

# Estudo Comparativo de Mecanismos de Segurança Aplicados a Autenticação e Autorização em Sistemas Web

Rafael Strack<sup>1</sup>, Adriano Ferrasa<sup>1</sup>

<sup>1</sup>Departamento de Informática – Universidade Estadual de Ponta Grossa (UEPG)  
84.030-900 – Ponta Grossa – PR – Brasil

rafa\_strack@hotmail.com, ferrasa@uepg.br

**Abstract.** *This article presents a comparative study of authentication and authorization mechanisms in web systems, aiming to provide an in-depth analysis of the available options and their characteristics. The study describes the most commonly used methods such as passwords, tokens, multifactor authentication, and OAuth, analyzing their advantages and disadvantages. Additionally, sequence diagrams are provided to illustrate the usage flow of each method. Finally, a comparison of the studied methods is conducted, evaluating their effectiveness in terms of security. Proper understanding of these mechanisms is crucial to ensure the security of web systems and guide the correct choice in future projects.*

**Resumo.** *Este artigo apresenta um estudo comparativo dos mecanismos de autenticação e autorização em sistemas web, visando fornecer uma análise aprofundada das opções disponíveis e suas características. O estudo descreve os métodos mais utilizados, como senhas, tokens, autenticação multifator e OAuth, analisando suas vantagens e desvantagens. Além disso, são apresentados diagramas de sequência para ilustrar o fluxo de utilização de cada método. Ao final, é realizada uma comparação dos métodos estudados, avaliando sua eficácia em termos de segurança. A compreensão adequada desses mecanismos é fundamental para garantir a segurança dos sistemas web e orientar a escolha correta em projetos futuros.*

## 1. Introdução

Com a expansão da internet, os sistemas web assumiram um papel crucial no cotidiano de bilhões de pessoas em todo o mundo. Desde o uso de redes sociais até o gerenciamento de negócios online, essas ferramentas se tornaram indispensáveis para diversas atividades. Tanto pessoas físicas quanto empresas dependem desses sistemas para garantir a eficiência e produtividade de suas operações. No entanto, a segurança desses sistemas é uma preocupação constante para desenvolvedores e usuários, pois há uma série de ameaças e vulnerabilidades que podem comprometer sua integridade.

A fundação OWASP (Open Worldwide Application Security Project) atualiza regularmente um relatório chamado OWASP Top 10, onde são descritos os 10 riscos de segurança mais críticos em sistemas web. Na última edição, realizada em 2021, a categoria que ficou em primeira colocação foi a quebra de controle de acesso. Em sétima colocação, ficou a categoria de falhas de identificação e autenticação [OWASP 2021]. Esses problemas são diretamente relacionados aos processos de autenticação e autorização de usuários, os quais são essenciais para garantir a proteção adequada dos sistemas.

De modo geral, a autenticação é o processo de validação de usuários, enquanto a autorização é o método que fornece as permissões de acesso corretas aos recursos para usuários previamente autenticados [Tumin and Encheva 2012]. Atualmente, existem diversos mecanismos de autenticação e autorização de usuários disponíveis, como senhas, tokens, autenticação multifator, OAuth, OpenID, entre outros. Cada um desses mecanismos apresenta características distintas, pontos positivos e negativos, sendo fundamental garantir a correta implementação dos mecanismos escolhidos, de forma a assegurar a efetividade da segurança dos sistemas web.

Diante desse contexto, o presente trabalho tem como objetivo realizar um estudo comparativo dos diferentes mecanismos de autenticação e autorização, com o propósito de fornecer uma análise aprofundada que auxilie na escolha adequada desses mecanismos em projetos de sistemas web. O estudo visa oferecer uma compreensão ampla das características, pontos fortes e limitações de cada mecanismo, permitindo a seleção correta e a implementação eficiente das medidas de segurança necessárias.

## **2. Autenticação e Autorização**

### **2.1. HTTP Basic Authentication**

### **2.2. HTTP Digest Authentication**

## **Referências**

- Chapman, N. and Chapman, J. (2012). *Authentication and Authorization on the Web*. MacAvon Media, Escócia, Reino Unido.
- OWASP (2021). Owasp top 10:2021. <https://owasp.org/Top10/>. Acesso em: 26 abr. 2023.
- Tumin, S. and Encheva, S. (2012). A closer look at authentication and authorization mechanisms for web-based applications. In *RECENT RESEARCHES in APPLIED INFORMATION SCIENCE*, pages 100–105, Faro, Portugal.