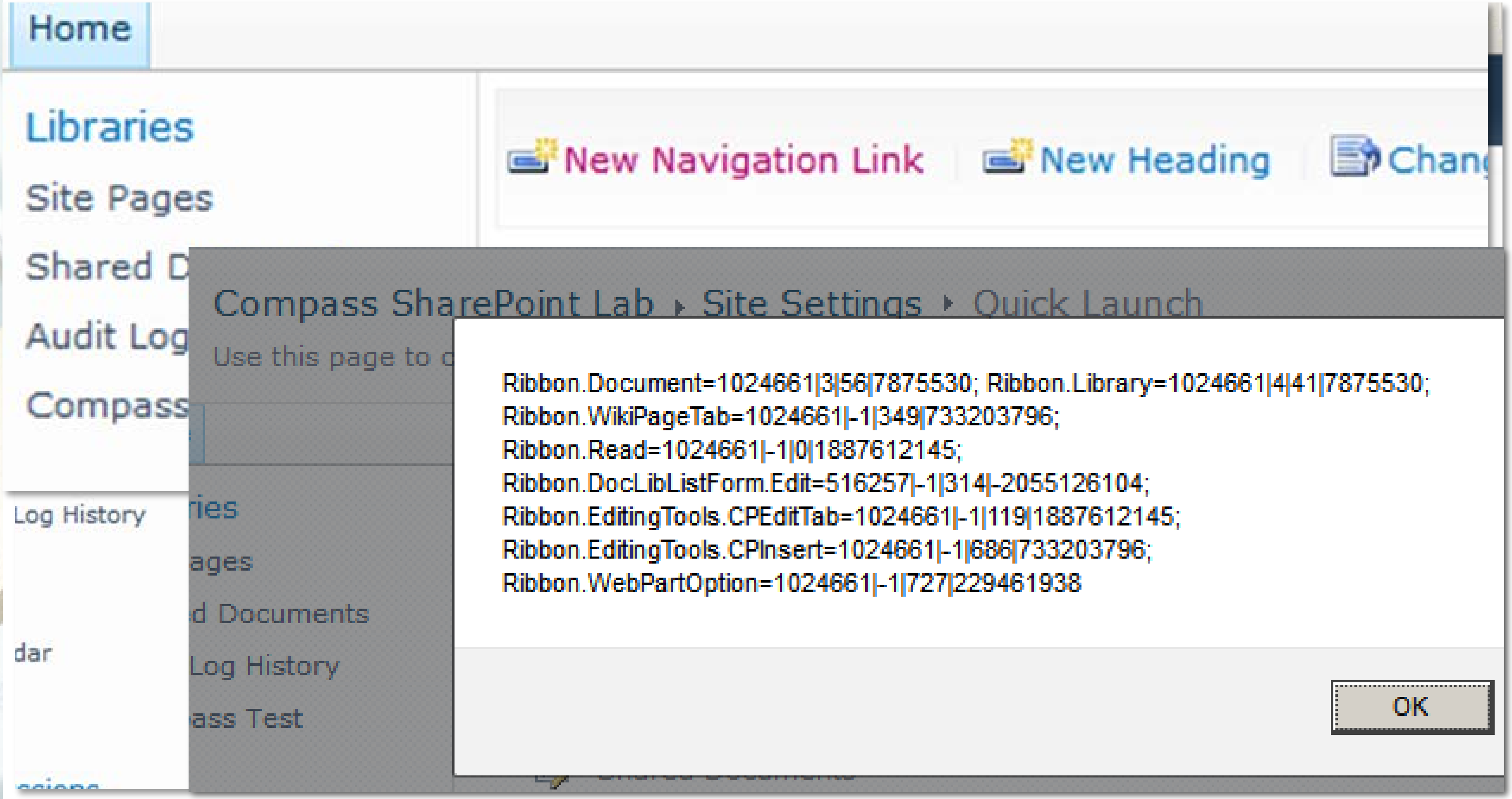
Sending requests on behalf of the currently logged in user.

On SharePoint 2013 the JavaScript Client-Side Object Model (CSOM) allows comfortable access to all the data stored in SharePoint.



Cross-Site Scripting – Navigation

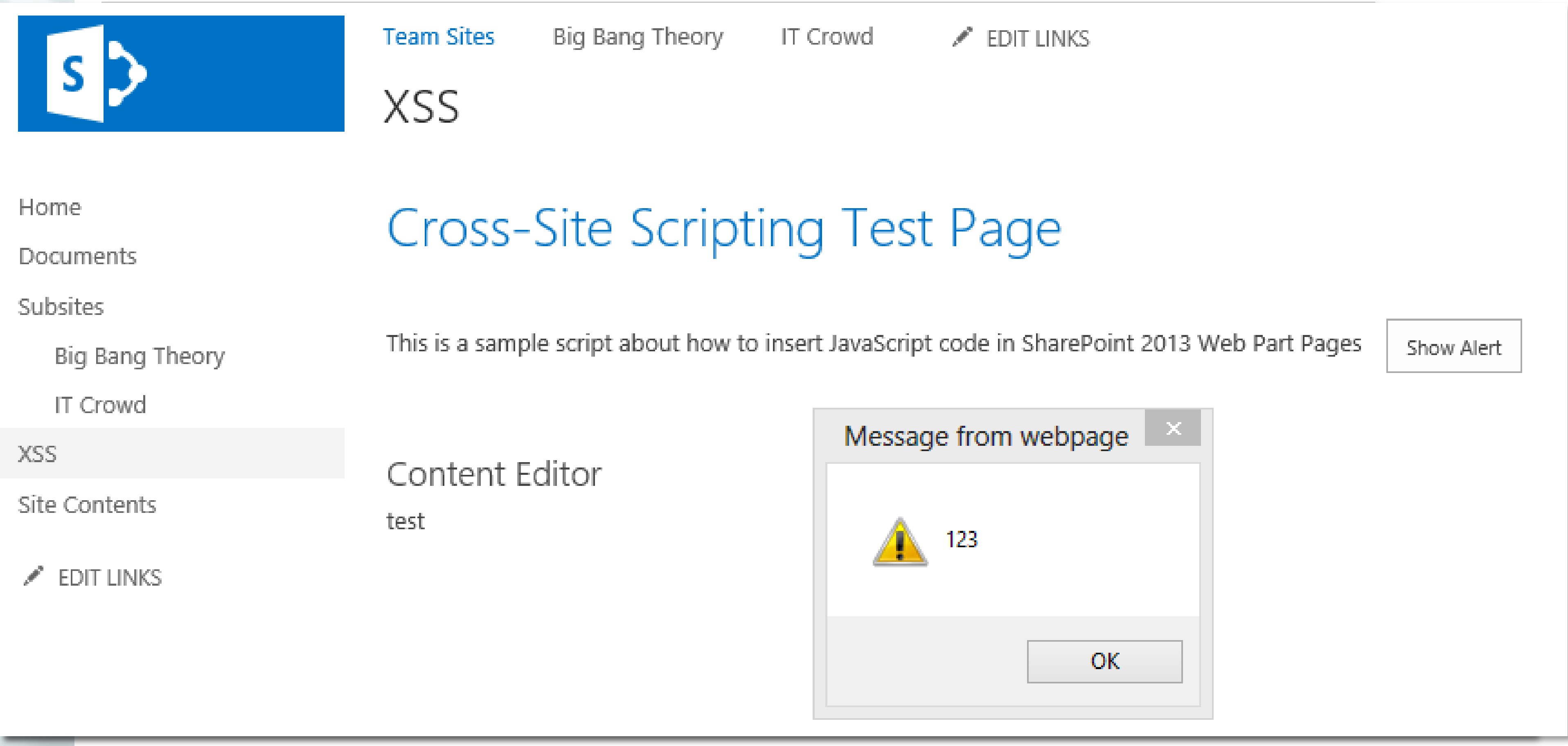
Default SharePoint Features: Navigation Links (2010 only)



```
Ribbon.Document=1024661|3|56|7875530; Ribbon.Library=1024661|4|41|7875530;
Ribbon.WikiPageTab=1024661|-1|349|733203796;
Ribbon.Read=1024661|-1|0|1887612145;
Ribbon.DocLibListForm.Edit=516257|-1|314|-2055126104;
Ribbon.EditingTools.CPEditTab=1024661|-1|119|1887612145;
Ribbon.EditingTools.CPInsert=1024661|-1|686|733203796;
Ribbon.WebPartOption=1024661|-1|727|229461938
```

Cross-Site Scripting – Web Parts

Default SharePoint Features: Web Parts (e.g. Script / Content Editor Web Parts)



XSS

Cross-Site Scripting Test Page

This is a sample script about how to insert JavaScript code in SharePoint 2013 Web Part Pages

Content Editor

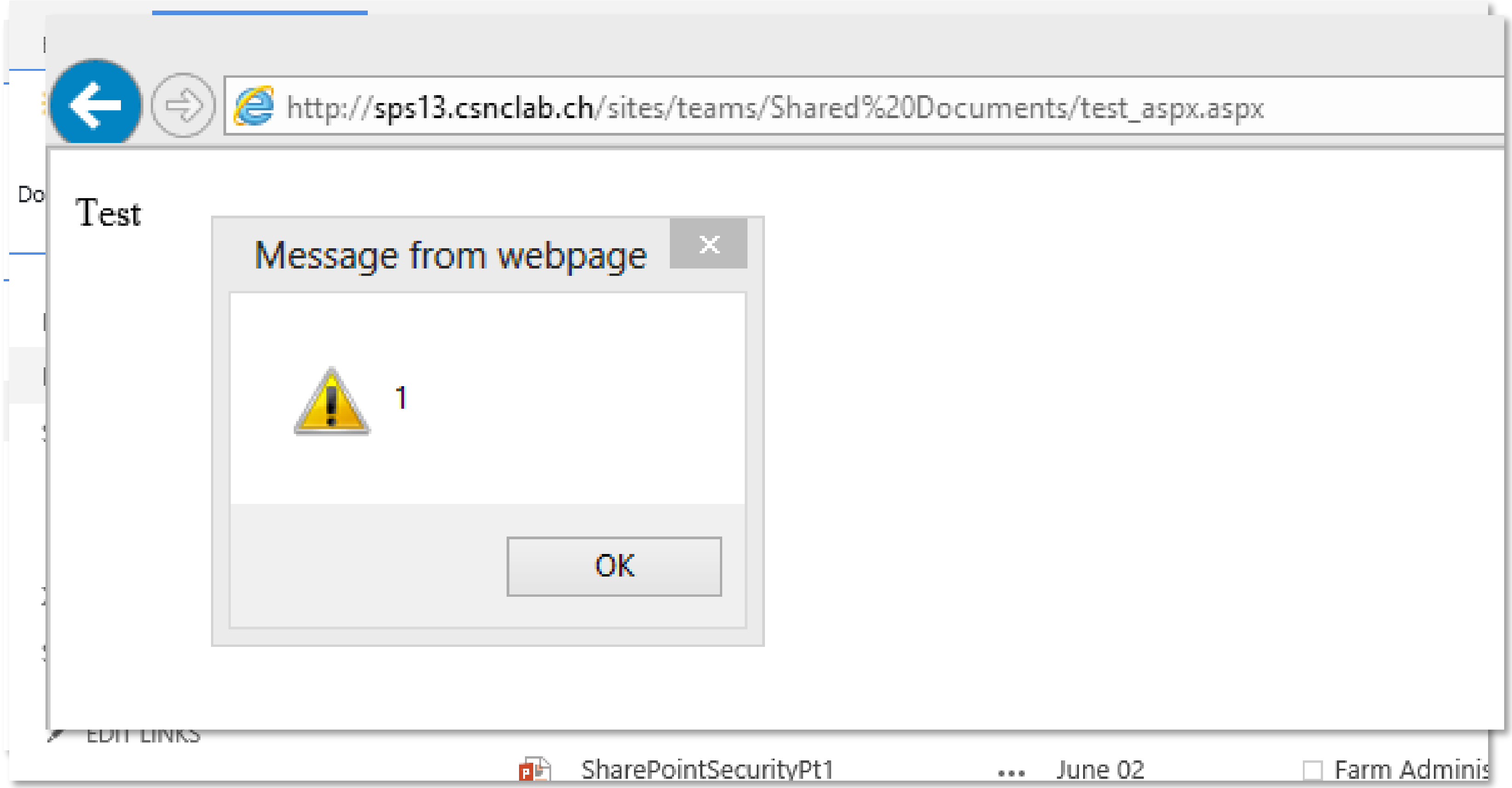
test

Message from webpage

123

Cross-Site Scripting – ASP.NET Pages

Default SharePoint Features: ASP.NET / Web Part Pages (Edit or upload .aspx page)



http://sps13.csnclab.ch/sites/teams/Shared%20Documents/test_aspx.aspx

Test

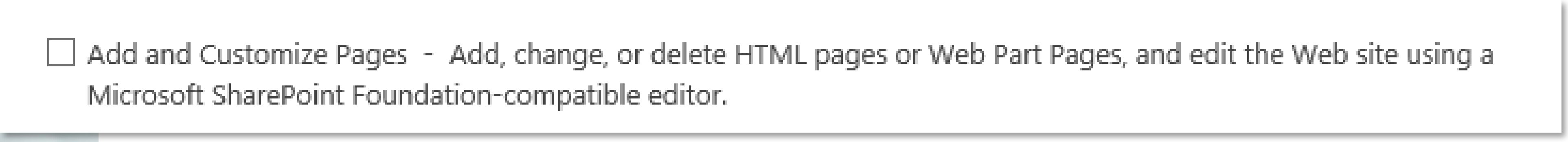
Message from webpage

1

Cross-Site Scripting – Web Parts

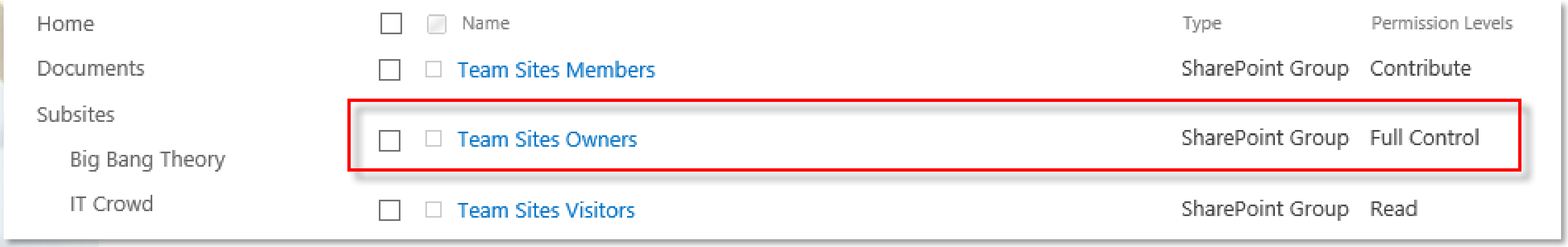
Pre-Conditions I:

- Users with sufficient permissions can include JavaScript by Design
- "**Add & Customize Pages**" Permission is required



□ Add and Customize Pages - Add, change, or delete HTML pages or Web Part Pages, and edit the Web site using a Microsoft SharePoint Foundation-compatible editor.

