

Malicious content in enterprise portals

Presented by Shalom Carmel
Shalom@venera.com

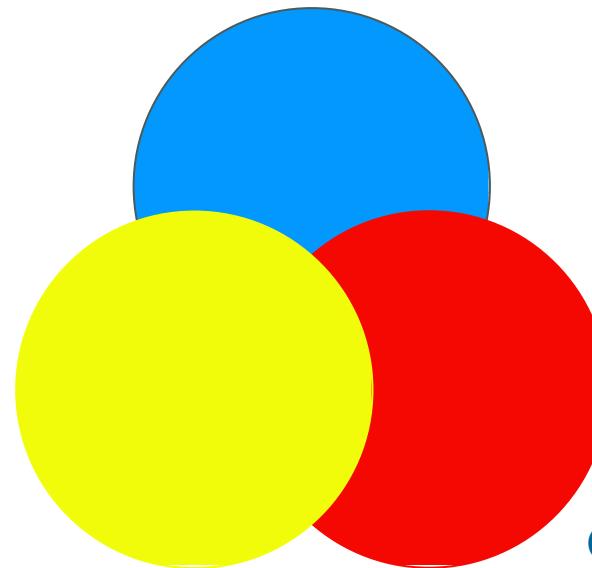


Why do we care?

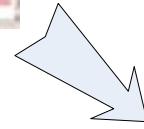
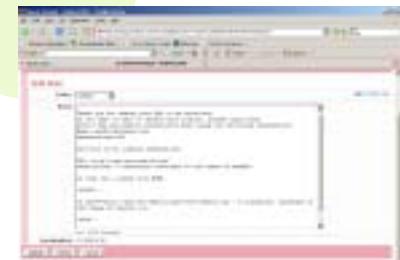
- Portals are more than Intranets
- Portals getting common
- Targeted applications
- Multitude of content sources
 - Many sources
 - Many formats
 - Many technologies
- Expensive to maintain

Content

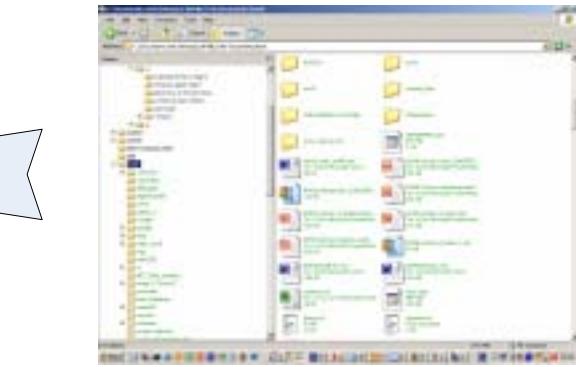
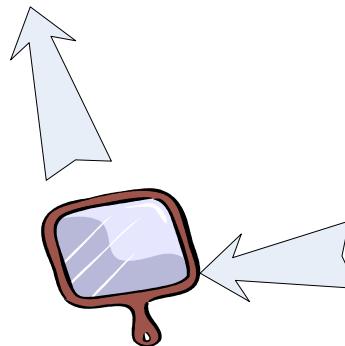
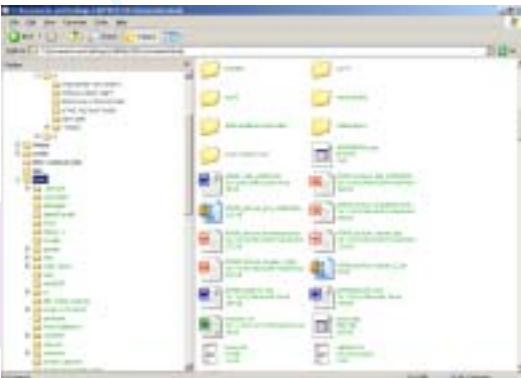
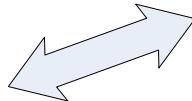
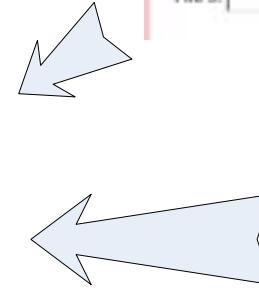
Delivery



Where does content come from?

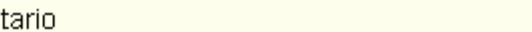


Portal



Content entry templates

- Just like in all CMS (Joomla, Mambo, PHPNuke, Zope, Plone, Jetspeed,...)

Titulo	<input type="text"/>
Comentario	<input type="text"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;">  </div>

