GT-EXSS: um Emulador educativo de ataques de *Cross-Site Scripting* (XSS)

Igor Monteiro Moraes, UFF

Demoday, novembro de 2024

Parceiros

HACKERS DO BEM

Universidade Federal Fluminense

CEFET/RJ

UERJ

UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO

Equipe

Igor Moraes
Professor, UFF
Coordenador

Marcelo Rubinstein
Professor, UERJ
Atualização tecnológica

Ian Bastos
Professor, UERJ
Atualização tecnológica

Dalbert Mascarenhas
Professor, CEFET/RJ
Atualização tecnológica

Isabela Alves
Graduação, CEFET/RJ
Desenvolvedora

Julia Souza
Graduação, CEFET/RJ
Desenvolvedora

Bianca Guarizi
Graduação, CEFET/RJ
Desenvolvedora

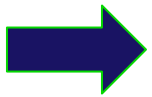
Guilherme Pimentel
Graduação, UFF
Desenvolvedor

João Watanabe
Graduação, UFF
Desenvolvedor

Objetivo

- Desenvolver um emulador de ataques *Cross-Site Scripting* (XSS)
  - Abordagem educacional

- Três pilares do aprendizado
  - Explorar vulnerabilidades
  - Identificar vulnerabilidades
  - Eliminar vulnerabilidades



Ambiente controlado!

70%

das **aplicações Web** são desenvolvidas com **brechas de segurança** severas

CyCognito, 2023

XSS está na OWASP Top 10

CyCognito, 2023

O que é um ataque XSS?

- Um atacante explora vulnerabilidades de sítios Web legítimos
  - Executa de trechos de código maliciosos nos navegadores dos usuários legítimos
  - Campos de sítios Web que permitem a entrada de dados e retornam alguma informação sobre os dados de entrada

Visão geral

- Usuários do emulador realizarão **atividades**
- As atividades são compostas por
  - Uma introdução teórica
  - Procedimentos práticos para realização de testes de exploração e identificação de vulnerabilidade XSS em servidores Web executados em máquinas virtuais
- O usuário é guiado passo-a-passo pelo emulador durante a execução das atividades
- Atividades para **diferentes níveis de conhecimento**

Resultado e público-alvo

- Produto mínimo viável (MVP)
  - Versão do software do emulador composta dos seguintes módulos
    - Interface do usuário
    - Catálogo de atividades
    - Análise de vulnerabilidades
    - Relatório técnico

- Público-alvo
  - Alunos de graduação e profissionais de TI

Oi, eu sou o Hacker Good.
Bem-vindo ao EXSS!

Você sabia que 89% dos funcionários disseram que seriam mais produtivos se o seu trabalho fosse mais gamificado?

2019 Gamification at Work Survey

Iniciante

HACKERS DO BEM

Introdução

XSS Refletido

XSS Armazenado

XSS DOM

11.11%

Pontuação: 10 XP

Logado como usuario

Trocar de Usuário

Olá, usuario!

Meu nome é Hacker Good e estarei te acompanhando nessa jornada!

