Avaliação de vulnerabilidades em aplicações utilizando OWASP Top 10

Leonardo Osvald de Souza[1], **Vitalino Pitt**[1]

[1]Ciência da Computação – Atitus Educação
Passo Fundo – RS – Brasil

aluno@atitus.edu.br, orientador@atitus.edu.br

Abstract. *Escreva seu resumo em língua estrangeira (inglês)...*

Resumo. *Resumo do trabalho (português)...*

1. Introdução

A segurança de aplicações web tornou-se um pilar fundamental no desenvolvimento de sistemas modernos, dada a crescente dependência do mundo digital para operações críticas e interações diárias. Com a grande crescente de serviços online, a superfície de ataque para cibercriminosos expandiu-se significativamente, tornando as aplicações web alvos constantes de exploração. A falha em proteger adequadamente essas aplicações pode resultar em perdas financeiras substanciais, comprometimento de dados sensíveis, danos à reputação e interrupção de serviços.

Nesse cenário, a compreensão das vulnerabilidades e a implementação de práticas de desenvolvimento seguro são imperativas. Segundo **ALMEIDA** "Uma vulnerabilidade pode ser definida como uma fraqueza ou falha em um sistema de informação que pode ser explorada por uma ameaça para comprometer a segurança do sistema". A identificação e mitigação dessas falhas são essenciais para garantir a integridade, confidencialidade e disponibilidade das informações processadas pelas aplicações web .

2. Referencial Teórico

Voltado ao objetivo geral (teoria por trás do método), deve conter os assuntos-base da pesquisa, fazendo citações indiretas e diretas curtas.

2.1. OWASP Top 10

A Open Web Application Security Project (OWASP) é uma comunidade global sem fins lucrativos dedicada a melhorar a segurança de software. Uma de suas iniciativas mais reconhecidas é o OWASP Top 10, um documento que lista e descreve os dez riscos de segurança mais críticos para aplicações web. Este ranking é atualizado periodicamente com base em dados de vulnerabilidades de milhares de aplicações, servindo como um guia essencial para desenvolvedores e profissionais de segurança .

O OWASP Top 10 não é uma lista exaustiva de todas as vulnerabilidades existentes, mas sim um consenso sobre os riscos mais prevalentes e impactantes que as organizações devem priorizar em seus esforços de segurança. Ele visa aumentar a conscientização sobre os riscos de segurança de aplicações e fornecer orientações para a mitigação eficaz . A compreensão e aplicação dos princípios do OWASP Top 10 são cruciais para o desenvolvimento de aplicações robustas e seguras.

2.2. Vulnerabilidades mais Comuns em Aplicações Web

As vulnerabilidades listadas no OWASP Top 10 abrangem uma vasta gama de falhas de segurança que podem ser exploradas por atacantes. Dentre as mais persistentes e perigosas, destacam-se:

2.2.1 Injeção (Injection)

As falhas de injeção, como SQL Injection, ocorrem quando dados não confiáveis são enviados a um interpretador como parte de um comando ou consulta. Os dados maliciosos do atacante podem enganar o interpretador para executar comandos não intencionais ou acessar dados sem autorização . Este tipo de ataque pode levar à divulgação completa de dados, modificação ou exclusão de informações, e até mesmo ao controle total do servidor . A prevenção envolve o uso de consultas parametrizadas, procedimentos armazenados e validação rigorosa de entrada .

2.2.2 Quebra de Autenticação e Gerenciamento de Sessão (Broken Authentication)

Essas vulnerabilidades permitem que atacantes comprometam senhas, chaves de sessão ou tokens de autenticação, ou explorem falhas na implementação de funções de autenticação ou gerenciamento de sessão para assumir a identidade de outros usuários. Isso pode incluir ataques de força bruta, credenciais fracas, ou falhas na expiração de sessão .

2.2.3 Cross-Site Scripting (XSS)

O XSS ocorre quando uma aplicação inclui dados não confiáveis em uma página web sem a validação ou escape adequado. Isso permite que atacantes injetem scripts maliciosos no navegador da vítima, que podem roubar cookies de sessão, redirecionar o usuário para sites maliciosos ou realizar outras ações maliciosas em nome do usuário . A mitigação de XSS requer a sanitização de todas as entradas e a codificação de saída para evitar a execução de scripts .

