Vulnerabilidades Encontradas e Possíveis Vulnerabilidades

1. Falta de Validação Adequada no Cadastro de Cursos

- **Nome do Curso:** Se o campo de nome do curso não for preenchido corretamente, o sistema deve impedir o cadastro. No entanto, se essa validação não estiver implementada ou for facilmente contornável, poderá ocorrer a inserção de cursos com nomes inválidos.
- **Descrição do Curso:** Sem uma descrição válida, os usuários não terão informações suficientes sobre o curso. A validação fraca ou ausente pode levar a descrições vazias ou inadequadas.
- **Instrutor:** A validação inadequada do nome do instrutor (permitindo números ou caracteres especiais) pode causar inconsistências no banco de dados e na apresentação dos dados.
- **URL da Imagem de Capa:** A aceitação de URLs inválidos pode resultar em imagens quebradas ou vulnerabilidades de segurança (e.g., inserção de scripts maliciosos).
- **Datas de Início e Fim:** A ausência de validação pode permitir o registro de datas inválidas (e.g., datas de fim anteriores às de início), o que compromete a integridade dos dados e a funcionalidade do sistema.
- **Número de Vagas:** Se o número de vagas não for validado corretamente, pode-se permitir valores inválidos, como números negativos ou zero, o que poderia causar problemas de alocação de recursos e lógica de negócios.

2. Falhas de Autenticação e Autorização

- **Acesso à Listagem de Cursos:** A listagem de todos os cursos sem verificar a autenticação do usuário pode expor informações sensíveis a usuários não autorizados.
- **Edição e Exclusão de Cursos:** Sem uma verificação adequada de permissões, qualquer usuário autenticado poderia potencialmente editar ou excluir cursos, levando a perda ou corrupção de dados importantes.

3. Falta de Restrições no Campo de Pesquisa

- **Busca por Nomes:** Se a busca não for restrita a um número mínimo de caracteres (como mencionado, pelo menos 3 caracteres), pode causar cargas excessivas no servidor e atrasos no desempenho.

- **Ordem dos Resultados:** A busca pode retornar resultados em uma ordem não esperada se não houver critérios de ordenação definidos, o que pode prejudicar a usabilidade e a experiência do usuário.
- **Feedback ao Usuário:** A falta de mensagens claras quando não há resultados pode confundir os usuários e diminuir a eficiência da interface.

4. Segurança da Aplicação Web

- **Injeção de Scripts (XSS):** Sem validação e sanitização adequadas dos dados inseridos pelos usuários, a aplicação pode estar vulnerável a ataques de injeção de scripts.
- **Ataques de Injeção de SQL:** Se as consultas ao banco de dados não forem parametrizadas, o sistema pode estar vulnerável a ataques de injeção de SQL, permitindo que atacantes acessem, modifiquem ou destruam dados arbitrariamente.

5. Performance e Escalabilidade

- **Tempo de Resposta:** Se a busca ou a listagem de cursos não forem otimizadas, a aplicação pode apresentar desempenho insatisfatório, especialmente com um grande número de registros.
- **Paginação Inadequada:** A falta de paginação ou paginação ineficaz pode sobrecarregar o servidor e degradar a experiência do usuário.

Possíveis Vulnerabilidades

- **Ataques de Força Bruta:** Se não houver proteção contra tentativas de login repetidas, a aplicação pode estar vulnerável a ataques de força bruta.
- **Falta de Criptografia:** Dados sensíveis, como credenciais de login e informações pessoais, podem estar vulneráveis se não forem devidamente criptografados durante o armazenamento e a transmissão.
- **Exposição de Informações Sensíveis:** Erros na manipulação de permissões e falhas de segurança podem expor informações sensíveis de funcionários e cursos para usuários não autorizados.

Mitigações Recomendadas

- **Implementação de Validações Rigorosas:** Assegurar que todos os campos de entrada de dados tenham validações robustas no lado do cliente e do servidor.

- **Revisão de Autenticação e Autorização:** Implementar um controle de acesso baseado em roles para garantir que somente usuários autorizados possam realizar ações críticas.
- **Sanitização de Entradas:** Implementar medidas de sanitização para todas as entradas de usuários para prevenir ataques de injeção de scripts e SQL.
- **Otimização de Desempenho:** Garantir que a aplicação use técnicas eficientes de paginação e busca para manter um desempenho aceitável.
- **Mensagens de Feedback Adequadas:** Prover feedback claro e útil para os usuários, especialmente em casos de erros ou ações não permitidas.
- **Proteção Contra Ataques de Força Bruta:** Implementar mecanismos de limitação de tentativas de login e captchas.
- **Criptografia de Dados Sensíveis:** Utilizar criptografia forte para proteger dados sensíveis tanto em repouso quanto em trânsito.