Funcionalidades de Segurança em Aplicações do Liferay DXP

Índice

Sumário Executivo

O Liferay Digital Experience Platform (DXP) é uma plataforma de alta segurança que combina portal e tecnologia CMS de ponta com importantes benefícios de negócio, incluindo integração, segurança, flexibilidade, eficiência de custo, escalabilidade e suporte 24x7. A tecnologia Liferay é uma escolha de confiança para muitas indústrias orientadas para a segurança como governo, forças armadas, serviços financeiros e serviços de saúde. O Liferay DXP permite que empresas gerenciem usuários e acesso ao site em uma plataforma certificada que tem flexibilidade para atender aos requisitos de compliance em constante mudança.

Gerenciar um website seguro envolve mais do que fazer uma proteção frente a ameaças externas. Falhas de segurança podem aparecer em processos internos e gestão de usuários, a exemplo de quando um usuário sem experiência recebe acesso total aos controles do website, ou quando as funcionalidades de senha não possuem requisitos customizáveis, expiração regular de senhas ou outras práticas recomendadas. O Liferay DXP endereça essas áreas no nível de aplicação e é altamente customizável. Isso garante que os processos vigentes sejam adequados para as necessidades específicas do seu negócio e que operem de maneira que faça sentido para seus colaboradores.

Esse documento oferece uma visão geral das funcionalidades de segurança no nível de aplicação no Liferay DXP. Essas funcionalidades dão aos clientes Liferay confiabilidade constante no Liferay DXP.

Segurança em Transporte

O Liferay DXP possui suporte HTTPS para todas as comunicações entre navegador, clientes móveis e servidores Liferay DXP. Todas as respostas do Liferay DXP contém cabeçalhos de segurança apropriados e sinalização de cookies para evitar vazamentos na sessão de usuário.

Criptografia

O Liferay DXP usa robustos algoritmos de criptografia para uma variedade de funcionalidades, incluindo senhas. Clientes usando a autenticação nativa do Liferay DXP se beneficiarão das senhas de usuários criptografadas através de algoritmos de alongamento da chave criptográfica. Por padrão, o Liferay DXP usa o algoritmo de criptografia PBKDF2WithHmacSHA1/160/128000, o qual gera hashes de 160 bits usando 128 mil rodadas para aplicar uma segurança muito boa com trade off de performance médio. O comprimento dos hashes e o número

de rodadas podem ser aumentados para gerar ainda mais força criptográfica. Além disso, se necessário, clientes podem escolher algoritmos de criptografia alternativos.

O Liferay DXP suporta criptografia de dados em rest para seu armazenamento de ativos binários e armazenamento de banco de dados. Clientes alavancando implementações on-premise podem implementar tecnologias de terceiros nos níveis de base de dados e sistema de arquivos para encriptar dados antes do armazenamento em mídia física. Aqueles que procuram usar provedores de infraestrutura como um Serviço (IaaS), como o Amazon Web Service (AWS), podem aproveitar funcionalidades similares em S3 e RDS que protejam dados em rest.

Camadas de Segurança em Web Service

O Liferay DXP adiciona uma nova política de acesso a serviço à segurança de web service da Liferay. Políticas de acesso a serviço definem métodos de serviços ou serviços que podem ser invocados remotamente, e se aplicam apenas a serviços remotos, não a serviços locais. Políticas de acesso a serviço são particularmente úteis quando aplicações remotas, a exemplo de dispositivos móveis ou instâncias do Liferay Sync, precisam acessar serviços web do Liferay Portal. Os administradores do seu portal podem usar a política de acesso a serviço para garantir que esses dispositivos possam acionar serviços remotos apenas de listas aprovadas que podem ser modificadas em tempo de execução.

Para ajudar na compreensão de como as políticas de acesso a serviços se encaixam no panorama geral, aqui está um resumo das camadas de segurança em web service do Liferay DXP:

Camada de permissão de IP: o endereço de IP a partir do qual uma requisição de serviço web se origina precisa estar na lista branca do documento de propriedades do portal do servidor do Liferay DXP. Qualquer tentativa de invocação de web service vinda de um endereço de IP não constante na lista falhará automaticamente.

Camada de política de acesso ao serviço: o método correspondente a uma requisição de web service precisa estar em lista branca para cada política de acesso a serviço vigente. Wildcards podem ser utilizados para reduzir o número de classes de serviço e métodos que precisam estar explicitamente em lista branca.

