APLICAÇÃO DA OWASP TOP TEN E VALIDAÇÃO DA ACESSIBILIDADE NO TREASUREHUNT

– UM GERADOR DE COMPETIÇÕES DE CTF

João Vitor Espig
Ricardo de la Rocha Ladeira
Luana Tillmann

INSTITUTO FEDERAL
Catarinense

Roteiro

- Introdução
- Atividades realizadas
- Resultados obtidos
- Considerações finais

Introdução: TreasureHunt

- Ferramenta criadora de competições CTF
- Aplicada no ensino de Segurança Computacional desde 2017
- Ampliar a acessibilidade à competição e à área de Segurança
- Promover competições com mais segurança

(LADEIRA et al., 2020)

Introdução: TreasureHunt

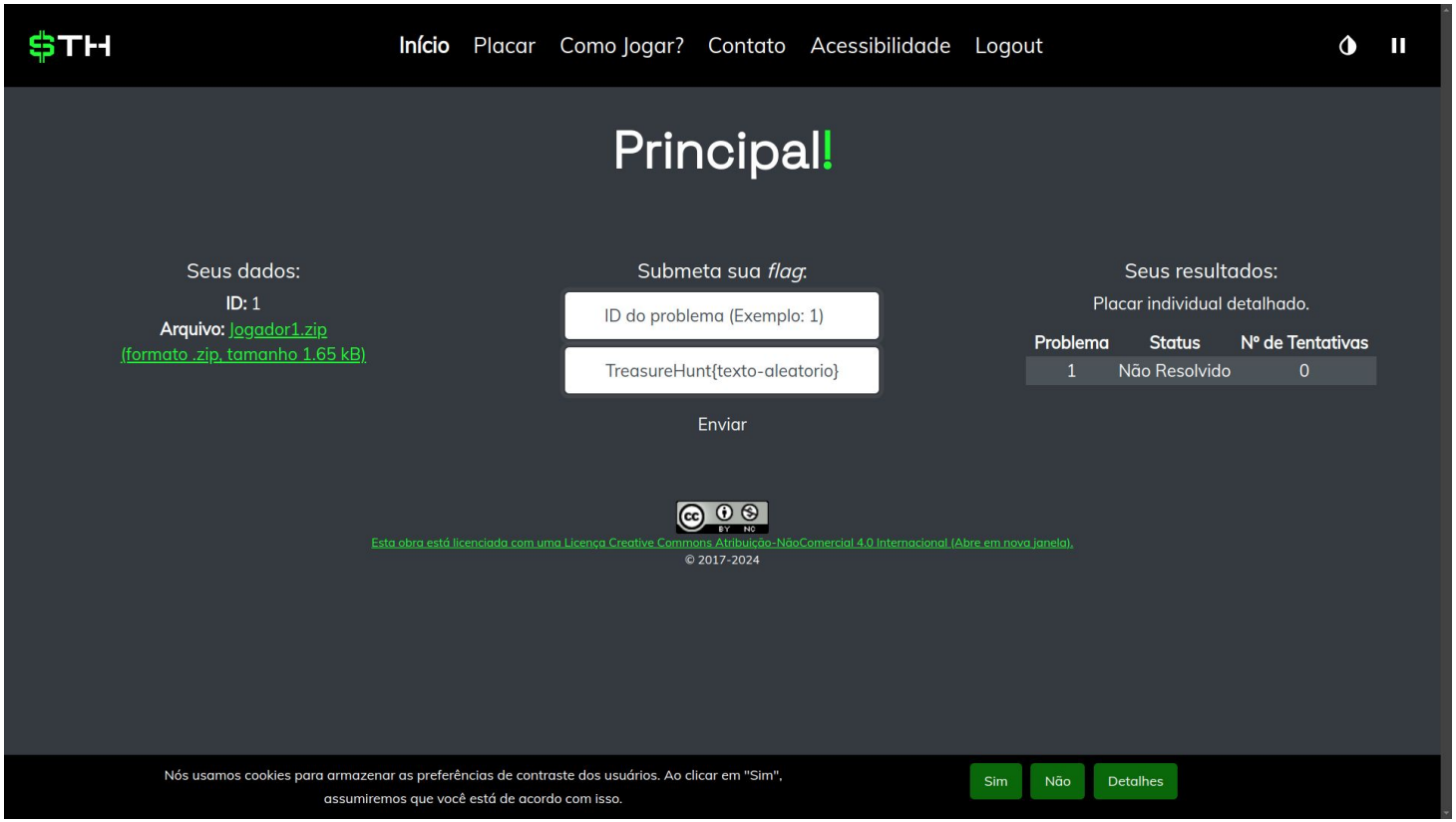


Figura: Interface web do jogador. Fonte: Autores