- Not included in "Contribute" permission level and below (Since SP 2010)
- Included in "Designer" and "Full Control" permission levels

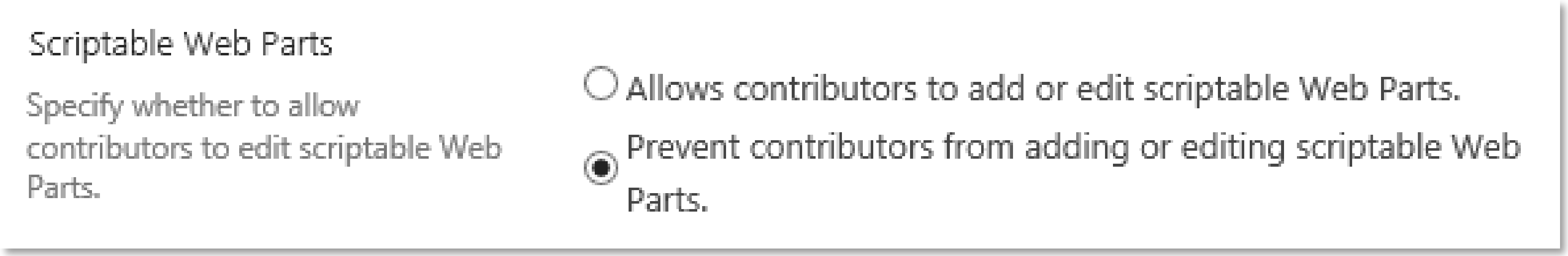


□	□ Name	Type	Permission Levels
□	□ Team Sites Members	SharePoint Group	Contribute
□	□ Team Sites Owners	SharePoint Group	Full Control
□	□ Team Sites Visitors	SharePoint Group	Read

Cross-Site Scripting – Web Parts

Pre-Conditions II:

- Only applied consequently if Web Part Security Setting is not changed:



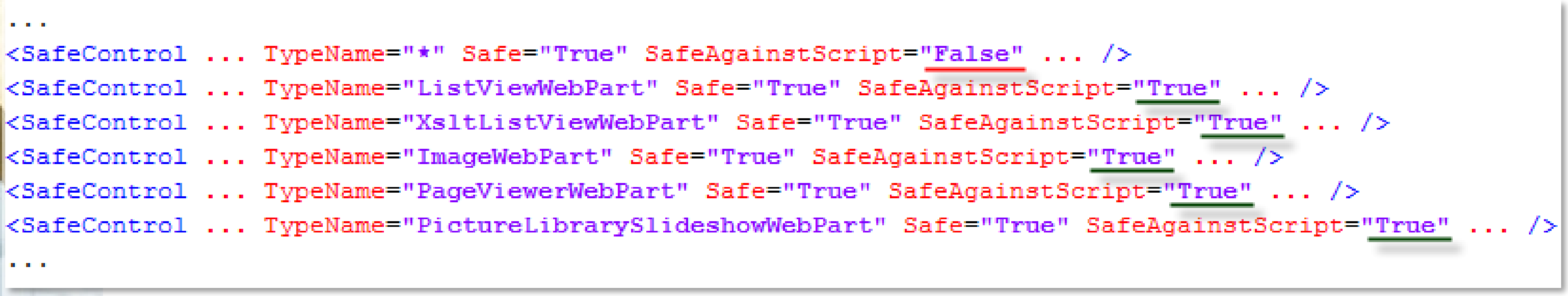
Scriptable Web Parts

Specify whether to allow contributors to edit scriptable Web Parts.

○ Allows contributors to add or edit scriptable Web Parts.

● Prevent contributors from adding or editing scriptable Web Parts.

- And Web Parts are declared correctly in the web.config



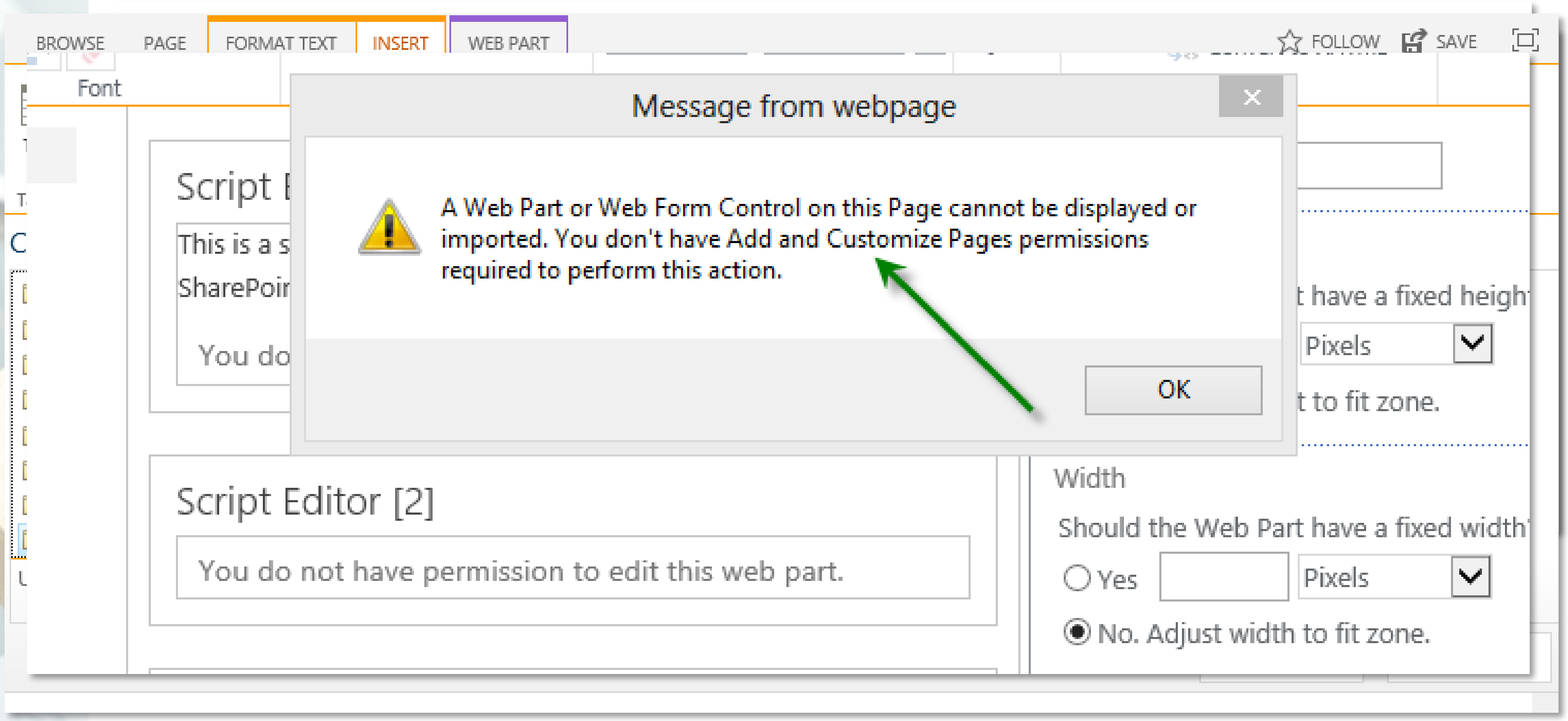
```
...
<SafeControl ... TypeName="*" Safe="True" SafeAgainstScript="False" ... />
<SafeControl ... TypeName="ListViewWebPart" Safe="True" SafeAgainstScript="True" ... />
<SafeControl ... TypeName="XsltListViewWebPart" Safe="True" SafeAgainstScript="True" ... />
<SafeControl ... TypeName="ImageWebPart" Safe="True" SafeAgainstScript="True" ... />
<SafeControl ... TypeName="PageViewerWebPart" Safe="True" SafeAgainstScript="True" ... />
<SafeControl ... TypeName="PictureLibrarySlideshowWebPart" Safe="True" SafeAgainstScript="True" ... />
...
```

Cross-Site Scripting – Web Parts

Permission Level	SharePoint Version	Web Part Security Setting	SafeAgainstScript
Full Control (Owner)	2007 and older	N/A	N/A
	2010 and newer	Allow Contributors	True
			False
		Prevent Contributors	True
			False
Contribute (Member)	2007 and older	N/A	N/A
	2010 and newer	Allow Contributors	True
			False
		Prevent Contributors	True
			False

Cross-Site Scripting – Web Parts

Trying to inject JavaScript code as Contributor without permissions



Message from webpage

A Web Part or Web Form Control on this Page cannot be displayed or imported. You don't have Add and Customize Pages permissions required to perform this action.

Script Editor [2]

You do not have permission to edit this web part.

Should the Web Part have a fixed width?

○ Yes Pixels

● No. Adjust width to fit zone.

Cross-Site Scripting – Web Sensitive Files

Web Sensitive Files can be used to embed malicious content like JavaScript

Therefore only users with "Add & Customize Pages" permissions are allowed to add and modify Web Sensitive Files

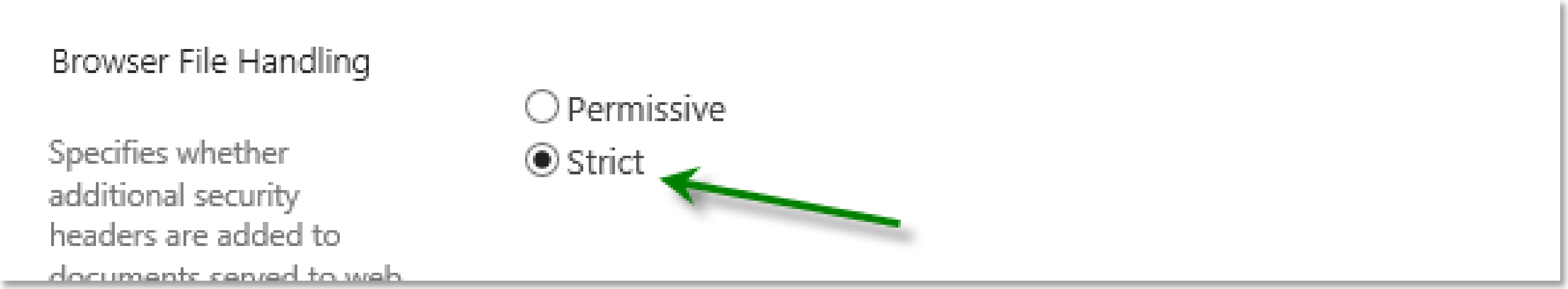
By default, Web Sensitive Files are:

- ascx
- asmx
- Aspx (ASP.NET pages)
- Jar (Java)
- master
- Swf (Flash)
- xap
- xsf
- xsn

Cross-Site Scripting – Web Sensitive Files

The Web Sensitive File Types are not complete. Other dangerous files like .html can be uploaded without the "Add & Customize Pages" permission

However, SharePoint Setting "Browser File Handling" prevents the browser from automatically render malicious files by default:



Browser File Handling

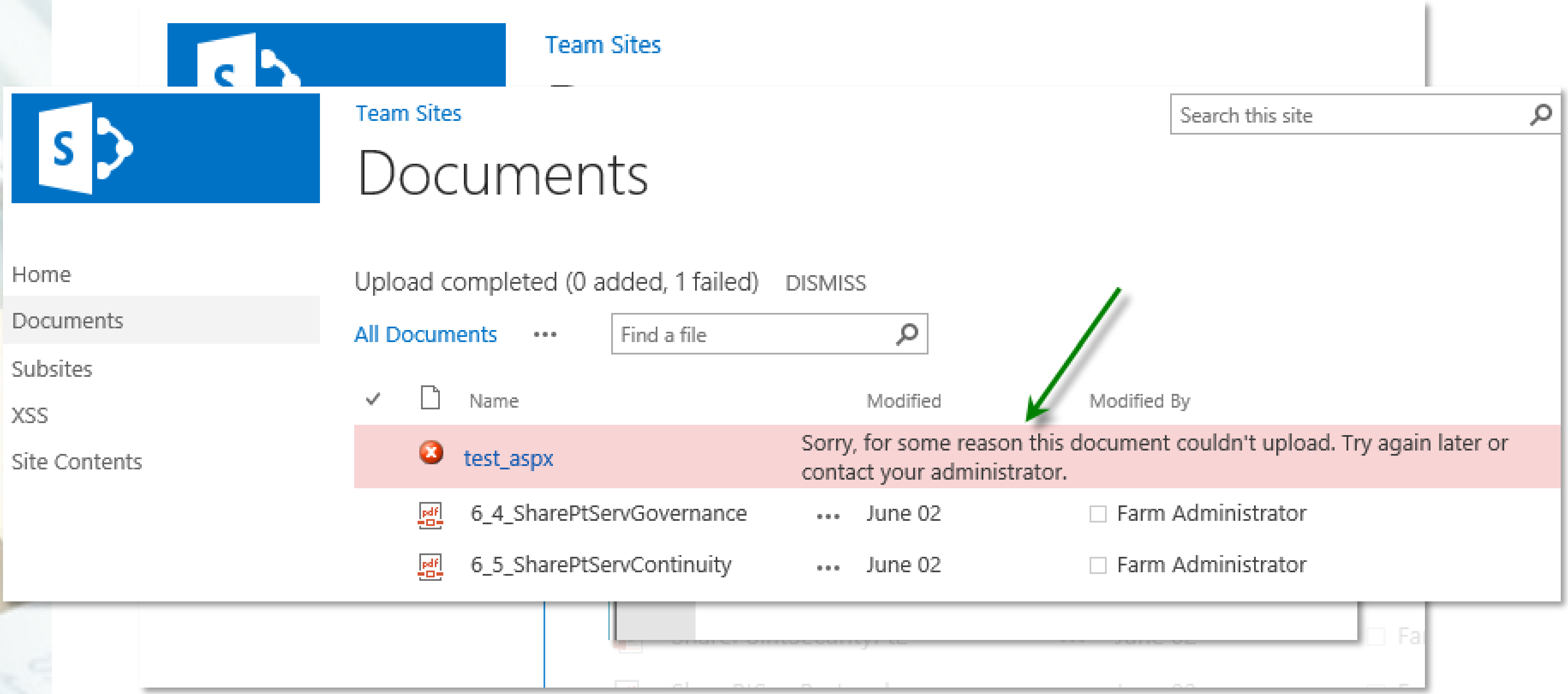
Specifies whether additional security headers are added to documents served to web

○ Permissive
● Strict

- **Strict:** Content-Disposition Header is set on every file type to force the file to be downloaded instead of rendering it in the browser.
- **Permissive:** Some file types, like *.html are rendered in the browser. If these files contain javascript it gets executed in the context of SharePoint.

