Um **simulador educativo** e **gamificado** para ensinar sobre um ciberataque frequente na Internet

Qual o tamanho do *déficit* de profissionais em cibersegurança?

85.000.000 até 2030

World Economic Forum

750.000 no Brasil

Fortinet

Loja Hackers do Bem

127.0.0.1/laboratorio/laboratory.php

Iniciante

HACKERS DO BEM

Página Inicial

Trilha de Progresso

Introdução

XSS Refletido

XSS Armazenado

XSS DOM

55.56%

Pontuação: 50 XP

Usuário Convidado

Trocar de Usuário

HACKERS DO BEM

Início Sobre Meus Produtos

Busque por um produto

Confira já o nosso mais novo produto:

BOX ANTIHACKER

Esteja protegido das ameaças de hackers mal intencionados com essa nova solução.

Box Anti Hacker

R$ 50.00

Saiba mais

Cofre de Senhas

R$ 30.00

Saiba mais

Firewall

R$ 40.00

Saiba mais

British Airways is facing a record fine of £183m for last year's breach of its security systems.

The airline, owned by IAG, says it is "surprised and disappointed" by the penalty from the Information Commissioner's Office (ICO).

At the time, BA said hackers had carried out a "sophisticated, malicious criminal attack" on its website.

The ICO said it was the biggest penalty it had handed out and the first to be made public under new rules.

What happened?

The ICO said the incident took place after users of British Airways' website were diverted to a fraudulent site. Through this false site, details of about 500,000 customers were harvested by the attackers, the ICO said.