Iniciante

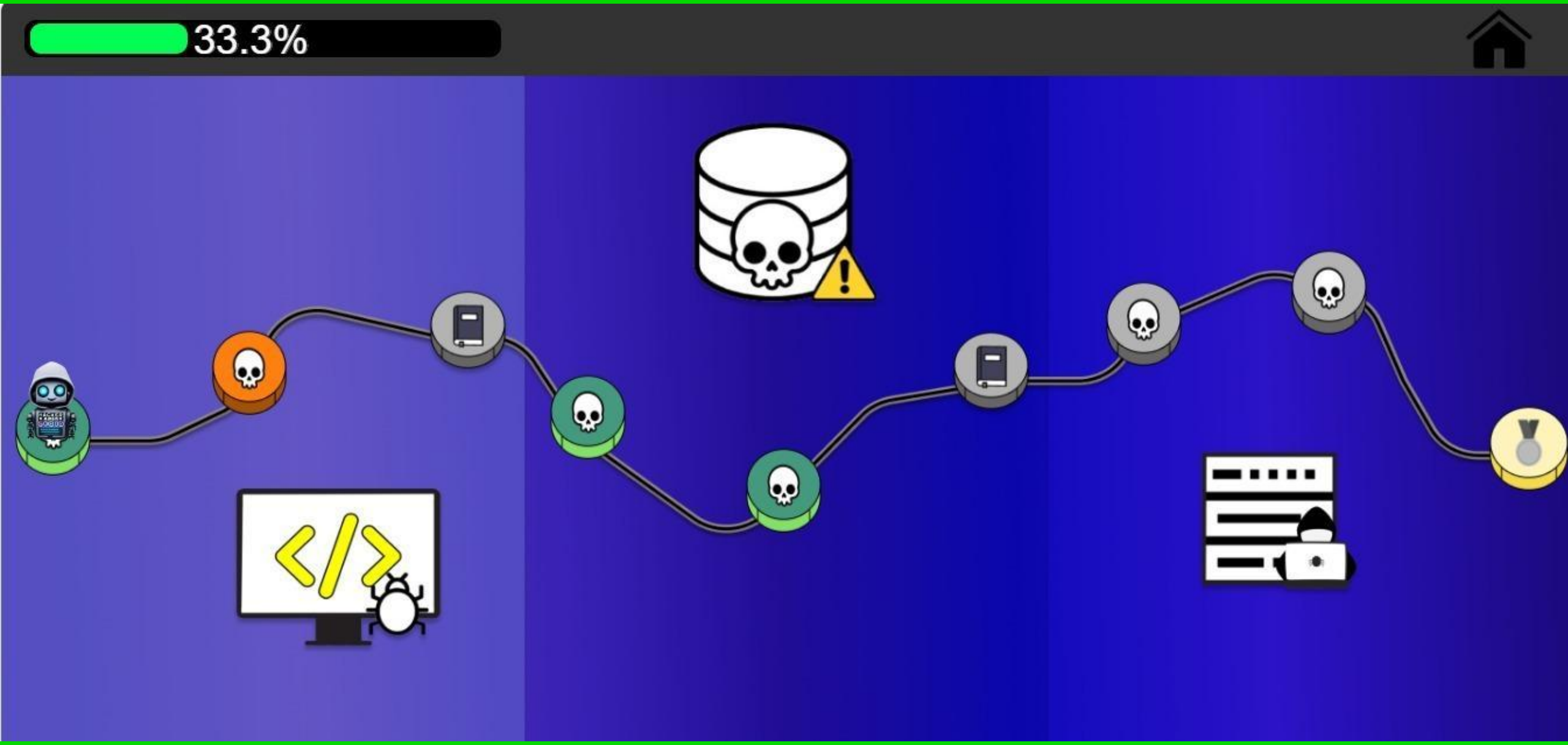
0101
1001

Intermediário

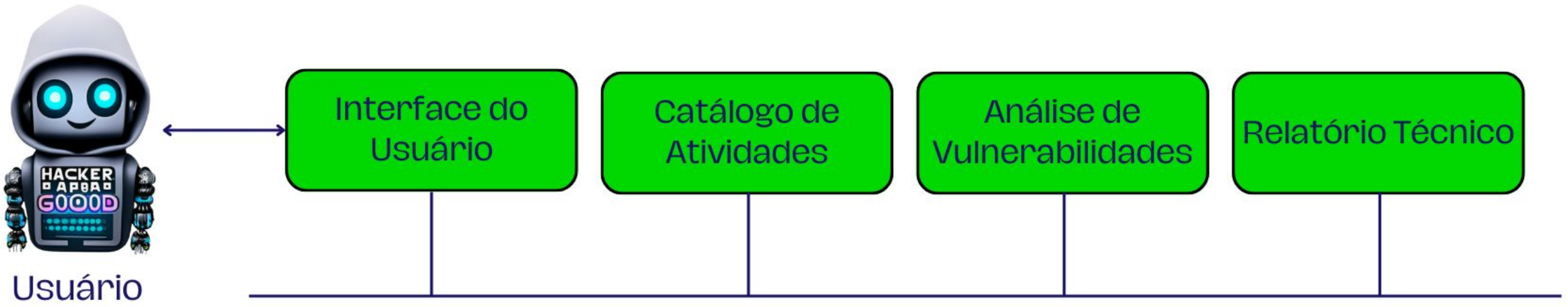
Avançado

Selecione nos botões acima qual nível será acessado.

Os níveis serão desbloqueados a medida que você completar o anterior.


33.3%

Módulos do emulador



Interface do Usuário

- Página principal
- Trilha sequencial de desenvolvimento do aluno
  - O aluno é recompensado com medalhas de conclusão como parte da experiência gamificada
  - Após a finalização de todas as atividades, o aluno receberá um certificado de conclusão
- Aba lateral expansível
  - Navegação do usuário por todas as atividades propostas
  - Cada atividade é composta por diferentes tarefas, desde a leitura de um texto explicativo até a realização de um ataque

Catálogo de Atividades

- É responsável pela definição das atividades
- Cada atividade é composta por uma introdução teórica sobre o assunto da atividade, seguida de procedimentos práticos para realização de testes de vulnerabilidade XSS
- A cada atividade é associado um nível de conhecimento necessário para o usuário realizá-la
  - Básico, intermediário e avançado

Motivação

As aplicações Web são uma parte essencial do dia-a-dia das pessoas. As corporações usam as aplicações Web para aumentar a qualidade dos seus serviços oferecidos e ao mesmo tempo alcançar uma audiência maior através da Internet. No entanto, as vantagens oferecidas pelas aplicações Web também são acompanhadas de riscos para os seus usuários. Informações sensíveis e confidenciais são, geralmente, armazenadas por grandes corporações através de suas aplicações Web, o que as tornam um grande atrativo para ciberataques. Os ataques XSS são um dos tipos de ataque mais frequentemente realizados sobre aplicações.

Este curso apresentará a motivação por trás dos ataques XSS e os seus impactos na sociedade e como o uso das tecnologias contemporâneas para o desenvolvimento de aplicações Web, sem a conscientização voltada para a segurança, contribui para o aumento dos ataques XSS.