Cross-Site Scripting – Web Sensitive Files

Trying to upload ASP.NET page with JavaScript code as Contributor without permissions



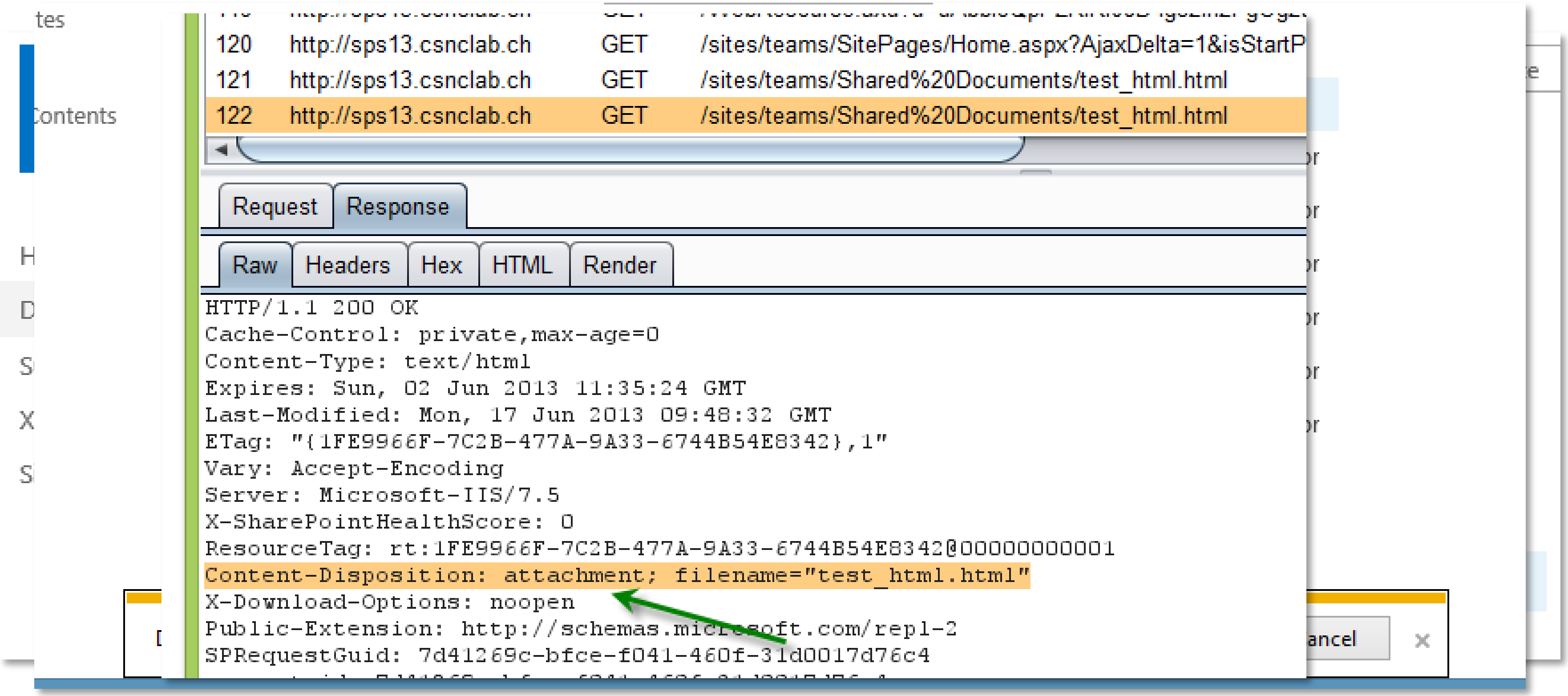
Documents

Upload completed (0 added, 1 failed) DISMISS

Name		Modified	Modified By
test_aspx	Sorry, for some reason this document couldn't upload. Try again later or contact your administrator.		
6_4_SharePtServGovernance	...	June 02	Farm Administrator
6_5_SharePtServContinuity	...	June 02	Farm Administrator

Cross-Site Scripting – Web Sensitive Files

Trying to download malicious HTML page uploaded by a Contributor



```
120   http://sps13.csnclab.ch   GET   /sites/teams/SitePages/Home.aspx?AjaxDelta=1&isStartP
121   http://sps13.csnclab.ch   GET   /sites/teams/Shared%20Documents/test_html.html
122   http://sps13.csnclab.ch   GET   /sites/teams/Shared%20Documents/test_html.html
```

```
HTTP/1.1 200 OK
Cache-Control: private,max-age=0
Content-Type: text/html
Expires: Sun, 02 Jun 2013 11:35:24 GMT
Last-Modified: Mon, 17 Jun 2013 09:48:32 GMT
ETag: "{1FE9966F-7C2B-477A-9A33-6744B54E8342},1"
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-SharePointHealthScore: 0
ResourceTag: rt:1FE9966F-7C2B-477A-9A33-6744B54E8342@00000000001
Content-Disposition: attachment; filename="test_html.html"
X-Download-Options: noopen
Public-Extension: http://schemas.microsoft.com/repl-2
SPRequestGuid: 7d41269c-bfce-f041-460f-31d0017d76c4
```

Cross-Site Scripting – Mitigation

Minimal trustful Owners:

- Only provide Owner permission level to trustful users
- Do not allow everyone to own a Site
- Disable Self-Site Creation or at least limit it to a dedicated domain

Careful Configuration:

- Do not allow untrusted users to “Add & Customize Pages” *(Custom Permission Levels)*
- Do not allow Contributors to use Web Parts not declared as “SafeAgainstScripts” *(Web Part Security Settings)*
- Do not change the “SafeAgainstScripts”-declaration of preinstalled Web Parts *(Web Config Settings)*
- Do not misconfigure the list of Web Sensitive Files
- Do not misconfigure the Browser File Handling

Cross-Site Scripting – Mitigation

3rd Party Code:

- Check correct declaration of 3rd party Web Parts which by design allow to embed JavaScript (“SafeAgainstScript=false”)
- Test 3rd party Web Parts declared as “SafeAgainstScript”, if they do not accidently allow embedding of JavaScript (XSS Vulnerability)

SharePoint Web Security

Cross-Site Request Forgery (CSRF)

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Cross-Site Request Forgery

An attacker must not be able to predict a valid request, which could be used to trick a victim to execute a given action in the already authenticated context. E.g.:

- Submitting a form to add a new user
- Submitting a form to delete a document
- …

Common best practice is to include an unpredictable element within every request which triggers immediate actions

This so called "Anti-XSRF" token should be included in every important html form

Cross-Site Request Forgery

An attacker must not be able to predict a valid request, which could be used to trick a victim to execute a given action in the already authenticated context. E.g.:

- Submitting a form to add a new user
- Submitting a form to delete a document
- …

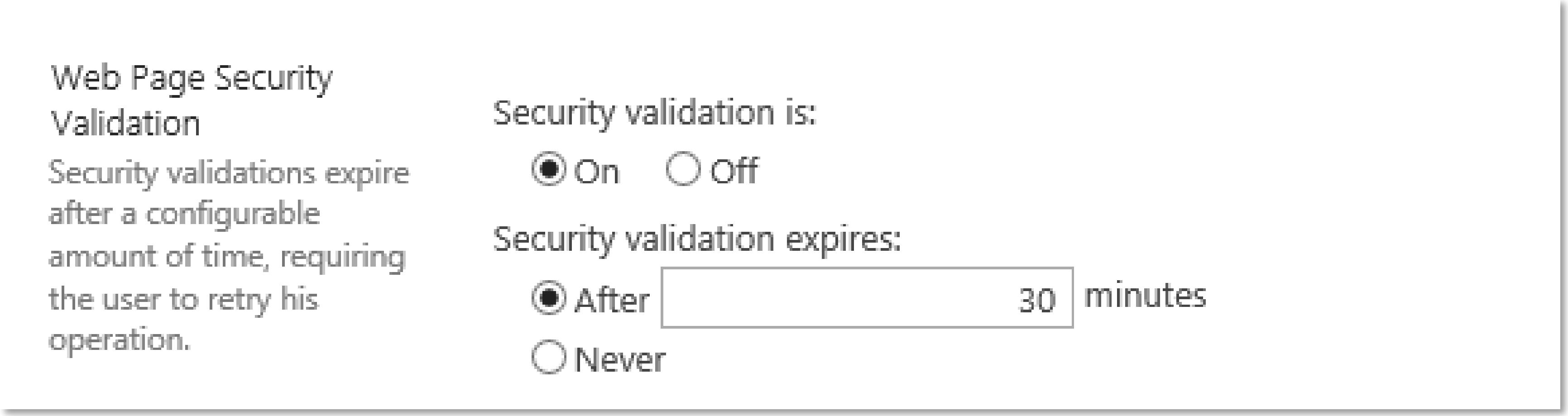
Common best practice is to include an unpredictable element within every request which triggers immediate actions

This so called "Anti-XSRF" token should be included in every important html form

Web Page Security Validation!

Cross-Site Request Forgery

Web Page Security Validation = Anti-XSRF Token



Web Page Security Validation

Security validations expire after a configurable amount of time, requiring the user to retry his operation.

Security validation is:

● On ○ Off

Security validation expires:

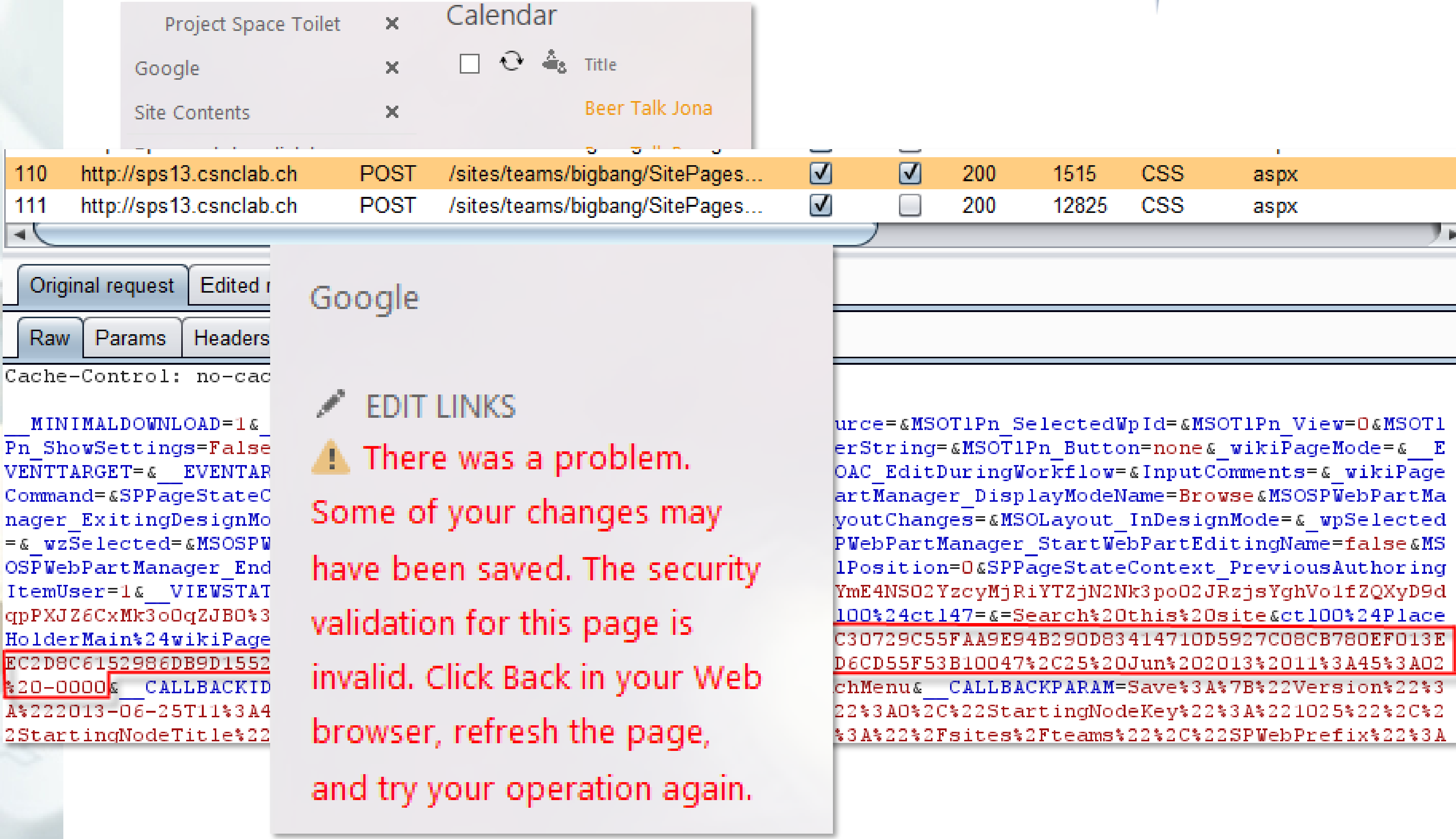
● After 30 minutes

○ Never

This feature is enabled by default on every ASP.NET page based on a SharePoint Master Page

3rd party solutions, which do not inherit from the SharePoint Master Page, must include the "*FormDigest*" control and check it by calling the "*ValidateFormDigest*" method before they execute an action

DEMO: Cross-Site Request Forgery



110	http://sps13.csnclab.ch	POST	/sites/teams/bigbang/SitePages...	☑	☑	200	1515	CSS	aspx
111	http://sps13.csnclab.ch	POST	/sites/teams/bigbang/SitePages...	☑	□	200	12825	CSS	aspx

```
Cache-Control: no-cac

__MINIMALDOWNLOAD=1&_
Pn_ShowSettings=False
VENTTARGET=&__EVENTAR
Command=&SPPageStateC
nager_ExitingDesignMo
=&_wzSelected=&MSOSPW
OSPWebPartManager_End
ItemUser=1&__VIEWSTAT
qpPXJZ6CxMk3oOqZJBO%3
HolderMain%24wikiPage
EC2D8C6152986DB9D1552
%20-0000&__CALLBACKID
A%222013-06-25T11%3A4
2StartingNodeTitle%22
```

```
urce=&MSOTlPn_SelectedWpId=&MSOTlPn_View=0&MSOTl
erString=&MSOTlPn_Button=none&_wikiPageMode=&__E
OAC_EditDuringWorkflow=&InputComments=&_wikiPage
artManager_DisplayModeName=Browse&MSOSPWebPartMa
youtChanges=&MSOLayout_InDesignMode=&_wpSelected
PWebPartManager_StartWebPartEditingName=false&MS
lPosition=0&SPPageStateContext_PreviousAuthoring
YmE4NSO2YzcyMjRiYTZjN2Nk3poO2JRzjsYghVolfZQXyD9d
l00%24ctl47=&=Search%20this%20site&ctl00%24Place
C30729C55FAA9E94B290D83414710D5927C08CB780EF013E
D6CD55F53B10047%2C25%20Jun%202013%2011%3A45%3A02
chMenu&__CALLBACKPARAM=Save%3A%7B%22Version%22%3
22%3A0%2C%22StartingNodeKey%22%3A%221025%22%2C%2
%3A%22%2Fsites%2Fteams%22%2C%22SPWebPrefix%22%3A
```

Google

EDIT LINKS

⚠ There was a problem.