70%

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

CyCognito, 2023

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

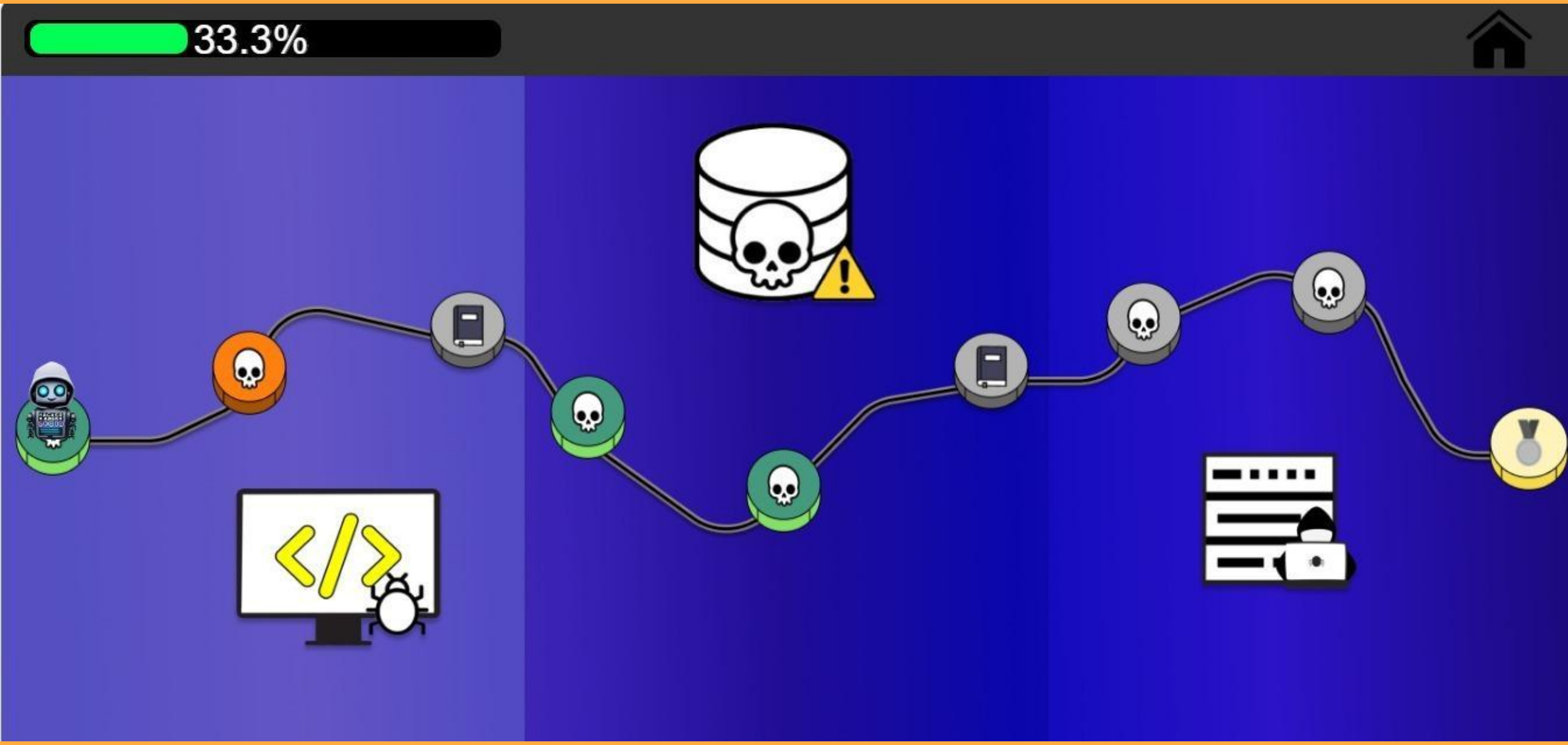
0101
1001

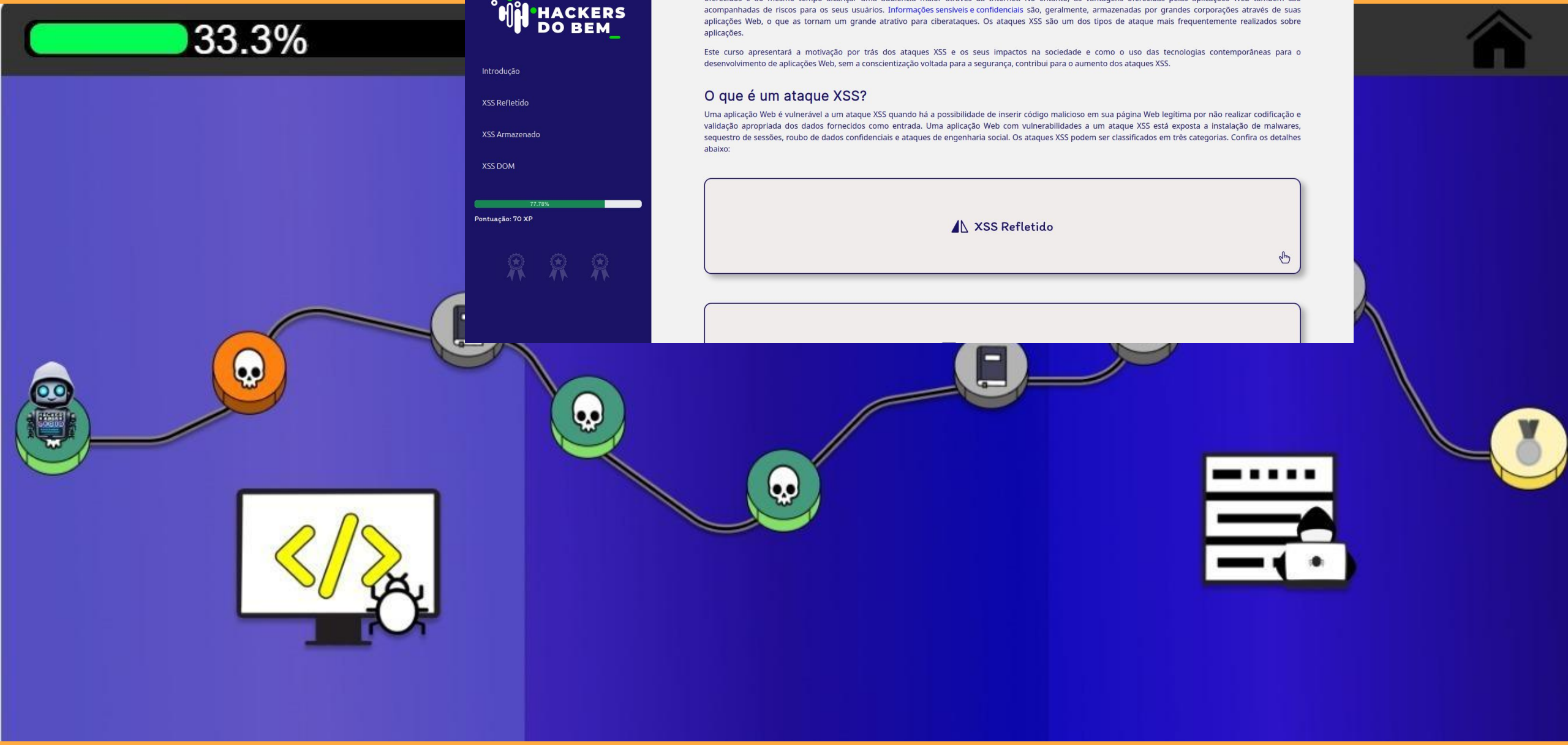
Intermediário

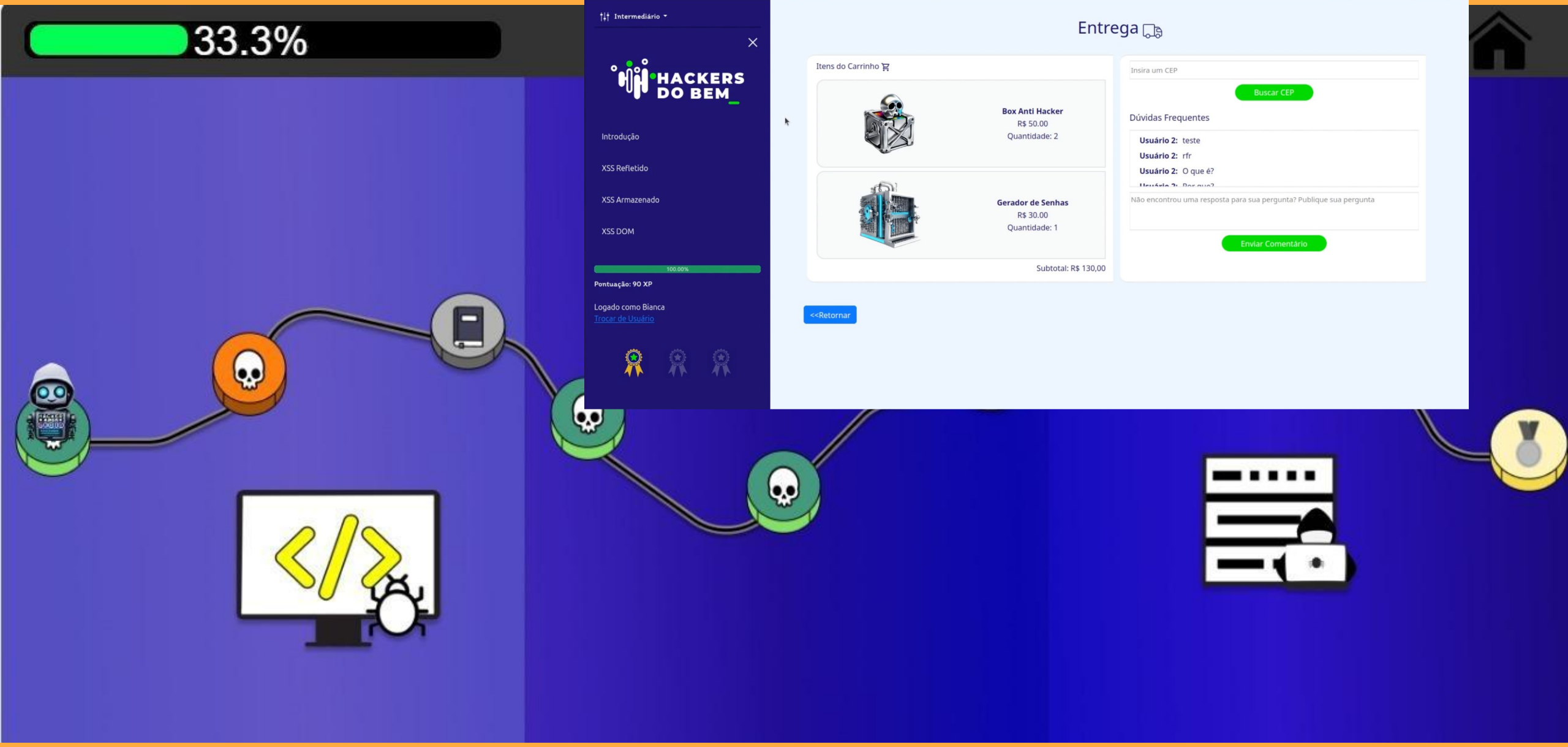
Avançado

Selecione nos botões acima qual nível será acessado.

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


33.3%


33.3%
Iniciante
HACKERS DO BEM
Introdução
XSS Refletido
XSS Armazenado
XSS DOM
77.78%
Pontuação: 70 XP
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


33.3%
Intermediário
HACKERS DO BEM
Introdução
XSS Refletido
XSS Armazenado
XSS DOM
100.00%
Pontuação: 90 XP
Logado como Bianca
Trocar de Usuário
Entrega
Itens do Carrinho
Box Anti Hacker
R$ 50.00
Quantidade: 2
Gerador de Senhas
R$ 30.00
Quantidade: 1
Subtotal: R$ 130,00
<<Retornar
Insira um CEP
Buscar CEP
Dúvidas Frequentes
Usuário 2: teste
Usuário 2: rfr
Usuário 2: O que é?
Não encontrou uma resposta para sua pergunta? Publique sua pergunta
Enviar Comentário

Gerar engajamento para capacitar pessoas em cibersegurança

Objetivos de Desenvolvimento Sustentável 4 e 9

Educação de qualidade

Indústria, inovação e infraestrutura

Quem usa?

