

CUMPRIMENTO DE CRITÉRIOS DE SEGURANÇA E ACESSIBILIDADE NO TREASUREHUNT

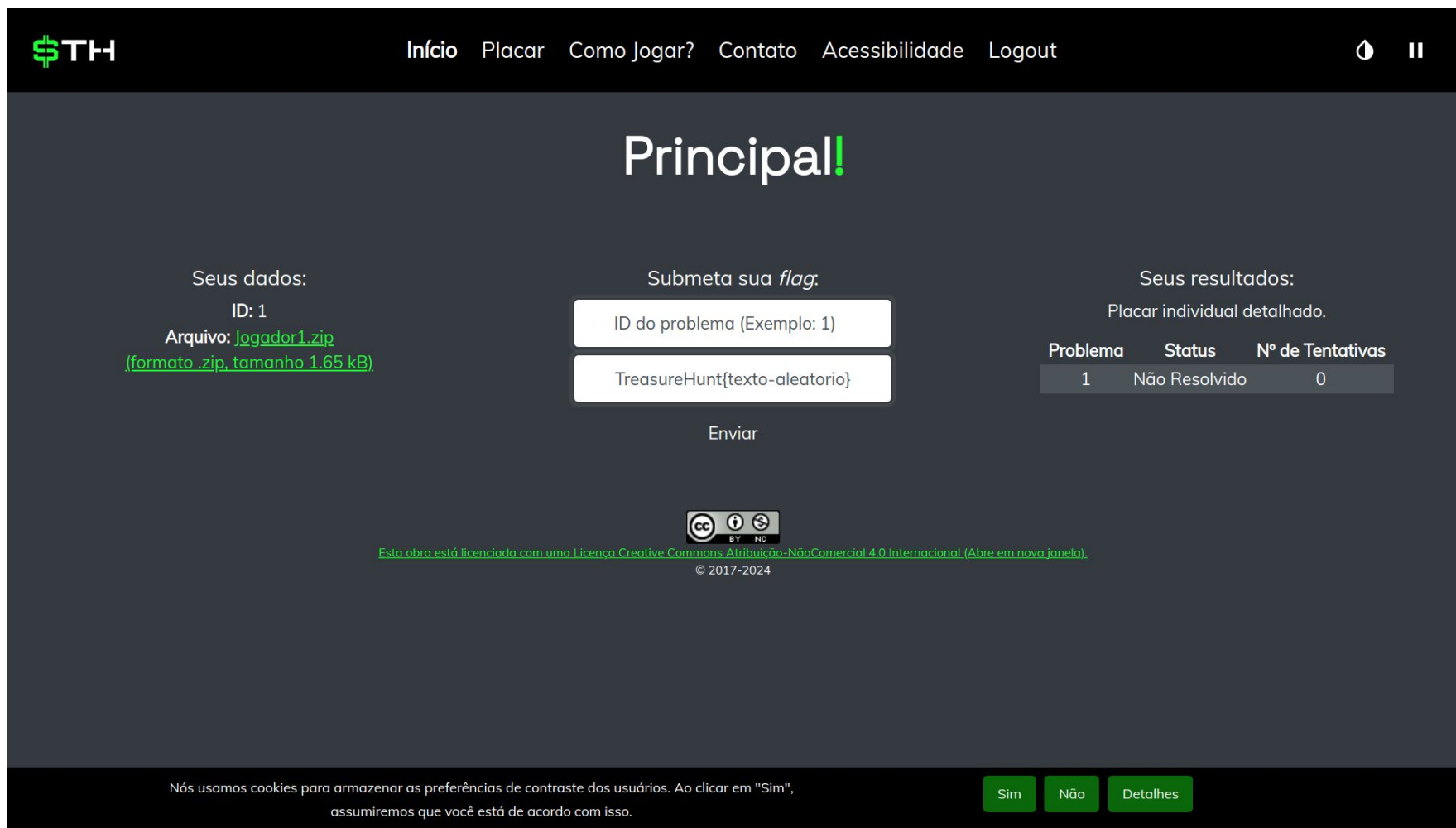
—

UM GERADOR DE COMPETIÇÕES DE CTF

João Vitor Espig
Ricardo de la Rocha Ladeira

- Introdução
- Atividades Realizadas
- Resultados Obtidos
- Considerações finais

- Gerador de competições CTF
- Utilizado no ensino de Segurança Computacional desde 2017
- Tornar o acesso à competição e à área de Segurança mais universal (acessibilidade).
- Realizar uma competição mais segura
(LADEIRA et al., 2020)



