

The background features several large, stylized, overlapping swirls in light green, light blue, and light purple. Scattered throughout the background are numerous small, yellow, triangular shapes, some pointing upwards and others downwards, creating a dynamic and abstract visual effect.

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

Source

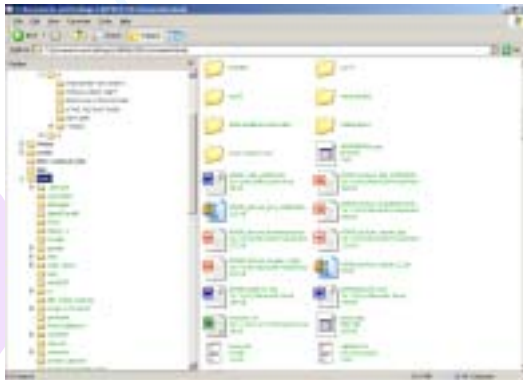
Consumer



Where does content come from?

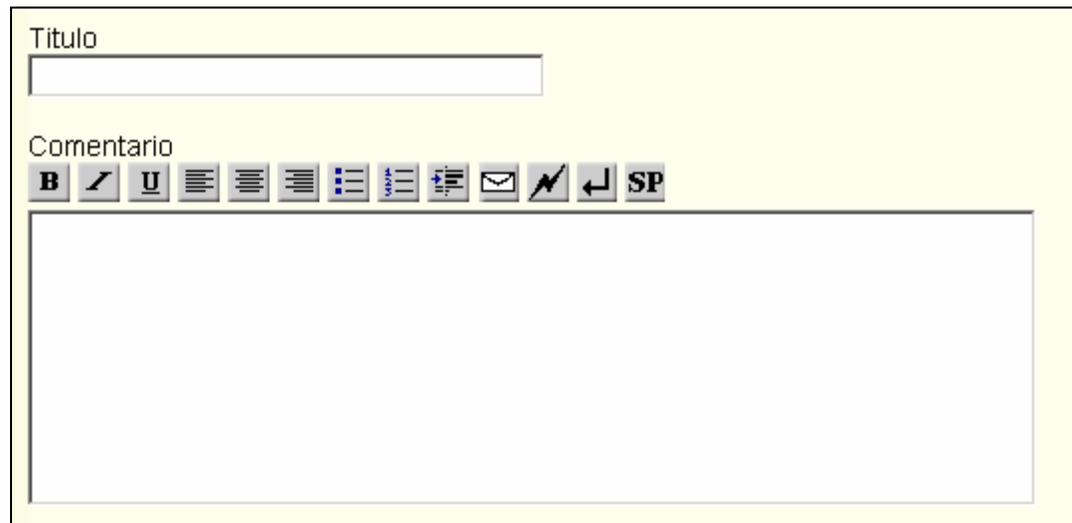


Portal



Content entry templates

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



The image shows a content entry form with a yellow background. At the top, there is a text input field labeled "Titulo". Below it is a section labeled "Comentario" which contains a rich text editor. The rich text editor has a toolbar with icons for bold (B), italic (I), underline (U), bulleted list, numbered list, decrease indent, increase indent, link, unlink, and a "SP" button. Below the toolbar is a large text area for the comment.



Content entry templates

Protection by web application firewall

YES!