2.2.4 Quebra de Controle de Acesso (Broken Access Control)

As falhas de controle de acesso ocorrem quando as restrições sobre o que usuários autenticados podem fazer não são aplicadas corretamente. Atacantes podem explorar essas falhas para acessar funcionalidades não autorizadas, visualizar ou modificar dados de outros usuários, ou alterar privilégios. A implementação de um controle de acesso robusto e a verificação de permissões em cada requisição são cruciais para prevenir essas vulnerabilidades .

2.3. Segurança de APIs

Com a arquitetura de microsserviços e a crescente adoção de APIs (Application Programming Interfaces) para comunicação entre sistemas, a segurança dessas interfaces tornou-se uma preocupação crítica. As APIs são frequentemente a porta de entrada para dados e funcionalidades de backend, tornando-as alvos atraentes para atacantes . O OWASP API Security Top 10 é uma iniciativa específica que foca nos riscos de segurança mais críticos para APIs, complementando o OWASP Top 10 tradicional .

As vulnerabilidades em APIs podem incluir quebras de autenticação e autorização, exposição excessiva de dados, injeção, e configurações de segurança inadequadas. A

análise de maneiras seguras no desenvolvimento de APIs, de acordo com as diretrizes do OWASP API Security Top 10, é fundamental para proteger os sistemas modernos . Isso envolve a implementação de autenticação e autorização robustas, validação de entrada e saída, gerenciamento de erros seguro e monitoramento contínuo .

2.4. Exemplos de citação direta curta

Segundo Spinello (2024) "o trabalho de conclusão deve ter citações retiradas de artigos científicos encontrados nas bases de dados". Note que para colocar um texto entre aspas, usamos o comando `\enquote{texto}`.

Ressalta-se que o "trabalho de conclusão deve ter citações retiradas de artigos científicos encontrados nas bases de dados" (Badgujar; Poulose; Gan, 2024).

No estudo comparativo apresentado em Rabello (2010, p. 107) ...

No trabalho de Souza, Nogueira e Lotufo (2020) ...

No artigo de Estêvão e Estêvão (2024) ...

Nos trabalhos de Badgujar, Poulose e Gan (2024) e Estêvão e Estêvão (2024) são aplicadas técnicas de ...

CITAÇÃO DIRETA LONGA DEVEM SER EVITADAS EM ARTIGOS CIENTÍFICOS!

3. Trabalhos Relacionados

Trabalhos semelhantes aos objetivos específicos, sempre detalhando ao final da seção a diferença com o trabalho proposto (quantidade – 5 trabalhos);

Neste item serão apresentados os principais trabalhos que possuem uma relação com o assunto definido neste estudo....

- **Título do artigo 01 (Ogliari, 2019)**
  Primeiro parágrafo indicar uma introdução do assunto...
  No segundo: o que o estudo procurou analisar, qual o objetivo...
  No terceiro: o que foi desenvolvido, qual aplicação/experimento foi realizado...
  Último: em quais conclusões o trabalho chegou
- **Título do artigo 02 (Autor, ano)**
  Primeiro parágrafo indicar uma introdução do assunto...
  No segundo: o que o estudo procurou analisar, qual o objetivo...
  No terceiro: o que foi desenvolvido, qual aplicação/experimento foi realizado...
  Último: em quais conclusões o trabalho chegou...

4. Materiais e Métodos

Tecnologias, instrumentos e procedimentos que serão usados no estudo. O Algoritmo 1 se refere ao método de ordenação `Bubblesort` expresso em linguagem `Python`.

Uma lista numérica:

1. Item 1
2. Item 2

Uma lista definida com letras sequenciais:

a) Item 1

b) Item 2

Algoritmo 1. Método de ordenação Bubblesort

```
1 def bubble_sort(alist):
2     for i in range(len(alist)-1,0,-1):
3         for j in range(i):
4             if alist[i]>alist[i+1]:
5                 temp = alist[i]
6                 alist[i] = alist[i+1]
7                 alist[i+1] = temp
```

5. Resultados e Discussão

Essa seção deverá ser escrita na segunda parte do trabalho, conhecida como TCC2, e deverá conter os resultados dos experimentos realizados, discussão comparando os resultados obtidos com outros encontrados em trabalhos similares, além de um parágrafo apontando as limitações da metodologia adotada.

