Ideas: Updated Content Security Policy in Canvas

Posted by Jon Fenton Oct 18, 2018

We previously posted to the community a proposal for a new security policy in Canvas. In that post, we discussed the open nature of Canvas and our desire to make Canvas as flexible as possible while still implementing good security practices. Balancing security with flexibility is a task that we take very seriously, and we're constantly reviewing and improving our approach and stance. As the world changes, we make adjustments when needed. At that time, we proposed a change to Canvas that would limit custom JavaScript from running in the Files section of Canvas.

We received a lot of great feedback from the community and we appreciate everyone who contributed. After additional discussion and research, we decided that a more comprehensive solution was needed. We've been working since then on a new approach that we would like to announce today. This new project will be completed in 3 phases:

Phase 1 - Serve user files from non-application domain

- Change the files domain from instructure.com to canvas-user-content.com. This will make it clear that the files are not owned by instructure, but rather by other canvas users. Users will most often see this domain when browsing files in the Files section of Canvas, or when a file requests a user's permission.
- Change the files subdomain from clusterXX-files to one based on the associated account and course of the file being served. This change will mean that when a user grants a file permission (to access a users webcam, for example) permission will only be given for files in that course, and not for all files in that institution.

Phase 2 - Allow domain whitelisting

Allow institutions to restrict custom JavaScript (JS) that runs in their instance of Canvas based on domain. This will be enabled by an updated Content Security Policy (CSP) from Instructure. Institutions will have the option to enable the new CSP as a setting at the account level. The new CSP will be opt-in, and institutions that choose not to enable it will have no changes to their account.

- Once the updated CSP is enabled, institutions will have a whitelist of acceptable domains that they maintain. We will automatically populate the list with all of the Instructure domains.
- Individual courses can be opted out of the CSP (e.g., a computer science class requiring the ability to render student-uploaded JS).
- All custom JS that is in violation of the whitelist will be blocked from running.

Phase 3 - Surface CSP violations to administrators

- We will present administrators with a log of any requested domains that are in violation of the CSP. This will allow them to monitor violations and update their whitelist as needed.

We believe this approach will give Canvas administrators fine-grained control over the security for their institution while also preserving flexibility. Our preferred approach is to make this change as part of our standard deployment process—first to beta where it can be evaluated by admins, and then to production. We plan on each phase being deployed independently. Work has already begun and we currently estimate that we will have Phase 1 completed in Q4, 2018, Phase 2 completed in Q1, 2019, and Phase 3 completed in Q2, 2019.

As always, we would love to hear your thoughts and feedback.
496 Views

Laura Gibbs
Oct 19, 2018 7:01 PM
Really glad to hear about this whitelisting option; filing that away for future reference if needed. Thank you!

Rob Ditto *in response to* Jon Fenton *on page 2*
Oct 19, 2018 6:16 PM
Good to know, Jon.
Thanks again.

Jon Fenton *in response to* Rob Ditto *on page 2*
Oct 19, 2018 4:44 PM
Hey Rob, great question! In Canvas today files are actually not served up from vanity domains. So they'll continue to work as they always have.

Let me know if you have any additional questions!

Rob Ditto
Oct 19, 2018 4:04 PM
Jon, this all sounds great! Question: how will vanity URLs work with the separate institutional-content domain?