Uploaded files

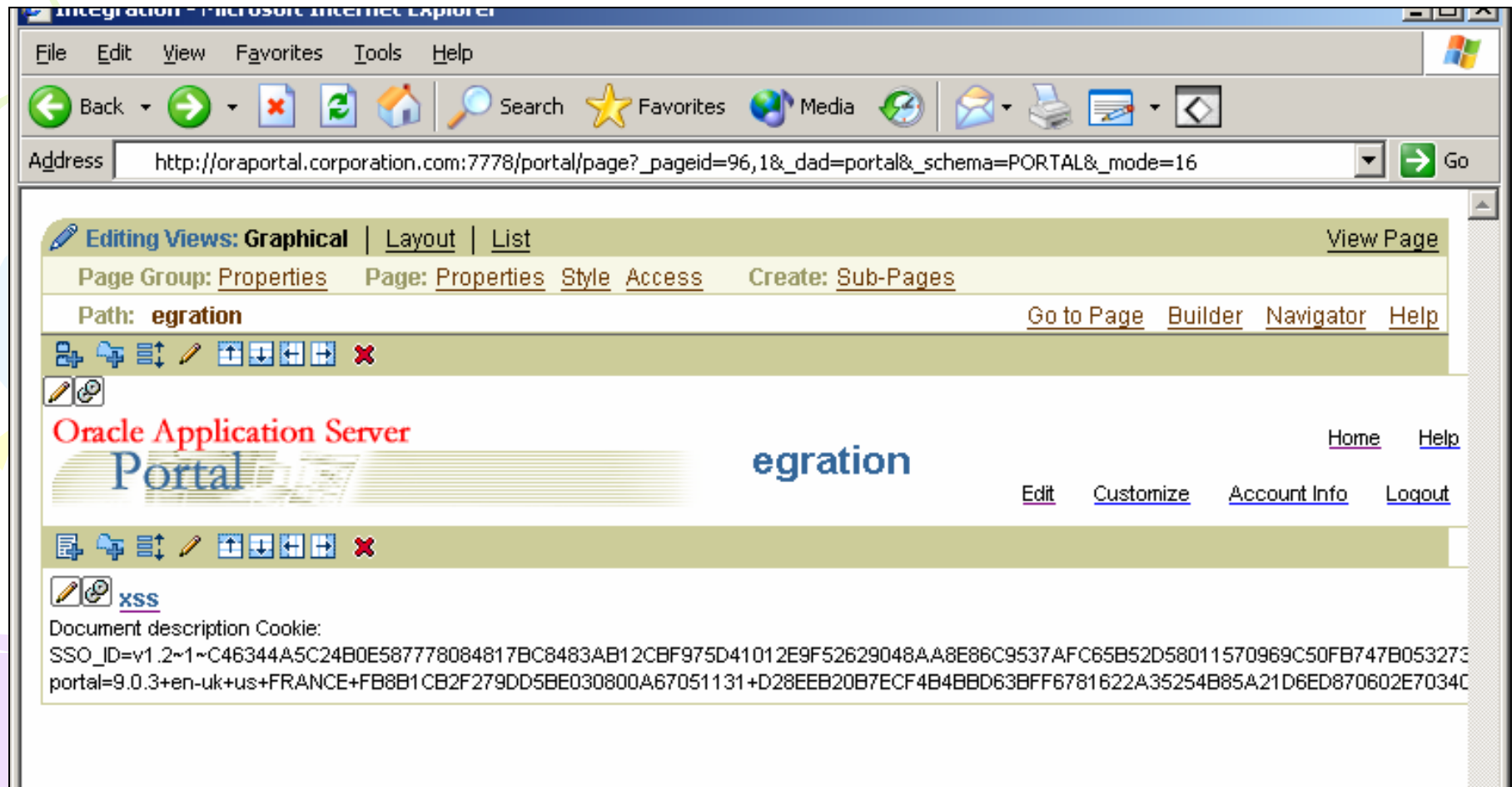
Poisoned at birth

The screenshot shows a web browser window displaying a portal page titled "Edit File: xss". The address bar shows a URL from "foraportal.corporation.com". The page has a navigation bar with links for "Home", "Builder", "Navigator", and "Help". Below the navigation bar, there's a section for "Attributes" with "Apply", "OK", and "Cancel" buttons. The main content area is titled "Item Attributes" and contains instructions: "Enter the location of the file that will be displayed when the item is clicked. Enter a display name for the item's link text which appears in the page area. Enter values for any additional item attributes that may appear below." The form fields are as follows:

- File Name:** xss.doc (with a red 'x' icon and a "Browse..." button)
- Display Name:** xss
- Category:** General (dropdown menu)
- Description:** Document description
<script>document.write("Cookie: " + document.cookie + "
");</script>
- Publish Date:** 07-MAY-2005 02:06 PM (DD-MON-YYYY HH:MM PM)

The browser's status bar at the bottom indicates "Internet".

