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

Rafael Strack[1], **Adriano Ferrasa**[1]

[1]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

Na maioria dos sistemas web, é necessário realizar um controle de acesso, para que somente certos usuários possam acessar recursos protegidos. Para isso, o mecanismo de controle de acesso depende de dois processos relacionados: a autenticação e a autorização [Sullivan and Liu 2011].

A autenticação pode ser definida como o processo de confirmação de identidade. Em sistemas web, devido a falta de conhecimento do mundo real, este processo pode não ser simples [Chapman and Chapman 2012]. Existem três grupos de fatores amplamente utilizados para confirmar a identidade de um usuário: algo que o usuário sabe, algo que o usuário é e algo que o usuário possui. No primeiro grupo, inclui-se as senhas, PINs (*Personal Identification Number*) e frases secretas. No segundo grupo, inclui-se certificados digitais, *smart cards* e *tokens* de segurança. O terceiro grupo inclui técnicas biométricas, como como impressões digitais, reconhecimento facial ou de voz, entre outras [Sullivan and Liu 2011].

A autorização é o processo pelo qual o sistema decide se um usuário previamente autenticado possui permissão para acessar um recurso ou executar uma determinada ação [Spilca 2020].

[...]

2.1. HTTP Basic Authentication

A HTTP (*Hypertext Transfer Protocol*) Basic Authentication foi definida na especificação RFC 2617 [IETF 1999] e atualizada na RFC 7617 [IETF 2015]. Neste tipo de autenticação, o servidor web recusa uma transação caso o cliente não esteja autenticado, desafiando-o para obter um nome de usuário e senha válidos. Este desafio de autenticação é iniciado retornando o status HTTP 401 (não autorizado) e especificando o domínio de segurança (*security realm*) a ser acessado, com o cabeçalho WWW-Authenticate. Ao receber o desafio, o navegador abre uma caixa de diálogo para que o usuário insira as credenciais para acesso ao domínio. O navegador então junta as informações de usuário e senha, colocando dois pontos entre eles, e os codifica usando o método de codificação base-64. Estas credenciais codificadas são colocadas no cabeçalho Authorization, e então

a requisição é enviada para o servidor, que fará a validação das credenciais e, caso validadas, retorna-se o status HTTP 200 (OK), e as informações da página web requisitada [Gourley and Totty 2002]. Um exemplo do funcionamento deste método de autenticação é mostrado na Figura 1.

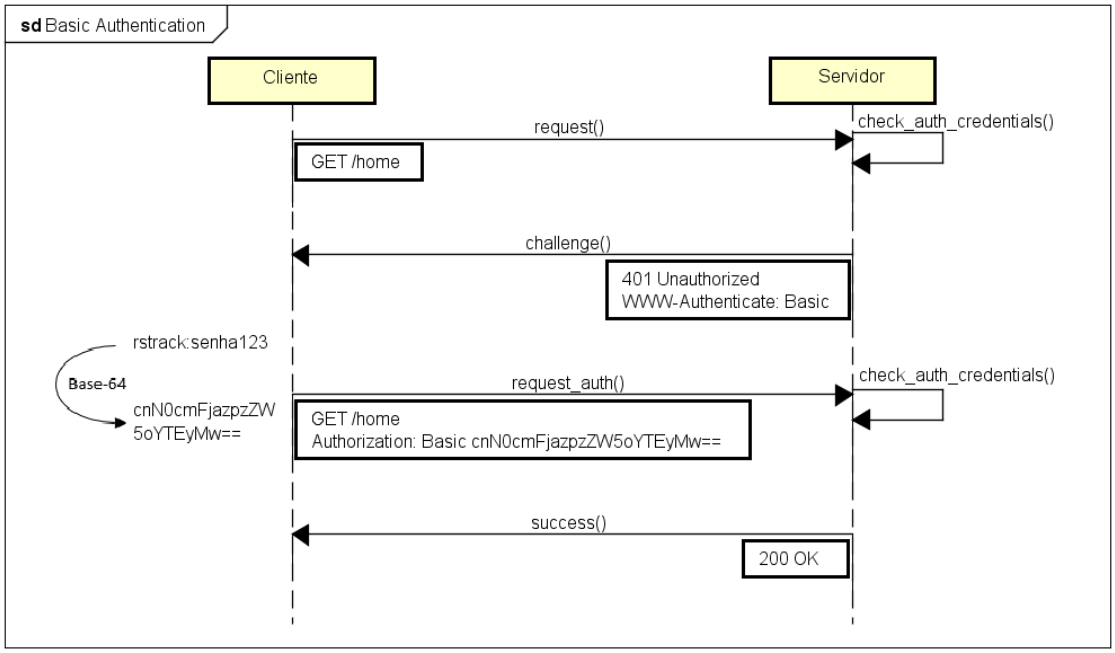

Figura 1. Exemplo de HTTP Basic Authentication

A diretiva de domínio (*realm*) utilizada na Basic Authentication define os espaços de proteção do sistema web. Esses domínios permitem que os recursos protegidos sejam particionados, cada um com seu próprio esquema de autenticação e/ou autorização [IETF 1999].

A HTTP Basic Authentication é simples e de fácil implementação, porém não possui segurança. As credenciais do usuário podem ser facilmente decodificadas, visto que a codificação base64 é facilmente reversível, podendo ser realizada em poucos segundos. Também é possível realizar ataques de reprodução, visto que terceiros podem capturar pacotes e replicá-los, mesmo que codificados, podendo obter acesso ao sistema. Este tipo de autenticação não possui proteção contra *proxies* ou *middlewares*, que podem facilmente modificar o corpo da mensagem, e também são vulneráveis a servidores falsificados, que se passam por outros para realizar o roubo de credenciais. Além Estes pontos negativos a autenticação básica não possui encerramento de sessão, fazendo com que o usuário permaneça conectado até o fechamento do navegador.

2.2. HTTP Digest Authentication

2.3. Session-Based Authentication

2.4. Token-Based Authentication

2.5. OAuth e OAuth2

2.6. OpenID

3. Materiais e Métodos

4. Resultados e Discussão

5. Conclusão

Referências

Chapman, N. and Chapman, J. (2012). *Authentication and Authorization on the Web*. MacAvon Media, Escócia, Reino Unido.

Gourley, D. and Totty, B. (2002). *HTTP: The Definitive Guide*. O'Reilly Media, Califórnia, Estados Unidos.

IETF (1999). Rfc 2617. `https://www.rfc-editor.org/rfc/rfc2617.txt`. Acesso em: 09 jun. 2023.

IETF (2015). Rfc 7617. `https://www.rfc-editor.org/rfc/rfc7617.txt`. Acesso em: 09 jun. 2023.

OWASP (2021). Owasp top 10:2021. `https://owasp.org/Top10/`. Acesso em: 26 abr. 2023.

Spilca, L. (2020). *Spring Security in Action*. Manning Publications, Nova Iorque, Estados Unidos.

Sullivan, B. and Liu, V. (2011). *Web Application Security, A Beginner's Guide*. McGraw-Hill, Estados Unidos.

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.