Implementando recursos de segurança no OpenEMR

Público-Alvo: Usuários intermediários Introdução: O OpenEMR é um sistema de registro eletrônico de saúde de código aberto amplamente utilizado em clínicas e hospitais. Neste artigo, discutiremos a importância da implementação de recursos de segurança no OpenEMR e como isso pode ajudar a proteger os dados sensíveis dos pacientes.

Exemplos:

1. Configurando autenticação de dois fatores:
    - Explique como configurar a autenticação de dois fatores no OpenEMR.
    - Forneça um código/script que demonstre a configuração passo a passo.
    - Comente cada linha do código/script, explicando sua função.

2. Habilitando o registro de auditoria:
    - Mostre como habilitar o registro de auditoria no OpenEMR para rastrear todas as atividades do sistema.
    - Forneça um código/script que demonstre a configuração necessária.
    - Explique os casos de uso comuns para o registro de auditoria e como ele pode ajudar a identificar atividades suspeitas.

3. Configurando acesso seguro via HTTPS:
    - Explique como configurar o OpenEMR para permitir apenas conexões seguras via HTTPS.
    - Forneça um código/script que demonstre a configuração necessária.
    - Aborde os desafios relacionados à configuração de certificados SSL e como superá-los.

Interatividade: Compartilhe este artigo com seus colegas de trabalho e amigos interessados em segurança de dados em sistemas de registro eletrônico de saúde. A implementação de recursos de segurança no OpenEMR é fundamental para proteger as informações confidenciais dos pacientes e garantir a conformidade com as regulamentações de privacidade.