PROGRAMAÇÃO WEB
Atividade 2

Prof.º Denilce de Almeida Oliveira Veloso
Disciplina: Programação Web

Kauã Granadier Costa 0030482411005

Sorocaba
Agosto/2025

SUMÁRIO

1. INTRODUÇÃO

A segurança em ambientes digitais tornou-se um dos pilares fundamentais para a confiabilidade das aplicações web. Com o crescimento do número de usuários e a diversidade de serviços disponíveis, surgiram protocolos e padrões voltados à proteção de dados e ao controle de acessos, como o OAuth e o JWT, que desempenham papéis centrais no processo de autenticação e autorização. Além disso, compreender e mitigar ameaças como o Cross-Site Scripting (XSS) e o Cross-Site Request Forgery (CSRF) é essencial para o desenvolvimento seguro de sistemas. Este trabalho aborda os conceitos e a importância dessas tecnologias, bem como as medidas de proteção associadas, destacando sua relevância para o fortalecimento da segurança da informação no contexto da programação web.

2. PROTEÇÃO E SEGURANÇA

A proteção e a segurança, tanto das redes quanto aplicações em geral, vêm ganhando grande destaque e importância com o fluxo massivo de novos usuários adquiridos ao longo dos anos. Assim, diversos protocolos, ferramentas e métodos de conduta surgiram para auxiliar na construção e manutenção da segurança nas redes e aplicativos, a seguir alguns destes serão descritos.

2.2. OAuth

A OpenAuth (OAuth), ou “Autorização Aberta” em português, pode ser descrita como um protocolo de autorização que possibilita os sites e aplicativos requisitarem informações do usuário a outras aplicações sem que a proteção de dados do usuário seja comprometida. Um bom exemplo disso é quando ao tentar criar uma conta em um site, muitas vezes em vez do usuário ser limitado a criar uma conta passo a passo (nome, e-mail, senha etc.) a opção de simplesmente criar uma conta utilizando as credenciais de sua conta Google ou Meta estão disponíveis, isso é a Autenticação Aberta.

A OAuth funciona utilizando tokens de autorização para comprovar a identidade do usuário para o fornecedor da aplicação. Deste modo, as informações cruciais da conta ficam protegidas, o software poderá utilizar suas informações dentro dos limites de permissão concedidos, no entanto não terá acesso aos dados de login.

2.3. JWT

O JWT (JSON Web Token) é um padrão de autenticação utilizado na web, permite uma transmissão de dados segura e compacta entre duas partes. Assim, esta estrutura é constituída por três partes: Header, Payload e Signature; Em suma, pode resumida em tipo do token (Header), local de armazenamento dos dados (Payload) e uma chave codificada do para o token (Signature), todas essas informações serão utilizadas em ambientes HTML e protocolos HTTP.

2.4. Segurança contra XSS/CSRF

XSS (Cross-Site Scripting) e CSRF (Cross-Site Request Forgery) são tipos de ataques cibernéticos que visam aplicações web. “O XSS age numa página web, podendo alterar o comportamento de uma aplicação sem que o usuário ou desenvolvedor perceba. Esta prática dá ao atacante a possibilidade de ler todo o conteúdo da página e de mandar informações para um servidor controlado pelo atacante, violando assim, o conceito de privacidade de uma aplicação.” (GONÇALVES, 2021). Já o CSRF é quando um atacante engana o usuário logado para executar ações sem o seu consentimento, explorando a sessão/autenticação ativa.

Para que a proteção contra XSS e CSRF ocorra, ações tanto no backend quanto no frontend devem ser tomadas. Assim, para o XSS, entrada de dados devem ser tratadas, restrições de execução de scripts e validação dos campos de dados devem ser considerados. E, para o CSRF, testes para confirmar a autenticidade do usuário precisam ser postos à prática, confirmações adicionais de usuário, como PIN e autenticação de dois fatores, tokens anti-CSRF, configurações de cookies e verificações de origem da requisição são alguns exemplos de medidas cabíveis para a segurança contra CSRF.

3. CONCLUSÃO

Diante do cenário atual, em que a segurança digital se mostra cada vez mais desafiadora, torna-se indispensável a adoção de protocolos e práticas eficazes para proteger dados e usuários. A OAuth e o JWT surgem como ferramentas relevantes para garantir autenticação e autorização seguras, permitindo maior controle e confiabilidade nas interações entre sistemas. Por outro lado, ataques como XSS e

CSRF demonstram a necessidade de medidas adicionais de prevenção, tanto no backend quanto no frontend, assegurando que a experiência do usuário não seja comprometida por vulnerabilidades exploráveis. Assim, compreender esses mecanismos e aplicá-los de forma consistente contribui não apenas para a proteção das aplicações, mas também para a consolidação de um ambiente digital mais confiável e robusto.

REFERÊNCIAS

AUTH0. *Introdução ao OAuth 2*. Auth0, 2025. Disponível em: https://auth0.com/pt/intro-to-iam/what-is-oauth-2. Acesso em: 18 ago. 2025

ARAKAKI, Eduardo. *Pesquisa e comparação de mecanismos de autenticação e autorização: estudo de caso do OAuth*. Monografia (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília (UNIVEM), Marília, 2015. Disponível em: https://aberto.univem.edu.br/handle/11077/1398. Acesso em: 18 ago. 2025

GONÇALVES, Lucas Matheus; CAMENAR, Letícia Maria de Oliveira. *Exploração de vulnerabilidades Cross-Site Scripting: uma análise das principais técnicas de ataques XSS*. In: LATINOWARE – Congresso Latino-Americano de Software Livre e Tecnologias Abertas, 2023. Disponível em: https://sol.sbc.org.br/index.php/latinoware/article/view/19909/19737. Acesso em: 18 ago. 2025

JWT.IO. *Introduction to JSON Web Tokens*. jwt.io, 2025. Disponível em: https://jwt.io/introduction. Acesso em: 18 ago. 2025

VARONIS. *O que é o OAuth? Definição e como funciona*. Varonis, 2022. Disponível em: https://www.varonis.com/pt-br/blog/what-is-oauth. Acesso em: 18 ago. 2025.

SEGUINS, Neilton. *O que é JSON Web Tokens?* Alura, 2022. Disponível em: https://www.alura.com.br/artigos/o-que-e-json-web-tokens. Acesso em: 18 ago. 2025