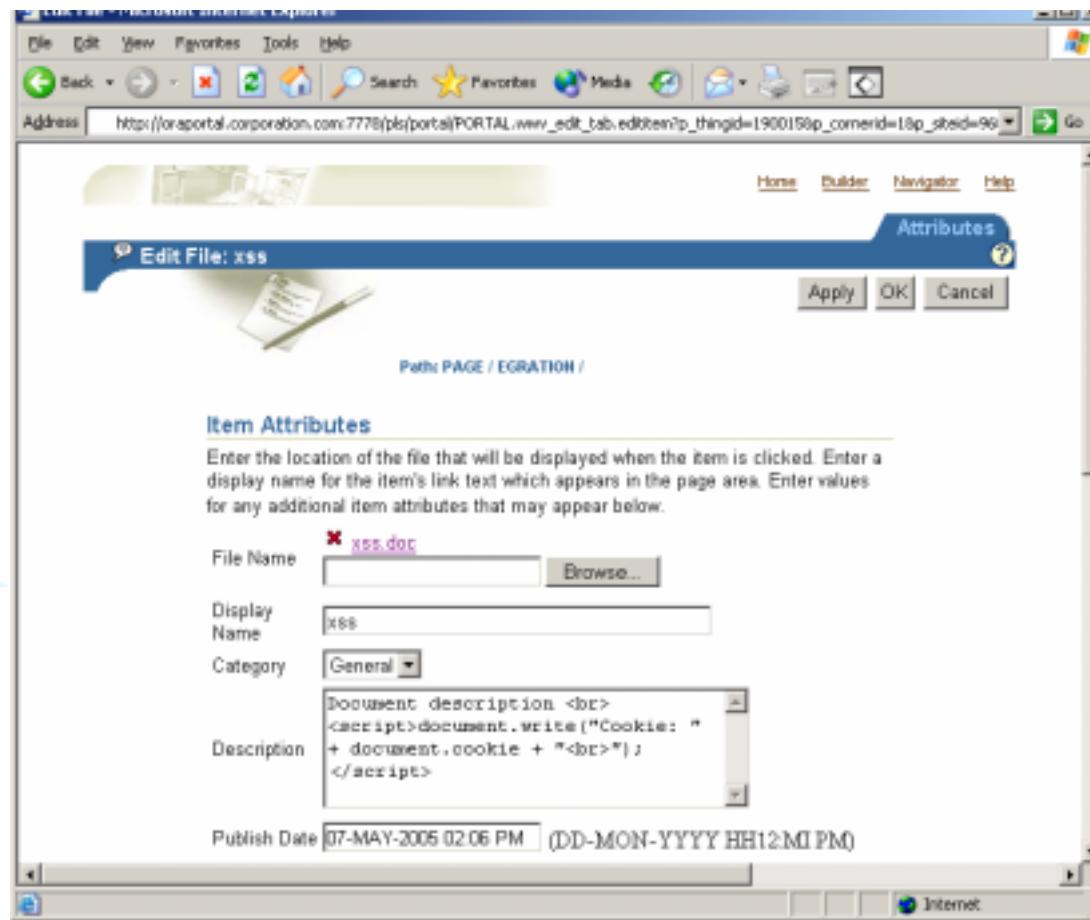
Content entry templates

Protection by web application firewall

YES!

Uploaded files

Poisoned at birth

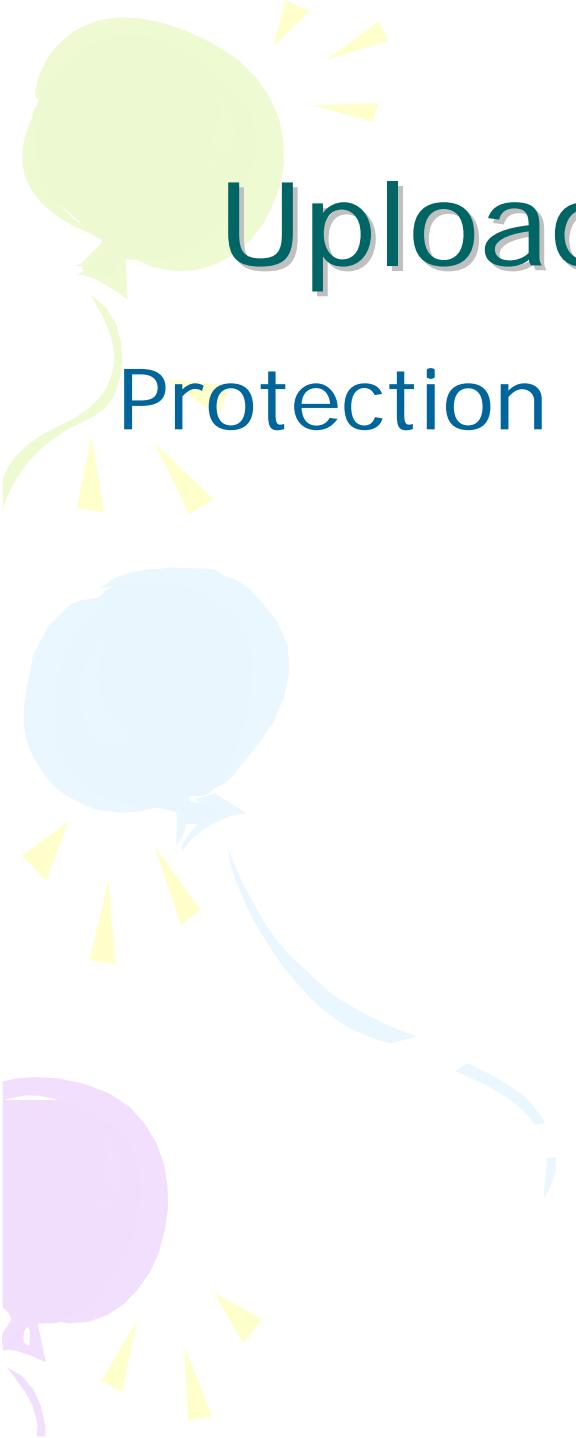


Result of upload

The screenshot shows a Microsoft Internet Explorer window displaying a graphical editing interface for a page in an Oracle Application Server Portal. The title bar reads "INTEGRATION - MICROSOFT INTERNET EXPLORER". The address bar shows the URL: http://oraportal.corporation.com:7778/portal/page?_pageid=96,18&_dad=portal&_schema=PORTAL&_mode=16.