Result of upload





Upload manual metadata

Protection by web application firewall

YES!

Uploaded files

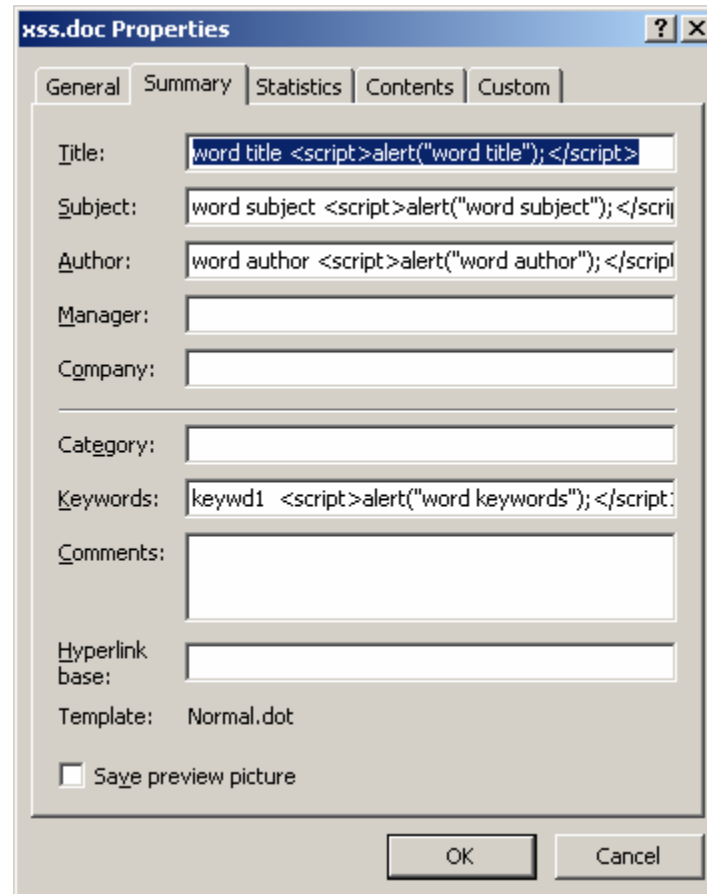
Document metadata → portal
metadata



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



xss.doc Properties [?] [X]

General | Summary | Statistics | Contents | Custom

Title: word title <script>alert("word title");</script>

Subject: word subject <script>alert("word subject");</script>

Author: word author <script>alert("word author");</script>

Manager:

Company:

Category:

Keywords: keywd1 <script>alert("word keywords");</script>

Comments:

Hyperlink base:

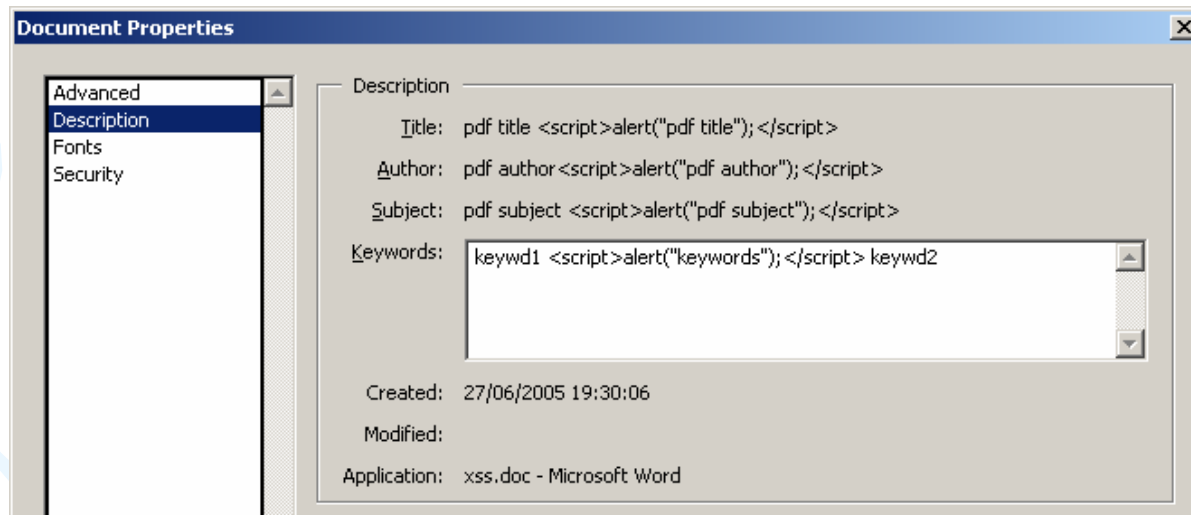
Template: Normal.dot

☐ Save preview picture

OK Cancel

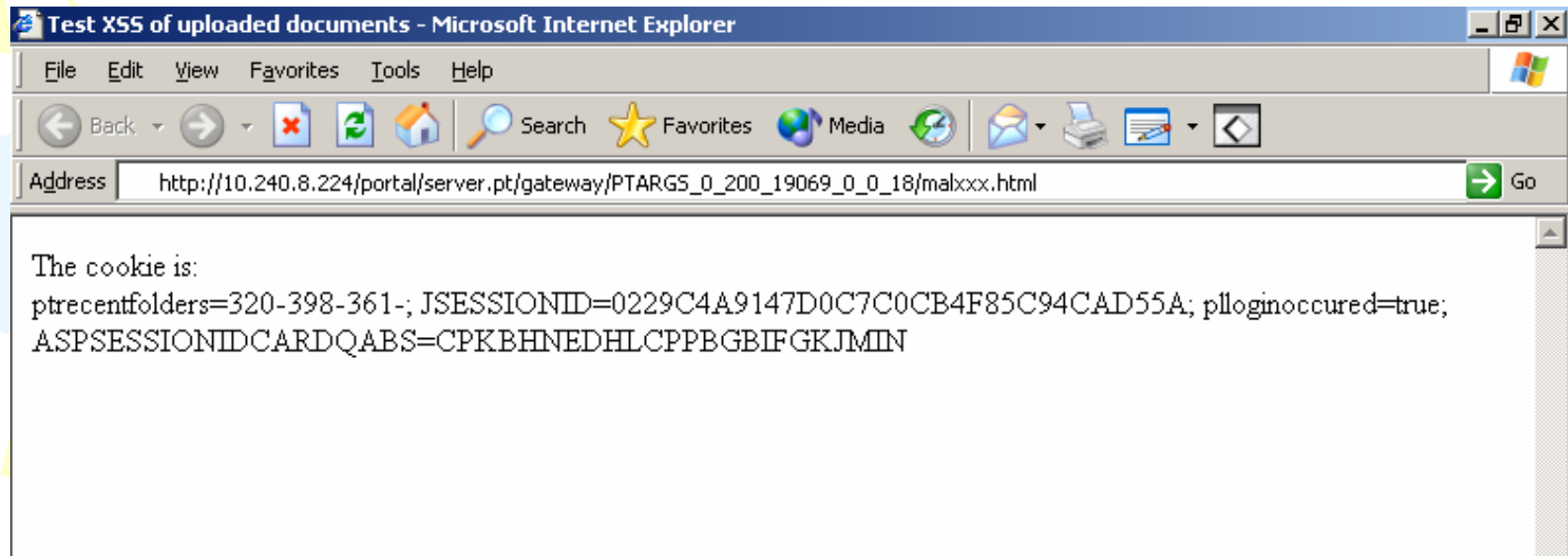
Uploaded files

Poisoned at conception - acrobat



Uploaded files

Poisoned at conception - html



Three stylized balloons in green, blue, and purple are positioned on the left side of the slide. Each balloon has a string and several small yellow triangular flags attached to it.

Uploaded files

WebDav

Oracle File System

SharePoint



Uploaded docs properties
Uploaded docs contents

Protection by web application firewall

?MAYBE?

Three stylized balloons in light green, light blue, and light purple are positioned on the left side of the slide. Each balloon has a small yellow starburst above it and a thin line trailing off to the left.

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_v12, BEA_BIP_Portal_Overview_simple_v12
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

© Shalom Carmel, 2006