INSTITUTO FEDERAL
Catarinense

Introdução: TreasureHunt

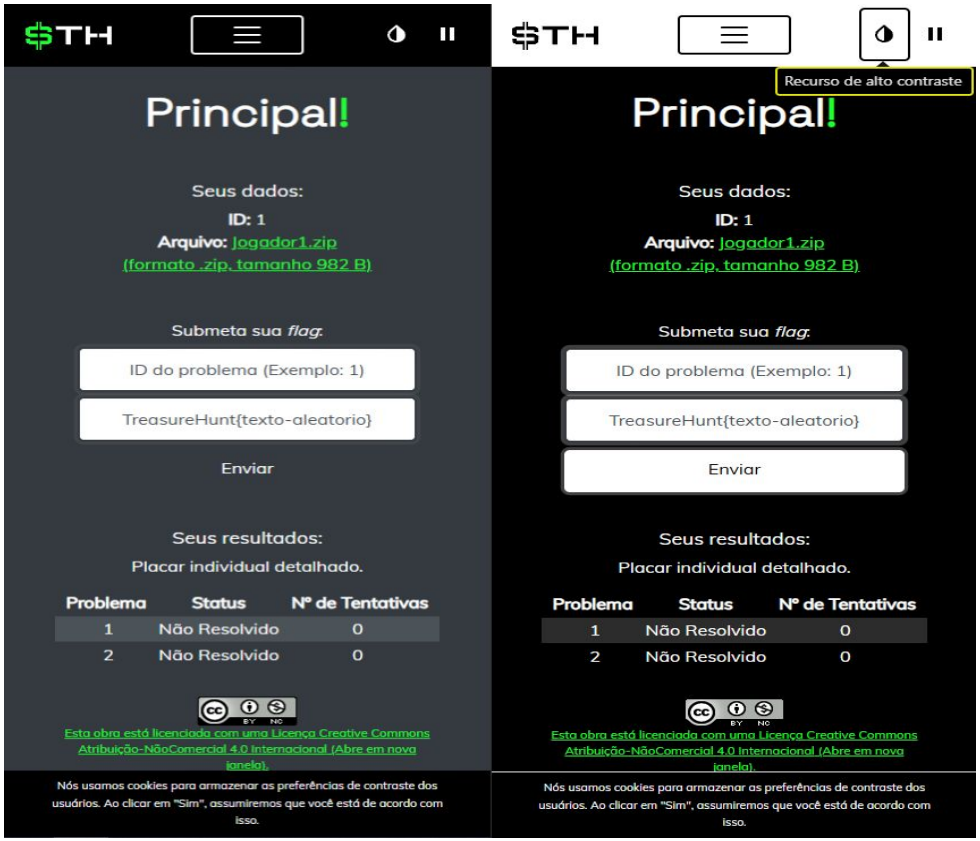


Figura: comparação dos temas de cores na versão mobile. Fonte: Autores

INSTITUTO FEDERAL
Catarinense

Introdução: TreasureHunt

```
~/downloads/th1/2/3
❯ outguess -r ronald.jpg saida.txt
Reading ronald.jpg....
Extracting usable bits:   2673090 bits
Steg retrieve: seed: 156, len: 23
~/downloads/th1/2/3
❯ cat saida.txt
TreasureHunt{s4whhvmk}
```

Figuras: Exemplo de resolução de desafio. Fonte: Autores

Introdução: Acessibilidade

- Acessibilidade baseada na WCAG 2.2 (2023)
- 87 critérios ao todo (CAMPBELL et al., 2023).

