Understanding mixed content

Background

Why do some links and some embedded items within D2L no longer work?

Shortly before the start of Millersville's fall 2013 semester, several web browser makers released new versions of their web browsers, new versions that deliberately established new and more restrictive rules for links, embedded items, and other web content. As a result, web browsers now decline to open or load web content that worked in the past.

Which web browsers are affected?

Of the browsers supported by Desire2Learn, Chrome, Firefox, and Internet Explorer (IE) have all been updated to follow more restrictive rules on what web content they load.

What links and other items are now blocked by web browsers?

Web browsers now block some so-called mixed content. Over time, the browser makers plan to block more types of mixed content until all of it is blocked.

Mixed Content

What is mixed content?

Mixed content is non-secure web content included on a secure web page.

Most content travels from web servers to web browsers (and back) over the HyperText Transfer Protocol (HTTP). HTTP works well for basic content, but as HTTP does not provide any protection from possible high tech eavesdroppers along the paths content takes as it crosses the Internet, HTTP isn't sufficient for online shopping, banking, or coursework.

Web servers, including D2L's servers, that exchange more sensitive information with web browsers do so over a secure variant of the HyperText Transfer Protocol known as HTTPS. HTTPS uses an encryption technology known as Secure Socket Layers (SSL) to protect content as it crosses the Internet.

A secure web page, one encrypted with SSL and transferred over HTTPS, that contains some non-secure, non-encrypted items is said to be made up of mixed content: secure and insecure.

What types of mixed content are blocked?

Effects

Why is D2L affected?

Would upgrading D2L help?

Are systems other than D2L affected?

In D2L, is only the Content tool affected?

Specifics

Links

What links in D2L are blocked by web browsers now?

How can I tell if a link leads to a secure or an insecure web page?

How can I set a link to open in a new window (or tab)?

Why can't I choose "Whole Window" or "Same Frame" for links to insecure (http:) web pages?

Can I change "http:" to "https:" to make my links secure?

Embeds

What embedded items in D2L are blocked by web browsers now?

How can I tell if an embed comes from a secure or an insecure web page?

Can I change "http:" URLs to "https:" URLs to make my embeds secure?

How should I embed YouTube videos?

Fixes and Workarounds

Can D2L, Millersville's Information Technology department, or PASSHE fix this problem?

As an instructor in one or more courses, how may I fix my content?

As someone attempting to use a page containing mixed content, are there any workarounds available to me?

Chrome

Firefox

Internet Explorer

Safari
Browser makers started by making their web browsers block mixed active content. Mixed active content includes:

- links
- scripts
- external style sheets
- two methods of embedding items: iframes and objects

Over time, browser makers plan to expand the list of items blocked to encompass mixed passive content as well. Mixed passive content includes:

- all images
- all embedded audio and video

Why block mixed content?

Mixed content web pages can appear completely protected and safe to those who visit them while actually exposing every visitor to possible information theft. In the past, web browsers displayed warning messages about mixed content pages, but these messages were often dismissed by users without being read. So, in response to continued growth in the number of cases of credit card and identity theft, web browser makers decided to be more firm and block insecure items on secure web pages.

Effects

Why is D2L affected?

To protect grades, student work, and faculty-created content within Desire2Learn, all communication between web browsers and the D2L servers is secure, made through HTTPS. A link to, or embed from, another web site though, can be secure (HTTPS) or insecure (HTTP) depending upon how the other server, the one hosting the item, has been configured.

Would upgrading D2L help?

No. The decision to block, rather than just warn about, mixed content was made by browser makers and implemented within web browsers. D2L, Inc. has no control over this decision, and there isn't anything they can do on the server side to instruct web browsers to stop blocking mixed content.

Are systems other than D2L affected?

Yes. On campus, other secure, web-based systems, including this wiki, have been affected, but the impact of the change reaches far beyond just Millersville systems. The effects of mixed content blocking are rippling clear across the Internet.

All web services that serve up secure pages have found their links to insecure sites, as well as their embedded items from insecure sites, blocked.

Meanwhile, web services, such as YouTube, that provide embeddable content using the insecure, HTTP method have begun seeking ways to offer that content via HTTPS so it can continue to be used.

In D2L, is only the Content tool affected?