Camada de autenticação/verificação (apenas no navegador): se uma requisição de serviço web vem de um navegador, ela precisa incluir um token de autenticação. Esse token é o valor do parâmetro de URL `p_auth`. O valor do token de autenticação é gerado pelo Liferay DXP e associado com a sessão do navegador. O parâmetro `p_auth` é fornecido automaticamente quando você requisita um web service do

Liferay Portal através da página API do JSON web service ou do Javascript usando `Liferay.Service(...)`. Se o Liferay DXP não for capaz de associar o token de autenticação do demandante com um usuário do portal, a requisição falhará.

Camada de permissão de usuário: serviços web devidamente implantados possuem checks de permissão. O usuário solicitando um web service precisa ter as permissões apropriadas no Liferay DXP para fazê-lo.

Note que políticas de acesso a serviço respeitam o sistema de permissões do Liferay DXP. Mesmo que uma política de acesso ao serviço dê acesso a um serviço remoto para um usuário, ele ainda precisará das permissões apropriadas para solicitar esse serviço.

Políticas de Senha

Clientes utilizando a autenticação nativa do Liferay DXP podem usar políticas de senha para incrementar a segurança da plataforma. Administradores podem definir requisitos de força e frequência para senhas, lockout de usuários e mais. Adicionalmente, administradores podem aplicar diferentes políticas de senha para distintos grupos de usuários. O administrador pode definir políticas de senhas customizadas ou delegar a autenticação do usuário para um servidor LDAP.

O formulário de configurações da Política de Senha contém os seguintes campos, os quais habilitam configurações específicas via prompts de caixa de seleção:

- **Nome:** exige que o administrador dê um nome para a política de senha.
- **Descrição** permite que o administrador descreva a política de senha.
- **Changeable:** determina se um usuário pode ou não mudar sua própria senha.
- **Change Required:** determina se um usuário deve ou não mudar sua senha depois do primeiro login no portal.
- **Idade mínima:** permite que o administrador escolha por quanto tempo uma senha deve ser válida antes que possa ser mudada.
- **Redefinir idade máxima do ticket:** determina por quanto tempo um link de redefinição de senha permanece válido.
- **Checagem da sintaxe** da senha permite ao administrador:
    - Definir o tamanho mínimo da senha;
    - Determinar se palavras do dicionário podem ser usadas em senhas; e
    - Requisitos detalhados como número mínimo de caracteres alfanuméricos, letras minúsculas e maiúsculas, números e símbolos.
- **Histórico de senha** permite ao administrador:
    - Manter um histórico (com um tamanho definido) de senhas; e
    - Previne que usuários mudem suas senhas por alguma já usada anteriormente.

- **Expiração de senha** permite ao administrador:
  - Escolher por quanto tempo senhas permanecem ativas antes de perderem validade; e
  - Seleciona a idade, aviso de tempo e limite de tolerância.
- **Lockout** permite que o administrador:
  - Defina a quantidade de tentativas falhas de log-in que acionem um bloqueio da conta do usuário; e
  - Escolha se um administrador é necessário para desbloquear a conta; ou
  - Determine se uma senha possa ser desbloqueada após um determinado período.

A partir da lista de políticas de senha, o administrador pode tomar as seguintes ações:

- **Editar:** permite que o administrador modifique a política de senha.
- **Permissões:** permite que o administrador define quais usuários, grupos de usuários ou papéis têm permissão para editar a política de senha.
- **Designar membros:** permite que o administrador busque e selecione usuários designados para cada política de senha.
- **Deletar:** aparece para todas as senhas adicionadas depois da política padrão.

Single Sign On (SSO)

O Liferay DXP fornece várias opções para aqueles que desejam implementar SSO. O Liferay DXP possui integração com qualquer Provedor de Identidade compatível com SAML 2.0 ao servir como um Provedor de Serviço SAML 2.0 via seu app SAML. Isso inclui Provedores de Identidade (IdP) populares como Ping Federate e Okta.

Para implementar o Liferay DXP on premise ou em uma nuvem privada, o Liferay DXP possui suporte SSO com Active Directory Federated Services (ADFS), Oracle Acess Manager, CA Siteminder, Tivoli Access Manager, Apache Shibboleth, OpenAM, Novell Identity Manager e CAS. A habilidade do Liferay DXP em servir como um Provedor de Serviços SAML 2.0 permite uma fácil integração com outros Provedores de Identidade on-premise baseados em SAML 2.0.

