Authenticated persistent XSS in Liferay DXP CMS (CVE-2022-38901 and CVE-2022-38902)

Rafal Lykowski, Oct. 5, 2022

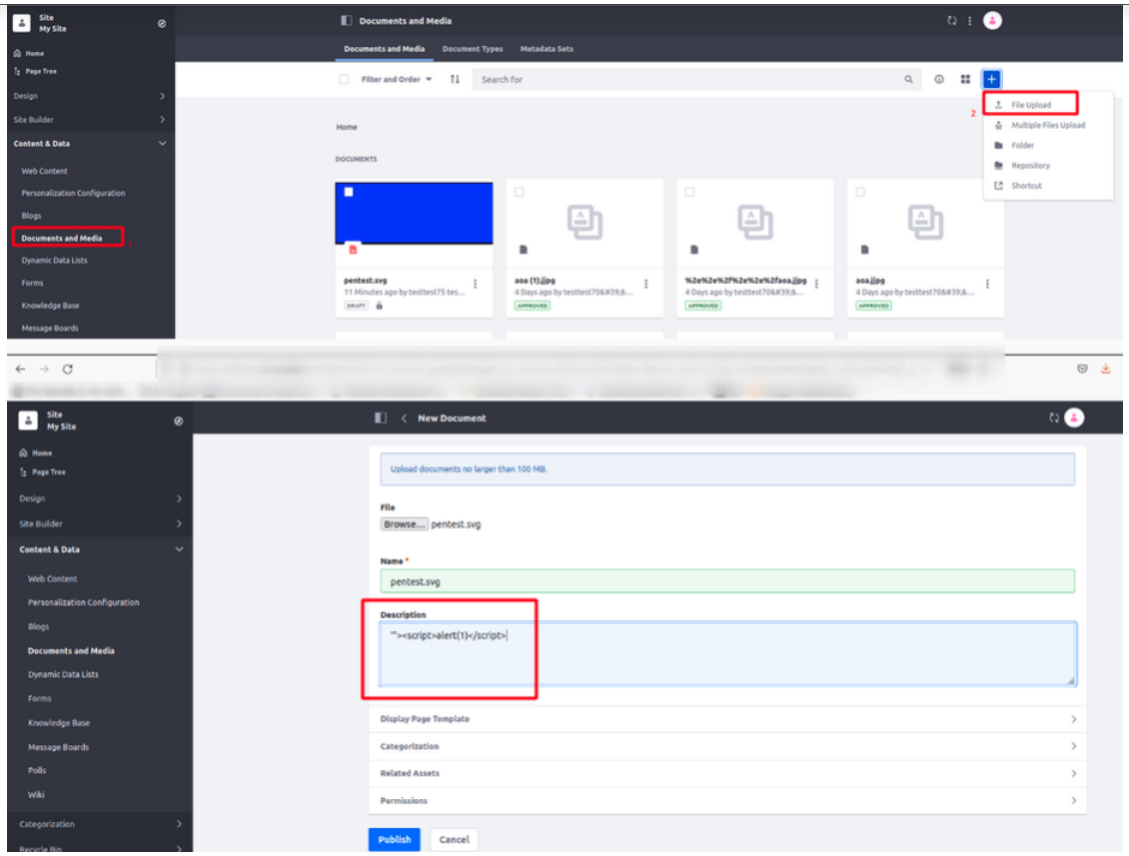
During a web application penetration test for one of our clients we identified two persistent Cross Site Scripting (XSS) vulnerabilities in the Liferay DXP content management system.

The first XSS security issue concerns the *file upload functionality* of the *Document and Media module*. Liferay is a content-management system which includes the feature to upload files that can later be used in the website. A user with privileges to upload files was able to put malicious JavaScript payload in the “Description” field of the SVG file being uploaded. As a result, any logged-in user who views the uploaded file and the description of the SVG file triggers the malicious JavaScript payload.
Affected products and versions: Liferay Portal 7.3.5 through 7.4.3.28, and Liferay DXP 7.3 before update 6, and 7.4 before update 29

This website uses cookies and other technology to customize advertising and provide you a more personalized experience. To find out more, see our Privacy Policy.

Unless you explicitly allow tracking, your data will not be collected using Google Analytics.