The interface includes the following elements:

- Toolbar:** Back, Forward, Stop, Refresh, Home, Search, Favorites, Media, Mail, Print, Help.
- Header:** File, Edit, View, Favorites, Tools, Help.
- Address Bar:** Address: http://oraportal.corporation.com:7778/portal/page?_pageid=96,18&_dad=portal&_schema=PORTAL&_mode=16.
- Editing Views:** Graphical, Layout, List.
- Page Group:** Properties.
- Page:** Properties, Style, Access.
- Create:** Sub-Pages.
- Path:** egration.
- Buttons:** Go to Page, Builder, Navigator, Help.
- Content Area:** Displays the Oracle Application Server Portal logo and the word "egration".
- Bottom Navigation:** Home, Help, Edit, Customize, Account Info, Logout.
- Bottom Left:** XSS button.
- Bottom Text:** Document description Cookie: SSO_ID=v1.2~1~C46344A5C24B0E587778084817BC8483AB12CBF975D41012E9F52629048AA8E86C9537AFC65B52D58011570969C50FB747B053273 portal=9.0.3+en-uk+us+FRANCE+FB8B1CB2F279DD5BE030800A67051131+D28EEB20B7ECF4B4BBD63BFF6781622A35254B85A21D6ED870602E7034C



Upload manual metadata

Protection by web application firewall

YES!

Uploaded files

Document metadata → portal
metadata

http://portal.plumtree.com - Document Properties - Mozilla Firefox

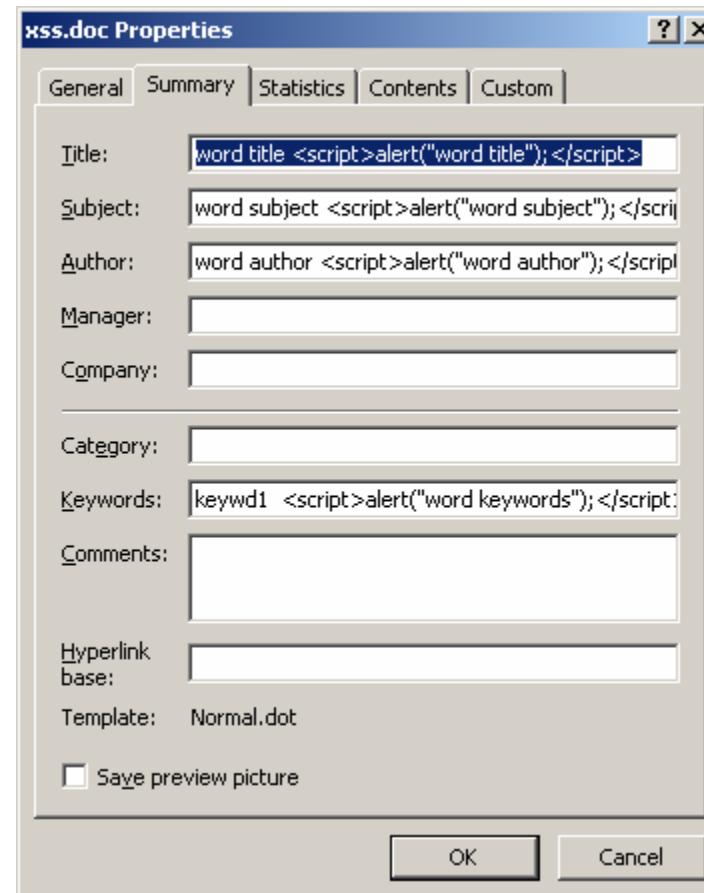
Name	Administrator's Guide for Plumtree Corporate Portal 5.0.2
Description	Learn to manage, maintain, and troubleshoot your Portal
Card Created	Feb 26, 2004 4:49:07 PM
Card LastModified	Aug 29, 2006 5:48:32 PM
Open Document URL	http://portal.plumtree.com/portal/server.pt/gateway/PTARGS_0_2_589171_0_0_18/AdministrationGuide_PlumtreeCorporatePortal_v5-0-2.pdf
Plumtree Document Type ID	419
Card Content Language	English
Crawler Tag	Manual
Class ID	18
Object ID	589171
UUID	{400CAE7D-6892-461D-90F7-10E25F5C0F20}

Customized Properties

Property	Value
Author	Plumtree Software
Created	Feb 26, 2004 4:49:00 PM
Document Title	Administrator's Guide for Plumtree Corporate Portal 5.0.2
Keywords	ProductName=Plumtree Corporate Portal, Version=5.0.2, DocumentationType=Administrators Guide,
Subject	Learn to manage, maintain, and troubleshoot your Portal
URL	./docfetch/DocFetch.aspx?path=%5C%5Cfile%5CPortal%5CDocumentation%5CKD_SupportCTR_docs%5CPlatform%5CPlatform_502%5CAdministrationGuide_PlumtreeCorpor