Clientes que não possuem um Provedor de Identidade dedicado ainda podem se beneficiar das funcionalidades SSO do Liferay DXP. O Liferay DXP possui uma integração LDAP com suporte para o Microsoft Active Directory (AD), Oracle LDAP, Novell Directory e outros provedores LDAP. Para clientes utilizando o Internet Explorer como seu navegador primário, o Liferay DXP oferece integração com NTLM.

Para clientes em busca de definição de uma estratégia de gerenciamento de identidade, o Liferay DXP pode servir como um Provedor de Identidade SAML 2.0. Isso dá mais flexibilidade para clientes que estão procurando aliar sua solução baseada no Liferay DXP com aplicações como Salesforce.com e Workday.

Gerenciamento de Direitos

Papéis e Permissões

O Liferay fornece uma plataforma central para determinação de políticas de conteúdo corporativo, incluindo quem pode editar e publicar conteúdo, arquivos, comunidades e aplicações. O Liferay usa um refinado sistema de controle de acesso baseado em papéis, que combina a utilização tanto de papéis quanto de permissões.

Permissões definem o acesso e a habilidade dada a uma determinada entidade (usuários, grupo de usuários, organizações, etc). Um papel é uma coleção de permissões que define uma função.

Papéis são muito poderosos e permitem que o administrador defina várias permissões em quaisquer combinações que desejar. Isso dá ao administrador o máximo de flexibilidade possível para construir o site com a hierarquia necessária para manter uma segurança adequada. Papéis podem ser delegados para uma entidade em diversos níveis e são o meio principal para prover acesso restrito a conteúdo. Quando um papel é delegado a um usuário, o usuário recebe permissões que foram definidas para o papel. Dessa forma, o Liferay permite que múltiplos tipos de usuários acessem uma mesma URL e acessem uma única visualização de página dependendo do papel do usuário, grupo, organização ou preferências pessoais.

Além dos papéis regulares, papéis de sites e papéis organizacionais, o Liferay também utiliza o conceito de times. Administradores de sites podem criar times dentro de um site específico. As permissões dadas para um time são definidas e aplicadas apenas dentro do site do time. As permissões definidas para papéis "regular, site e organização", em oposição, são definidas em nível de portal, ainda que aplicadas em escopos diferentes. As diferenças entre os quatro tipos de papéis podem ser descritas conforme abaixo:

- **Regular:** permissões são definidas no nível de portal e aplicadas no nível de *portal*
- **Site:** permissões são definidas no nível de portal e aplicadas a um *site* específico
- **Organização:** permissões são definidas no nível de portal e aplicadas para uma *organização* específica
- **Time:** permissões são definidas em um site específico e aplicadas neste *site* específico

Definindo Permissões em um Papel

Papéis servem como repositórios de permissões. Quando um papel é designado para um usuário, ele recebe todas as permissões definidas pelo papel. Então, para usar um papel, você precisa designar membros e definir as permissões que receberão.

Permissões no portal cobrem as atividades em diversas categorias como site, organização, localização, política de senha e mais. Isso permite que o administrador defina um papel que, por exemplo, possa criar novos sites dentro do portal. Isso permite que o administrador dê uma permissão específica para os usuários sem que eles se tornem administradores do portal como um todo.

No Liferay, as permissões se enquadram na seguinte hierarquia de categorias:

PAINEL DE CONTROLE

- Permissões Gerais
- Usuários
  - Usuários e Organizações
  - Grupos de Usuários
  - Papéis
  - Políticas de Senhas
  - Monitoramento
- Sites
  - Sites
  - Templates de Sites
  - Templates de Páginas
- Apps
  - Loja
  - Itens Comprados
  - Gerenciador de Apps
  - Configuração de Plugins
  - Gerenciamento de Licenças
- Configuração
  - Definições do Portal
  - Campos Customizados
  - Administração do Servidor
  - Instâncias do Portal

ADMINISTRAÇÃO DO SITE

- Páginas
  - Páginas do site
- Conteúdo
  - Conteúdo Recente
  - Conteúdo Web
  - Documentos e Mídia
  - Blogs
  - Quadros de Mensagens
  - Wiki
  - Listas de Dados Dinâmicas
  - Marcadores
  - Enquetes
  - Catálogo de Software
  - Tags
  - Categorias
  - Lixeira
- Usuários
  - Associação do Site
  - Times do Site
- Configuração

