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

Introdução

Jogos são ferramentas eficazes em engajamento e aprendizagem [1]. Na Cibersegurança, é comum o uso de jogos de tabuleiro [2], *videogames* [3] e caça ao tesouro. Nesse contexto, é crescente o uso de jogos de caça ao tesouro do tipo *capture the flag* (CTF) [4]. Neles os(as) jogadores(as) pontuam ao encontrarem *flags* (palavras secretas) atacando ou defendendo sistemas, ou resolvendo desafios em áreas como forense e descompilação [5].

O TreasureHunt é um gerador de CTFs utilizado na educação formal desde 2017 [6]. Ele cria competições com desafios de classes distintas, envolve diversas técnicas e conta com as seguintes contribuições: (i) os desafios gerados podem envolver uma ou duas técnicas (Figura 1); (ii) jogadores(as) recebem desafios de igual dificuldade; (iii) as instâncias de desafios são únicas, permitindo a replicação da atividade com instâncias inéditas e impedindo o compartilhamento de *flags*; (iv) a ferramenta gera exercícios e prepara o ambiente da competição; e (v) a interface para interação dos(as) jogadores(as) é acessível, promovendo a inclusão de pessoas com deficiência.

Figura 1. Desafio *esteganografia* ○ *base64*.

Comparação com Trabalhos Relacionados

A geração automática de desafios está presente nos CTFs MetaCTF [7], PicoCTF [8] e SecGen [9], mas 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 comparativo dos trabalhos relacionados.

Ferramenta	Composição de problemas	Uniformidade de problemas	Nível de geração
MetaCTF [8]	✓	✗	Competição
PicoCTF 9]	✗	✓	Problema
SecGen [10]	✓	✗	Competição
TreasureHunt	✓	✓	Competição

A interface acessível (Figura 2) também distingue o TreasureHunt das demais ferramentas. Estudos mostram que a acessibilidade é uma barreira para a cibersegurança [10], incluindo os CTFs [11]. A integração de Segurança e Acessibilidade é importante, e o acesso pleno e seguro de pessoas com deficiência às tecnologias é uma necessidade reconhecida [11]. Em especial, os critérios de acessibilidade da W3C [12] são seguidos na interface do TreasureHunt, mas estão ausentes em outras plataformas populares na área [13].

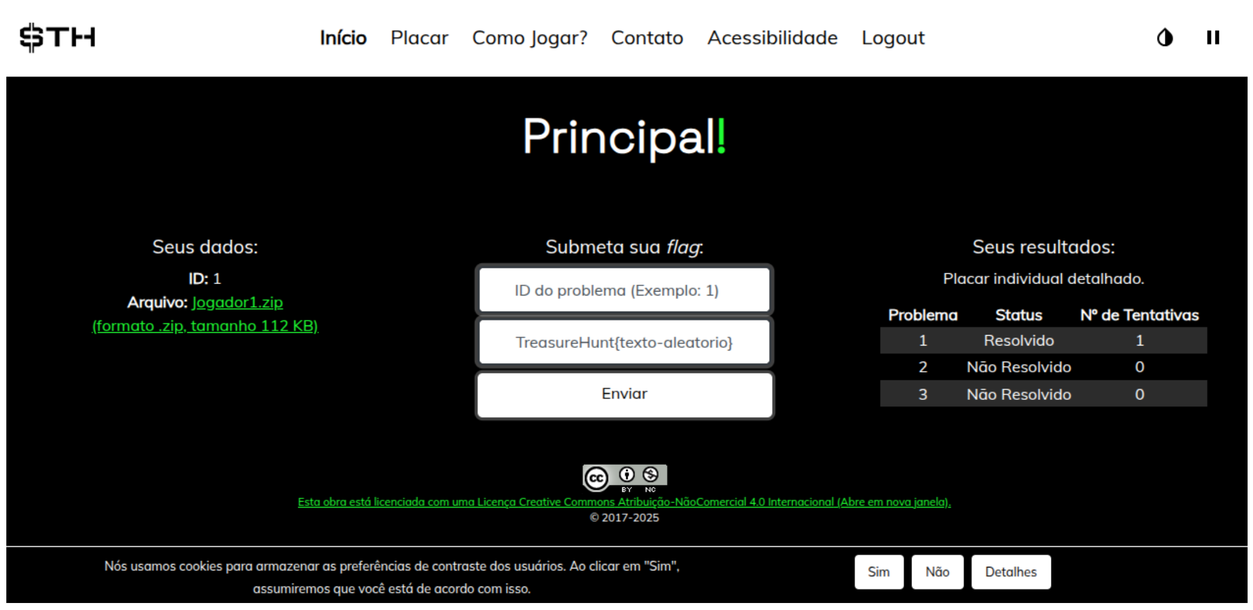

Figura 2. Interface acessível do TreasureHunt.