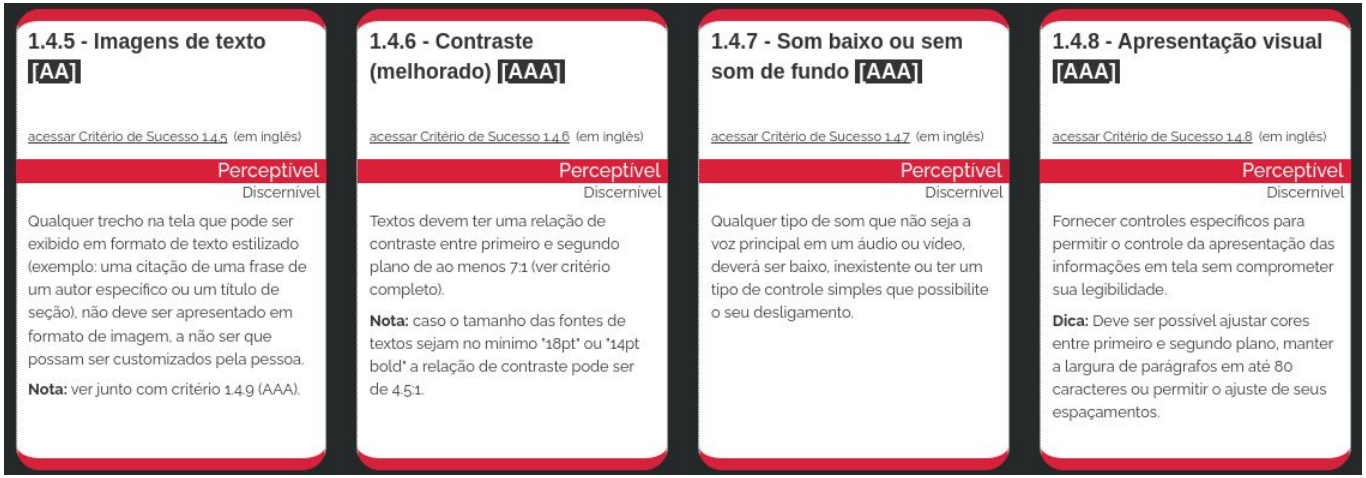


Figura: cartões de critérios de acessibilidade da *WCAG* 2.2. Fonte: guia-wcag.com/

Introdução: Segurança

- Segurança da aplicação baseada na OWASP Top Ten
- As 10 principais vulnerabilidades (OWASP, 2021).