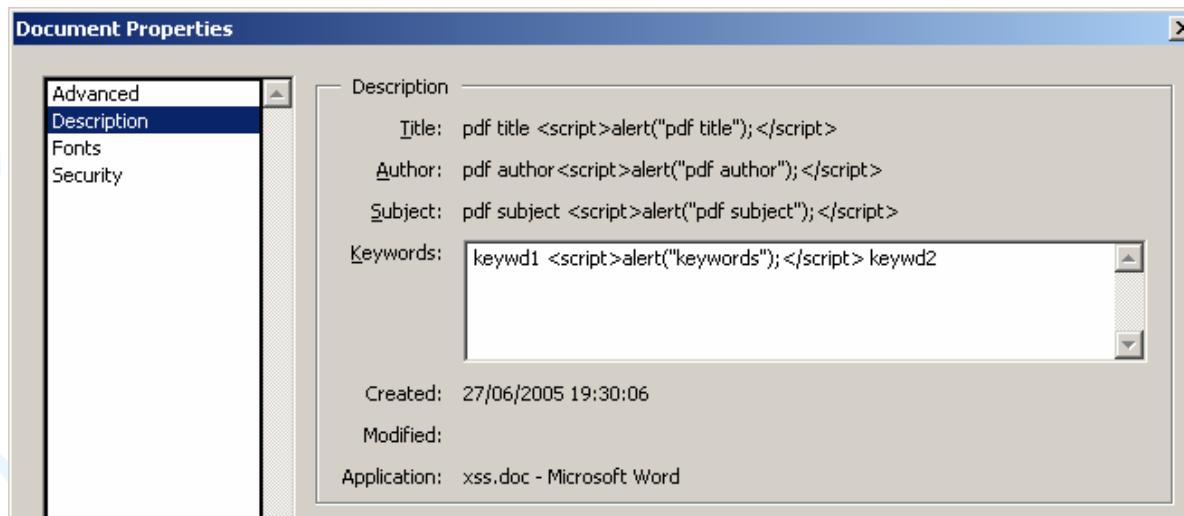
Uploaded files

Poisoned at conception - ms office



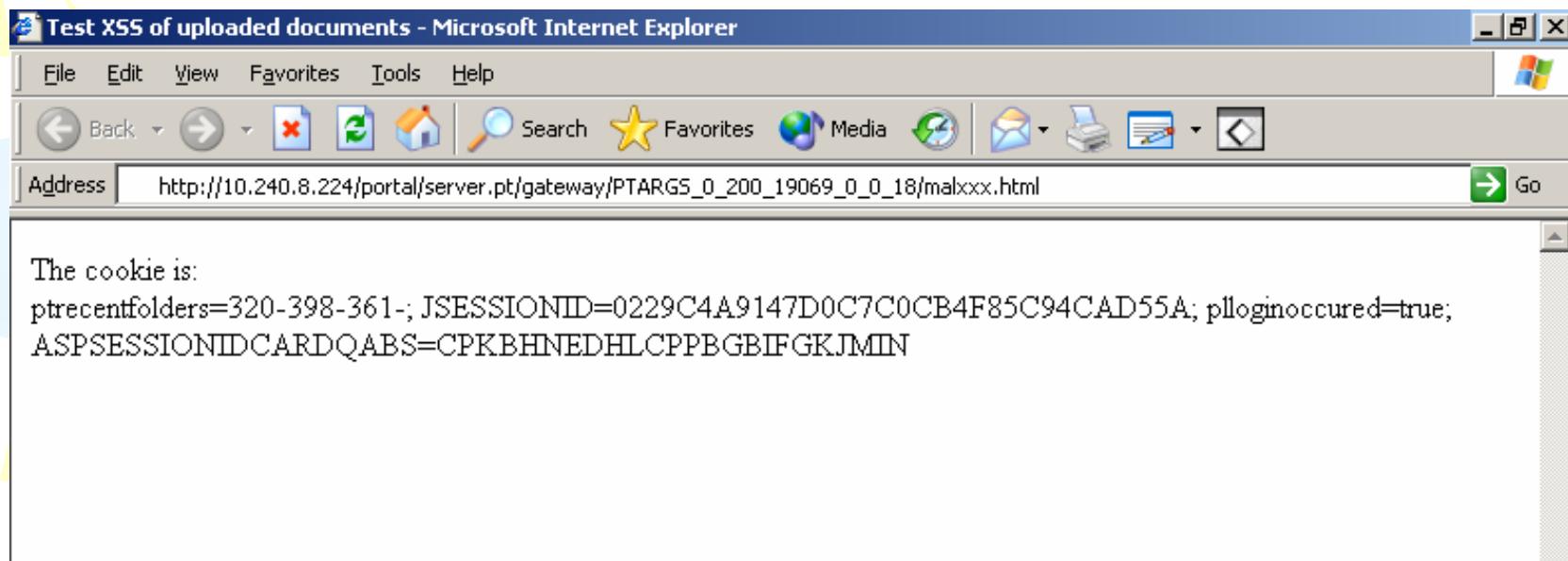
Uploaded files

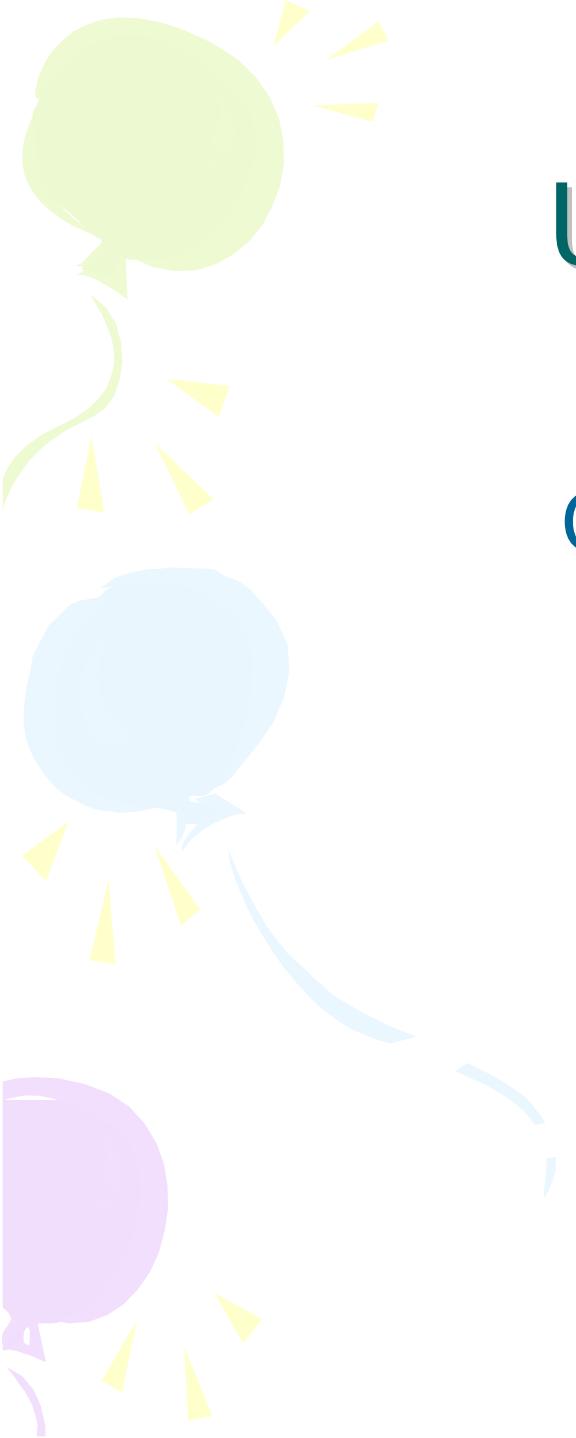
Poisoned at conception - acrobat



