











Análise de Vulnerabilidades da Plataforma Moodle com base no Top 10 da OWASP

Leonardo Frangello, **Silvio E. Quincozes**, Juliano Kazienko e Vagner Quincozes

















Meus dados estão seguros na plataforma Moodle?









Introdução

- Moodle é uma plataforma Web que contém informações acadêmicas e pessoais de mais 316 milhões de usuários.
- Aumento de ataques cibernéticos no mundo!
 - → 1.636 ataques hackers por semana no segundo trimestre de 2024.
 - → Aumento de 30% em relação ao ano anterior!

Mas e a plataforma Moodle, o quão segura ela está?













Justificativa

- Faltam estudos recentes sobre a segurança da plataforma Moodle!
 - Estudos da literatura consideram versões anteriores da plataforma Moodle.
- Faltam estudos sobre vulnerabilidades mais frequentes em aplicações web atuais!
 - Lista de referência defasada! Ex. OWASP Top 10 de 2017
 - Em setembro de 2021 foi publicada uma relação atualizada das principais vulnerabilidades.











Justificativa

2017 2021 A01:2017-Injection A01:2021-Broken Access Control A02:2017-Broken Authentication A02:2021-Cryptographic Failures A03:2021-Injection A03:2017-Sensitive Data Exposure A04:2017-XML External Entities (XXE) (New) A04:2021-Insecure Design A05:2017-Broken Access Control A05:2021-Security Misconfiguration A06:2017-Security Misconfiguration A06:2021-Vulnerable and Outdated Components A07:2017-Cross-Site Scripting (XSS) A07:2021-Identification and Authentication Failures A08:2017-Insecure Deserialization (New) A08:2021-Software and Data Integrity Failures A09:2017-Using Components with Known Vulnerabilities A09:2021-Security Logging and Monitoring Failures* A10:2017-Insufficient Logging & Monitoring (New) A10:2021-Server-Side Request Forgery (SSRF)* * From the Survey











Objetivo

- Estudo de caso atualizado:
 - Versão mais recente do Moodle!
 - Versão mais recente do OWASP Top 10!
- Varredura de vulnerabilidades e análise dos alertas.
 - Ferramenta de varredura OWASP ZAP.





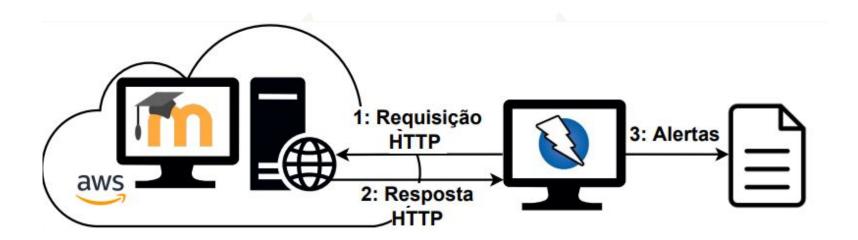








Metodologia













Resultados

Relatório: 894 alertas (impacto alto, médio, baixo e informativo)

Foram 5 alertas de **SQL Injection!**





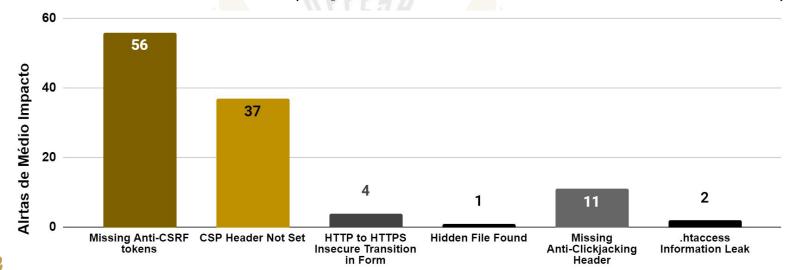






Resultados

Relatório: 894 alertas (impacto alto, médio, baixo e informativo)







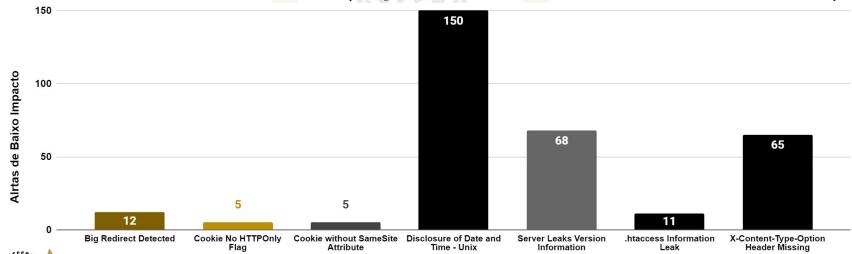






Resultados

Relatório: 894 alertas (impacto alto, médio, baixo e informativo)













Considerações Finais

- A plataforma Moodle não parece estar totalmente segura!
 - Identificamos 894 alertas através da ferramenta OWASP ZAP:
 - Esses alertas representam 20 tipos de vulnerabilidades.











Considerações Finais

- A plataforma Moodle não parece estar totalmente segura!
 - Identificamos 894 alertas através da ferramenta OWASP ZAP;
 - Esses alertas representam 20 tipos de vulnerabilidades.
- Trabalhos futuros
 - **Explorar essas vulnerabilidades!**
 - Em 2025, uma nova lista do OWASP Top Ten estará disponível!
 - Experimentos comparativos com versões futuras do Moodle também são importantes!















Obrigado!

silvioquincozes@unipampa.edu.br





