

Relatório de Auditoria Técnica – Sistema de Biblioteca

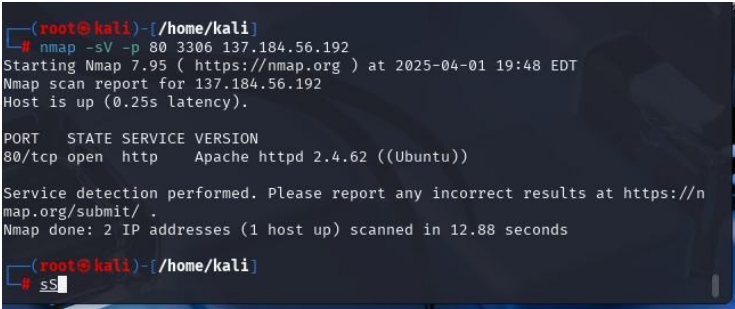
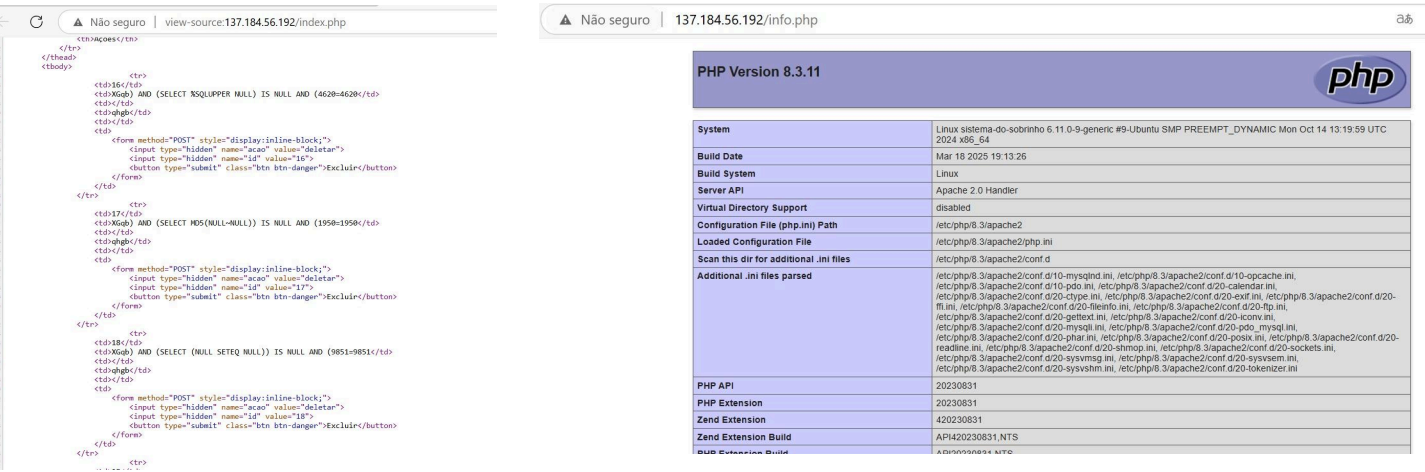
Data da Auditoria: 01/04/2025
Local da Auditoria: Sala Maker – Fatec Araras
Auditor: Pedro Beck Bratfich Penteado
Especialidade: Desenvolvimento de Software
Cliente: Seu Antonio
Data de início do Relatório: 04/04/2025

Estruturação do sistema

Após uma avaliação do programa, ficou evidente que o sistema apesar de funcional não aplica os métodos recomendados para o desenvolvimento de programas. A estrutura do código carece de organização, sem um modelo estabelecido, o que torna a correção de erros e a compreensão um desafio. Observou-se também que a aplicação junta a linguagem de estilização com a de logica tornado o código saturado e sem divisão. Notou-se, ainda, a falta de anotações e explicações, o que dificulta a interpretação por outros programadores.

Segurança

A segurança é, sem dúvida, o ponto mais crítico do sistema. As informações inseridas nos formulários (como título, autor, etc.) são passadas diretamente sem nenhum tipo de proteção ou verificação. Permitindo que qualquer um com acesso ao link da aplicação possa adicionar ou deletar informações do sistema. Isso abre uma brecha gravíssima onde uma pessoa mal-intencionada poderia, por exemplo, apagar todos os livros da biblioteca, acessar dados sigilosos. Além disso, o usuário consegue ter acesso a parte do código e as versões dos sistemas, deixando brechas no sistemas que podem ser exploradas, como tambem a pagina de informações do seu sistema.



Apesar disso não foi possível atacar o sistema e com injeções SQL pois a plataforma de hospedagem do site derruba a aplicação sempre que se tenta atacar o site, dificultando o ataque mas também a utilização da aplicação em si.

Viabilidade

Atualmente, o sistema está disponível apenas por meio de um de um link que leva para a aplicação em um endereço numérico. Para resolver isso, é necessário registrar um domínio, que é um nome personalizado e fácil de lembrar O registro de um domínio com final .com.br custa em média R\$ 40,00 por ano, e pode ser feito de forma simples pelo site oficial registro.br, onde o senhor pode pesquisar se o nome desejado está disponível e concluir a compra. Além do domínio, é preciso que o sistema esteja hospedado em um lugar onde ele fique sempre disponível na internet. Por esse motivo, recomendo a troca da hospedagem para um serviço mais simples e com suporte técnico, como os oferecidos pela Hostinger, Locaweb, KingHost ou UOLHost. Esses provedores oferecem um painel de controle amigável, atendimento em português e serviços como e-mails personalizados, backups automáticos e instalação facilitada de sistemas PHP. Os planos de hospedagem básica costumam variar entre R\$ 15 e R\$ 30 por mês, o que pode atender perfeitamente às necessidades do seu sistema de biblioteca, com mais segurança e facilidade no uso do dia a dia. Diferente da hospedada na DigitalOcean, que exige conhecimento técnico para manter o servidor funcionando, atualizar o sistema e proteger contra ataques.

Conclusão

Após a realização de testes de performance, usabilidade, segurança e pentest (teste de invasão controlado), conclui-se que, embora o sistema atual atenda minimamente ao propósito de cadastrar livros, ele apresenta sérias limitações técnicas que comprometem tanto a segurança quanto a manutenção futura. O código está desorganizado, vulnerável a ataques como injeção de SQL, e dificulta a inclusão de novos recursos, como o sistema de login/logout solicitado. Além disso, por não seguir boas práticas de desenvolvimento, o sistema se torna difícil de expandir, o que compromete sua escalabilidade a longo prazo. Dessa forma, recomenda-se reescrever totalmente a aplicação, utilizando uma estrutura moderna, segura e organizada, que permita ao sistema crescer de forma sólida e confiável. Também é recomendado que a hospedagem seja transferida para um serviço mais voltado ao público leigo, com suporte em português, painel de controle simples e atendimento ao cliente, como Hostinger, Locaweb ou KingHost. Essas mudanças tornarão o sistema mais seguro, estável e fácil de usar para o Seu Antônio e qualquer outro usuário no futuro.