ISSN: 2319-0124
josif 2023
15ª JORNADA CIENTÍFICA E TECNOLÓGICA
12º SIMPÓSIO DE PÓS-GRADUAÇÃO
DO IFSULDEMINAS
REALIZAÇÃO INSTITUTO FEDERAL Sul de Minas Gerais
APOIO FAPEMIG CNPq

IMPLEMENTAÇÃO DE CAMADAS DE SEGURANÇA NA PLATAFORMA DIGITAL ARTE DE CADERNO

Cristhian C. BARBOSA[1]; Beatriz P. NEAIME[2]; Caroline F. MELO[3]; Douglas F. S. NUNES[4]; Giselle C. CARDOSO[5]; Jônata M. SOUSA[6]; Márcio L. BESS[7]; Rebeca D. ROSA[8]

RESUMO

A preocupação com a segurança de plataformas digitais vem crescendo a cada dia, tendo em vista que elas armazenam diversos dados críticos de pessoas ou empresas. Devido ao mundo cada vez mais conectado, métodos de proteção devem ser aplicados. A proposta deste trabalho é desenvolver e aplicar conceitos de proteção de dados, muitos recomendados pela Lei Geral de Proteção dos Dados (LGPD), na plataforma digital Arte de Caderno. Para isso foi realizada uma pesquisa bibliográfica na área de segurança da informação para delinear o desenvolvimento deste trabalho e sua documentação. É esperado que sejam desenvolvidos e aplicados métodos na plataforma, visando manter a integridade e proteção dos dados mantidos por ela.

Palavras-chave:
Segurança digital, Proteção de dados, Criptografia de senha.

1. INTRODUÇÃO

A plataforma Arte de Caderno tem como objetivo modernizar e simplificar o processo de catalogar as manifestações artísticas de alunos da rede pública do país. O projeto, que conta com apoio do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais, campus Poços de Caldas, consiste em evitar a vandalização de patrimônio público, sem coibir expressões artísticas. O projeto promove concursos artísticos e vem recebendo, ao longo dos anos, centenas de desenhos, de todas as localidades do país. As obras são submetidas a uma banca avaliadora, que classifica um quantitativo de artes que, então, seguem para votação popular. Ao final, as obras melhores classificadas são premiadas.

Os métodos de envio, recebimento, catalogação e julgamento das obras sempre foram

[1] Discente de Bacharelado em Engenharia de Computação, IFSULDEMINAS - *campus* Poços de Caldas. E-mail: cristhian.barbosa@alunos.ifsuldeminas.edu.br
[2] Bolsista de Extensão, IFSULDEMINAS - *campus* Poços de Caldas. E-mail: beatriz.neaime@alunos.ifsuldeminas.edu.br
[3] Bolsista de Extensão, IFSULDEMINAS - *campus* Poços de Caldas. E-mail: caroline.melo@alunos.ifsuldeminas.edu.br
[4] Orientador, IFSULDEMINAS - *campus* Poços de Caldas. E-mail: douglas.nunes@ifsuldeminas.edu.br
[5] Docente de Bacharelado de Engenharia de Computação, IFSULDEMINAS - *campus* Poços de Caldas. E-mail: giselle.cardoso@ifsuldeminas.edu.br
[6] Bolsista de Extensão, IFSULDEMINAS - *campus* Poços de Caldas. E-mail: jonata.martins@alunos.ifsuldeminas.edu.br
[7] Docente de Artes, IFSULDEMINAS - *campus* Poços de Caldas. E-mail: marcio.bess@ifsuldeminas.edu.br
[8] Discente de Bacharelado de Engenharia de Computação, IFSULDEMINAS - campus Poços de Caldas. E-mail: rebeca.rosa@alunos.ifsuldeminas.edu.br

realizados manualmente, com grande carga de trabalho aos envolvidos. Neste sentido, para aprimorar todos esses processos, surgiu a proposição de uma plataforma digital Arte de Caderno.

Trazendo a essência do Arte de Caderno para o meio digital, foram acrescentadas novas responsabilidades, como a segurança e cuidado com os dados dos usuários mantidos pela plataforma. De acordo com a lei geral de proteção dos dados nº 13.709, de 14 de agosto de 2018, é de responsabilidade do controlador e operador de dados garantir a segurança de informações sensíveis provenientes dos usuários.

2. FUNDAMENTAÇÃO TEÓRICA

Em um mundo conectado, a segurança da informação vem se tornando cada vez mais essencial para a garantia da privacidade e proteção dos dados de quem utiliza a internet. Os desafios aumentam a cada dia com novas tecnologias, surgindo novos métodos de burlar a segurança.

> A área de segurança de rede e de Internet consiste de medidas para desviar, prevenir, detectar e corrigir violações de segurança que envolvam a transmissão de informações. Essa é uma definição abrangente que envolve várias possibilidades.(STALLINGS, 2015, p.6)

Visando manter o acesso restrito apenas a usuários credenciados, uma medida de autenticação aplicada diretamente à plataforma seria a autenticação de dois fatores, via SMS (serviço de mensagens) ou e-mail como medida de proteção. Conforme recomendado no guia orientativo do Governo Federal, os usuários do sistema terão nível mínimo de acesso necessário para realizar suas atividades.

