O uso de um CTF na educação formal: desafios e perspectivas

Ricardo de la Rocha Ladeira, Luana Tillmann, João Vitor Espig

Instituto Federal Catarinense – Campus Blumenau – Blumenau/SC – Brasil

{ricardo.ladeira, luana.tillmann}@ifc.edu.br, jotinha1300@gmail.com

Abstract. *Games are effective for engaging and promoting learning. In Cybersecurity courses, one of the most commonly used games is capture the flag (CTF). The competitive factor can be motivating, but it is essential that the primary goal be learning. Therefore, games should be designed to align challenge and pedagogical content, ensuring that the experience contributes to educational objectives. This paper describes challenges and prospects regarding the maintenance of the TreasureHunt, a CTFs generator that has been used in Cybersecurity classes for the last eight years.*

Resumo. *Jogos são eficazes em estimular o engajamento e promover a aprendizagem. No âmbito de disciplinas de Cibersegurança, um dos jogos populares é o capture the flag (CTF). Embora o fator competitivo seja motivador, é importante que o foco principal seja a aprendizagem. Nesse sentido, jogos devem ser planejados de forma a alinhar desafio e conteúdo pedagógico, garantindo que a experiência contribua para os objetivos educacionais. Este trabalho relata os principais desafios — e perspectivas de trabalhos futuros — acerca da manutenção do TreasureHunt, um gerador de CTFs aplicado em aulas de Segurança Computacional há oito anos.*

1. Introdução

Jogos são ferramentas motivadoras e têm se mostrado eficazes no ensino, pois unem engajamento e aprendizagem [Cheung *et al*. 2011]. Na Computação e na Cibersegurança, é comum o uso de jogos de tabuleiro [Tseng *et al*. 2024], *videogames* [Irvine *et al*. 2005], caça ao tesouro [Vigna 2003], entre outros. Nesse contexto, é crescente o uso de jogos de caça ao tesouro chamados *capture the flags* (CTFs) [Zouahi 2023]. Nos CTFs, jogadores(as) pontuam ao encontrarem *flags* (palavras secretas) usando ferramentas de segurança, atacando ou defendendo sistemas, nos CTFs *Red vs Blue*, ou resolvendo desafios em áreas como forense e descompilação, nos CTFs *Jeopardy* [Kuo *et al*. 2018].

O TreasureHunt é um gerador de CTFs *Jeopardy* utilizado na educação formal desde 2017 [Ladeira 2018]. Ele cria competições com desafios de diferentes classes, envolve diversas técnicas e conta com as seguintes contribuições: (1) os desafios gerados podem envolver uma ou duas técnicas; (2) as instâncias de desafios são uniformes, jogadores(as) recebem problemas de igual dificuldade; (3) as instâncias de desafios são únicas, permitindo a replicação da atividade com instâncias inéditas e impedindo o compartilhamento de *flags*; (4) a ferramenta gera exercícios e prepara todo ambiente da competição; e (5) a interface para interação dos(as) jogadores(as) é responsiva e acessível (Figura 1), propiciando a inclusão de pessoas com deficiência.

Este artigo relata desafios e perspectivas futuras sobre a manutenção do TreasureHunt, um gerador de CTFs aplicado no ensino de Cibersegurança.

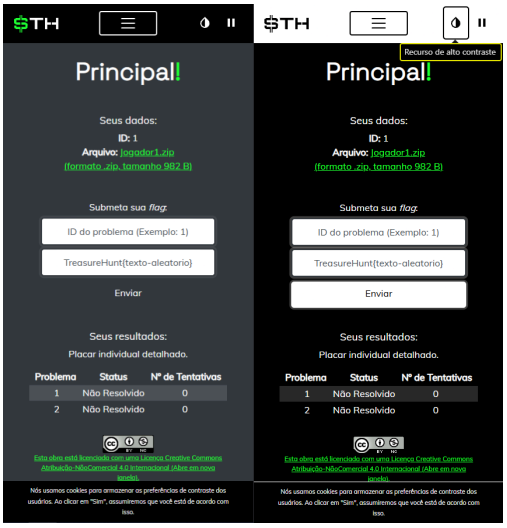

Figura 1. Interface acessível e responsiva (a) normal e (b) em alto contraste.