Uploaded files

Poisoned at conception - html



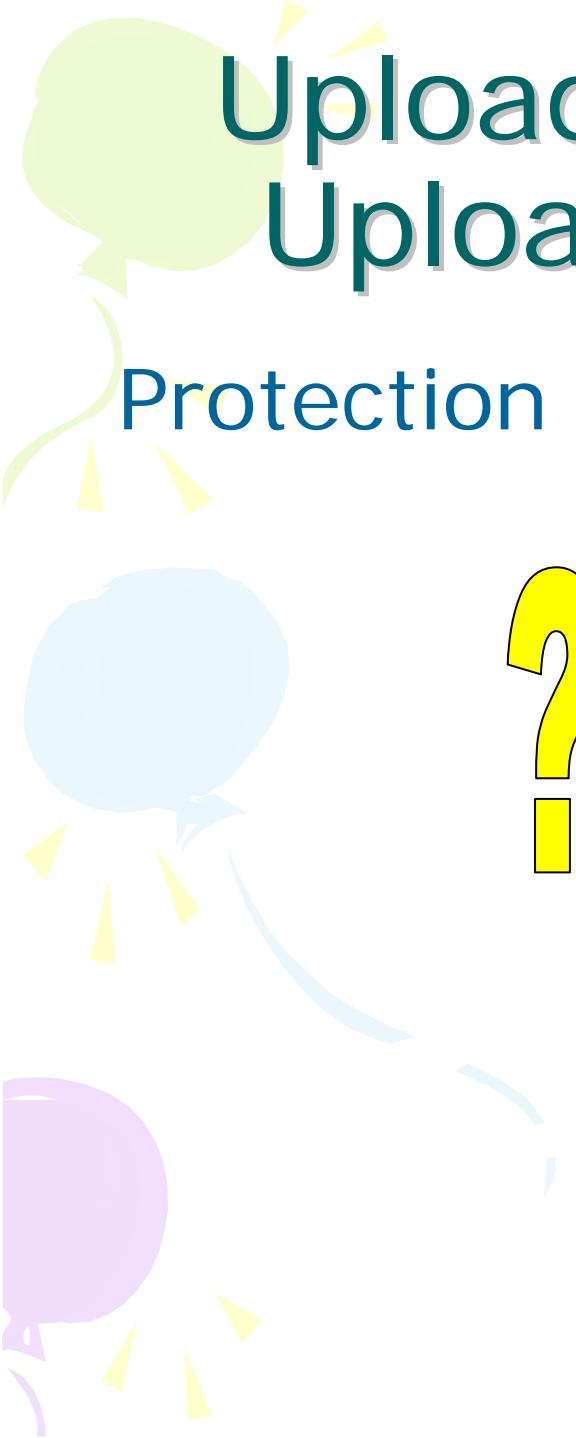


Uploaded files

WebDav

Oracle File System

SharePoint



Uploaded docs properties Uploaded docs contents

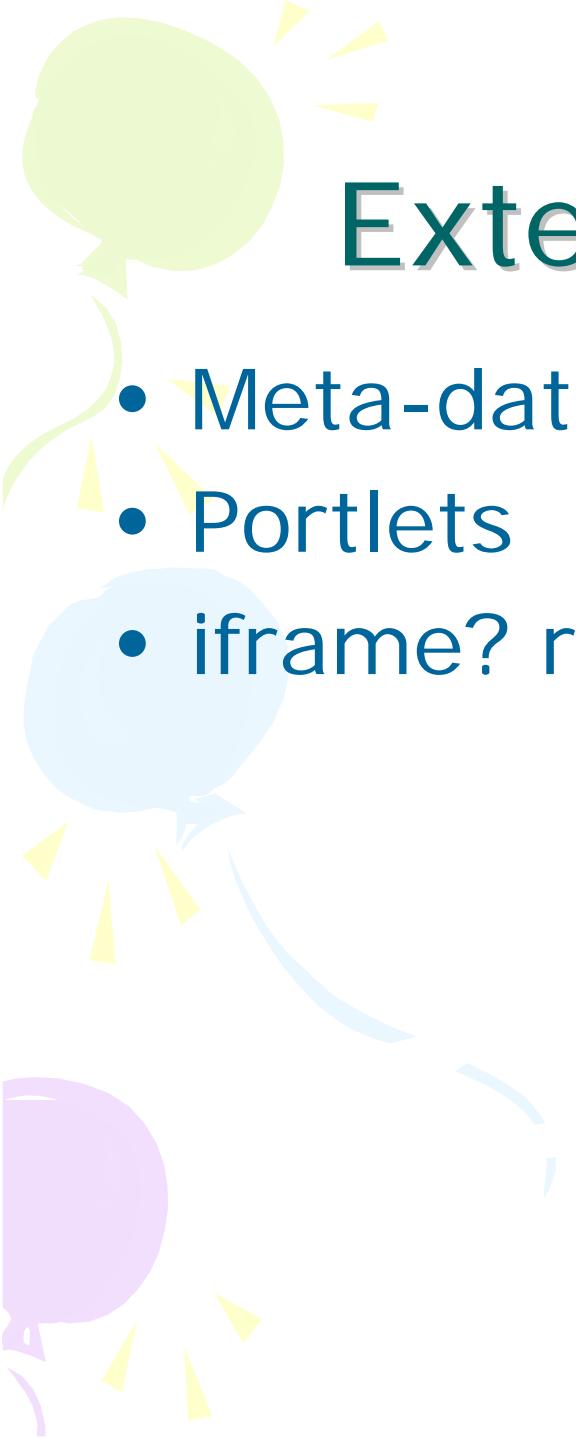