Some of your changes may have been saved. The security validation for this page is invalid. Click Back in your Web browser, refresh the page, and try your operation again.

SharePoint Web Security

SQL Injection

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

SQL Injection

The default pages and web parts of SharePoint are most likely not vulnerable to SQL Injection attacks

However, 3rd Party Solutions need to be checked carefully

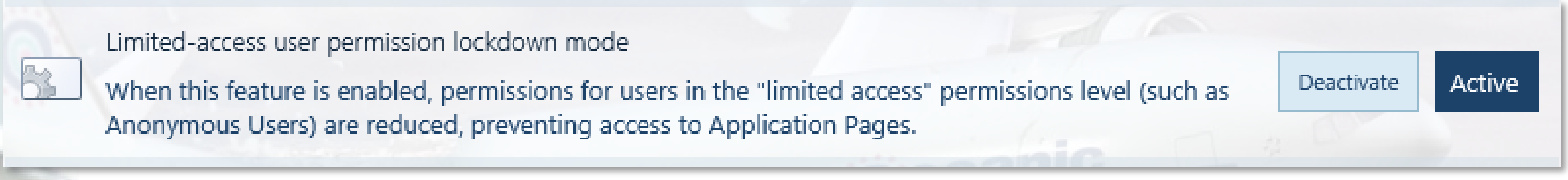
- Which data sources do these pages / web parts use?
- Do they access the database?
- Do they use Stored Procedures / Prepared Statements?
- …

Hardening Considerations

Lockdown Anonymous Access

Lockdown Feature (DE: Sperrmodus)

Lockdown mode is a Site Collection Feature that you can use to secure published sites:



Limited-access user permission lockdown mode

When this feature is enabled, permissions for users in the "limited access" permissions level (such as Anonymous Users) are reduced, preventing access to Application Pages.

By enabling lockdown mode on a site, you can remove unnecessary permissions for anonymous users.

Lockdown Feature (DE: Sperrmodus)

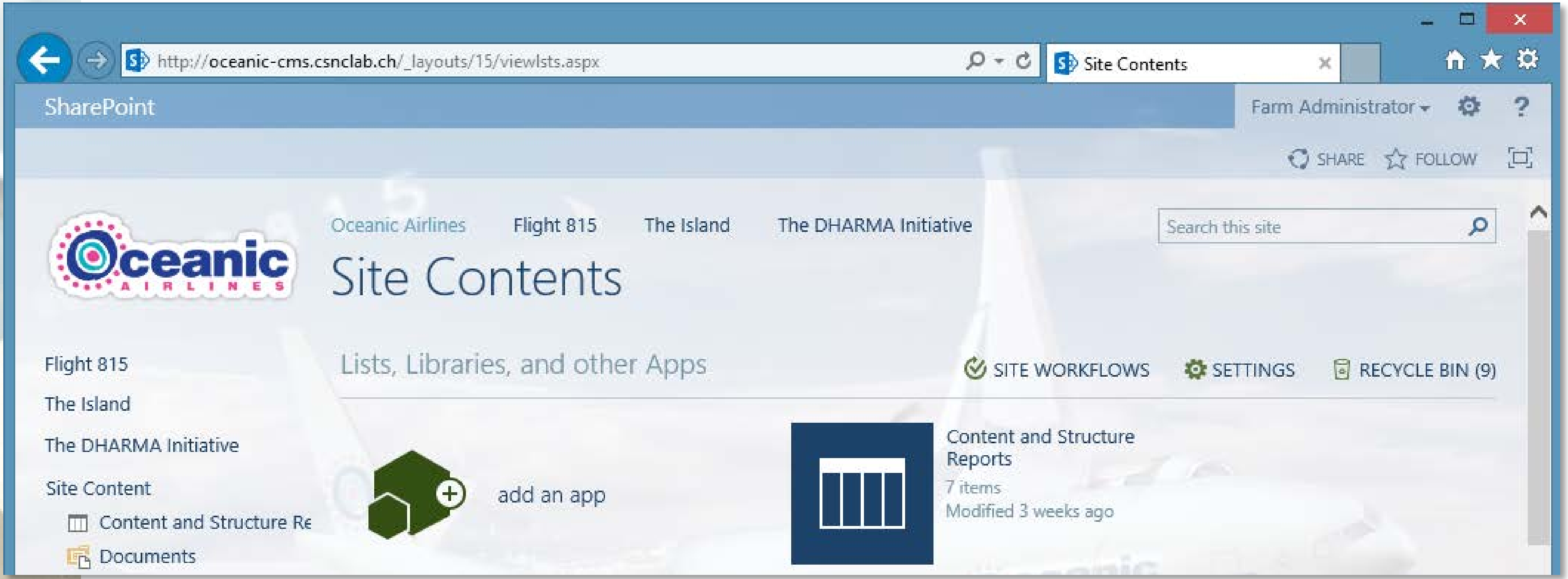
When lockdown mode is turned on, fine-grain permissions for the limited access permission level are reduced:

Permission	**Limited access — default**	**Limited access — lockdown mode**
List permissions: **View Application Pages**	Yes	No
Site permissions: Browse User Information	Yes	Yes
Site permissions: **Use Remote Interfaces**	Yes	No
Site permissions: Use Client Integration Features	Yes	Yes
Site permissions: Open	Yes	Yes

- Removes the permission to access application pages like *_layouts/viewlsts.aspx*, which can be used to shows all available lists in a site
- Removes the permission to use remote interfaces like SOAP and REST API

Lockdown Feature (DE: Sperrmodus)

View lists as authenticated user (e.g. Editor):



http://oceanic-cms.csnclab.ch/_layouts/15/viewlsts.aspx

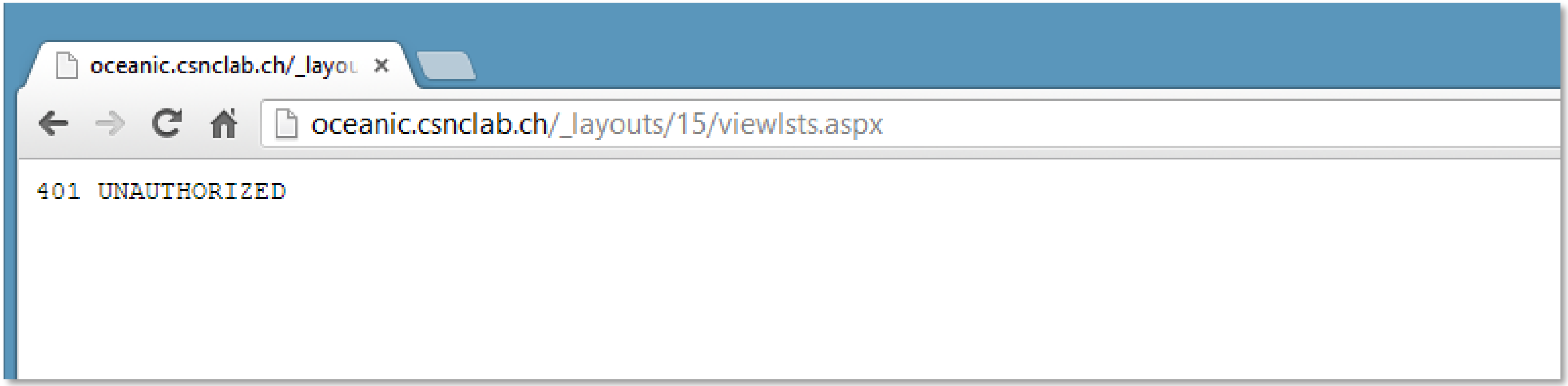
Site Contents

Lists, Libraries, and other Apps

Content and Structure Reports
7 items
Modified 3 weeks ago

Lockdown Feature (DE: Sperrmodus)

View lists as anonymous user (not authorized):


oceanic.csnclab.ch/_layou ×
oceanic.csnclab.ch/_layouts/15/viewlsts.aspx

```
401 UNAUTHORIZED
```

==> Access still possible with Remote Interfaces if Web Application is poorly configured!

Hardening Considerations

Remote Interfaces

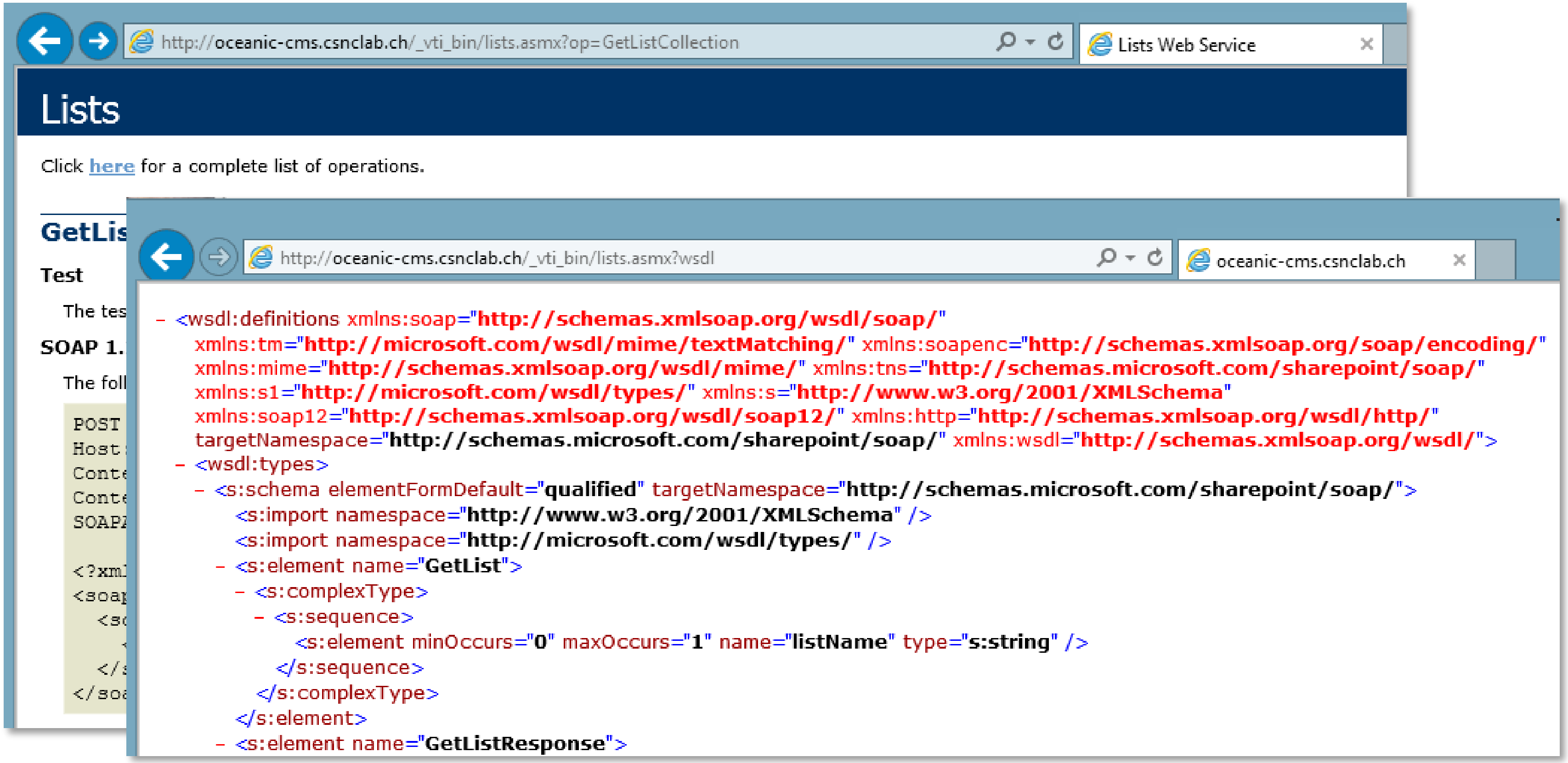
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Remote Interfaces – SOAP

Traditional SharePoint SOAP Web Services:

- *<site>/_vti_bin/lists.asmx*
- *<site>/_vti_bin/sites.asmx*
- …



http://oceanic-cms.csnclab.ch/_vti_bin/lists.asmx?op=GetListCollection
Lists Web Service

Lists

Click here for a complete list of operations.

GetLis

Test

The tes

SOAP 1.