The screenshot shows the main interface of the TreasureHunt web application. At the top, there is a navigation bar with links: Início, Placar, Como Jogar?, Contato, Acessibilidade, and Logout. The main heading is "Principal!". Below this, the interface is divided into three sections:

- Seus dados:** ID: 1, Arquivo: [Jogador1.zip](#) (formato .zip, tamanho 1.65 kB).
- Submeta sua flag:** A form with a label "ID do problema (Exemplo: 1)" and a text input field containing "TreasureHunt{texto-aleatorio}". Below the input is an "Enviar" button.
- Seus resultados:** Placar individual detalhado. A table showing the current status:

Problema	Status	Nº de Tentativas
1	Não Resolvido	0

At the bottom, there is a Creative Commons license notice: "Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial 4.0 Internacional (Abre em nova janela)." and a copyright notice "© 2017-2024". A cookie consent banner is also visible at the very bottom, with buttons for "Sim", "Não", and "Detalhes".

Figura: Interface web do jogador. Fonte: Autores

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).

1.4.5 - Imagens de texto [AA] acessar Critério de Sucesso 1.4.5 (em inglês) Perceptível Discernível Qualquer trecho na tela que pode ser exibido em formato de texto estilizado (exemplo: uma citação de uma frase de um autor específico ou um título de seção), não deve ser apresentado em formato de imagem, a não ser que possam ser customizados pela pessoa. Nota: ver junto com critério 1.4.9 (AAA).	1.4.6 - Contraste (melhorado) [AAA] acessar Critério de Sucesso 1.4.6 (em inglês) Perceptível Discernível Textos devem ter uma relação de contraste entre primeiro e segundo plano de ao menos 7:1 (ver critério completo). Nota: caso o tamanho das fontes de textos sejam no mínimo "18pt" ou "14pt bold" a relação de contraste pode ser de 4.5:1.	1.4.7 - Som baixo ou sem som de fundo [AAA] acessar Critério de Sucesso 1.4.7 (em inglês) Perceptível Discernível Qualquer tipo de som que não seja a voz principal em um áudio ou vídeo, deverá ser baixo, inexistente ou ter um tipo de controle simples que possibilite o seu desligamento.	1.4.8 - Apresentação visual [AAA] acessar Critério de Sucesso 1.4.8 (em inglês) Perceptível Discernível Fornecer controles específicos para permitir o controle da apresentação das informações em tela sem comprometer sua legibilidade. Dica: Deve ser possível ajustar cores entre primeiro e segundo plano, manter a largura de parágrafos em até 80 caracteres ou permitir o ajuste de seus espaçamentos.
---	--	---	---

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).

