SEGURANÇA DE DADOS NO NAVEGADOR: ESTRATÉGIAS E BOAS PRÁTICAS PARA PREVENÇÃO DE VAZAMENTOS DE INFORMAÇÕES SENSÍVEIS

Paulo Mário Valente Bumba[1], Leonardo M. Zonta[2], Kauã Everton Camargo[3], Alexandre José Ribeiro[4], Fabiano O. Wonzoski[5]

1. Docente do curso de graduação em Ciência da Compuação, Unoesc, Videira, SC
2. Docente do curso de graduação em Ciência da Compuação, Unoesc, Videira, SC
3. Docente do curso de graduação em Ciência da Compuação, Unoesc, Videira, SC
4. Docente do curso de graduação em Ciência da Compuação, Unoesc, Videira, SC
5. Docente do curso de graduação em Ciência da Compuação, Unoesc, Videira, SC

Autor correspondente: Paulo Mário Valente Bumba, paulomvbumba@gmail.com

Área: Ciências Exatas e Tecnológicas

Introdução: A segurança de dados no navegador é um tema crítico devido ao aumento de ataques cibernéticos e vazamentos de informações sensíveis. Diferentes métodos de armazenamento no navegador, como Cookies, LocalStorage, SessionStorage e IndexedDB, apresentam níveis variados de risco e aplicabilidade. O estudo justifica-se pela necessidade de conscientizar desenvolvedores sobre boas práticas de proteção de dados e alinhamento com diretrizes de segurança reconhecidas. **Objetivo:** Identificar os principais riscos de vazamento de dados no navegador e apresentar estratégias eficazes para mitigá-los. **Método:** Foi realizada revisão bibliográfica considerando publicações acadêmicas, documentações oficiais e diretrizes de segurança, com foco em armazenamento de dados em Cookies, LocalStorage, SessionStorage e IndexedDB. Foram analisadas vulnerabilidades, capacidade, persistência, acessibilidade e recomendações de mitigação de riscos, incluindo proteção contra XSS e CSR. **Resultados:** A análise indicou que Cookies configurados com HttpOnly, Secure e SameSite oferecem maior proteção para autenticação. LocalStorage e SessionStorage são vulneráveis a ataques XSS e inadequados para informações sensíveis. IndexedDB mostrou-se mais seguro para armazenamento de grandes volumes de dados estruturados. Estratégias como Content Security Policy e uso de HTTPS reforçam a proteção dos dados no navegador. **Conclusão:** A escolha adequada do método de armazenamento e a implementação de múltiplas camadas de proteção reduzem significativamente o risco de vazamento de dados. Cookies e IndexedDB, combinados com práticas como CSP, HTTPS e proteção contra CSRF, fortalecem a segurança das aplicações web e contribuem para a proteção de informações sensíveis dos usuários.

Palavras-chave: Segurança no navegador; Vazamento de dados; Cross site scripting; Cross site request forgery; Proteção de dados.

Agradecimentos: Agradeço a todos que contribuíram direta ou indiretamente para a realização deste trabalho. Em especial, às comunidades de segurança da informação e desenvolvedores que compartilham conhecimento abertamente, permitindo a evolução constante das boas práticas em segurança web. Reconheço também o apoio de colegas, professores e profissionais que, de diferentes formas, incentivaram a pesquisa e o aprofundamento no tema de proteção de dados no navegador