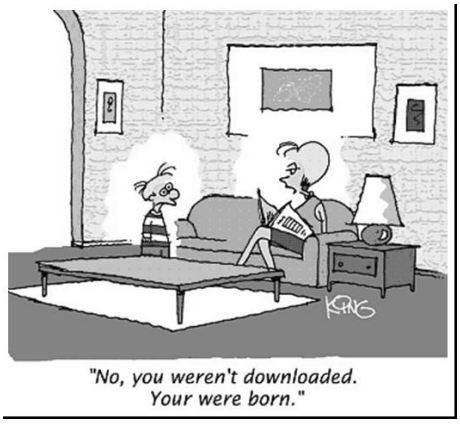
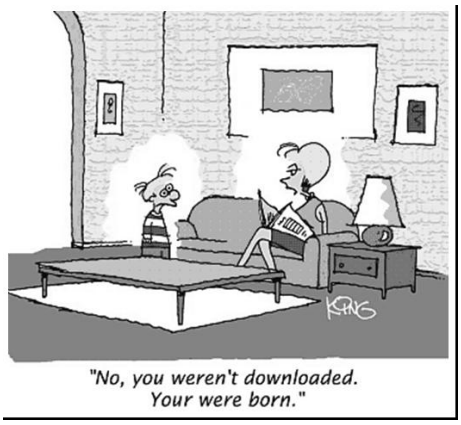


Figura 1. Exemplo de uso de figura

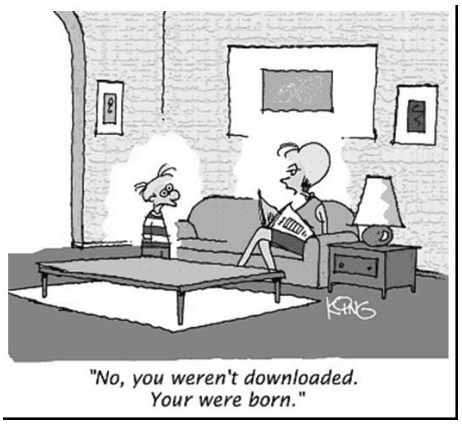
Tabela 1. Minha tabela

cabeçalho 1	**cabeçalho 2**
texto à esquerda	Existem muitas variações das passagens do Lorem Ipsum disponíveis, mas a maior parte sofreu alterações de alguma forma.

Figura 2. Exemplo com sub-figuras



(a) Sub-figura 1



(b) Sub-figura 2

Tabela 2. Tabela com sub-tabelas

cabeçalho 1	**cabeçalho 2**
Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old.	The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested.

(a) Sub-tabela da esquerda

cabeçalho 1	**cabeçalho 2**
Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old.	The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested.

(b) Sub-tabela da direita

6. Considerações Finais

Essa seção deverá ser escrita na segunda parte do trabalho, conhecida como TCC2.

Referências

BADGUJAR, C. M.; POULOSE, A.; GAN, H. Agricultural object detection with You Only Look Once (YOLO) Algorithm: A bibliometric and systematic literature review. **Computers and Electronics in Agriculture**, v. 223, p. 109090, 2024. Disponível em: https://www.sciencedirect.com/science/article/pii/S0168169924004812. Acesso em: 1 ago. 2024.

ESTÊVÃO, J. M. C.; ESTÊVÃO, M. D. Inteligência Artificial na avaliação tradicional: aquisição de conhecimento vs Prompt Engineering. *In:* CONGRESSO NACIONAL DE PRÁTICAS PEDAGÓGICAS NO ENSINO SUPERIOR, 9., 2023, Faro. **Livro de Atas**.

Faro: UAlg Editora, maio 2024. Disponível em: http://hdl.handle.net/10400.1/27060. Acesso em: 1 abr. 2025.

OGLIARI, R. **Internet das Coisas para Desenvolvedores**. São Paulo: Novatec Editora, 2019. 264 p.

RABELLO, L. S. **Promoção da saúde: a construção social de um conceito em perspectiva comparada**. Rio de Janeiro: Editora FIOCRUZ, 2010. 228 p. Disponível em: http://dx.doi.org/10.7476/9788575413524.

SOUZA, F.; NOGUEIRA, R.; LOTUFO, R. BERTimbau: Pretrained BERT Models for Brazilian Portuguese. *In:* BRAZILIAN CONFERENCE ON INTELLIGENT SYSTEMS (BRACIS), 9., 2020, Rio Grande. **Intelligent Systems**. Cham: Springer Cham, 2020. Disponível em: https://doi.org/10.1007/978-3-030-61377-8_28. Acesso em: 1 abr. 2025.

SPINELLO, S. S. **Orientação de TCC**. [*S. l.: s. n.*], 2024. Disponível em: .... Acesso em: 01 jan. 2024.