O que é um ataque XSS?

Uma aplicação Web é vulnerável a um ataque XSS quando há a possibilidade de inserir código malicioso em sua página Web legítima por não realizar codificação e validação apropriada dos dados fornecidos como entrada. Uma aplicação Web com vulnerabilidades a um ataque XSS está exposta a instalação de malwares, sequestro de sessões, roubo de dados confidenciais e ataques de engenharia social. Os ataques XSS podem ser classificados em três categorias. Confira os detalhes abaixo:

XSS Refletido

Catálogo de Atividades

- Atividade 1: XSS Refletido
- Atividade 2: XSS Armazenado
- Atividade 3: XSS baseado em *Document Object Model* (DOM)
- Atividade 4: Desenvolvimento Seguro

Catálogo de Atividades

- Nível básico
  - Familiarizar os usuários com o emulador e ataques XSS
  - Identificar e compreender as vulnerabilidades de XSS
- Nível intermediário e avançado
  - Experimentar scripts que explorem a vulnerabilidade XSS
  - Aplicar correções nos códigos das páginas

Análise de Vulnerabilidades

- Hospeda sítios Web em uma máquina virtual que executa um servidor Web
  - Ambiente controlado e próximo a um ambiente de produção para aprendizado
- Sítios Web das atividades estão integrados a um pequeno comércio eletrônico desenvolvido para o emulador

Iniciante

HACKERS DO BEM

- Página Inicial
- Introdução
- XSS Refletido
- XSS Armazenado
- XSS DOM

Box Anti Hacker

R$ 50.00

Saiba mais

Cofre de Senhas

R$ 30.00

Saiba mais

Firewall

R$ 40.00

Saiba mais

Relatório Técnico

- É responsável por dar o *feedback* ao usuário sobre a atividade realizada
- Experiência gamificada
  - Pontos de experiência, medalhas e certificado

Para reforçarmos o conteúdo aprendido neste módulo, vamos realizar os exercícios de fixação?