2. Comparação com Trabalhos Relacionados

A geração automática de desafios com instâncias únicas está presente nos CTFs de Feng (2015), Burket *et al*. (2015) e Schreuders *et al*. (2017). Porém, eles se diferenciam na quantidade de técnicas por desafio, na uniformidade dos problemas e no nível de geração adotado. A Tabela 1 resume as diferenças entre os CTFs citados e o TreasureHunt.

Tabela 1. Resumo das principais características dos trabalhos relacionados.

Ferramenta	Composição de problemas	Uniformidade de problemas	Nível de geração
MetaCTF [Feng 2015]	✔	✗	Competição
PicoCTF [Burket *et al*. 2015]	✗	✔	Problema
SecGen [Schreuders *et al*. 2017]	✔	✗	Competição
TreasureHunt	✔	✔	Competição

A interface acessível distingue o TreasureHunt das demais ferramentas. Estudos mostram que a acessibilidade é uma barreira para a cibersegurança [Furnell *et al*. 2021; Stelea *et al*. 2025], incluindo os CTFs [De La Cruz & Das 2022]. Um estudo comparou a acessibilidade de interfaces de CTFs e mostrou que há muitos critérios não cumpridos em plataformas populares na área [Otto & Ladeira 2021].

Renaud (2021) e De La Cruz & Das (2022) destacam a importância de integrar Segurança e Acessibilidade e reconhecem a necessidade de acesso pleno e seguro de pessoas com deficiência às tecnologias. Em especial, os critérios de acessibilidade da W3C (2023) são seguidos na interface do TreasureHunt.

3. Desafios e Perspectivas

Ao longo dos anos, percebeu-se que alunos com deficiência enfrentariam dificuldades

para jogar CTFs. Por isso, pensou-se em cumprir critérios de acessibilidade na interface do jogo com base na W3C (2023), que devem ser monitorados constantemente. Além disso, muitos exercícios não são acessíveis, apresentando códigos ilegíveis que dificultam a compreensão. A interface do organizador — um *script* — dispõe apenas de função de acessibilidade: (des)ativação do alto contraste. A opinião de pessoas com deficiência é fundamental, e atualmente o projeto conta com a colaboração de uma profissional com cegueira total que tem contribuído para melhorias.

Até 2023, a análise dos dados do jogo, como acertos, erros e cópias de respostas, era manual, o que tornava o processo lento e sujeito a erros. Esse problema foi resolvido com um *script* automatizado que gera relatórios instantâneos ao final da competição.

Atualizar ferramentas exige testes rigorosos, pois mudanças nas configurações podem causar falhas e novos problemas. Usuários maliciosos e avanços tecnológicos também exigem foco na segurança. A equipe prioriza mitigar vulnerabilidades do padrão OWASP Top Ten. Como gerador de competições de segurança, o TreasureHunt deve ser confiável. Atualmente, conta-se com uma lista de testes baseada no OWASP Top Ten, com a qual a equipe valida e corrige o código da ferramenta, mantendo um processo contínuo de verificação de funcionalidades.

Estratégias de ensino devem acompanhar avanços sociais; o que já foi divertido pode perder apelo. O jogo precisa passar por constantes atualizações, incluindo as técnicas dos desafios. Estudantes verticalizam, participando no ensino médio e depois no superior, o que exige que o jogo siga motivador e relevante nos diferentes níveis. *Feedbacks*, sobretudo os recentes, são essenciais para manter a experiência atualizada.

Os comentários sobre a atividade são majoritariamente positivos, com estudantes manifestando interesse em participar novamente. Contudo, repetir o jogo sem novidades pode desmotivar. Além disso, turmas pequenas limitam a análise estatística dos dados e dificultam a identificação de padrões gerais.