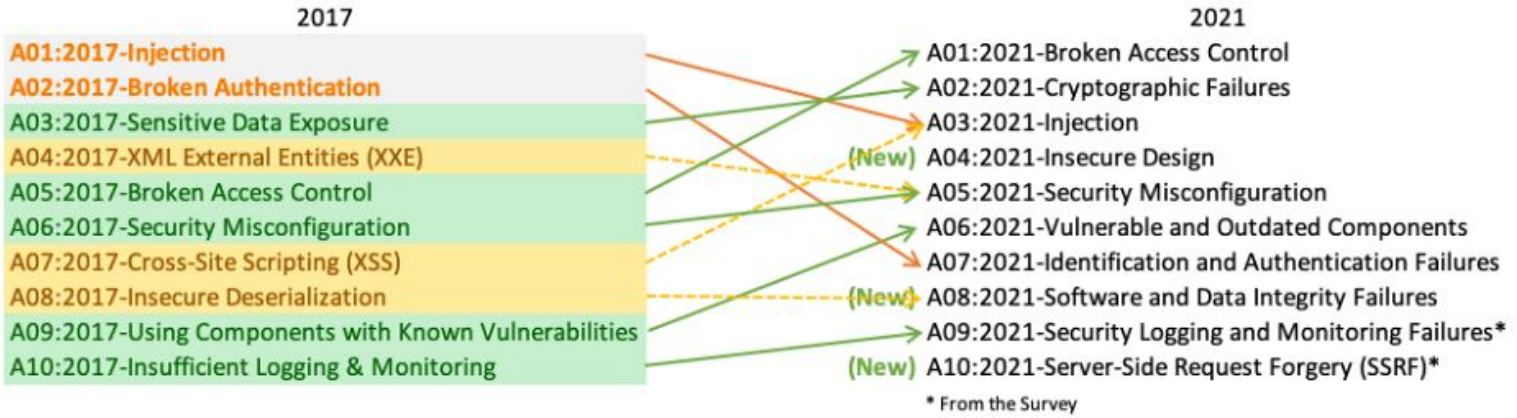


Figura: *OWASP Top Ten* 2017 e 2021. Fonte: *OWASP*

Introdução: Objetivos

- Desenvolver, incrementar e corrigir funcionalidades
- Revisão dos critérios de acessibilidade da WCAG
- Adoção das diretrizes da OWASP Top Ten

Introdução: Metodologia

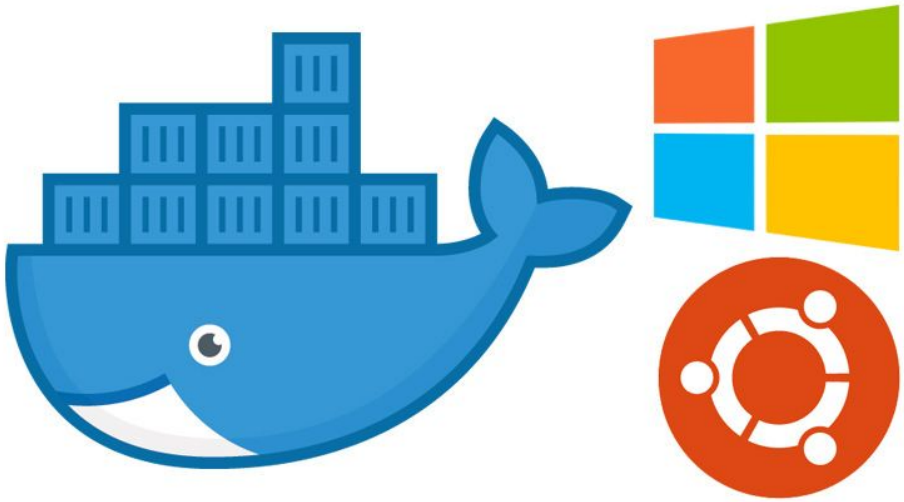
- Caráter Exploratório
- Caráter Explicativo
- Ciclo de tarefas
- Análise de dados após realização da competição

Atividades realizadas

- Melhora na portabilidade do projeto: Docker
- Tradução de checklist estrangeira sobre a OWASP
- Validação da acessibilidade de maneira prática
- Correção dos problemas encontrados:
  - Mostrar senha
  - Troca de contexto
  - Outras pequenas correções

Atividades: Docker

- Encapsulamento da aplicação com Docker
- Permite o uso em diversos ambientes
- Melhora na portabilidade da plataforma