Alunos de graduação em ciência da computação e áreas afins e **profissionais de TI**

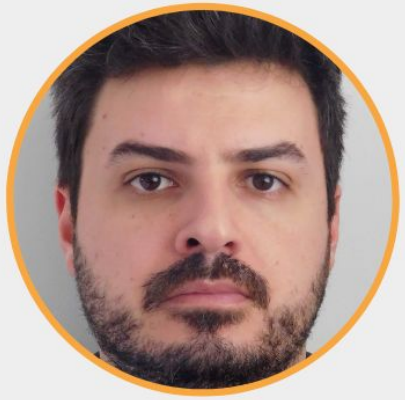
Quem paga?

Empresas e organizações interessadas em capacitar pessoas em cibersegurança

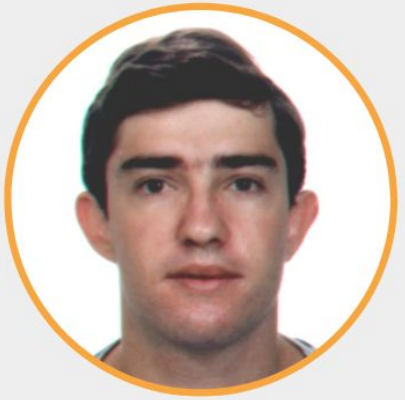
B2B:
financiamento de capacitação

Soluções	Interface do Usuário	Base de Dados	Servidor Web	Atividades	*Feedback* técnico	Suporte para pt-br	Facilidade de instalação	Offline
EXSS	Bootstrap, HTML, CSS, PHP, JS, JQuery	MySQL	Apache 2	Práticas e teóricas	XP, medalhas e certificados e recomendações de contramedidas	**Sim**	Usa uma máquina virtual VirtualBox	**Sim**
Portswigger	Não possui código-fonte aberto			Práticas e teóricas	Solução dos laboratórios de teste	Não	Ferramentas de auxílio a instalação pagas	Não
OWASP Juice Shop	Node.js, Angular, Express, Google Material Design	SQLite, MarsDB	Heroku	Mais práticas	Sistema de pontuação com recompensas	Não	Usa conteinêres Docker	Não
Google XSS Game	Não possui código-fonte aberto			Práticas	Dicas para resolução do problema proposto	Não	Site próprio	Não
OWASP Webgoat	Java, Spring Framework, JSP	Java Database Connectvity	Tomcat	Práticas e teóricas	Recomendações de contramedidas	Sim	Usa conteinêres Docker	Não
TryHackMe	Não possui código-fonte aberto			Práticas e teóricas	Medidas de acompanhamento dos usuários	Não	Usa máquinas virtuais	Não

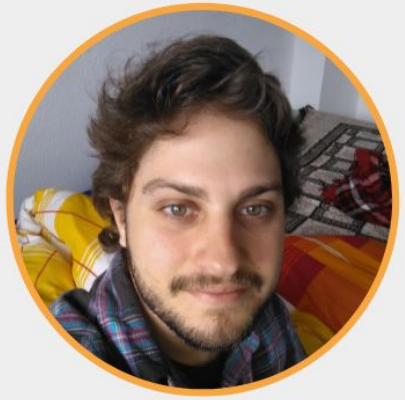
Equipe



Igor Moraes
Professor, UFF
Coordenador



Marcelo Rubinstein
Professor, UERJ
Atualização tecnológica

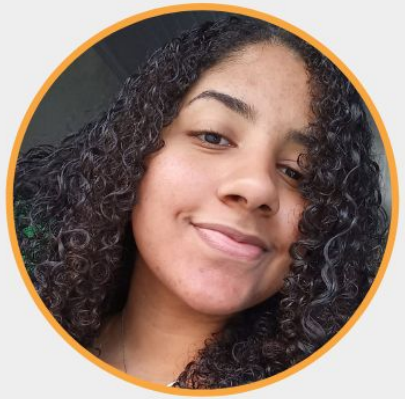


Ian Bastos
Professor, UERJ
Atualização tecnológica

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

SBSeg24
SÃO JOSÉ DOS CAMPOS

Certificamos que o trabalho **"EXSS: Um Emulador Educativo de Ataques Cross-Site Scripting"**, de autoria de Bianca Guarizi (CEFET-RJ), Isabela Alves (CEFET-RJ), Júlia Souza (CEFET-RJ), Guilherme Pimentel (UFF), João Watanabe (UFF), Dalbert Mascarenhas (CEFET-RJ), Ian Vilar Bastos (UERJ), Marcelo Rubinstein (UERJ) e Igor Moraes (UFF) recebeu o prêmio de

MENÇÃO HONROSA

no Salão de Ferramentas (SF) do 24º Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais.

Lourenço Alves Pereira Jr., Ph.D
Coordenador Geral
Instituto Tecnológico de Aeronáutica

Diego Kreutz, Ph.D
Coordenador Geral
Universidade Federal do Pampa

Faça o *download* e avalie nosso simulador!

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