Desafios & Perspectivas

Ao longo dos anos, percebeu-se que **acessibilidade em CTFs é um desafio para alunos com deficiência**. Muitos exercícios ainda não são acessíveis, apresentando códigos ilegíveis que dificultam a assimilação. Por isso, a opinião de usuários com deficiência é fundamental. Uma usuária de tecnologias assistivas compõe a equipe do TreasureHunt desde 2025, contribuindo diretamente no aprimoramento da acessibilidade.

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. Isto foi resolvido com um *script* automatizado que gera relatórios instantâneos ao final da competição. Entretanto, **turmas pequenas limitam a análise dos dados** e dificultam a identificação de padrões.

Atualizar a ferramenta exige testes rigorosos, pois mudanças podem causar novos problemas. Usuários maliciosos e avanços tecnológicos também exigem foco na segurança. Como gerador de competições de Segurança, o TreasureHunt deve ser confiável. Por isso, a equipe prioriza mitigar vulnerabilidades do OWASP Top Ten e mantém uma lista de testes baseada neste padrão para atualização do código da ferramenta.

Estratégias de ensino devem acompanhar avanços sociais; o que já foi divertido pode perder apelo. 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 têm sido majoritariamente positivos, com manifestações de interesse em competir novamente. Contudo, repetir o jogo sem novidades pode desmotivar.

Adequação legal é outro aspecto digno de atenção, pois leis podem ser propostas e alteradas. Com a criação da Lei nº 13709/2018, foi necessário detalhar a finalidade de uso de *cookies*.

Por fim, **integrar Inteligência Artificial** é essencial, pois pode ajudar a criar desafios, melhorar códigos, sugerir alterações e indicar CTFs relacionados. Deseja-se criar o *modo individual customizado*, personalizando exercícios e ajustando-os de acordo com dificuldade, interesse e dados de desempenho dos(as) jogadores(as).

Conclusão

Os desafios de manter um gerador de CTF sugerem a necessidade de integrar aspectos técnicos, pedagógicos e experienciais para impactar positivamente os(as) estudantes.

Os trabalhos futuros envolvem manter e aprimorar a segurança e a acessibilidade da ferramenta, tornando-a ainda mais robusta e universal. Entre outras ações, deseja-se expandir o rol de técnicas utilizadas nos exercícios, aumentando a quantidade de tópicos de segurança trabalhados nas competições geradas pelo TreasureHunt.

Referências

1. Cheung, R.S., Cohen, J.P., Lo, H.Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. SAM'11.
2. 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.
3. Irvine, C.E., Thompson, M.F., & Allen, K. (2005). CyberCIEGE: gaming for information assurance. IEEE Sec. & Privacy.
4. Zouahi, H. (2023). Gamifying Cybersecurity Education: A CTF-based Approach to Engaging Students in Software Security Laboratories. CEEA.
5. Kuo, C.C., Chain, K., & Yang, C.S. (2018). Cyber attack and defense training: Using emulab as a platform. IJICIC.
6. Ladeira, R.R. (2018). TreasureHunt: Geração automática de desafios aplicados no ensino de segurança computacional (Dissertação de mestrado). UDESC, Joinville.
7. Feng, W.C. (2015). A Scaffolded, Metamorphic CTF for Reverse Engineering. 3GSE'15.
8. Burket, J., Chapman, P., Becker, T., Ganas, C., & Brumley, D. (2015). Automatic problem generation for Capture-the-Flag competitions. 3GSE'15.
9. 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.
10. 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.
11. 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.
12. W3C. (2023). Web Content Accessibility Guidelines (WCAG) 2.2. World Wide Web Consortium (W3C).
13. 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.