No. Despite this browser change being about "mixed content", the change affects every tool within D2L.

Specifics

Links

What links in D2L are blocked by web browsers now?

A link within D2L is blocked by browsers when both of the following are true for that link:

- the link is to an insecure web site
- the link is not set to open in a new window (or tab)

How can I tell if a link leads to a secure or an insecure web page?

- Links that begin with "https:" go to secure sites.
- Links that begin with "http:" go to insecure sites.

How can I set a link to open in a new window (or tab)?

When you create a new URL QuickLink, D2L offers three "Open In" options for the link:

- Whole Window
- Same Frame
- New Window

Choose "New Window".
Why can't I choose "Whole Window" or "Same Frame" for links to insecure (http:) web pages?
Both "Whole Window" and "Same Frame" open the insecure web page inside D2L's own, secure web page. That would create a mixed content page, so web browsers block the opening of the link now.

Can I choose "Whole Window" or "Same Frame" for links to secure (https:) web pages?
Yes.

Can I change "http:" to "https:" to make my links secure?
In most cases, this will not work. Some web sites do offer their web pages over both HTTP and HTTPS though, so feel free to try it. Be sure to test your edited link to see if it works. If it doesn't, you will need to change the link back to "http:".

Embeds
What embedded items in D2L are blocked by web browsers now?
An embedded item within D2L is blocked by browsers when both of the following are true for that item:
- the embedded item comes from an insecure web site
- the embed is accomplished using:
  - an <iframe> tag
  - an <object> tag with a data attribute

How can I tell if an embed comes from a secure or an insecure web page?
You will need to look at the item’s embed code. Within the embed code, look for URLs (links).
- URLs that begin with "https:" are for secure sites.
- URLs that begin with "http:" are for insecure sites.

Can I change "http:" URLs to "https:" URLs to make my embeds secure?
In most cases, this will not work. Some web sites do offer their embeddable content via both HTTP and HTTPS though, so feel free to try it. For instance, this change works for some YouTube videos.

Please look carefully at your embed codes, as many contain multiple URLs. Be sure to edit all of them. Be sure to thoroughly test your edited embed code to see if it works. If it doesn't, you will need to change all the URLs in the embed code back to "http:".

Some embed codes contain multiple sections, with the different sections designed to be used by different web browsers. Therefore, testing an embedded item in just one or two web browsers can be insufficient to prove a change successful.

How should I embed YouTube videos?
Do not use the "YouTube" option within Insert Stuff. The YouTube option in the left column of the Insert Stuff window creates embedded items using <iframe> tags. Iframes are now blocked by browsers.

Instead, choose the "Enter Embed Code" option from the left column of the Insert Stuff window. This will provide you with a text box into which you may paste embed code from YouTube.

To get the embed code for a YouTube video:
1. On YouTube.com, open the page for the video you wish to embed.
2. On that page, under the video, click the "Share" tab.
3. On the Share tab, click "Embed". Note: By default YouTube now provides an <iframe>-based embed code. Do not use this embed code. Instead, continue on with these instructions.
4. Under the text box that contains embed code, choose size you wish to embed.
5. Also under the text box that contains embed code, check the box for "Use old embed code".
6. If the "Use HTTPS" option is available, check that box as well.

Fixes and Workarounds
Can D2L, Millersville's Information Technology department, or PASSHE fix this problem?
No. This change was implemented by browser makers. Please see the answers to the previous questions above.

As an instructor in one or more courses, how may I fix my content?
Please see the information above regarding links and embeds. If you require additional guidance as you update your content, please contact the IT Help Desk.
As someone attempting to use a page containing mixed content, are there any workarounds available to me?

Yes, each browser offers a per-page option to allow mixed content.

**Chrome**

When viewing a web page that contains mixed content, a small icon of a shield will appear at the right end of the address bar.

1. Click the shield.
2. Select "Load unsafe script".

**Firefox**

When viewing a web page that contains mixed content, a small icon of a shield will appear at the left end of the address bar.

1. Click the shield.
2. Click the "more actions" arrow.
3. Select "Disable Protection on this page".

**Internet Explorer**

When viewing a web page that contains mixed content, a popup will appear at the bottom of the page that says "Only secure content is displayed".

1. Click "Show all content".

**Safari**

Safari does not block mixed content yet.