Exercícios de Fixação

1. O que caracteriza um ataque XSS refletido?

- ○ a. A injeção de código malicioso que é armazenado no servidor e executado por qualquer usuário que acessar a página.
- ○ b. A injeção de código malicioso através de um URL que é refletido de volta pelo servidor e executado no navegador do usuário.
- ○ c. A execução de código malicioso diretamente no servidor, comprometendo os dados armazenados.

2. Como o ataque XSS refletido é comumente iniciado?

- ○ a. Enviando um código malicioso diretamente para o servidor através de uma conexão segura.
- ○ b. Inserindo código malicioso em arquivos de configuração do servidor Web.
- ○ c. Induzindo o usuário a clicar em um link contendo um URL malicioso enviado por e-mail, página Web ou outras técnicas de engenharia social.

3. Por que o ataque XSS refletido é considerado não-persistente?

- ○ a. Porque o código malicioso é armazenado permanentemente no servidor.

Ambiente de execução do emulador

- Uso da virtualização é imperativo
  - O emulador tem que ser executado em um ambiente computacional com recursos isolados
    - Atividades práticas que envolvam a exploração de vulnerabilidades não afetem os recursos computacionais de produção

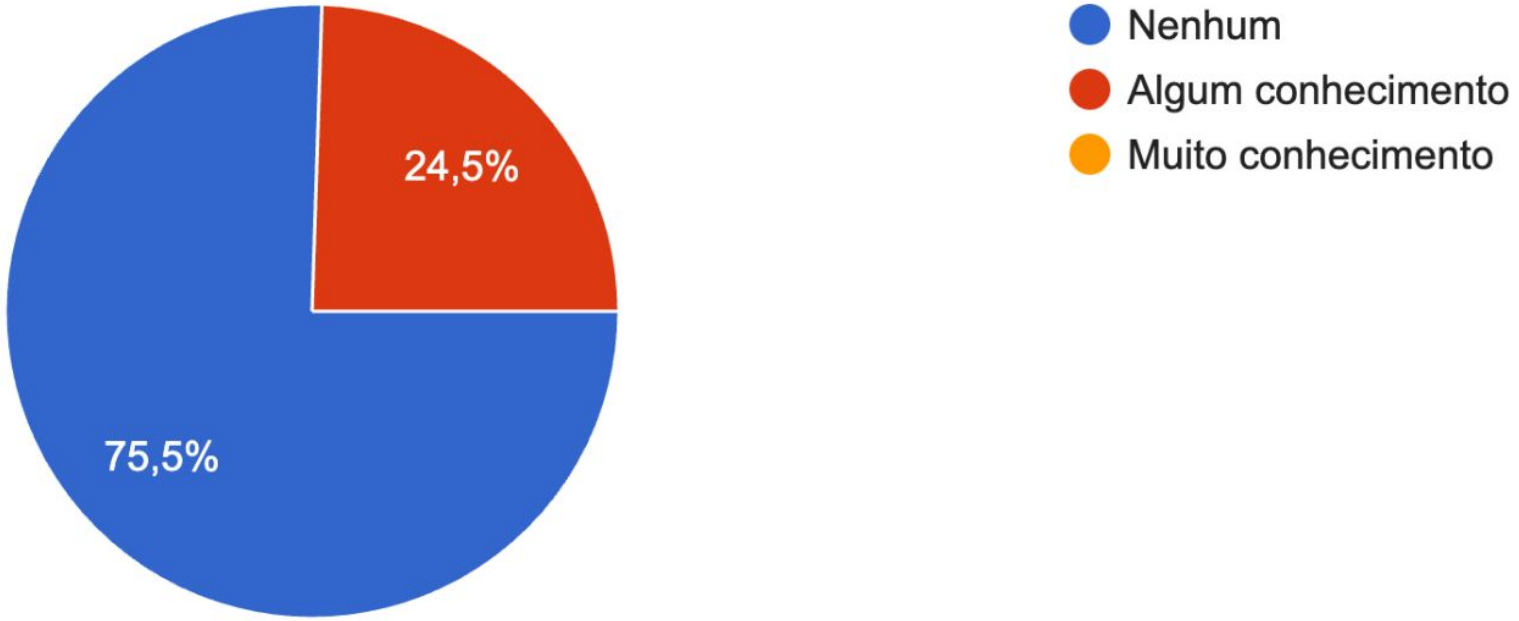
- Máquina virtual: VirtualBox que executa o sistema operacional Ubuntu
  - Facilidade de instalação e uso