Allow tracking Do not track



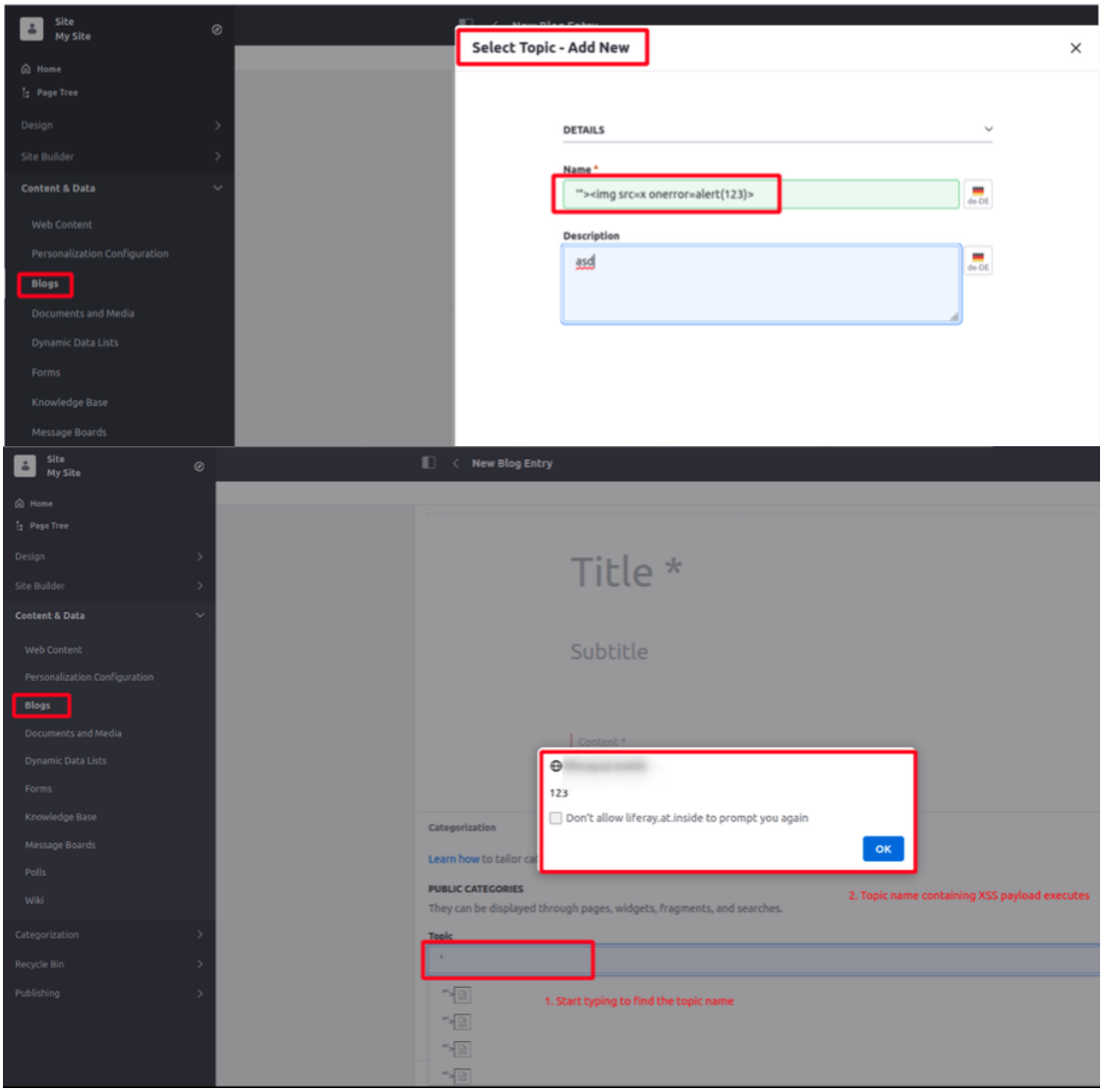
In the second case, a persistent XSS vulnerability allows authenticated remote attackers to inject arbitrary JS script payload into the *Name* text field of a category. This affected the application on a larger scale than the first mentioned vulnerability because the issue affected any asset that supports categories.

The vulnerable input field could be reached for example in the *Content & Data > Blogs module > new blog entry > categorization section*. Using this functionality it is possible to select the “topic” of the blog post. New topics can be created by giving a name and a description. It has been discovered that the *name* field was vulnerable to cross-site-scripting. As mentioned above, the result of the attack is execution of the JavaScript every time the user browses categories in order to assign one to the specified asset.

This website uses cookies and other technology to customize advertising and provide you a more personalized experience. To find out more, see our Privacy Policy.

Unless you explicitly allow tracking, your data will not be collected using Google Analytics.

Allow tracking Do not track



In both cases, a successful attack could lead to the execution of arbitrary actions by the victim user, potentially leading to privilege escalation.

Both issues were reported to the vendor Liferay as a responsible disclosure, they were assigned with the two following CVE numbers:

- CVE-2022-38901
- CVE-2022-38902

This website uses cookies and other technology to customize advertising and provide you a more personalized experience. To find out more, see our Privacy Policy.

Unless you explicitly allow tracking, your data will not be collected using Google Analytics.

Allow tracking Do not track

Product

Offensity

Resources

Blog
FAQ

About

A1 Digital
About Us

Germany

St. Martin Straße 59
81669 Munich
Germany

Austria

Lassallestraße 9
1020 Vienna
Austria

Contact
Privacy Policy
Imprint

This website uses cookies and other technology to customize advertising and provide you a more personalized experience. To find out more, see our Privacy Policy.

Unless you explicitly allow tracking, your data will not be collected using Google Analytics.

Allow tracking | Do not track