- Definições do Site
- Definições de Template de Site
- Templates de Display de Aplicação
- Atividade Social
- Famílias de Dispositivos Móveis
- Aplicações
- [muitos itens para serem listados]

MINHA CONTA

- Definições de Conta
- Minhas Páginas

As três categorias básicas de permissões são: Painel de Controle, Administração do Site e Minha Conta. Por padrão, qualquer usuário pode gerenciar sua conta através das permissões pertencentes à categoria Minha Conta. Administradores do site podem acessar as ferramentas de administração do site que pertencem à categoria Administração de Site. Os administradores do portal podem acessar o Painel de Controle em sua totalidade. Para papéis customizados, o administrador pode combinar permissões a partir de quantas categorias forem necessárias. O administrador pode refinar quais ações são definidas para um papel dentro de uma aplicação específica como Quadros de Mensagens.

Permissão para Delegar a Administração

Com permissões, os administradores do site também são capazes de delegar responsabilidade por tarefas administrativas a outros usuários, a exemplo da configuração de atividades sociais. Uma vez que essas permissões forem definidas para o papel escolhido, qualquer usuário com este papel poderá gerenciar a configuração do site.

OAuth

O OAuth delega a autenticação do usuário para o provedor do serviço. Um plugin ativado por OAuth usa um token para provar que está autorizado a acessar o perfil de dados do usuário e solicitar serviços autorizados. Ao implementar o OAuth em seu plugin, você obtém o melhor de dois mundos - acesso a um provedor de serviços externo e a confiança de seu usuário de que o plugin não terá acesso aos seus recursos protegidos.

Além disso, as instâncias do Liferay DXP podem atuar como provedores de serviço OAuth: você pode fornecer um meio para seus usuários utilizarem suas credenciais do portal para acessar outros serviços que possuem o OAuth configurado. Nos referimos a tais portais como Portais de Serviço Liferay. O framework OAuth permite que os administradores do Portal de Serviços Liferay especifiquem autorizações de serviço bem definidas. Uma vez autorizados, os usuários podem demandar serviços via clientes OAuth.

Auditoria de Aplicação

O app Liferay Audit torna fácil visualizar o histórico do que os usuários estão fazendo nas aplicações com o objetivo de determinar a causa de eventos que perturbem a segurança. O app armazena trilhas de auditoria em arquivos de log, uma base de dados ou ferramenta de análise de log avançado como Splunk ou Elastic ELK para que elas possam ser buscadas. Os times de segurança do cliente podem utilizar esses logs para identificar eventos e usuários que dão início a esses eventos.

Nativamente, o app Liferay Audit captura eventos para login, logout, mudança de senha, mudanças em papéis e permissões, mudanças na filiação a um grupo e mais.

Conclusão

Atualmente, todos os negócios funcionam através de software e é importante para as empresas questionar as funcionalidades de segurança em um produto. Quando decisões de compra são feitas sem atenção aos processos de segurança, empresas podem introduzir vulnerabilidades aos seus dados e sistemas críticos. Com extensivas opções para implementar processos seguros, o Liferay Digital Experience Platform é capaz de assegurar segurança de nível empresarial para todas as suas aplicações.

Seguindo em Frente

Agende uma Demo

Um membro da equipe Liferay está disponível para lhe dar uma visão aprofundada dos recursos e soluções possíveis com a versão mais recente do Liferay DXP. Centenas de organizações em serviços financeiros, serviços em saúde, governo, seguros, varejo, manufatura e outras indústrias usam Liferay. Solicite uma demo gratuita em liferay.com/request-a-demo

Global Services Liferay

Conheça como o time de Global Services da Liferay pode dar suporte ao seu projeto de Liferay DXP com uma consultoria Go Live. Entre em contato com sales-latam@liferay.com para mais informações.

A Liferay desenvolve software que permite a criação de experiências digitais na web, em dispositivos móveis e outros canais. Nossa plataforma é open source, o que a possibilita maior inovação, confiabilidade e segurança. Através de soluções de negócio e tecnologia, a empresa visa a causar um impacto positivo no mundo. Centenas de organizações do setor financeiro, de assistência médica, governo, seguros, varejo, manufatura e outras verticais de negócios usam Liferay. Para mais informações, visite: liferay.com

210528