|  |
| --- |
| **Projeto Integrador – Segurança em Sistemas – Etapa 03**  **Nome:** Alan Silva Pereira David |

**Identificação e Correção de Problema de Segurança no Sistema de Bate-Papo**

**Problema Identificado: Falta de Validação e Sanitização de Entradas**

Durante o desenvolvimento do sistema de bate-papo, foi identificada uma vulnerabilidade relacionada à falta de validação e sanitização de entradas. Essa falha de segurança permite que usuários mal-intencionados insiram códigos maliciosos, como scripts JavaScript, em mensagens de bate-papo, o que pode resultar em ataques de Cross-Site Scripting (XSS) e comprometer tanto a integridade do sistema quanto a segurança dos usuários.

**Estratégia de Solução: Implementação de Validação e Sanitização de Entradas**

Para mitigar essa vulnerabilidade, a solução implementada consiste na sanitização das mensagens enviadas e recebidas pelo sistema de bate-papo. Isso envolve a criação de uma classe InputSanitizer responsável por filtrar e substituir caracteres potencialmente perigosos.

O processo de sanitização é aplicado em dois momentos críticos:

1. **No Cliente:** Antes de enviar a mensagem, o texto é sanitizado, substituindo caracteres que poderiam ser usados para injetar código malicioso.
2. **No Servidor:** Ao receber a mensagem, o servidor também realiza a sanitização, garantindo que qualquer mensagem transmitida para outros usuários esteja livre de conteúdo malicioso.

**Referências**

* OWASP Foundation. (2024). Cross Site Scripting (XSS) Prevention Cheat Sheet. Recuperado em 17 de agosto de 2024, de <https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html>
* Oracle. (2024). Java SE Documentation. Recuperado em 17 de agosto de 2024, de <https://docs.oracle.com/javase/8/docs/>