Blackboard

Mixed Content and the ANGEL LMS

Date Published: Sep 10,2013 **Category:** Product:ANGEL; Version:ANGEL_8_0,ANGEL_7_4 **Article No.:** 000034122

Product: ANGEL

Issue Description: An overview of mixed content and the impact of such content within the ANGEL LMS.

Symptoms:

What is mixed content?
Mixed content is when a web site delivers both HTTP and HTTPS content on the same web page. Most browsers distinguish between passive mixed content and active mixed content. Active mixed content can be used to deliver malicious code or intercept sensitive data. Examples of active mixed content include hyperlinks and script tags. Passive mixed content is HTTP content that cannot be used to modify the behavior of other content on the page and carries a lower security risk. An example of passive mixed content is an embedded image served over HTTP.

Why is mixed content a concern?
In a time where Internet users must be ever more careful of phishing schemes, identify theft, and other Internet scams, SSL certificates are serving an increasingly important role in Internet security. SSL certificates allow for a web site to exchange secure, encrypted communication with users via HTTPS. Additionally, SSL certificates from recognized certificate authorities help validate the identity of a web site.
Mixed content occurs when a website with an SSL certificate delivers a web page which in turn delivers content from a server without using SSL. Often times it is transparent to the user that some of the page content is being delivered from another server. This could allow malicious code to be delivered to the user. The user could also be misled into thinking that all of their activity is being sent via secured communication.

Why should mixed content be a concern within ANGEL?
In addition to the security concerns noted above, modern browsers are increasingly taking mixed content seriously and implementing efforts to protect their users from these potential security risks. The implementation of mixed content protection varies from browser to browser but may include blocking the delivery of HTTP content by default.

Rather than relying upon any browser's current policy of blocking or allowing mixed content, clients are encouraged to review their own content and take steps toward eliminating the delivery of mixed content.

Resolution/Workaround:

Below are the most common areas in which mixed content may occur within an ANGEL environment and recommendations on avoiding the use of mixed content.

Links within pages and other content items
The HTML editor can be used within most text fields to add hyperlinks to other web sites. Common locations for links to external resources include nuggets, page content items, and instructions on content items such as discussion forums and drop boxes.

Determine the current target of a link
1. Open the settings of the content item or the editor for the nugget to access the HTML Editor.
2. Right-click on the link and select Edit Link.
3. On the Link Info tab, make note of the protocol in use (http:// or https://).
4. On the Target tab, make note of the target in use.

Avoiding mixed content

1. If the current protocol of the link is HTTP, check if HTTPS will work for the same link. This can be done by opening a new browser tab and entering https:// followed by the URL. If the HTTPS link works, simply change the protocol of the link to https://.
2. If the HTTPS link does not work, change the target of the link to New Window (_blank). By default links created via the HTML Editor are opened within the ANGEL frame. If the ANGEL web site is secured with an SSL certificate and the link uses the http:// protocol, the destination of the link will be treated as mixed content. The New Window (_blank) target will open the link in a new browser tab outside of the ANGEL frame and thus will not be mixed content.

Link content items
Link content items are content items which load another web site within the ANGEL frame.

Determine the current target of a link content item
1. Click the settings link under the content item.
2. Check if the Link URL uses http:// or https://.

Avoiding mixed content
1. If the link is currently using http://, check if HTTPS will work for the same link. This can be done by opening a new browser tab, copying and pasting the Link URL into the address bar, and changing the URL to use https://. If the HTTPS link works, simply change the Link URL to use https://.
2. All of the Link Targets on a link content item, including New Window, will open the link URL within an ANGEL frame. It is necessary to open the URL within an ANGEL frame to support features such as user tracking and agents. If an HTTPS link is not available use the steps below to configure an agent on the content item which will redirect to the HTTP URL outside of the ANGEL frame. By performing the redirect as an agent, the content item will be loaded first, allowing for user tracking and execution of any other agents applied to the content item. The HTTP content is then loaded in an external frame so that it is not mixed content.