The foll

```
POST
Host:
Conte
Conte
SOAPA

<?xml
<soap
  <so
    <
  </s
</soa
```

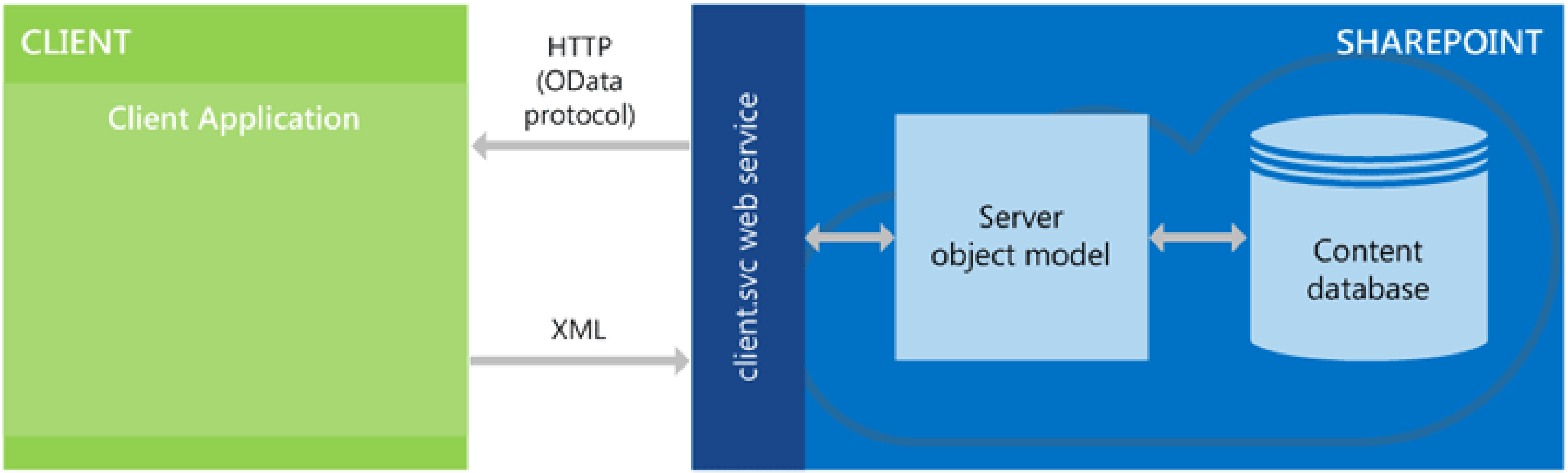
http://oceanic-cms.csnclab.ch/_vti_bin/lists.asmx?wsdl
oceanic-cms.csnclab.ch

```
- <wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
    xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:tns="http://schemas.microsoft.com/sharepoint/soap/"
    xmlns:s1="http://microsoft.com/wsdl/types/" xmlns:s="http://www.w3.org/2001/XMLSchema"
    xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
    targetNamespace="http://schemas.microsoft.com/sharepoint/soap/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  - <wsdl:types>
    - <s:schema elementFormDefault="qualified" targetNamespace="http://schemas.microsoft.com/sharepoint/soap/">
        <s:import namespace="http://www.w3.org/2001/XMLSchema" />
        <s:import namespace="http://microsoft.com/wsdl/types/" />
      - <s:element name="GetList">
        - <s:complexType>
          - <s:sequence>
              <s:element minOccurs="0" maxOccurs="1" name="listName" type="s:string" />
            </s:sequence>
          </s:complexType>
        </s:element>
      - <s:element name="GetListResponse">
```

Remote Interfaces – CSOM

Client-Side Object Model CSOM:

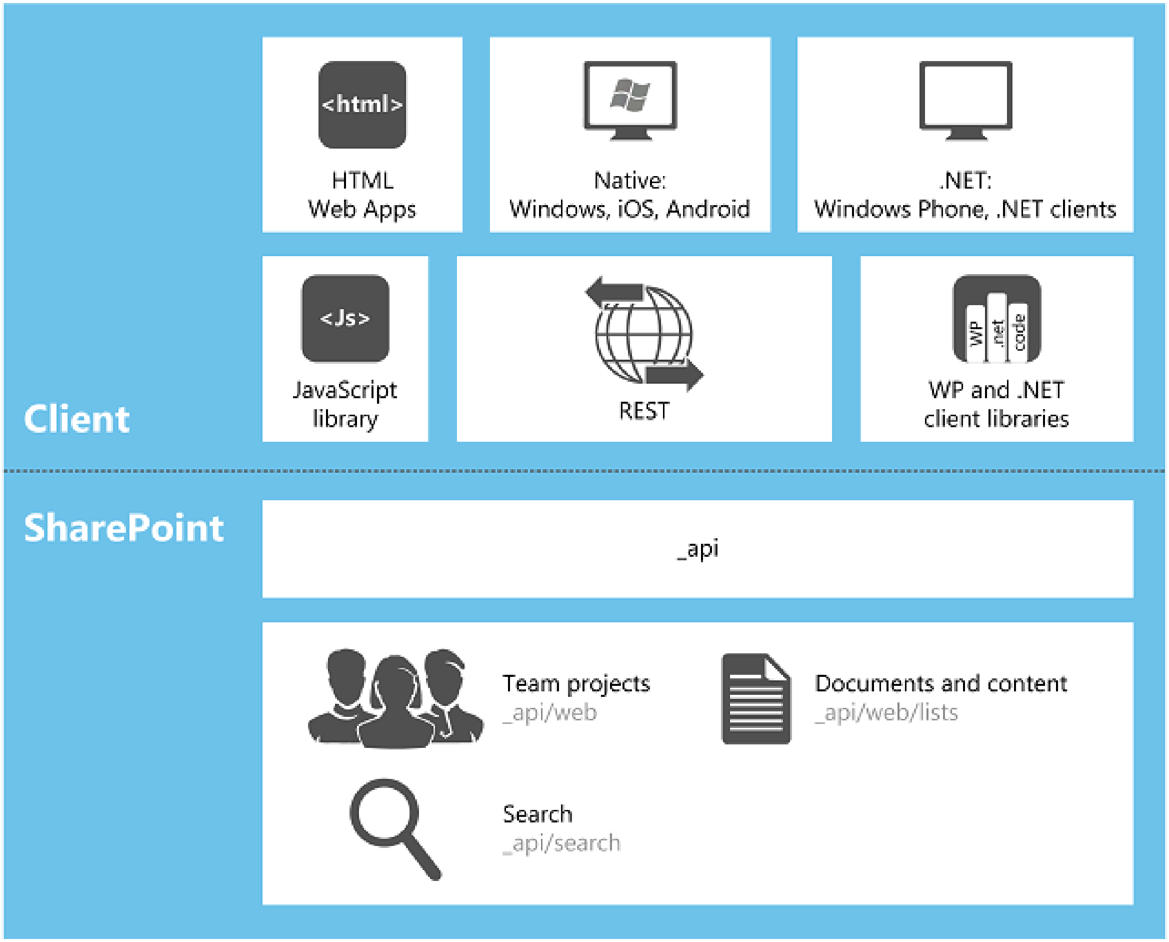
- Client Applications can use the web service <*site*>/_vti_bin/client.svc to access the SharePoint Object Model
- They provide better performance because they batch requests and perform all operations asynchronously
- The semantics are more familiar and easier to be used for SharePoint developers



Remote Interfaces – CSOM + REST

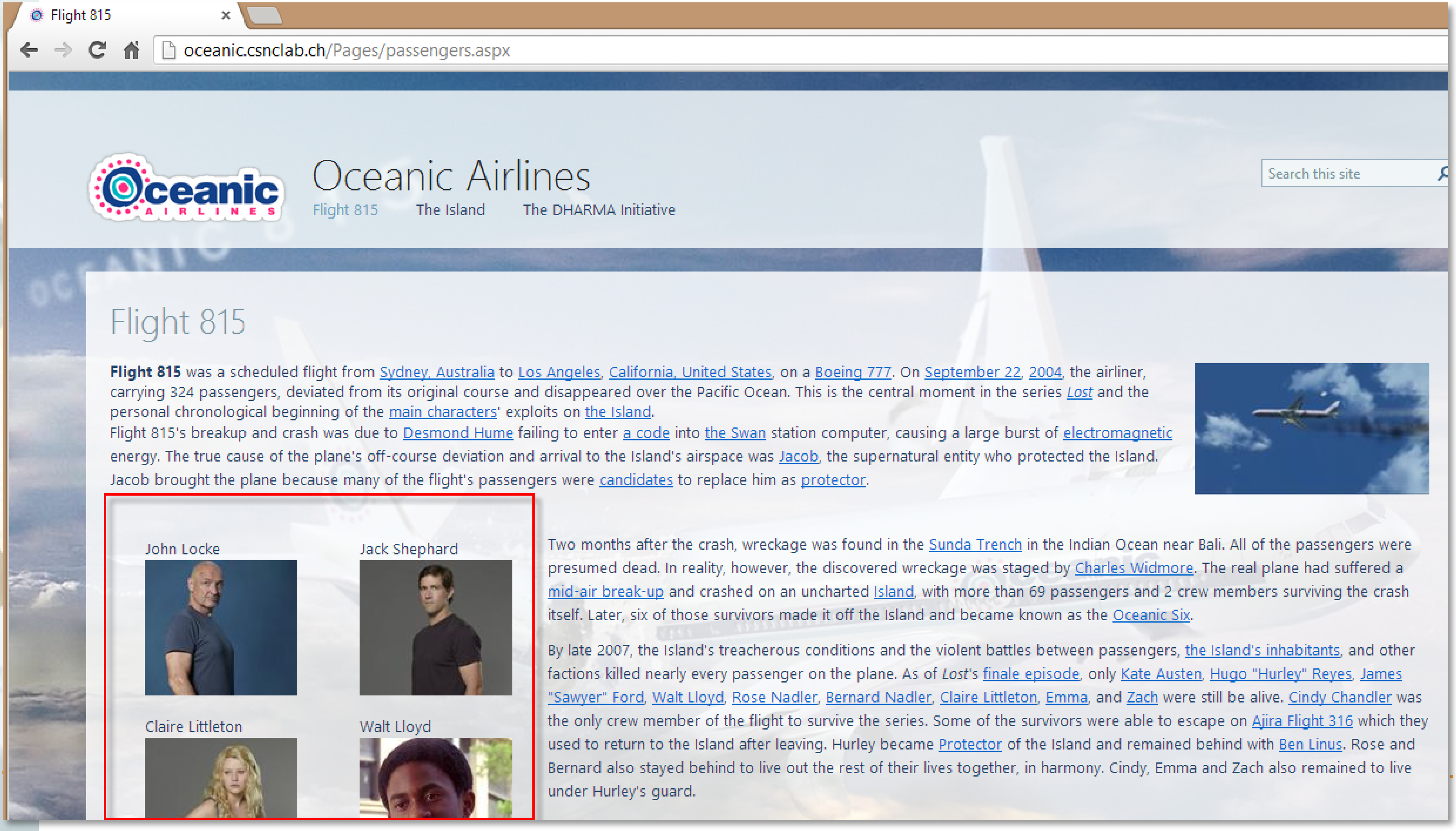
The CSOM can be used with…

- JavaScript or .NET APIs
- REST Endpoints on URL: *<site>/_api* (new in SP 2013)



Demo: Remote Interfaces

Passenger Information is pulled from a list called "Passenger List"



Oceanic Airlines

Flight 815 The Island The DHARMA Initiative

Flight 815

Flight 815 was a scheduled flight from Sydney, Australia to Los Angeles, California, United States, on a Boeing 777. On September 22, 2004, the airliner, carrying 324 passengers, deviated from its original course and disappeared over the Pacific Ocean. This is the central moment in the series *Lost* and the personal chronological beginning of the main characters' exploits on the Island.

Flight 815's breakup and crash was due to Desmond Hume failing to enter a code into the Swan station computer, causing a large burst of electromagnetic energy. The true cause of the plane's off-course deviation and arrival to the Island's airspace was Jacob, the supernatural entity who protected the Island. Jacob brought the plane because many of the flight's passengers were candidates to replace him as protector.

John Locke

Jack Shephard

Claire Littleton

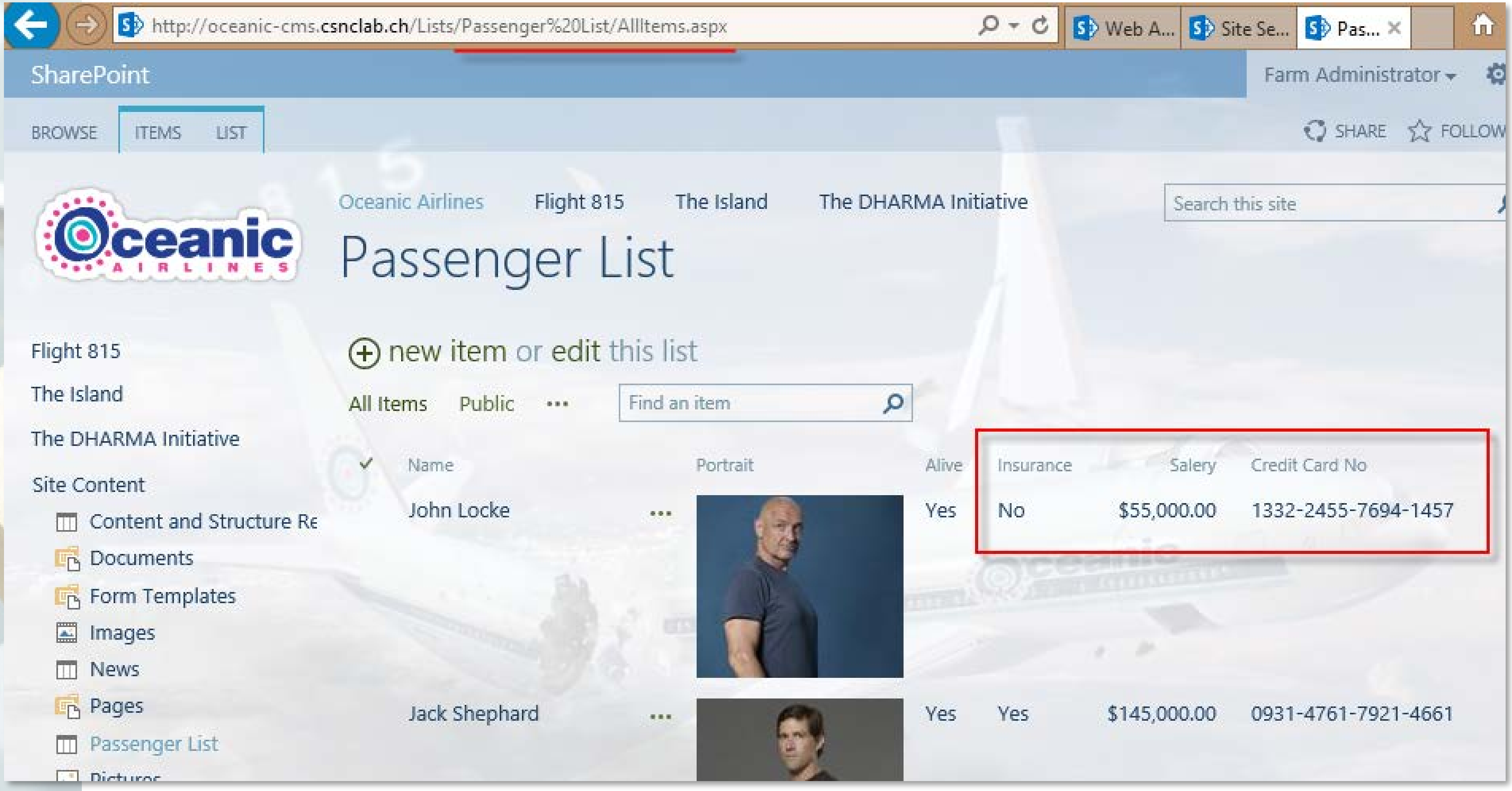
Walt Lloyd

Two months after the crash, wreckage was found in the Sunda Trench in the Indian Ocean near Bali. All of the passengers were presumed dead. In reality, however, the discovered wreckage was staged by Charles Widmore. The real plane had suffered a mid-air break-up and crashed on an uncharted Island, with more than 69 passengers and 2 crew members surviving the crash itself. Later, six of those survivors made it off the Island and became known as the Oceanic Six.