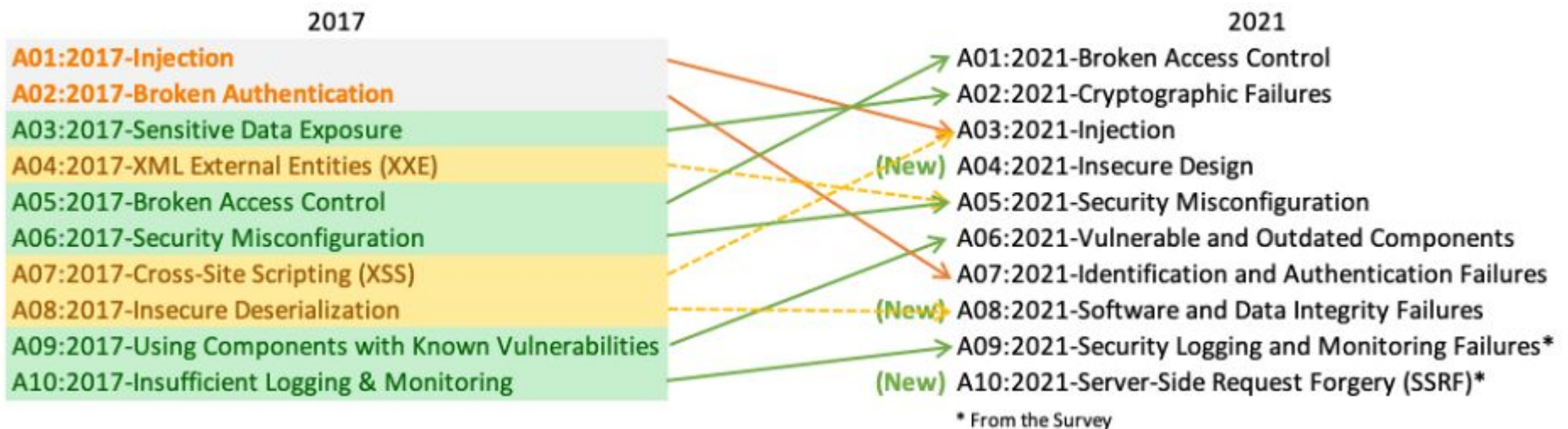
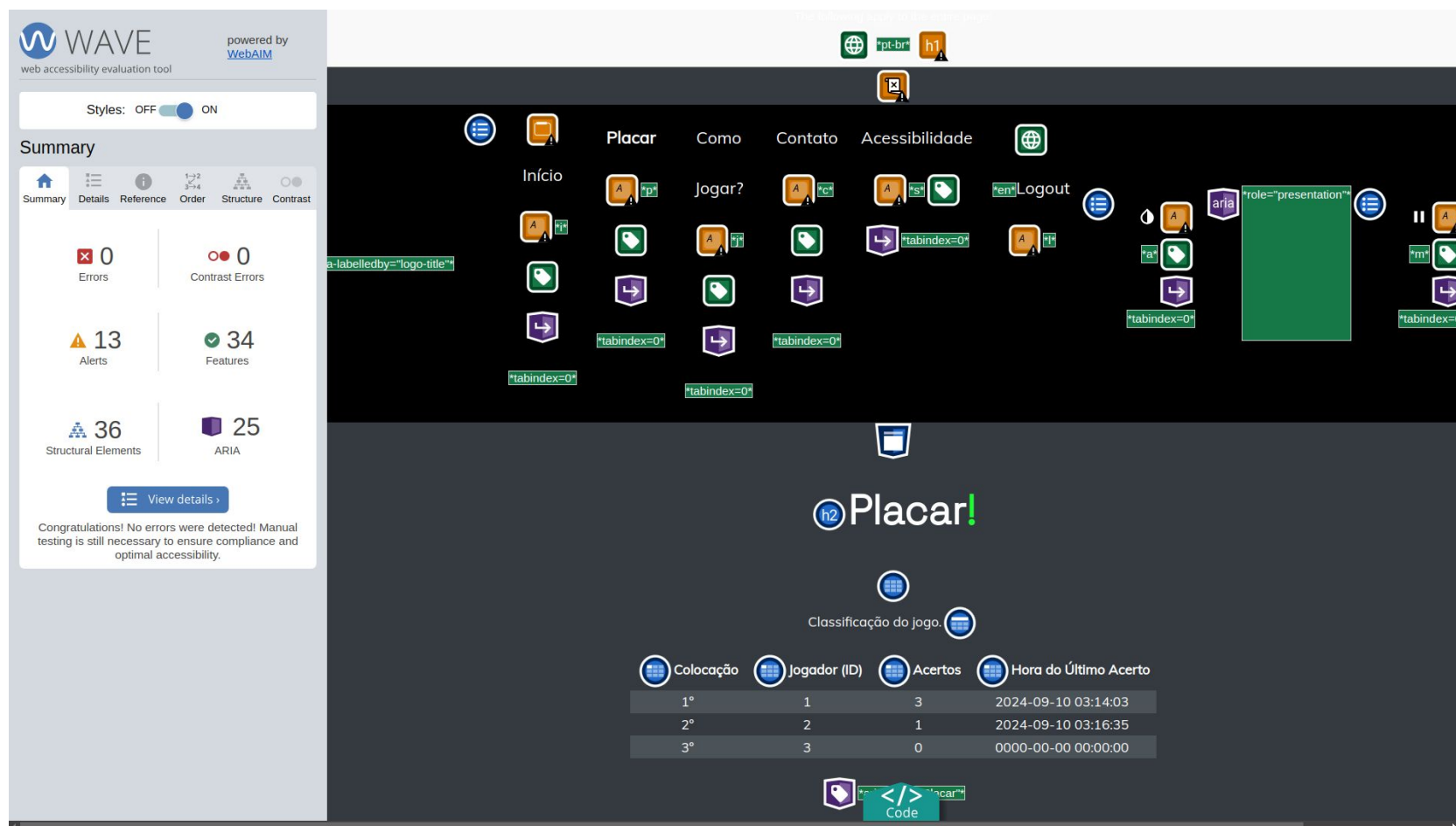


