Nome: Sérgio Medeiros Fonte

Curso: Framework Front-End com Consumo de API

O termo "Design Inseguro" refere-se a práticas de desenvolvimento de software que podem levar a vulnerabilidades de segurança. Essas práticas incluem a falta de atenção aos padrões de segurança, a falta de validação de dados e a falta de atualizações de software.

Uma forma eficaz de garantir que a segurança seja considerada desde o início é através da modelagem de ameaças, uma técnica usada para identificar ameaças e vulnerabilidades potenciais em um sistema e gerar requisitos de segurança. Ao realizar a modelagem de ameaças nas primeiras etapas do ciclo de desenvolvimento, as equipes podem antecipar e mitigar vulnerabilidades de segurança, economizando tempo e dinheiro em correções tardias e possíveis brechas de segurança.

Algumas práticas que podem ajudar de acordo com o OWASP:

1. Estabeleça e use um ciclo de vida de desenvolvimento seguro com profissionais de AppSec para ajudar a avaliar e projetar controles relacionados à segurança e privacidade;
2. Estabeleça e use bibliotecas de padrões de projeto seguros ou componentes de paved road prontos para usar;
3. Use Modelagem de Ameaças para autenticação crítica, controle de acesso, lógica de negócios e fluxos de chaves;
4. Integre a linguagem e os controles de segurança às histórias de usuários;
5. Integre verificações de plausibilidade em cada camada da sua aplicação (do front-end ao back-end);
6. Escreva testes de unidade e integração para validar se todos os fluxos críticos são resistentes ao modelo de ameaça. Compile casos de uso de sucesso e casos de uso indevido para cada camada da sua aplicação;
7. Separe as camadas de nível no sistema e nas camadas de rede, dependendo das necessidades de exposição e proteção;
8. Separe os tenants de maneira robusta por design em todas as camadas;
9. Limite o consumo de recursos por usuário ou serviço;
10. Gerenciamento adequado de identidade e acesso;
11. Evitar vazamentos de dados por meio de mensagens de erro.

Ao seguir essas práticas recomendadas, você pode minimizar o risco de design inseguro e garantir a segurança e confiabilidade. Outra boa prática é manter o software atualizado. Isso inclui atualizar o próprio software e as bibliotecas de terceiros que ele utiliza. Manter o software atualizado pode ajudar a prevenir a exploração de vulnerabilidades conhecidas.

Por fim, é importante seguir as melhores práticas de segurança, como a utilização de HTTPS para proteger a comunicação entre o navegador e o servidor, e a implementação de autenticação e autorização para proteger os recursos do site.