By late 2007, the Island's treacherous conditions and the violent battles between passengers, the Island's inhabitants, and other factions killed nearly every passenger on the plane. As of *Lost*'s finale episode, only Kate Austen, Hugo "Hurley" Reyes, James "Sawyer" Ford, Walt Lloyd, Rose Nadler, Bernard Nadler, Claire Littleton, Emma, and Zach were still be alive. Cindy Chandler was the only crew member of the flight to survive the series. Some of the survivors were able to escape on Ajira Flight 316 which they used to return to the Island after leaving. Hurley became Protector of the Island and remained behind with Ben Linus. Rose and Bernard also stayed behind to live out the rest of their lives together, in harmony. Cindy, Emma and Zach also remained to live under Hurley's guard.

Demo: Remote Interfaces

Trying to access Passenger List as Editor (sensitive information)



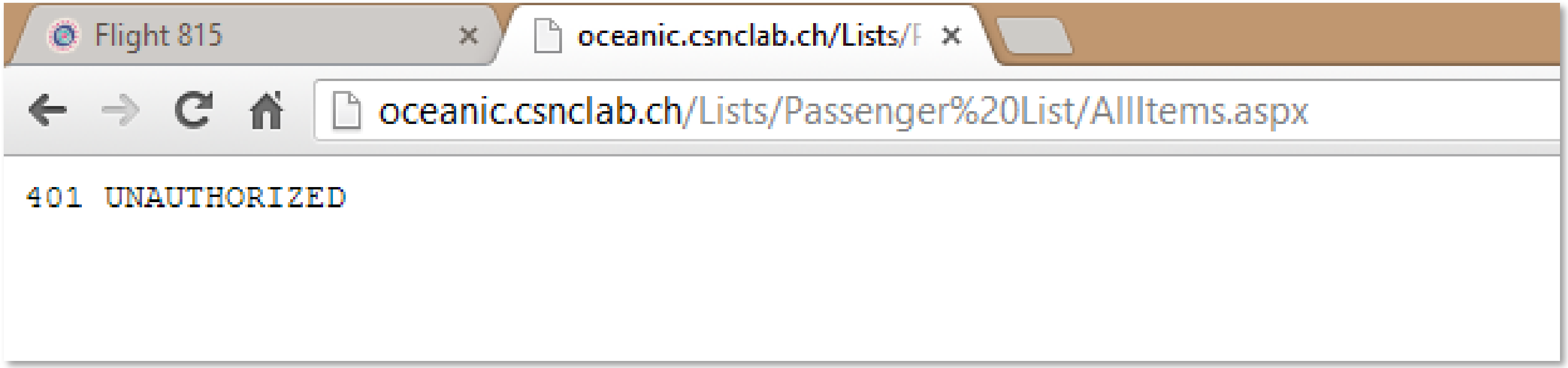
http://oceanic-cms.csnclab.ch/Lists/Passenger%20List/AllItems.aspx

Passenger List

✓	Name	Portrait	Alive	Insurance	Salery	Credit Card No
	John Locke •••		Yes	No	$55,000.00	1332-2455-7694-1457
	Jack Shephard •••		Yes	Yes	$145,000.00	0931-4761-7921-4661

Demo: Remote Interfaces

Trying to access Passenger List as Anonymous User



oceanic.csnclab.ch/Lists/Passenger%20List/AllItems.aspx

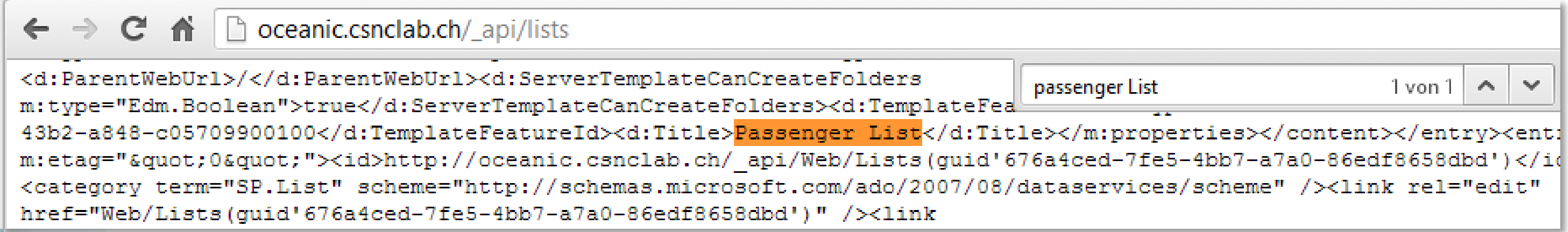
```
401 UNAUTHORIZED
```

Demo: Remote Interfaces

Access Passenger List with CSOM REST API:

- http://oceanic.csnclab.ch/_api/lists
- http://oceanic.csnclab.ch/_api/lists/?$select=Title
- http://oceanic.csnclab.ch/_api/lists/getbytitle('Passenger%20List')
- http://oceanic.csnclab.ch/_api/lists/getbytitle('Passenger%20List')/title
- http://oceanic.csnclab.ch/_api/lists/getbytitle('Passenger%20List')/Items
- http://oceanic.csnclab.ch/_api/lists/getbytitle('Passenger%20List')/Items?$select=Title
- http://oceanic.csnclab.ch/_api/lists/getbytitle('Passenger%20List')/Items?$select=Title,Credit_x0020_Card_x0020_No

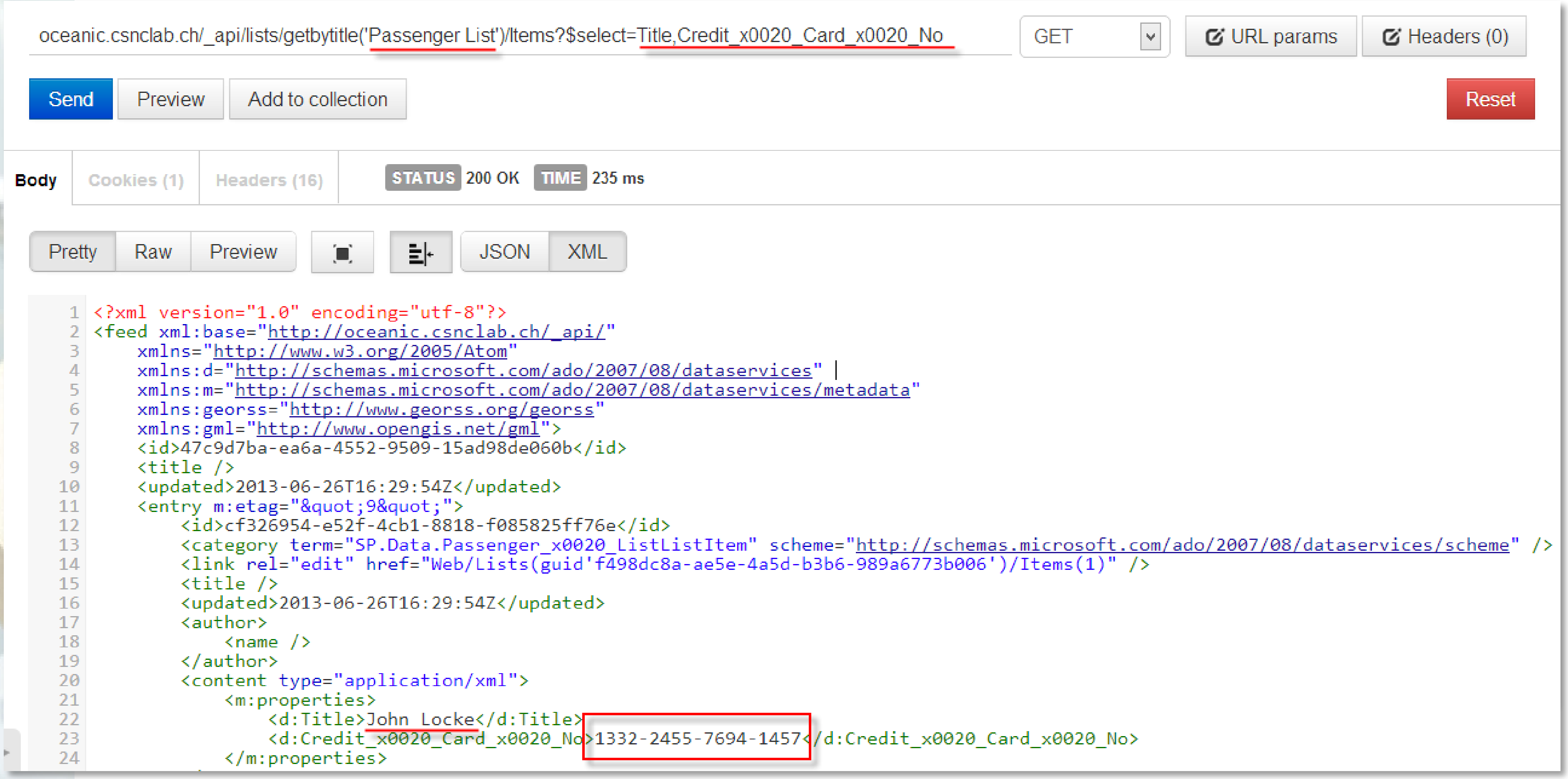
Raw in browser (e.g. chrome):



```
<d:ParentWebUrl>/</d:ParentWebUrl><d:ServerTemplateCanCreateFolders
m:type="Edm.Boolean">true</d:ServerTemplateCanCreateFolders><d:TemplateFea
43b2-a848-c05709900100</d:TemplateFeatureId><d:Title>Passenger List</d:Title></m:properties></content></entry><ent
m:etag="&quot;0&quot;"><id>http://oceanic.csnclab.ch/_api/Web/Lists(guid'676a4ced-7fe5-4bb7-a7a0-86edf8658dbd')</i
<category term="SP.List" scheme="http://schemas.microsoft.com/ado/2007/08/dataservices/scheme" /><link rel="edit"
href="Web/Lists(guid'676a4ced-7fe5-4bb7-a7a0-86edf8658dbd')" /><link
```

Demo: Remote Interfaces

REST Chrome Apps like Dev HTTP Client, Postman – REST Client:



oceanic.csnclab.ch/_api/lists/getbytitle('Passenger List')/Items?$select=Title,Credit_x0020_Card_x0020_No

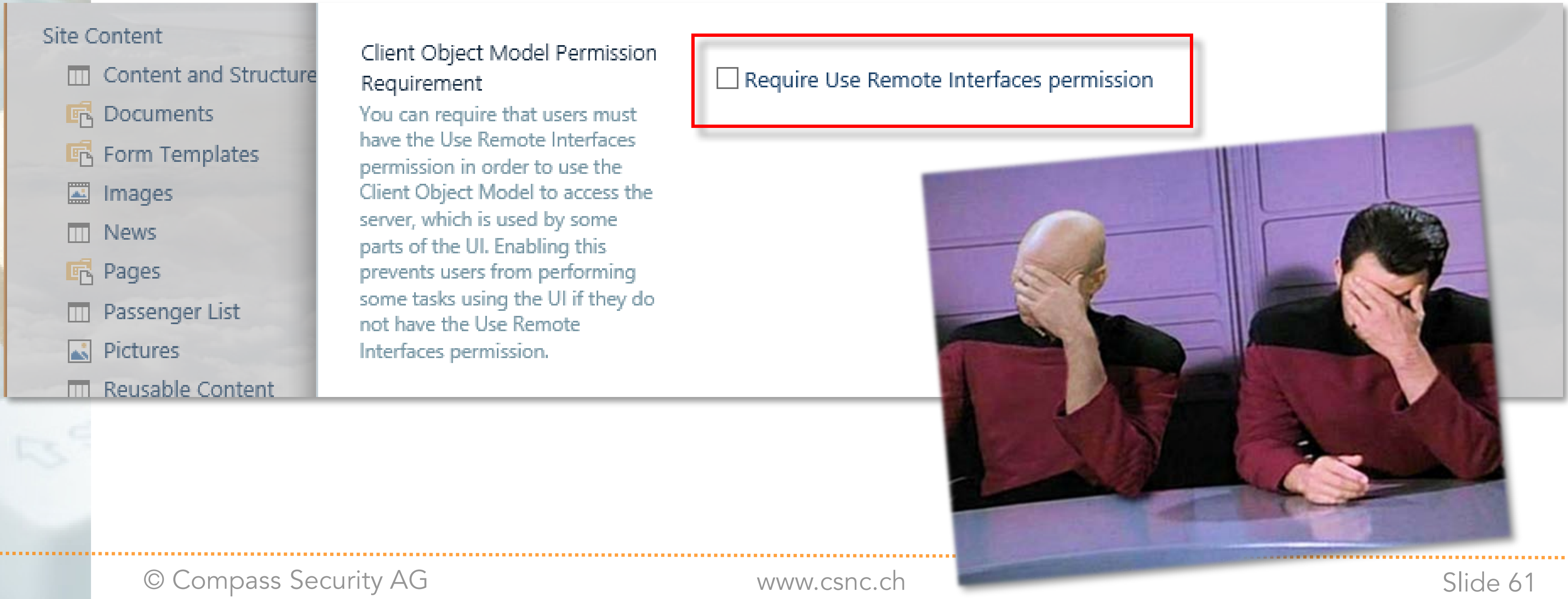
```
<?xml version="1.0" encoding="utf-8"?>
<feed xml:base="http://oceanic.csnclab.ch/_api/"
    xmlns="http://www.w3.org/2005/Atom"
    xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
    xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata"
    xmlns:georss="http://www.georss.org/georss"
    xmlns:gml="http://www.opengis.net/gml">
    <id>47c9d7ba-ea6a-4552-9509-15ad98de060b</id>
    <title />
    <updated>2013-06-26T16:29:54Z</updated>
    <entry m:etag="&quot;9&quot;">
        <id>cf326954-e52f-4cb1-8818-f085825ff76e</id>
        <category term="SP.Data.Passenger_x0020_ListListItem" scheme="http://schemas.microsoft.com/ado/2007/08/dataservices/scheme" />
        <link rel="edit" href="Web/Lists(guid'f498dc8a-ae5e-4a5d-b3b6-989a6773b006')/Items(1)" />
        <title />
        <updated>2013-06-26T16:29:54Z</updated>
        <author>
            <name />
        </author>
        <content type="application/xml">
            <m:properties>
                <d:Title>John Locke</d:Title>
                <d:Credit_x0020_Card_x0020_No>1332-2455-7694-1457</d:Credit_x0020_Card_x0020_No>
            </m:properties>
```