Testes de uso

Testes de uso

Qual o seu nível de conhecimento sobre Cross-Site Scripting (XSS) antes do uso do emulador?

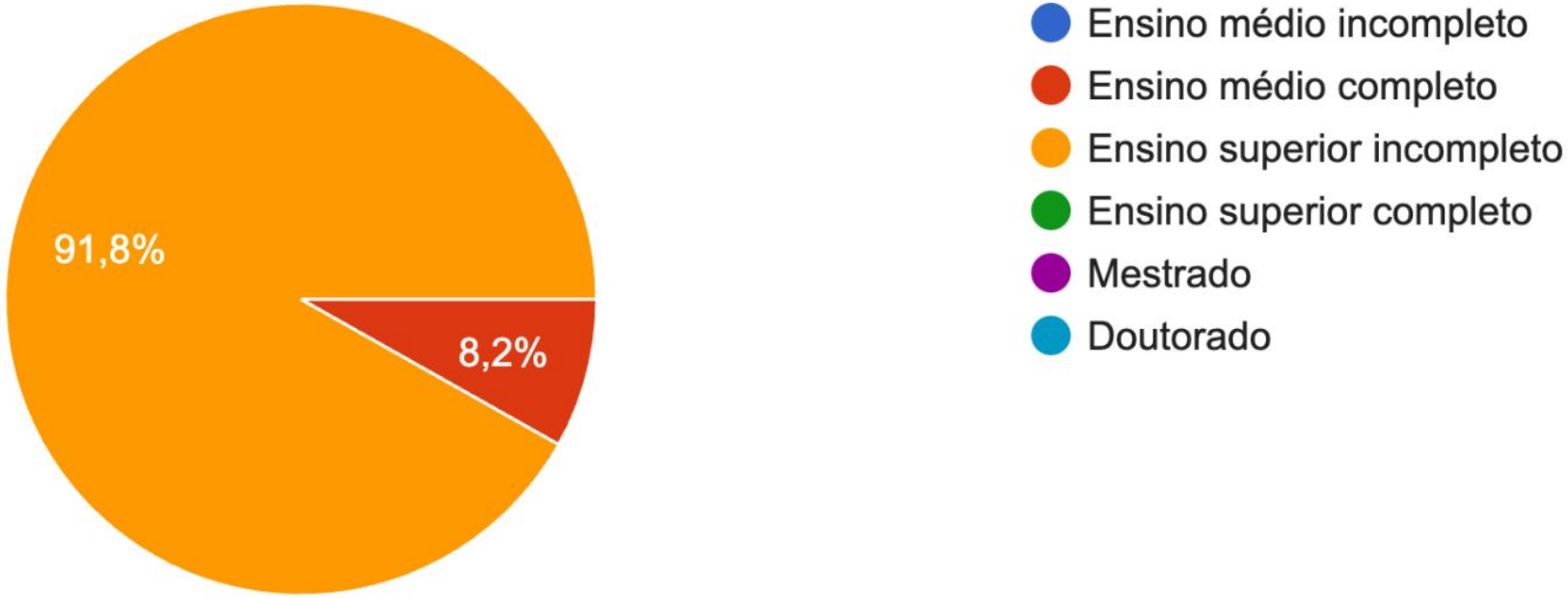
49 respostas



Testes de uso

Qual o seu nível de escolaridade?