> A premissa que deve ser aplicada é a do princípio do menos privilégio (need to know), ou seja, os usuários de um sistema terão o menor nível de acesso necessário para a realização de suas atividades. Funções de alto nível, tais como as de administrador de sistema, devem ser restringidas apenas àqueles funcionários que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade (ANPD, 2021).

Outra abordagem de segurança bastante comum para a proteção de senhas é por meio da tecnologia *hash*, um algoritmo que mapeia dados de qualquer tamanho para dados de tamanho fixo. Com ela, as senhas dos usuários nunca são armazenadas no modo texto aberto, ou seja dados mantidos sem nenhuma forma de criptografia, mas sim uma sequência de caracteres ininteligível gerados por essa tecnologia. Essa abordagem agrega uma camada de proteção, tendo em vista que, se o banco de dados por algum motivo for violado e seu conteúdo exposto na internet, os criminosos terão dificuldades em conseguir acesso aos dados que em algum momento foram disponibilizados na internet sem autorização ou consentimento do proprietário. Para desenvolver e aplicar as medidas necessárias vistas, deve-se partir para a codificação no *backend,* o qual previamente foi desenvolvido em Node.js, uma plataforma de código aberto que irá permitir que o código em JavaScript seja executado em várias plataformas e Express. Visando testar a confiabilidade do sistema, é necessário passar a plataforma por ferramentas de pentest que irão

avaliar a segurança simulando um ataque malicioso e verificar a efetividade das barreiras de proteção e configurações de rede.

3. MATERIAL E MÉTODOS

Foi verificada a relevância da aplicação do tema no atual mundo conectado, e, para isso, foram realizadas pesquisas na literatura visando compreender melhor a aplicação em diversas estruturas digitais que comportam dados críticos. Diversas plataformas estão operando de forma desprotegida ou até se omitindo dessa responsabilidade, que é zelar por esses dados, mostrando brechas na segurança e proteção das informações, promovendo preocupações significativas quanto à privacidade, integridade e confiabilidade das informações armazenadas através do meio digital. Nesse contexto, surge a necessidade da discussão e aplicação de soluções para mitigar ameaças à plataforma digital Arte de Caderno. Visto isso as hipóteses levantadas foram:

1. Aplicar técnicas predefinidas de criptografia utilizando a tecnologia *hash*.
2. Tratamento contra injeções sql no banco de dados.
3. Verificação de login em duas etapas.
4. Token JWT para navegação na plataforma.
5. Configurações no *firewall*, e recomendações contra engenharia social e políticas de senhas fortes.

4. RESULTADOS E DISCUSSÃO

Com os trabalhos iniciados, tornou-se necessária a realização da criptografia das senhas no banco de dados, utilizando a biblioteca *crypto* do NodeJS. A técnica empregada foi o *hash* com sal (figura 1), a qual envolve a geração de um código aleatório para ser usado na criptografia da senha fornecida pelo usuário. Logo após a criptografia da senha, esta é armazenada no banco de dados juntamente com o código gerado, separados pelo caractere dois-pontos (:).

“password”:"787ed87fb7db6e2f7fff263c9583c47d:c9ee1524ff941421d2826042da5b3808db45a961c257040f2da3779a62903e6a02a19e9e157a1fb98e389ddf5b4ae507561db999bf417d3d0bd3d389c27af52b"

Após a realização da criptografia e o armazenamento da senha no banco de dados, será necessário efetuar o login com a senha no novo padrão hexadecimal, juntamente com o código aleatório.

Para validar um login bem-sucedido, tornou-se necessário comparar a senha armazenada no banco, separando-a do código aleatório, e verificar se a senha fornecida durante a tentativa de login corresponde à mesma sequência de caracteres cadastrada na base de dados.

Foi empregado o *token JWT*, utilizando a biblioteca *jsonwebtoken* do NodeJS. O referido

token possui uma validade de 1 dia; após esse período, o usuário precisará fazer o login novamente para obter outro token válido. Esse processo é aplicado nas rotas de navegação da plataforma, o que demanda que o usuário esteja sempre em posse de um código válido para poder navegar.

Figura 1 - Função para criptografia das senhas

```
import { scryptSync, randomBytes, timingSafeEqual } from 'crypto'

async function createHashWithSalt(password){
    const salt = randomBytes(16).toString('hex');
    const passwordHash = scryptSync(password,salt,64).toString('hex');

    return `${salt}:${passwordHash}`;
}

export default createHashWithSalt;
```

5. CONCLUSÃO

A implementação destes métodos contribuiu efetivamente para a melhoria da segurança dos dados que a plataforma possuia e virá a possuir. As recomendações para os futuros administradores surtirão efeito ao manterem a página sempre com acesso restrito e ao cuidarem dos dados críticos, mantendo os princípios das recomendações da Lei Geral de Proteção de Dados (LGPD).

Para futuras melhorias, a autenticação de dois fatores será implementada, adicionando, dessa forma, uma nova camada de segurança. Posteriormente, opções de login com Google e Facebook serão implementadas, assim como serão fornecidas recomendações aos usuários no momento da criação de senhas.

REFERÊNCIAS

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas.6ª ed. São Paulo: Pearson Education do Brasil, 2015.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018.

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. 1. ed. Brasília, DF: ANPD, 2021.