Cause: Misconfiguration

The Lockdown Feature:

- prevents access to /_vti_bin and /_layouts folders
- removes the Remote Interface Permissions for anonymous users

But there is an important flag on two separate locations, which overrules the Remote Interface Permission if set wrongly



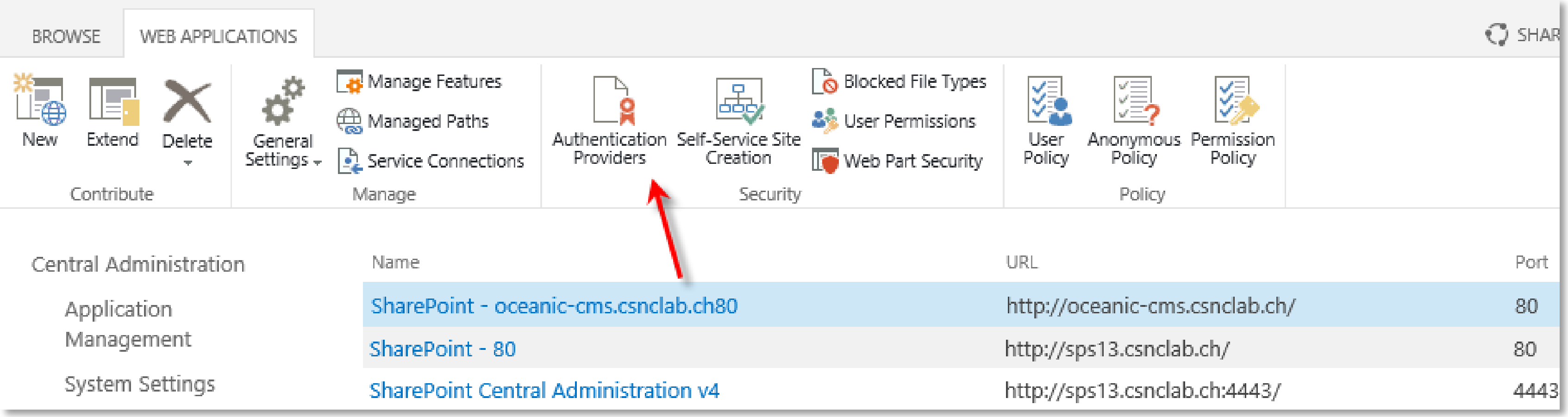
Client Object Model Permission Requirement

You can require that users must have the Use Remote Interfaces permission in order to use the Client Object Model to access the server, which is used by some parts of the UI. Enabling this prevents users from performing some tasks using the UI if they do not have the Use Remote Interfaces permission.

□ Require Use Remote Interfaces permission

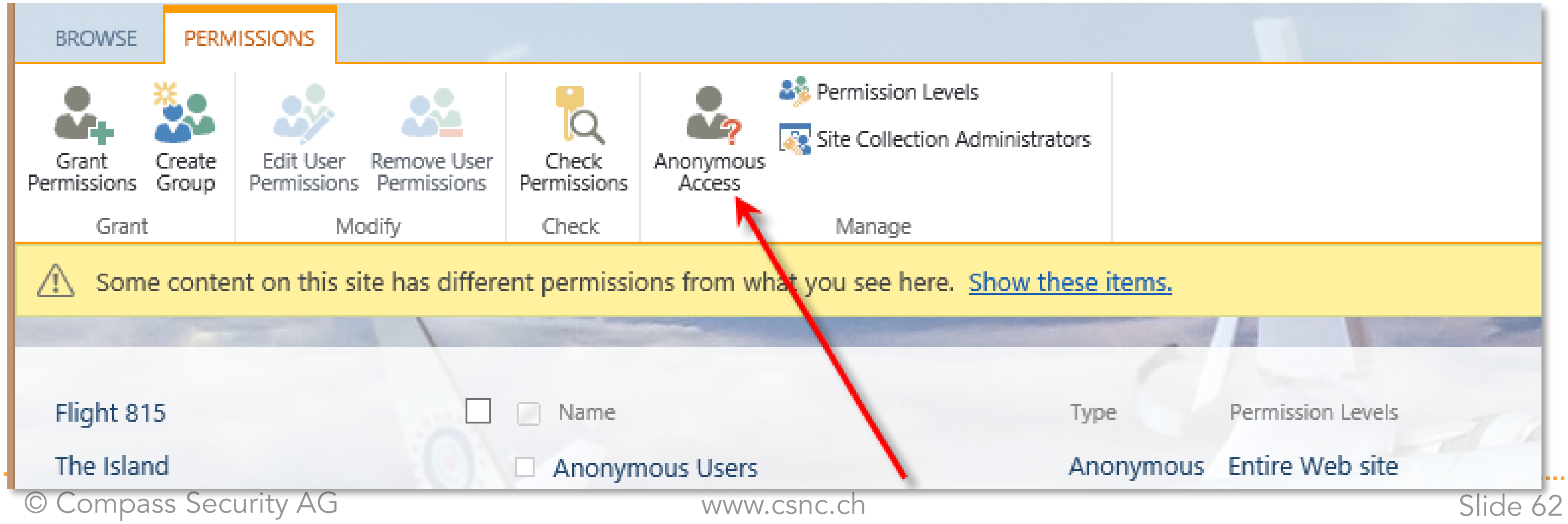
Cause: Misconfiguration

#1: Authentication Provider (Web Application Settings)



Name	URL	Port
SharePoint - oceanic-cms.csnclab.ch80	http://oceanic-cms.csnclab.ch/	80
SharePoint - 80	http://sps13.csnclab.ch/	80
SharePoint Central Administration v4	http://sps13.csnclab.ch:4443/	4443

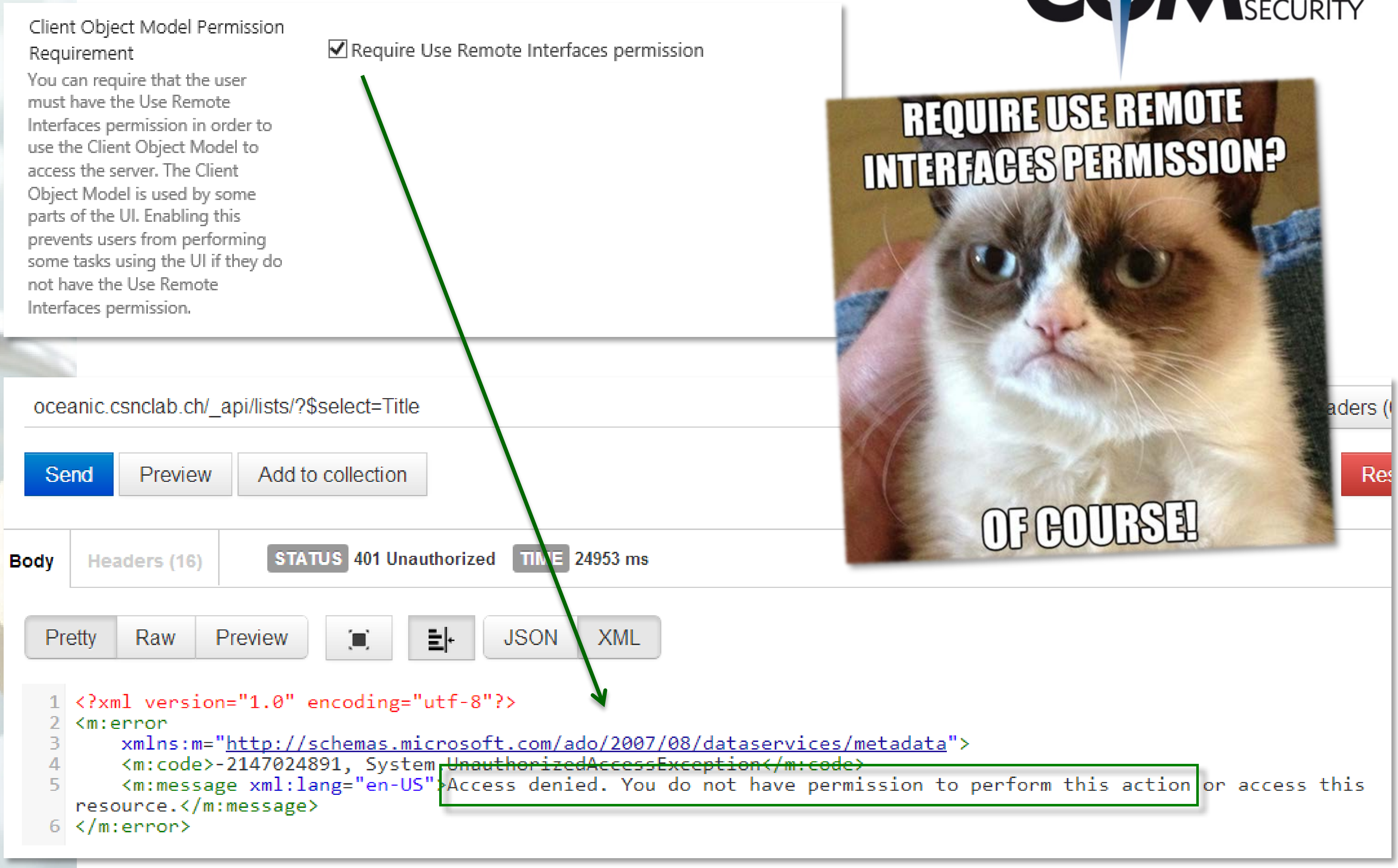
#2: Anonymous Access Configuration (Site Permissions)



⚠ Some content on this site has different permissions from what you see here. Show these items.

	Name	Type	Permission Levels
□	Anonymous Users	Anonymous	Entire Web site

Mitigation I – Remote Interface Perm.



Client Object Model Permission Requirement

You can require that the user must have the Use Remote Interfaces permission in order to use the Client Object Model to access the server. The Client Object Model is used by some parts of the UI. Enabling this prevents users from performing some tasks using the UI if they do not have the Use Remote Interfaces permission.

☑ Require Use Remote Interfaces permission

oceanic.csnclab.ch/_api/lists/?$select=Title

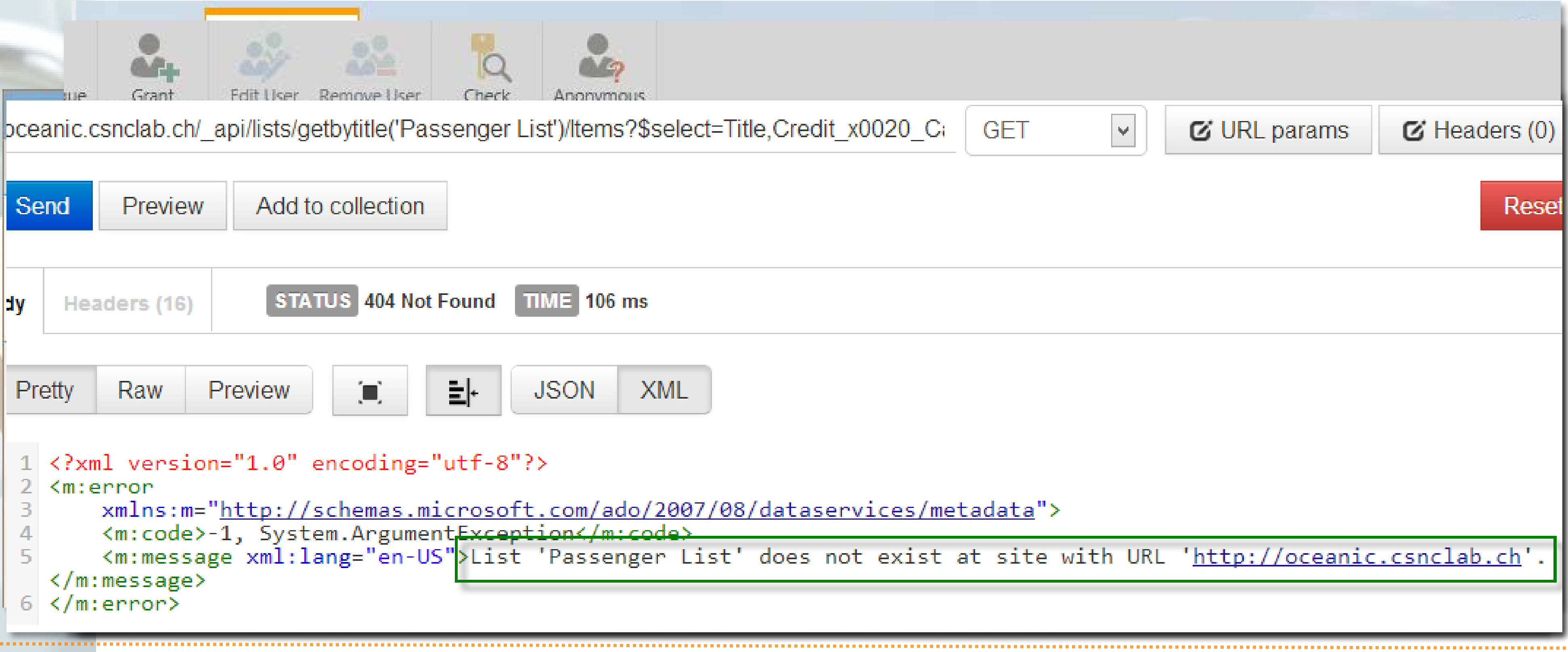
STATUS 401 Unauthorized TIME 24953 ms

```
<?xml version="1.0" encoding="utf-8"?>
<m:error
    xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata">
    <m:code>-2147024891, System.UnauthorizedAccessException</m:code>
    <m:message xml:lang="en-US">Access denied. You do not have permission to perform this action or access this
resource.</m:message>
</m:error>
```

Mitigation II – List Permissions

If you need CSOM for some client side features like search or other highly dynamic Ajax features:

==> Explicitly deny access for Anonymous Users on “hidden” lists



oceanic.csnclab.ch/_api/lists/getbytitle('Passenger List')/Items?$select=Title,Credit_x0020_Ca

