XIV ENCONTRO ANUAL DE TECNOLOGIA DA INFORMAÇÃO
ANAIS DO XIV ENCONTRO ANUAL DE TECNOLOGIA DA INFORMAÇÃO - EATI
| ANO 12, N. 1 | NOVEMBRO / 2023

APIs na Era Digital: Um Enfoque na Segurança e Conscientização

Gabriel Henrique Lenz[1] Roberto Franciscatto[2]

[1] Sistemas de Informação – Universidade Federal de Santa Maria (UFSM)
[2] Departamento de Tecnologia da Informação – Universidade Federal de Santa Maria (UFSM)

gabriel.lenz@acad.ufsm.br
roberto.franciscatto@ufsm.br

Abstract. *As the increasing use of information systems that provide critical processes and data continues, the security risk associated with them is gaining more prominence. APIs (Application Programming Interfaces) have become a significant target for malicious actors. To protect critical data and systems, it is essential to understand and mitigate the risks associated with APIs. This work aims to implement an educational and interactive website, focusing on explaining essential concepts related to APIs in a clear and accessible manner. Topics covered include types of APIs, vulnerabilities, security standards, how a user can exploit flaws, and appropriate prevention methods.*

Resumo. *Assim como a crescente utilização de sistemas de informação que disponibilizam de processos e dados críticos, o risco à sua segurança vem tomando cada vez mais destaque. Um grande alvo de agentes mal intencionados vem sendo as APIs (Application Programming Interface). Para proteger dados e sistemas críticos, é fundamental entender e mitigar os riscos associados às APIs. Este trabalho objetiva realizar a implementação de um website educativo e interativo, se dedicando em explicar de forma clara e acessível os conceitos essenciais relacionados às APIs, como tipos de APIs, vulnerabilidades, padrões de segurança, como um usuário pode se aproveitar de falhas e formas de prevenção adequadas.*

1. Introdução

Atualmente a utilização de *APIs* tem grande influência em como sistemas são estruturados. Para isso, é necessário seguir padrões e tomar cuidados para que a aplicação seja o menos vulnerável possível. Esse projeto objetiva explorar os principais e mais importantes conceitos relacionados às *APIs*, com foco na necessidade de garantir segurança à aplicação.Voltado para a conscientização e educação sobre os riscos de seguranças em *APIs*, o presente artigo detalha o processo que será realizado na construção de um website educativo e interativo, mostrando ao usuário os principais tópicos sobre *APIs* com enfoque na sua segurança. A seção 2 fornece detalhes aprofundados sobre o que será abordado no trabalho. A seção 3 conta com detalhes como serão os conteúdos disponibilizados no WebSite. A seção 4 aprofunda sobre os principais riscos em *APIs* listados pela OWASP (Open Worldwide Application Security Project). A seção 5 apresenta a solução da proposta e tecnologias que serão utilizadas para isso. Por fim, a seção 6 aborda os resultados parciais até o presente momento.

2. Referencial teórico e tecnologias

O projeto visa explorar os principais conceitos relacionados às *APIs*, bem como vulnerabilidades que podem afetá-las, levando em consideração o top 10 riscos de segurança de *APIs* segundo a OWASP, que consiste em ser um projeto aberto de segurança em aplicações web [OWASP 2023]. Outros conceitos que serão destacados se referem sobre o que são *APIs*, seus tipos e benefícios, vulnerabilidades em *APIs*, padrões de segurança em *APIs* e a segurança de dados e privacidade.

APIs podem ser definidas como um conjunto de regras e protocolos que permitem que diferentes sistemas de software se comuniquem e interajam uns com os outros. Podem ser utilizadas de várias maneiras, como na integração de sistemas diferentes, onde um aplicativo web se comunica com uma *API* de serviço de pagamento online para consultar dados ou realizar procedimentos. As *APIs* podem ser classificadas em diferentes tipos, como *API* web, que são baseadas em padrões web, *APIs* de biblioteca que podem ser utilizadas por desenvolvedores para acessar recursos específicos. *APIs* de serviços web, permitindo a comunicação de sistemas diferentes, como sistemas operacionais, bancos de dados ou provedores de serviços em nuvem [TheFemTech 2023].

