

6

Passos para desenvolver um software mais seguro

Grupos bem-preparados e mal-intencionados usam técnicas avançadas para explorar as fragilidades presentes em aplicações – isso com a finalidade de se beneficiar. Para proteger quem for usufruir do seu projeto, esteja um passo à frente. **Confira 6 passos importantes que você deve seguir:**

Proteja

1

É preciso proteger a base de dados da aplicação que está desenvolvendo contra códigos maliciosos e erros operacionais. Há pelo menos **nove tipos de ataques de injeção de código** e cada um pode ser prevenido de maneiras diferentes

Todos os dados recebidos de usuários ou de outros sistemas têm potencial malicioso e precisam ser validados antes de serem armazenados. Desenvolva seu software de forma segura usando **regras de validação**.

Valide

2

Exigir **senhas maiores** e, até mesmo, uma **autenticação multi-fatores** das pessoas que forem utilizar o seu software ajudará a assegurar a segurança delas. Inicialmente, elas poderão ver esses critérios como inconveniências, mas os benefícios são inúmeros.

Difículte

3

A criptografia não é mais uma opção – **é uma necessidade**. A proteção dos dados trocados entre usuário e servidor previnem o vazamento de informações dos primeiros e dificulta a revelação de brechas de segurança no software que você está desenvolvendo.

Criptografe

4

Se você **está trabalhando em uma empresa**, provavelmente já existem pessoas voltadas para a execução de testes de segurança. No entanto, você pode fortalecer essa testagem ao incluir **testes de segurança ao longo do desenvolvimento**.

Teste

5

Novas ameaças e brechas são descobertas diariamente e saber quais são elas te ajudará a desenvolver softwares mais seguros. Comece com as nossas dicas e **consuma conteúdo sobre segurança da informação** de fontes confiáveis como a [OWASP](#).

Informe-se

6

Em busca de novas oportunidades de trabalho? [Ative o nosso alerta de vagas.](#)
Siga-nos nas redes sociais