STATUS 404 Not Found TIME 106 ms

```
<?xml version="1.0" encoding="utf-8"?>
<m:error
    xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata">
    <m:code>-1, System.ArgumentException</m:code>
    <m:message xml:lang="en-US">List 'Passenger List' does not exist at site with URL 'http://oceanic.csnclab.ch'.
</m:message>
</m:error>
```

Hardening Considerations

Server-Side Controls, Sandboxing and further hardening recommendations

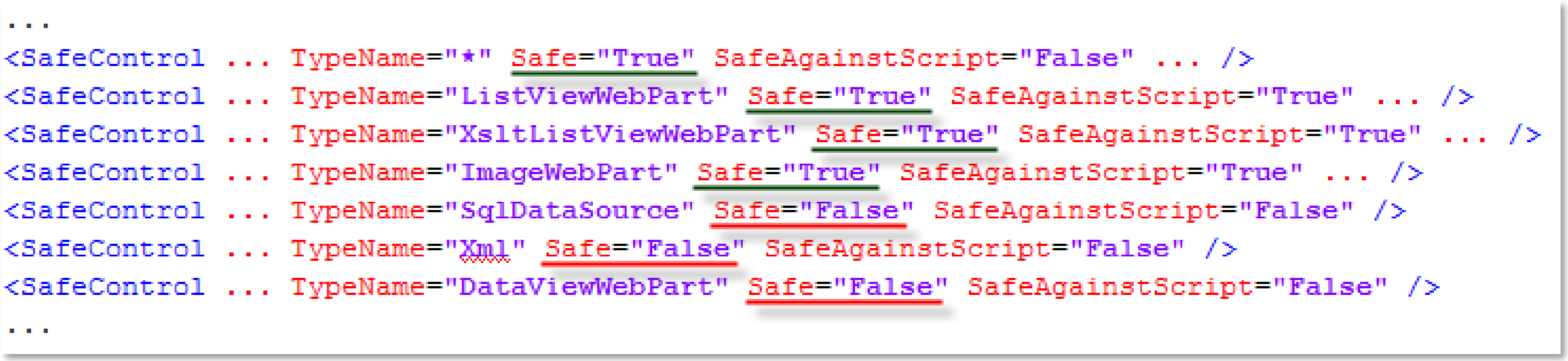
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Server-Side Controls

Make sure that only controls from trustful sources are in the list of safe ASP.NET controls in the web.config:

- Dangerous controls which should not be usable within .aspx pages are marked as **Safe="False"** by default.
  (E.g. controls allowing the execution of server-side code or similar)
- Controls / Web Parts marked as **Safe="True"** can be used in .aspx pages (whitelisting).



```
...
<SafeControl ... TypeName="*" Safe="True" SafeAgainstScript="False" ... />
<SafeControl ... TypeName="ListViewWebPart" Safe="True" SafeAgainstScript="True" ... />
<SafeControl ... TypeName="XsltListViewWebPart" Safe="True" SafeAgainstScript="True" ... />
<SafeControl ... TypeName="ImageWebPart" Safe="True" SafeAgainstScript="True" ... />
<SafeControl ... TypeName="SqlDataSource" Safe="False" SafeAgainstScript="False" />
<SafeControl ... TypeName="Xml" Safe="False" SafeAgainstScript="False" />
<SafeControl ... TypeName="DataViewWebPart" Safe="False" SafeAgainstScript="False" />
...
```

==> The list of default controls should only be extended with a very good reason!

.NET Sandbox

Make sure that only trustful code (Web Parts / ASP.NET Controls) deployed with a Full Trust Level

Global Assembly Cache:

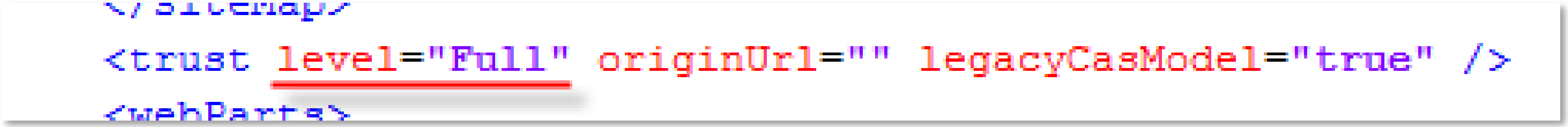
- Runs with a full trust level
- Can be used by every SharePoint Web Application
- Assemblies are signed and need to be installed by an Administrator

Bin directory of Web Application:

- Runs with the trust level *WSS_Minimal* (<= SP 2010)
- Only available to that single Web Application
- Can be deployed by everyone with write access to that directory
- Developers need to explicitly specify which privileges their code need (CAS polices)

.NET Sandbox

With SharePoint 2013, Microsoft changed the default trust level of code in the Bin directory to full trust!



```
</siteMap>
<trust level="Full" originUrl="" legacyCasModel="true" />
<webParts>
```

==> Only allow 3rd party code which is reviewed and trusted to run with a full trust level

==> Try to change trust level back to *WSS_Minimal*

==> Use Sandboxed Solutions or Apps if possible

Sandboxed Solutions / Apps

Sandboxed Solutions:

- Run isolated in the User Code Service in a dedicated process
- Running under a very strict CAS policy only allowing a minimum of calls

Apps:

- Are hosted in an isolated SharePoint site, farm or either in the cloud
- Are not allowed to use server-side code
- Need to use the client object model to connect back to the SharePoint farm

Best Practices:

- Only deploy trusted code (Farm Solutions) to the GAC or the Bin directory
- 3rd party developers should use Sandboxed Solutions or Apps
- Sandbox solutions are deprecated but are still working in SharePoint 2013
- Use SharePoint Apps for 3rd party code in SharePoint 2013

Hardening Recommendations

Is SharePoint Designer disabled?

Are unnecessary or suspicious features disabled?

Is Self-Service Site Creation disabled?

Check the list of blocked file types?

Check the Web Part gallery, which really need to be used?

Is the Developer Dashboard disabled?

Is the Audit Log configured properly?

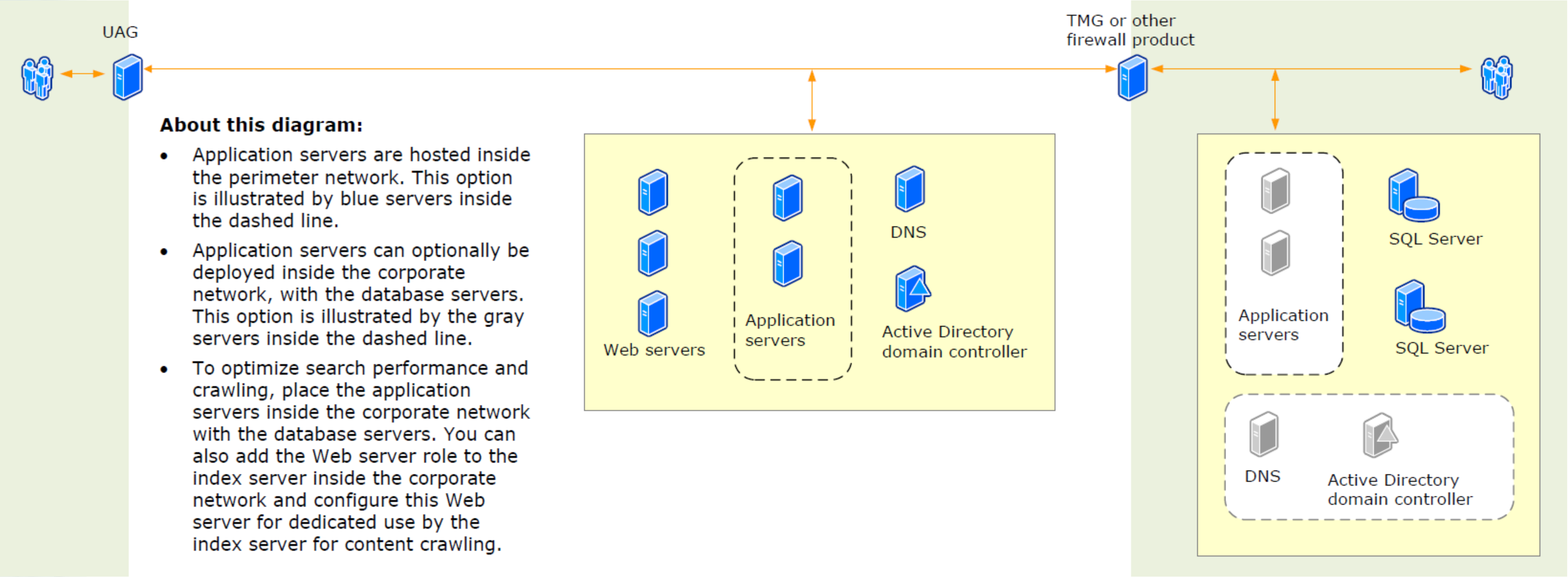
Is HTML Field Security configured properly (SP 2013)?

Who are your Site Collection Administrators?

Hardening Recommendations

Do we use a proper architecture for our deployment?

Split back-to-back



About this diagram:

- Application servers are hosted inside the perimeter network. This option is illustrated by blue servers inside the dashed line.
- Application servers can optionally be deployed inside the corporate network, with the database servers. This option is illustrated by the gray servers inside the dashed line.
- To optimize search performance and crawling, place the application servers inside the corporate network with the database servers. You can also add the Web server role to the index server inside the corporate network and configure this Web server for dedicated use by the index server for content crawling.

UAG
TMG or other firewall product
Web servers
Application servers
DNS
Active Directory domain controller
Application servers
SQL Server
SQL Server
DNS
Active Directory domain controller

Conclusion

Conclusion

SharePoint 2010+ by default secure

-> Do not misconfigure!

Conclusion

Do not trust 3rd party code (e.g. Web Parts)

-> Wrong declarations in web.config?

-> XSS, CSRF and SQL Injection vulnerabilities?

Quiz and Q&A

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Quiz

How much do you still know?

Questions

References

- MS Technet: SharePoint 2013
  http://technet.microsoft.com/de-de/library/cc303422.aspx

- Allow or prevent Contributors ability to edit scriptable Web Parts
  http://technet.microsoft.com/en-us/library/hh272820

- Are you Safe Against Script?
  http://www.bluedoglimited.com/SharePointThoughts/Lists/Posts/Post.aspx?ID=303

- Web Sensitive Files and SharePoint 2010
  http://support.microsoft.com/kb/2483447
  https://www.nothingbutsharepoint.com/sites/itpro/Pages/Web-Sensitive-Files-and-SharePoint-2010.aspx

- SharePoint Security Best Practices: Cross-Site Request Forgery
  http://msdn.microsoft.com/en-us/library/gg552614.aspx#bestpractice_crossrequest

- Security Validation and Making Posts to Update Data
  http://msdn.microsoft.com/en-us/library/ms472879.aspx

References

- Plan security for an external anonymous access environment
  http://technet.microsoft.com/en-us/library/cc263468.aspx

- How to lock down external anonymous access SharePoint sites
  http://blogs.technet.com/b/vedant/archive/2009/07/13/locking-down-sharepoint-sites.aspx

- Deciding Which SharePoint 2010 API to Use
  http://msdn.microsoft.com/en-us/library/hh313619%28v=office.14%29.aspx

- Programming using the SharePoint 2013 REST service
  http://msdn.microsoft.com/en-us/library/fp142385.aspx

- Understanding and Programming with SharePoint Web Services
  http://de.slideshare.net/newsteplearning/understanding-and-programming-with-sharepoint-web-services

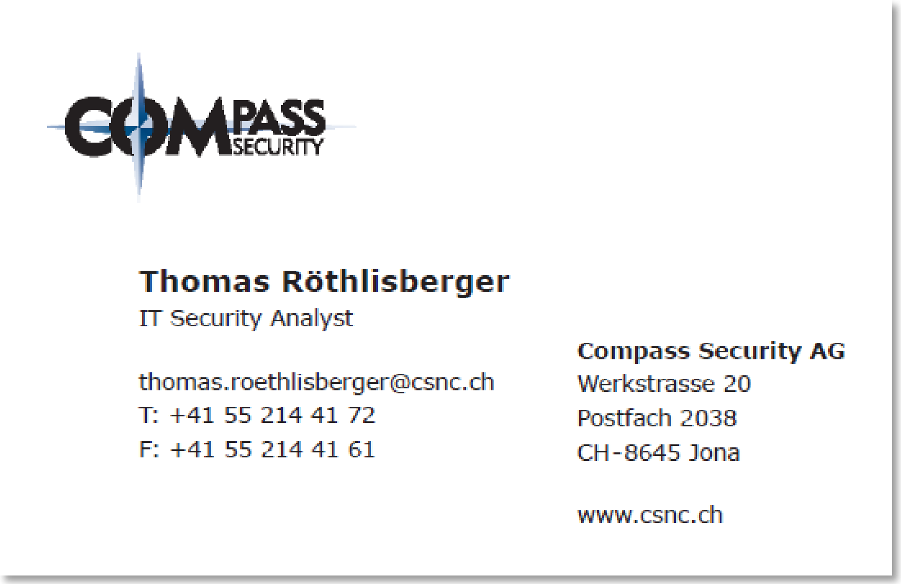
- Basic operations with the SharePoint .NET client object model
  http://msdn.microsoft.com/en-us/library/fp179912.aspx#BasicOps_SPCSOMOps

References

- Choose the right API set in SharePoint 2013
  http://msdn.microsoft.com/en-us/library/jj164060.aspx
- Safe Controls list
  http://technet.microsoft.com/en-us/library/cc261736#BKMK_SafeControls
- Security for SharePoint Solutions
  http://msdn.microsoft.com/en-us/library/ee696753.aspx
- Configure and deploy Web Parts
  http://technet.microsoft.com/en-us/library/cc261736
- Microsoft Windows SharePoint Services and Code Access Security
  http://msdn.microsoft.com/en-us/library/ms916855.aspx
- What to do? Farm solution vs Sandbox vs App
  http://sharepointdragons.com/2012/09/03/sharepoint-2013-what-to-do-farm-solution-vs-sandbox-vs-app/

References

- Using the Developer Dashboard
  http://msdn.microsoft.com/en-us/library/ff512745.aspx
- SharePoint Hacking Diggity Project
  http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/
- Research for SharePoint (MOSS)
  https://www.owasp.org/index.php/Research_for_SharePoint_%28MOSS%29
- …



Thomas Röthlisberger
IT Security Analyst

thomas.roethlisberger@csnc.ch
T: +41 55 214 41 72
F: +41 55 214 41 61

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

www.csnc.ch