Redirecting HTTP link content items
1. Click settings for the link content item.
2. Set the Link Target to New Window.
3. Save.
4. Go to the course Automate tab.
5. Click Add New Agent.
6. Enter a name for the Agent.
7. Select Content Agent.
8. Click “Select content to monitor”.
9. Select Link from the Lesson Type drop-down menu and select the “Specific links” radio button.
10. Select the appropriate link content item and click the Add button.
11. Click the Close Window button.
12. Ensure that “viewed” is selected in the drop-down menu below the added content item.
13. Click Next.
14. Click Next on Step 2 of the Create Agent wizard to accept the default settings.
15. Select Redirect from the Choose Action Type drop-down menu.
16. Enter the URL, including http://.
17. Optionally add a delay on the redirect. Ignore the Target setting as the Link Target setting applied to the content item in step 2 will ultimately determine where the web page is opened.
18. Click Next.
19. Click Save.
20. Test accessing the link content item. The web page should be loaded in a new browser tab.

Google Rich Media Content
The Google Rich Media tool in the HTML editor allows users to embed YouTube videos and Picasa images or insert links to these resources.
Use of the YouTube and Picasa search features requires the ANGEL website to make requests to Google’s servers to retrieve the search results. Currently these requests are sent via HTTP and will be viewed as mixed content on an ANGEL environment using an SSL certificate. Additionally, using the Google Rich Media tool to embed or link to a YouTube video or embed a Picasa image adds HTML to the page which uses HTTP.

Avoiding mixed content
1. Blackboard has prepared a patch for these two issues which is compatible with ANGEL 8.0. Blackboard

Managed Hosting has applied this patch to all hosted ANGEL 8.0 environments. Self-hosted clients may obtain the patch by entering a support case via https://behind.blackboard.com. Changes made by the patch will be added to mainline code in ANGEL 8.0 Service Pack 9. Please note that end users will have to clear their browser cache in order to receive the benefit of the patch.
2. For existing embedded YouTube and Picasa content, open the HTML editor and click the Source button to toggle to the HTML source code. Use the browser's search feature (Ctrl+F) to locate all instances of http:// and change them to https://. Save and retest the content.

Video Anywhere
Video Anywhere is a new feature added in ANGEL 8.0 Service Pack 8 which provides an integration within the ANGEL HTML editor to allow the user to record a video using their webcam, upload the video to YouTube, and embed the video into ANGEL content. The integration requires authenticating against Google servers. If using the default system setting to allow ANGEL to authenticate to YouTube (as opposed to an institution's Google API key and client ID) the authentication process involves a request to a Blackboard server. This request is currently made over HTTP and may be blocked as mixed content by some browsers. In such browsers, users may still record and embed new videos without permitting mixed content but cannot browse their library of existing videos.

Avoiding mixed content
Blackboard has added an SSL certificate to the server and prepared a patch to start making the authentication request using HTTPS. Blackboard Managed Hosting will apply the patch to hosted environments during the scheduled maintenance window for installing Service Pack 8. Self-hosted clients may obtain the patch by entering a support case via https://behind.blackboard.com. Changes made by the patch will be added to mainline code in ANGEL 8.0 Service Pack 9. Please note that end users will have to clear their browser cache in order to receive the benefit of the patch. Additionally, end users may need to configure their browser to accept pop-ups from https://angellearning.com in order to access the login prompt.

Embedded images
Images can be embedded into nearly any text field including nuggets, page content items, and assessment questions. Images which are uploaded via the HTML Editor are saved to the ANGEL file server and thus delivered from the same server as the rest of the page and cannot be mixed content. However, if the embedded image is actually saved on a different server, it could be mixed content.

Determine the current location of the image
1. Open the settings of the content item or editor of the nugget to access the HTML Editor.
2. Right-click on the image and select Image Properties.
3. Review the value in the URL field. If the URL includes “AngelUploads”, the image is saved on the ANGEL file server and no action is required. If the URL is to another web site and starts with http://, the image will be mixed content.

Avoid mixed content
1. If the URL of the image is currently using http://, check if HTTPS will work for the same URL. This can be done by opening a new browser tab, copying and pasting the URL into the address bar, and changing the URL to use https://. If the HTTPS link works, simply change the URL to use https://.
2. If the HTTPS URL does not work, save a copy of the image locally and upload it to ANGEL via the Insert/Edit Image tool in the HTML editor. Applicable copyright and rights of use policies should be observed when re-using images from other web sites.

Legal Disclaimer: Statements regarding our product development initiatives, including new products and future product upgrades, maintenance, fixes, updates or enhancements represent our current intentions, but may be modified, delayed or abandoned without prior notice and there is no assurance that such offering, upgrades, maintenance, fixes, updates or functionality will become available unless and until they have been made generally available to our customers.