Atividades: Checklist OWASP

- Tradução e adoção da checklist da OWASP
- Aplicação de testes de segurança

4. Teste de autenticação					
Testar credenciais padrão	- Determinar se a aplicação tem usuários com senhas padrão	A7		Passou	Esse teste passa se considerar que as senhas geradas pelo script não sejam "padrão"
Testar mecanismos de bloqueio fracos	- Avaliar o mecanismo de bloqueio de conta para mitigar técnicas como força bruta - Avaliar o sistema de resistência de liberação para contas não autorizadas	A7		Não passa totalmente	Contem sistema de detecção de força bruta, porém não faz nada para impedir
Testar bypassing o esquema de autenticação	- Garantir que a autenticação é aplicada em todos os serviços que a requerem - Force borwsing (tentar acessar áreas de admin sem a devida autorização), Parameter Modification, Session ID prediction, SQL Injection	A1, A7		Passa	home.php é protegida, assim como o download dos arquivos .zip com os problemas
Testar por vulnerabilidade de lembrar senha	- Testar que a sessão gerada é gerenciada com segurança e que as credenciais do usuário não são colocadas em perigo - Verificar que as credenciais não são salvas em texto limpo, mas sim em hashs	A4, A5		Passou	Senhas são salvas como hashes (bcrypt), usando o comando: htpasswd -bnBC 10
Testar por "fraquezas" no cache do browser	- Revisar se a aplicação guarda informação sensível no lado do cliente - Revisar se o acesso por ocorrer sem autorização - Verificar problema no histórico do navegador clickando no botão de voltar depois de dar logout - Verificar problema no cache do navegador nos cabeçalhos de resposta HTTP (Cache-Control: no-cache)	A4		Passa com ressalvas	- PHPSESSION não é explicitado SameSite como Strict (está vazio, que deixa a cargo do browser), possível CSRF
Testar política de senhas fracas	- Determinar a resistência da aplicação contra ataques de força bruta na senha usando dicionários de senhas avaliando o tamanho, complexidade, reuso das senhas - Revisar se novas contas de usuário são criadas com senhas fracas ou previsíveis	A7		Não passa	Senhas são geradas de maneira previsível (ainda mais se você sabe uma senha)
Testar por segurança fraca em resposta de questões	- Determinar a complexidade e a clareza das perguntas (perguntas fracas pré-geradas, perguntas fracas auto-geradas). - Avaliar possíveis respostas do usuário e capacidades de ataque por força bruta.	A7		Não se aplica	Não tem perguntas de segurança no th

Atividades: Validação acessibilidade

- Validação da acessibilidade através de testes práticos
- Testes e *feedback* real através da servidora Luana
- Uma melhor interpretação dos critérios de acessibilidade

Resultados obtidos

- Melhor portabilidade da plataforma
- Melhora na compreensão da segurança
- Aplicação mais segura
- Melhora na conceituação dos pontos de acessibilidade
- Ferramenta mais acessível

Resultados obtidos

Característica	2024	2025
Portabilidade	Linux	• Linux • Windows • MacOS • E outros ambientes que suportam Docker
Acessibilidade (Critérios WCAG)	73/74 (98.64%)	74/74 (100.00%)
Classes de vulnerabilidades	Injeção (parcial)	• Injeção • autenticação

Considerações finais

- Os resultados obtidos estão dentro do esperado
- Atividades no momento:
  - validação dos pontos da checklist da OWASP
- Trabalhos futuros:
  - Continuar a validação da segurança e acessibilidade
  - Adicionar novas técnicas abordadas na ferramenta

Referências

- LADEIRA, Ricardo de la Rocha et al. TreasureHunt: um gerador automático de competições de Segurança Computacional. Revista de Sistemas e Computação-RSC, v. 9, n. 2, 2020.
- CAMPBELL, Alastair et al. Web Content Accessibility Guidelines (WCAG) 2.2. W3C Recommendation, 05 out. 2023. Disponível em: https://www.w3.org/TR/2023/REC-WCAG22-20231005/. Acesso em: 10 set. 2024.
- OWASP Top Ten - 2021: The Ten Most Critical Web Application Security Risks. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em: 10 set. 2024.