REFERÊNCIAS BIBLIOGRÁFICAS

Este documento compila as referências técnicas utilizadas como base para o desenvolvimento do portal “Casos da Impacta” e para a compreensão das vulnerabilidades e mecanismos de proteção abordados.

**Vulnerabilidades Web (OWASP - Open Web Application Security Project)**

1. OWASP. **SQL Injection Prevention Cheat Sheet**. OWASP Cheat Sheet Series. Disponível em: https://cheatsheetseries.owasp.org/cheatsheets/SQL\_Injection\_Prevention\_Cheat\_Sheet.html. Acesso em: 29 abr. 2025.
   * *Descrição*: Documentação fundamental sobre os riscos de SQL Injection e as principais estratégias de prevenção, como o uso de Prepared Statements e validação de entrada, que foram intencionalmente ignoradas em partes do código para fins de demonstração.
2. OWASP. **Cross Site Scripting Prevention Cheat Sheet**. OWASP Cheat Sheet Series. Disponível em: https://cheatsheetseries.owasp.org/cheatsheets/Cross\_Site\_Scripting\_Prevention\_Cheat\_Sheet.html. Acesso em: 29 abr. 2025.
   * *Descrição*: Guia essencial sobre os diferentes tipos de ataques XSS (Reflected, Stored, DOM-based) e as técnicas de mitigação, como codificação de saída (output encoding) e validação de entrada, que foram deliberadamente omitidas na seção de comentários para demonstrar a vulnerabilidade.
3. OWASP. **Cross-Site Request Forgery Prevention Cheat Sheet**. OWASP Cheat Sheet Series. Disponível em: https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site\_Request\_Forgery\_Prevention\_Cheat\_Sheet.html. Acesso em: 29 abr. 2025.
   * *Descrição*: Detalha os mecanismos de ataque CSRF e as defesas recomendadas, principalmente o uso de tokens anti-CSRF (Synchronizer Token Pattern), cuja ausência no formulário administrativo simulado permite a exploração da vulnerabilidade.

**Web Application Firewalls (WAF)**

1. FORTINET. **FortiWeb - Web Application Firewall (WAF) & API Protection**. Fortinet Products. Disponível em: https://www.fortinet.com/products/web-application-firewall/fortiweb. Acesso em: 29 abr. 2025.
   * *Descrição*: Visão geral do produto FortiWeb WAF da Fortinet, utilizado como referência conceitual sobre as funcionalidades e capacidades gerais de um WAF comercial.
2. FORTINET. **FortiWeb Documentation**. Fortinet Document Library. Disponível em: https://docs.fortinet.com/product/fortiweb. Acesso em: 29 abr. 2025.
   * *Descrição*: Documentação técnica detalhada do FortiWeb, consultada para entender aspectos específicos de configuração e operação de WAFs.
3. MICROSOFT AZURE. **Azure Web Application Firewall (WAF)**. Azure Products. Disponível em: https://azure.microsoft.com/en-us/products/web-application-firewall. Acesso em: 29 abr. 2025.
   * *Descrição*: Página oficial do produto Azure WAF, descrevendo suas funcionalidades, benefícios e integração com outros serviços Azure, como Application Gateway e Front Door. Essencial para o contexto do projeto.
4. MICROSOFT LEARN. **Web Application Firewall documentation**. Azure Documentation. Disponível em: https://learn.microsoft.com/en-us/azure/web-application-firewall/. Acesso em: 29 abr. 2025.
   * *Descrição*: Portal central da documentação do Azure WAF, contendo guias de introdução, configuração, gerenciamento de regras (OWASP Core Rule Set - CRS), políticas e solução de problemas. Fonte primária para o manual de instalação e configuração.
5. MICROSOFT LEARN. **Introduction to Azure Web Application Firewall**. Azure Documentation. Disponível em: https://learn.microsoft.com/en-us/azure/web-application-firewall/overview. Acesso em: 29 abr. 2025.
   * *Descrição*: Documento introdutório que explica os conceitos básicos do Azure WAF, como ele protege aplicações web contra explorações e vulnerabilidades comuns, e os serviços com os quais pode ser implantado.

**Observação**: O formato ABNT pode variar ligeiramente. Esta formatação busca seguir os padrões comuns para referências de recursos online.