Existe uma crescente importância das *APIs* na arquitetura de sistemas de informação, e com ela a necessidade de garantir cada vez mais a sua segurança. Com o aumento de ameaças cibernéticas, é fundamental entender e mitigar os riscos associados às *APIs* para proteger dados e sistemas críticos. Para se proteger é necessário saber os principais riscos de segurança. O projeto se concentra nas principais vulnerabilidades identificadas na lista "OWASP Top 10 *API* Security Risks - 2023", que inclui ameaças como autorização em nível de objeto quebrado, autenticação quebrada, autorização de nível de propriedade de objeto quebrado, entre outros [OWASP 2023].

Para se proteger ainda mais desses riscos de segurança é crucial o conhecimento de padrões de segurança em *APIs*. Serão exploradas boas práticas de design de *APIs* seguras, métodos de autenticação e autorização como o OAuth 2.0, que desempenha um papel vital na autenticação, autorização e controle de acesso em *APIs* [Arakaki 2015].

3. Conteúdo e Recursos Educativos

O conteúdo presente no site contemplará os principais tópicos relacionados às *APIs*, fornecendo informações detalhadas, práticas e relevantes. Os conteúdos serão catalogados em diferentes abas, abordando temas gerais como o que são *APIs*, seus principais tipos, como funcionam, o que os distinguem e seus pontos positivos e negativos.

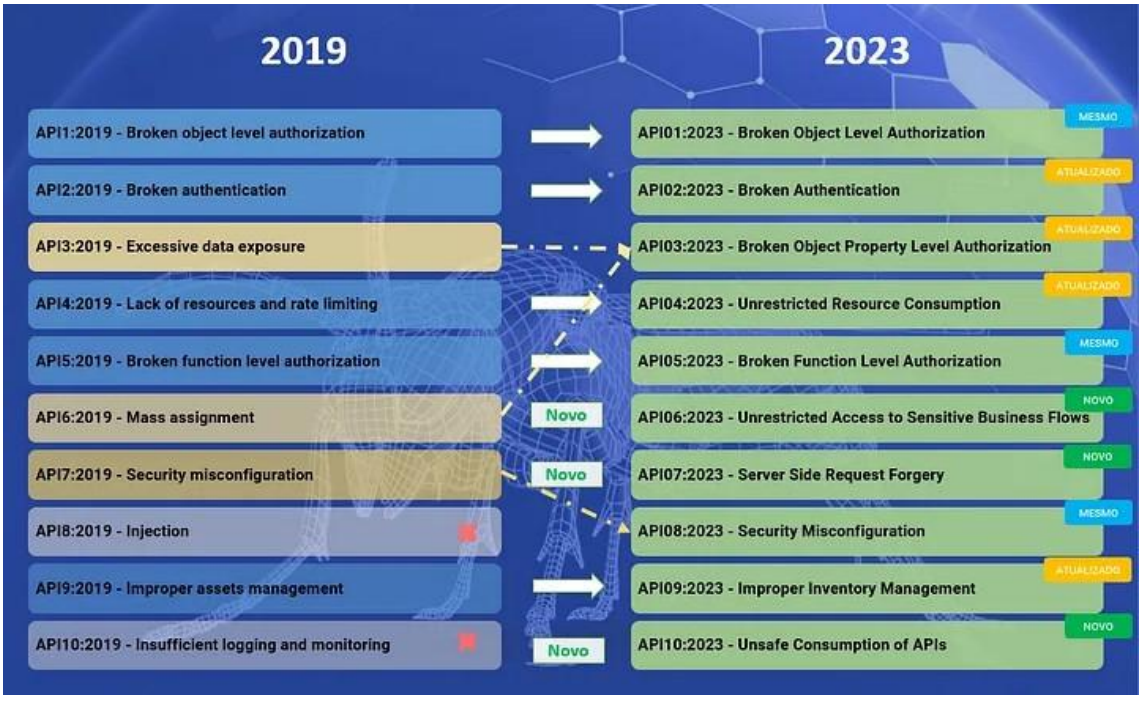
Para abordar as vulnerabilidades em *APIS* será utilizado como base o Top 10 riscos de segurança a *APIs* segundo a OWASP, onde o usuário poderá explorar cada um deles de forma detalhada e interativa, contando com um passo a passo de como um agente malicioso se aproveita de brechas deixadas por quem desenvolveu a aplicação e formas de prevenir que isso ocorra, demonstrando as falhas presentes no código e como é possível realizar uma aplicação mais segura. Serão apresentadas ao usuário boas práticas de design para garantir a segurança das *APIs*, com foco em tecnologias

conhecidas como o OAuth 2.0 e JSON Web Tokens (JWT), que desempenham papéis cruciais na autenticação, autorização e no controle de acesso em *APIs*.