A adequação legal é outro ponto importante. Com a Lei Geral de Proteção de Dados (LGPD), foi necessário detalhar o uso dos *cookies*. Essa exigência foi cumprida, mas alterações futuras na lei e novas legislações requerem atenção constante.

Por fim, integrar Inteligência Artificial (IA) é essencial, pois pode ajudar a criar desafios, melhorar códigos, sugerir alterações e indicar CTFs relacionados. Deseja-se criar o *modo individual customizado*, em que a IA analise o comportamento do jogador para personalizar exercícios, ajustando-os de acordo com dificuldade, interesse e dados de desempenho.

4. Conclusão

Este trabalho relatou desafios e perspectivas futuras para a manutenção do gerador de CTFs TreasureHunt. Os desafios já elencados sugerem a necessidade de integrar aspectos técnicos da ferramenta, como confiabilidade, segurança e acessibilidade; pedagógicos, como o valor da atividade para o desenvolvimento de habilidades em Segurança; e experienciais, como o potencial da atividade para motivar, divertir e envolver, promovendo uma experiência positiva aos(às) estudantes.

O futuro da pesquisa envolve a atualização da ferramenta baseada nos principais

padrões de Cibersegurança e Acessibilidade, bem como o aumento de técnicas usadas na geração de exercícios. Espera-se ainda aplicar IA na ferramenta, possibilitando, entre outros, a criação de um módulo inteligente de entrega de desafios.

Referências

Burket, J., Chapman, P., Becker, T., Ganas, C., & Brumley, D. (2015). Automatic problem generation for Capture-the-Flag competitions. *3GSE'15*.

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. *SAM'11*, 1.

De La Cruz, J. & Das, S. (2022). SoK: a proposal for incorporating accessible gamified cybersecurity awareness training informed by a systematic literature review. *USEC'22*.

Feng, W. C. (2015). A Scaffolded, Metamorphic CTF for Reverse Engineering. *3GSE'15*.

Furnell, S., Helkala, K., & Woods, N. (2021). Disadvantaged by disability: examining the accessibility of cyber security. *HCI International*, 197-212.

Irvine, C. E., Thompson, M. F., & Allen, K. (2005). CyberCIEGE: gaming for information assurance. *IEEE Security & Privacy*, 3(3), 61-64.

Kuo, C. C., Chain, K., & Yang, C. S. (2018). Cyber attack and defense training: Using emulab as a platform. *IJICIC*, 14(6), 2245-2258.

Ladeira, R. R. (2018). *TreasureHunt: Geração automática de desafios aplicados no ensino de segurança computacional* (Dissertação de mestrado). UDESC, Joinville.

Otto, V. A. U., & Ladeira, R. R. (2021). Uma Análise de Critérios de Acessibilidade em Interfaces web de Jogos de Segurança Computacional. *COTB'21*, 12, 563-566.

Renaud, K. (2021). Accessible cyber security: the next frontier?. *International Conference on Information Systems Security and Privacy*, 9-18.

Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., & Ordean, M. (2017). Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events. *ASE' 17*.

Stelea, G. A., Sangeorzan, L., & Enache-David, N. (2025). When Cybersecurity Meets Accessibility: A Holistic Development Architecture for Inclusive Cyber-Secure Web Applications and Websites. *Future Internet*, 17(2), 67.

Tseng, S. S., Yang, T. Y., Shih, W. C., & Shan, B. Y. (2024). Building a self-evolving iMonsters board game for cyber-security education. *Interactive Learning Environments*, 32(4), 1300-1318.

Vigna, G. (2003). Teaching network security through live exercises: Red team/blue team, capture the flag, and treasure hunt. *WISE 2003*, 3-18.

W3C. (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*. World Wide Web Consortium (W3C). `https://www.w3.org/TR/WCAG22/`.

Zouahi, H. (2023). Gamifying Cybersecurity Education: A CTF-based Approach to Engaging Students in Software Security Laboratories. *CEEA*.