49 respostas



Testes de uso

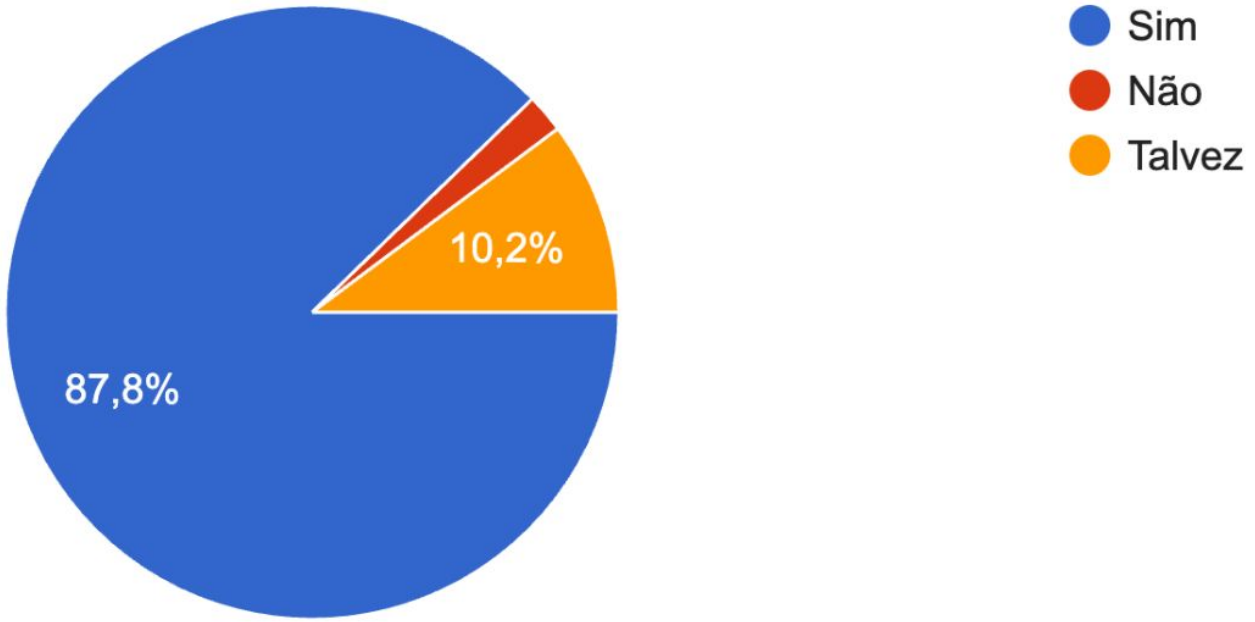
14) Qual o seu nível de satisfação com o nível básico do emulador em termos dos conteúdos teórico e prático sobre XSS?

49 respostas

Testes de uso

13) Você recomendaria este emulador para outras pessoas interessadas em aprender sobre XSS?

49 respostas



Conclusão

- Versão preliminar do MVP disponível para *download* e avaliação
  - Formulário de avaliação construído com ajuda da Wylinka

- Menção honrosa
  - **Entre as três melhores ferramentas** do Salão de Ferramentas do SBSeg 2024

Faça o *download* e avalie nosso emulador!

http://www.midiacom.uff.br/gt-exss

Emulador

Formulário de Avaliação

GT-EXSS: um Emulador educativo de ataques de *Cross-Site Scripting* (XSS)

Igor Monteiro Moraes, UFF

Demoday, novembro de 2024