4. Entendendo o OWASP Top 10 riscos de segurança à APIs

A OWASP é uma ferramenta consolidada entre desenvolvedores e equipes de segurança para aprender e se prevenir de riscos à segurança em aplicações Web. Devido ao aumento constante no consumo de *APIs* a OWASP aderiu em 2019 a criação de uma lista contendo as 10 principais vulnerabilidades em *APIs*. É possível ver na figura 1 os riscos presentes na sua primeira versão e na segunda e mais atual.

Figura 1. Mudanças OWASP API Security Top 10 2023



Fonte: Silva 2023 [Silva 2023]

A segunda versão, lançada em 2023, conta com algumas mudanças, removendo e introduzindo riscos para garantir que sejam abordadas problemáticas mais específicas sobre *APIs*. Por exemplo, o risco de *Injection*, ou injeção, ainda que seja um risco pertinente em *APIs* muito explorado, porém, é um risco genérico, e não se comporta de forma diferente em *APIs*, por esse motivo acabou sendo removido para dar espaço a outro risco de segurança que mereça atenção especial em *APIs*.

5. Solução da Proposta e tecnologias utilizadas

Para alcançar o objetivo de criar um website educativo e interativo onde usuários possam aprender e se conscientizar sobre os principais conceitos voltados às *APIs*, assim como suas implicações em termos de segurança, serão utilizadas diferentes

tecnologias com a finalidade de mostrar ao usuário como vulnerabilidades podem ser prejudiciais à aplicação.

Na criação da interface gráfica, o *front-end*, será utilizado o *React*, um *framework* JavaScript usado para criar interfaces de usuário em aplicações web. Para garantir que o usuário tenha uma experiência real de como alguém pode se aproveitar de vulnerabilidades presentes no código, a sua interação com os principais riscos de segurança em *APIs* será realizada diretamente com diferentes tipos de *APIs*, como o padrão *Rest* e o Graphql. Essas *APIs* serão desenvolvidas em Java, utilizando o Spring Boot, uma extensão do *framework Spring*, e terão erros de segurança comumente deixados por desenvolvedores. Os usuários terão um passo a passo de como realizar a invasão de dados ou serviços críticos, e, após isso, uma demonstração de como o código na *API* foi estruturado junto de uma solução para esse problema com a finalidade de educar de forma clara o desenvolvedor a se proteger de possíveis invasores. Essas *APIs* se comunicarão com um banco de dados relacional, tornando a ação o mais real possível.

6. Resultados Parciais

No presente momento o projeto está na sua fase inicial de planejamento e concepção, onde ainda não se iniciou a implementação do website sobre segurança em *APIs*. Todavia, algumas etapas cruciais já foram estabelecidas e alcançadas. Dentre as principais etapas alcançadas estão a definição do escopo do projeto, identificando e estabelecendo tópicos que serão abordados, assim como a arquitetura do sistema que começou a ser esboçada, sendo definidas as tecnologias a serem utilizadas.

Referências

Arakaki, E. (2015) “Pesquisa e Comparação de Mecanismos de Autenticação e Autorização: Estudo de caso do OAUTH” **Univem**. Disponível em: <https://aberto.univem.edu.br/bitstream/handle/11077/1398/Eduardo%20Arakaki.pdf?sequence=1&isAllowed=y>. Último acesso em: 02/10/2023.

OWASP (2023) “OWASP Top 10 API Security Risks - 2023” **Open Web Application Security Project (OWASP)**. Disponível em: <https://owasp.org/API-Security/editions/2023/en/0x11-t10/>. Último acesso em: 01/10/2023.

Silva, F. (2023) “Principais mudanças do OWASP API Security Top 10 2023”. **Medium**. Disponível em: <https://fernando-silva.medium.com/principais-mudan%C3%A7as-do-owasp-api-security-top-10-2023-545356c3b246>. Último acesso em: 05/10/2023.

TheFemTech. (2023) “APIs o que são? Como utiliza-las e seus tipos” **Linkedin**. Disponível em: <https://www.linkedin.com/pulse/apis-o-que-s%C3%A3o-como-utiliza-las-e-seus-tipos-thefemtech/?originalSubdomain=pt>. Último acesso em: 01/10/2023.