Liferay DXP Security Overview

Liferay follows the OWASP Top 10 (2013) and CWE/SANS Top 25 lists to ensure that Liferay DXP is as secure as possible. Following these recommendations protects the portal against known kinds of attacks and security vulnerabilities. For example, Liferay DXP's persistence layer is generated and maintained by the Service Builder framework which prevents SQL Injection using Hibernate and parameter based queries.

To prevent Cross Site Scripting (XSS), user-submitted values are escaped on output. To support integration features, Liferay DXP doesn't encode input. Data is stored in the original form as submitted by the user. Liferay DXP includes built-in protection against CSRF attacks, Local File Inclusion, Open Redirects, Uploading and serving files of dangerous types, Content Sniffing, Clickjacking, Path Traversal, and many other common attacks.

To stay on top, Liferay DXP also contains fixes for state-of-the-art attacks and techniques to improve product security. For example, Liferay DXP uses PBKDF2 to store passwords. Liferay DXP also contains mitigation for Quadratic Blowup XXE attack, Rosetta Flash vulnerability, Reflected File Download, and other kinds of attacks.

Authentication Overview

Liferay DXP user authentication can take place using any of a variety of prepared solutions:

- Form authentication using the Sign In Portlet with extensible adapters for checking and storing credentials (portal database, LDAP)
- Single-Sign-On (SSO) solutions - NTLM, CAS, SiteMinder, OpenSSO, OpenID, Facebook
- SAML plugin (https://www.liferay.com/marketplace/-/mp/application/15188711)
- JAAS integration with application server

Note: Although Liferay's SSO solutions are incompatible with WebDAV, they can be used in conjunction with Liferay Sync. See the Publishing Files article for more information on WebDAV and Liferay Sync.

Remote application authentication and authorization can be done using the `AuthVerifier` layer:

- Password based HTTP Basic + Digest authentication
- Token based OAuth plugin

Both user authentication and remote application authentication are extensible in Liferay DXP. Developers can create custom Login portlets and plugins, extend the default Login portlet `auth.pipeline`, create `AutoLogin` extensions for SSO, or create custom `AuthVerifier` implementations.

Authorization and Permission Checking

There are several adjustable authorization layers in place to prevent unauthorized or unsecured access to data:

- Remote IP and HTTPS transport check to limit access to Liferay DXP's Java servlets
- Extensible Access Control Policies layer to perform any portal service related authorization check
- Extensible role-based permission framework for almost any portal entity or data (stored in the portal database or elsewhere)
- Portlet Container security checks to control portlet access
- Remote IP check for portal remote API authentication methods
- Service Access Policies to control access to portal remote API

Additional Security Features

Liferay DXP supports other features, too. Liferay DXP users can be assigned to sites, teams, user groups, or organizations. Custom roles can be created, permissions can be assigned to those roles, and those roles can be applied to users. Roles are scoped to apply only with a specific context like a site, an organization, or globally. See Liferay DXP's Roles and Permissions (not yet written) documentation for more information.

Note: Liferay DXP relies on the application server for sanitizing CRLF in HTTP headers. You should, therefore, make sure this is properly configured in your application server, or you may experience false positives in reports from automatic security verification software such as Veracode. There is one exception to this for Resin, which does not have support for this feature. In this case, Liferay DXP sanitizes HTTP headers.

There are additional security plugins available from Liferay Marketplace. For example, you can find an Audit plugin for tracking user actions or an AntiSamy plugin for clearing HTML from XSS vectors.

Liferay DXP provides plenty of configuration options that allow its various security features to be fine-tuned or disabled. Here are a few examples of these kinds of configuration actions:

- Disable the Sign In portlet's *Create Account* link
- Configure Liferay DXP's HTTPS web server address
- Configure the list of allowed servers to which users can be redirected
- Configure the list of portlets that can be accessed from any page
- Configure the file types allowed to be uploaded and downloaded

Secure Development Recommendations

Liferay DXP also provides tools to fight vulnerabilities in code.

For secure development, it's important to have security-mined colleagues in your team. These individuals should consider the security aspects of each stage of the product lifecycle. It's important to start a discussion about security early in the project-planning stage so that threats to user privacy, data, and the system can be identified.

Later, during the implementation phase, developers can use the following list of APIs to address some of the most common vulnerabilities. These APIs should be used consistently across Liferay DXP.

Before releasing a product, it's important to "hack yourself first". I.e., you should conduct penetration tests or source code reviews to catch the low-hanging security-flavored fruit. External penetration testing is also an option for many companies. It's becoming a more popular and less expensive service.

Here's short list of Liferay DXP security APIs:

- `HtmlUtil` - to prevent XSS
- `HtmlUtil#escapeXPath` - prevent XPath injection
- `AuthTokenUtil#checkCSRFToken` - check CSRF tokens
- `FileUtil#createTempFile*` - prevent file system related issues
- `PortalUtil#escapeRedirect` - prevent open redirects
- `StringUtil#random*` - insecure but random enough strings
- `PwdGenerator#getPassword`, `SecureRandomUtil` – cryptographically strong pseudorandom output, optimized for performance
- `PasswordEncryptorUtil` - verification and creation of strong password hashes, configured to use PBKDF2 by default
- `DigesterUtil` - SHA-1 hashes, nowadays usable at most for file checksums

Secure Configuration and Run Recommendations

Liferay DXP is built using the "secure by default" concept in mind. Thus, Liferay DXP's default configuration is already very secure. It's not recommended to disable built-in protections or to allow all values in security white-lists. Such acts may lead to security misconfiguration and an insecure Liferay DXP deployment.

For more information about securing a Liferay DXP installation, please see https://liferay.com/security and https://portal.liferay.dev/people/community-security-team and the resources listed on those pages.

For community and CE deployments, the only way to stay secure is to use always the latest community version, which contains all previous security patches. Until a new version is released, the Community Security Team issues patches for the latest CE version via the https://portal.liferay.dev/people/community-security-team page.

« Liferay DXP Security

What is SAML? »

¿Fue útil este artículo?

Sí No

Usuarios a los que les pareció útil: 2 de 2

¿Necesitas más ayuda?

Abre un ticket

Contacta con nosotros

Pregunta en la Comunidad

Liferay University

Forma a tu equipo en los puntos esenciales del uso de Liferay con videos detallados y ejercicios prácticos diseñados para simular una formación presencial

Liferay Global Services

Aumenta tu conocimiento sobre el producto y el desarrollo gracias a expertos que te ayudarán a maximizar tu ROI

© 2023 LIFERAY INC. ALL RIGHTS RESERVED