APLICAÇÃO DA OWASP TOP TEN E VALIDAÇÃO DA ACESSIBILIDADE NO TREASUREHUNT – UM GERADOR DE COMPETIÇÕES DE CTF

João Vitor Espig[1]
Ricardo de la Rocha Ladeira[2]

Capture The Flag (CTF) é um tipo de competição de Segurança Computacional onde quem participa precisa resolver desafios utilizando ferramentas de segurança para encontrar palavras secretas (*flags*) em troca de recompensas como pontos, prêmios ou emblemas. Esses desafios podem envolver diversas áreas, tais como programação, configuração de sistemas e codificação. O TreasureHunt é uma ferramenta que cria competições de CTF do estilo *Jeopardy*!. A plataforma é usada no ensino de Segurança Computacional desde 2017, com o objetivo de incentivar o aprendizado do tema e ajudar a identificar novos talentos na área. Nos últimos anos, a ferramenta teve como foco garantir um alto índice de acessibilidade, seguindo as diretrizes da WCAG (*Web Content Accessibility Guidelines*). Além disso, o projeto adota boas práticas de segurança para evitar ataques e fraudes no sistema, utilizando como base o padrão definido pela lista *OWASP Top Ten*. O presente trabalho tem como proposta desenvolver, incrementar e corrigir funcionalidades na ferramenta TreasureHunt, assim como seguir os critérios de acessibilidade da WCAG e utilizar como base a lista da *OWASP top ten*. Para tal, o projeto usa como metodologia a pesquisa bibliográfica de caráter exploratório, por conta da natureza prática das suas atividades. Para atingir este propósito, foi realizada, na prática, a validação da acessibilidade da plataforma, bem como a certificação dos seus processos, sendo utilizada como base uma lista de verificação baseada na *OWASP Top Ten*. Para realizar a validação das capacidades relacionadas à acessibilidade do TreasureHunt, a equipe de desenvolvimento recebeu uma nova integrante que faz uso diário de tecnologias assistivas, de forma a contribuir com testes práticos e *feedback* real sobre a interpretação da equipe acerca do cumprimento dos critérios de acessibilidade — que já atigem mais de 90% de cobertura — e com apontamentos valiosos para melhorias necessárias. Em relação às validações da *checklist* de segurança, até o momento, foram feitos alguns testes da categoria "Validação de dados", que define, de forma simplificada, o que pode ser enviado pelo usuário; assim como todos os testes da categoria "Autenticação", que trata da capacidade da aplicação manter a confidencialidade do sistema, pilar fundamental da Segurança da Informação. Pretende-se, até o fim do ano, aumentar a quantidade de testes e categorias abrangidas pela *checklist*. Em última análise, a segurança e a acessibilidade da ferramenta necessitam de constante monitoramento, tanto por conta da evolução contínua das diretrizes da *WCAG* quanto pela descoberta de novas vulnerabilidades e possíveis erros relacionados à segurança da aplicação.

---

[1] Aluno do curso de Ciência da Computação, IFC Campus Blumenau, jotinha1300@gmail.com
[2] Professor (Informática), IFC Campus Blumenau, ricardo.ladeira@ifc.edu.br