Protection by web application firewall

?MAYBE?



External web content

Until now we had some control!



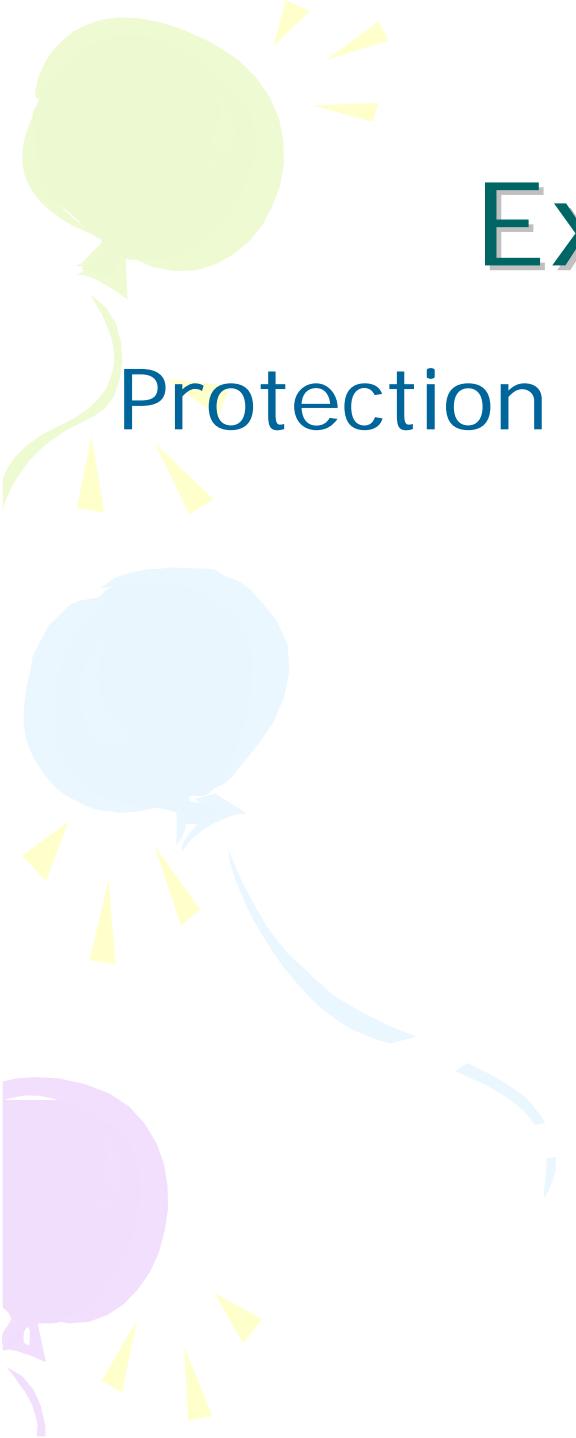
External web content

- Meta-data
- Portlets
- iframe? reverse proxy? custom code?