Figura: OWASP Top Ten 2017 e 2021. Fonte: OWASP

- Desenvolver, incrementar e corrigir funcionalidades
- Revisar e cumprir novos critérios de acessibilidade da *WCAG*
- Adoção das diretrizes da *OWASP Top Ten*

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

- Atualização da documentação
- Aplicação da ferramenta *WAVE*
- Aprimoramento do contraste
- Revisão e cumprimento dos critérios de acessibilidade
- Mitigação de ataques e testes de segurança
- Script de finalização de competição



WAVE powered by WebAIM
web accessibility evaluation tool

Styles: OFF ☐ ON

Summary

- Summary Details Reference Order Structure Contrast

0 Errors

0 Contrast Errors

13 Alerts

34 Features

36 Structural Elements

25 ARIA

[View details >](#)

Congratulations! No errors were detected! Manual testing is still necessary to ensure compliance and optimal accessibility.

Placar

Como Contato Acessibilidade

Início

Jogar?

Logout

h2 Placar!

Classificação do jogo.

Colocação	Jogador (ID)	Acertos	Hora do Último Acerto
1°	1	3	2024-09-10 03:14:03
2°	2	1	2024-09-10 03:16:35
3°	3	0	0000-00-00 00:00:00

Code

Figura: Uso do *WAVE* no TreasureHunt. Fonte: Autores

- Identificado pela ferramenta *WAVE*
- Corrigido em todas as páginas
- Razão de contraste: 1.82 para 8.44

TreasureHunt{Security}



TreasureHunt{Security}

Figura: Versão antiga vs. versão nova. Fonte: Autores

- Revisão dos critérios de acessibilidade
- *WCAG* critério 3.3.6
- Última diretriz restante a se aplicar

3.3.6 - Prevenção de erro (todos) [AAA]

[acessar Critério de Sucesso 3.3.6 \(em inglês\)](#)

Compreensível

Assistência a entrada

Deve ser fornecida uma forma de confirmação de dados ou a possibilidade de cancelamento do envio, sempre que campos de formulários exigirem o preenchimento de dados (qualquer tipo de dado).

Nota: ao atender este critério, o critério 3.3.4 (AA) também será atendido.

Fonte: guia-wcag.com

- Mitigação de ataques de injeção de código
- Checklist baseada na *OWASP Top Ten*
- Documento de relatório e análise de segurança
- Testes manuais e automáticos

Atividades: Script de finalização

```
~/dev/TreasureHunt/Jogo/Scripts/Finaliza master
> ./Finaliza.sh
-----
Script de finalização
-----

Este script:
* gerará as estatísticas da competição;
* fará um backup do banco de dados; e
* poderá redefinir as regras de acesso da pasta TreasureHunt no servidor web

Você tem certeza que deseja iniciar esta ação?
Obs.: Certifique-se de ter removido eventuais dados inválidos, tais como submissões realizadas após o tempo
estipulado para a atividade ou de usuários não participantes, tais como o(s) organizador(es).

Sua escolha
1: Sim
2: Não
-----
Digite uma das opções acima: █
```

Figura: Demonstração do uso do script. Fonte: Autores

Resultados Obtidos

- Cumprimento de 100% das diretrizes aplicáveis da *WCAG*
- Ferramenta mais acessível
- Melhor organização na análise de segurança
- Aplicação mais segura

- Os resultados obtidos estão dentro do esperado
- Atividades no momento:
 - Alto contraste no script de finalização
 - Aprimoramento da checklist da *OWASP*
- Trabalhos futuros:
 - Acessibilidade no terminal
 - Manutenção do TreasureHunt

- 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.



MEPEC

Mostra de Ensino, Pesquisa, Extensão e Cidadania

FIM
Dúvidas?