# Relatório de Segurança – Tópico 1.1

## Objetivo

Evitar que dados maliciosos ou inválidos causem falhas ou brechas de segurança no sistema.

## Ações Realizadas

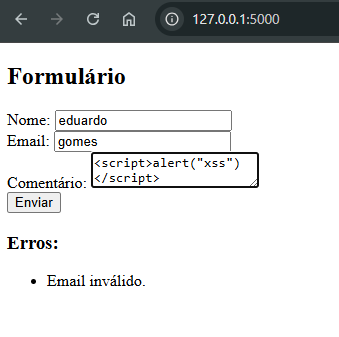
- Desenvolvido um formulário web com os campos: nome, e-mail e comentário.  
- Aplicadas as seguintes validações:  
 - Nome: mínimo de 3 caracteres.  
 - Email: formato com '@' e domínio obrigatório (regex).  
 - Comentário: limitado a 300 caracteres.  
- Utilizada a biblioteca bleach para sanitizar os campos antes do processamento, removendo qualquer HTML ou JavaScript injetado.

## Testes Realizados

|  |  |  |  |
| --- | --- | --- | --- |
| **Campo** | **Entrada Testada** | **Resultado Esperado** | **Resultado Obtido** |
| Nome | eduardo | Válido | Aceito |
| Email | gomes | Inválido | Bloqueado |
| Comentário | <script>alert("xss")</script> | Remover o código script | Sanitizado com sucesso |

## Captura de Tela

Abaixo, a imagem que mostra o formulário com o campo de comentário sanitizado e o e-mail inválido bloqueado:



## Conclusão

A sanitização e validação das entradas foram implementadas corretamente, evitando entradas malformadas ou maliciosas.  
O código bloqueia entradas inválidas e remove scripts antes de processar ou exibir os dados, conforme exigido pelas boas práticas de segurança.