External web content

- reverse proxy example

General Document Properties	
Property	Value
Name	December 15, 2005 New Product Roadmap Vision for BEAs Portal.ppt
Description	Presentation
Card Created	Dec 20, 2005 12:49:09 PM
Card LastModified	Mar 30, 2006 2:18:03 PM
Open Document URL	http://portal.plumtree.com/portal/server.pt/gateway/PTARGS_0_2_2805427_0_0_18/December%2015,%202005%20New%20Product%20Roadmap%20Vision%20for%20BEAs%20Portal.ppt
Plumtree Document Type ID	585
Card Content Language	English
Keywords	BEA_BIP_Portal_Overview_simple_v3, BEA_BIP_Portal_Overview_simple_v12, BEA_BIP_Portal_Overview_simple_v1
Security	Employees-Only
Subject	BEA_BIP_Portal_Overview_Simple
URL	http://prodauth02.plumtree.com/ntcws/docfetch/DocFetch.aspx?path=%5C%5Cfile%5Cportal%5CEvents%5C2005+Presentations%5CDecember+15%2C+2005+New+Product+Roadmap+Vision+for+BEAs+Portal.ppt&signature=632702527040150000&locale=



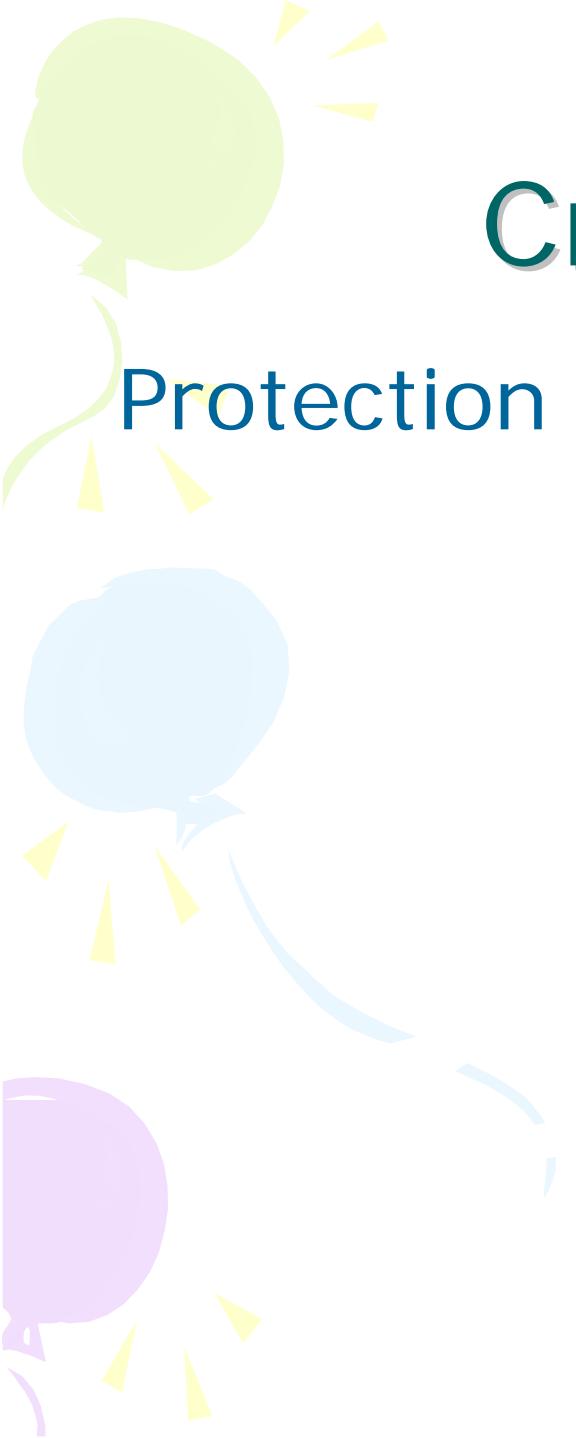
External content

Protection by web application firewall

NO!

Crawl and index

- Special case of external content
- Web, file systems, email, databases



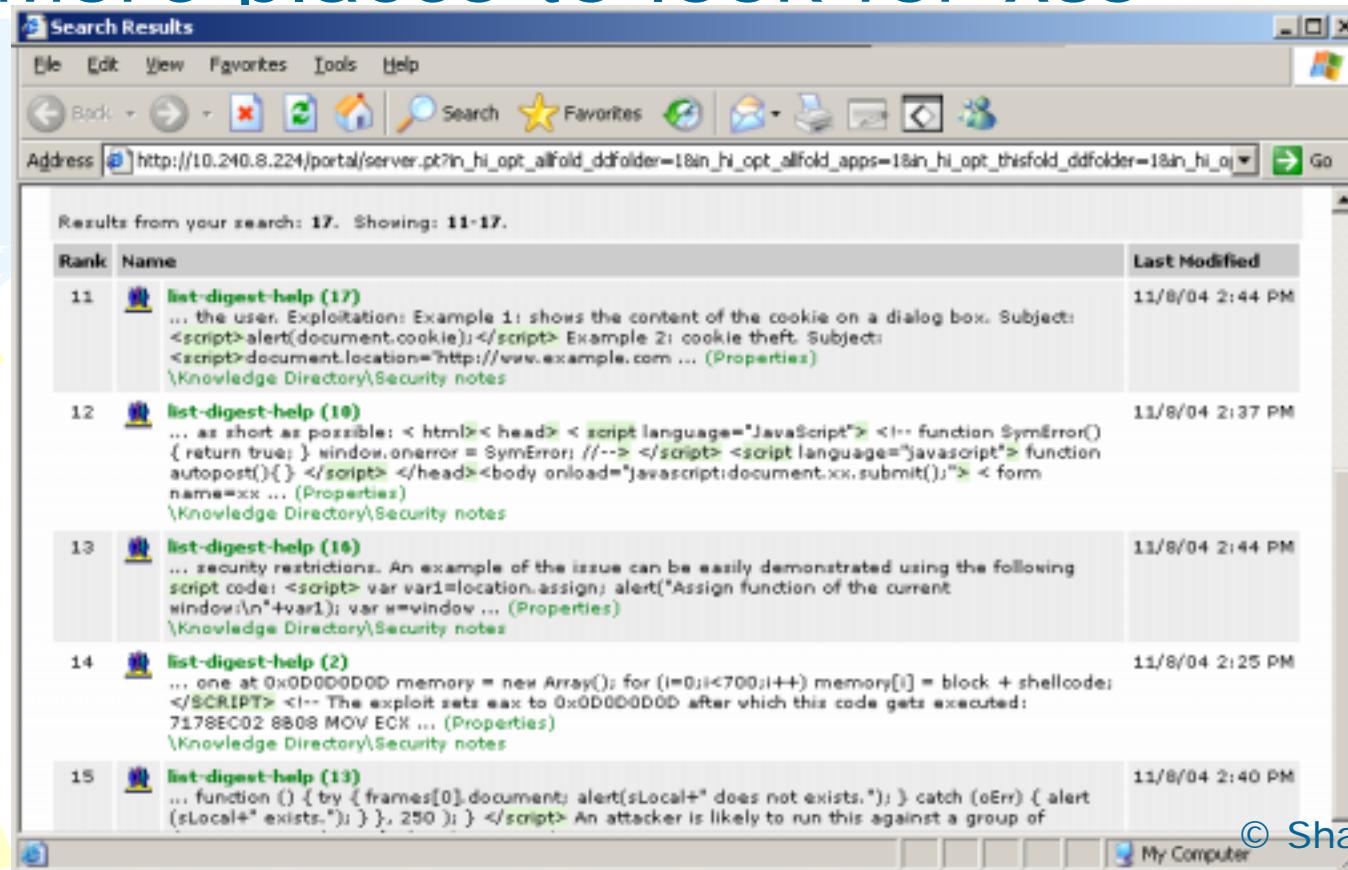
Crawled content

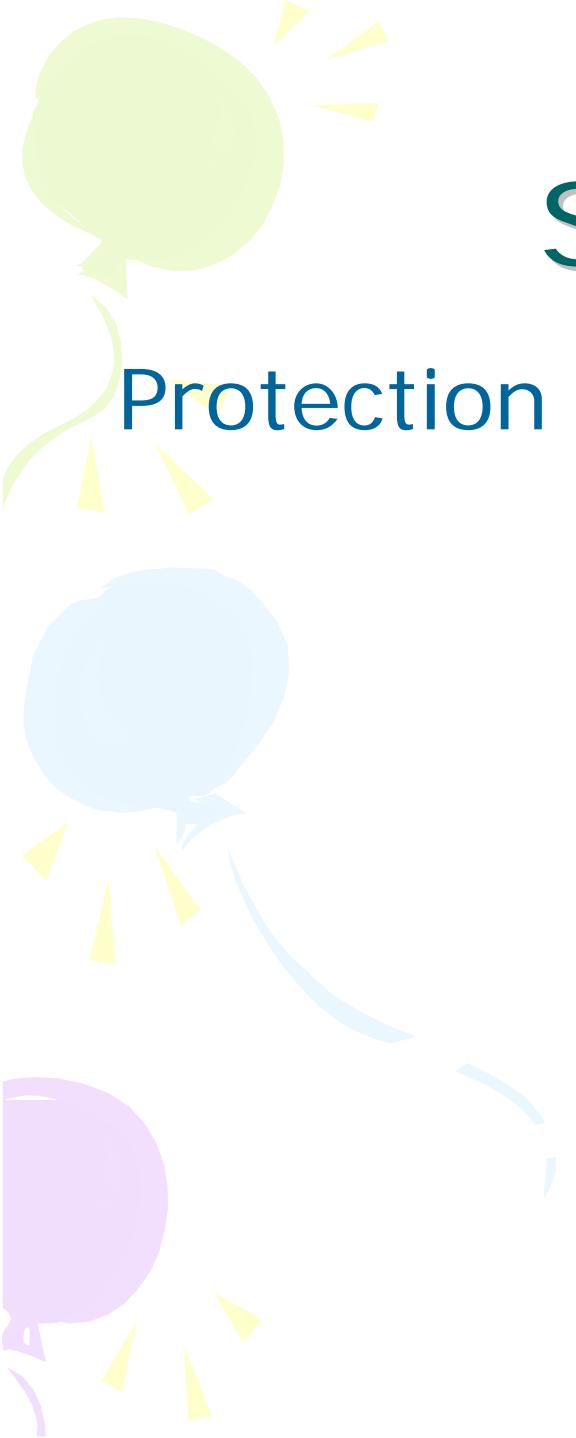
Protection by web application firewall

NO!

Search and retrieve

- Federated search
- More places to look for xss





Search results

Protection by web application firewall

NO!

Protection by web application firewall

Content entry templates	YES
Upload manual metadata	YES
Uploaded docs properties	Maybe
Uploaded docs contents	Maybe
External content	NO*
Crawled content	NO*
Search results	NO*

*Technically possible but very difficult implementation