UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

MATHEUS SYDOR

OWNEDBOX: UMA PLATAFORMA DE ENSINO PARA SEGURANÇA WEB OFENSIVA E DEFENSIVA

GUARAPUAVA

2025

MATHEUS SYDOR

OWNEDBOX: UMA PLATAFORMA DE ENSINO PARA SEGURANÇA WEB OFENSIVA E DEFENSIVA

OwnedBox: A Teaching Platform for Offensive and Defensive Web Security

Proposta de Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Técnologo em Tecnologia em Sistemas para Internet do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Roni Fabio Banaszewski

GUARAPUAVA

2025

4.0 Internacional

Esta licença permite compartilhamento, remixe, adaptação e criação a partir do trabalho, mesmo para fins comerciais, desde que sejam atribuídos créditos ao(s) autor(es). Conteúdos elaborados por terceiros, citados e referenciados nesta obra não são cobertos pela licença.

LISTA DE ABREVIATURAS E SIGLAS

Siglas

MVP	*Produto Mínimo Viável, do inglês Minimum Viable Product*
TCC	*Trabalho de conclusão de curso*

SUMÁRIO

1 INTRODUÇÃO 3

1.1 Considerações iniciais 3

1.2 Objetivos 4

1.2.1 Objetivo geral 4

2 TRABALHOS RELACIONADOS 5

3 PROPOSTA 6

3.1 Perfis de usuários 6

3.2 Funcionalidades Essenciais 6

4 CONSIDERAÇÕES FINAIS 8

REFERÊNCIAS 9

1 INTRODUÇÃO

Este trabalho tem como objetivo principal apresentar a proposta de *Trabalho de conclusão de curso* (TCC) que pretende abordar as principais vulnerabilidades web e o desenvolvimento de um sistema web de aprendizado na área de cibersegurança ofensiva e defensiva.

O sistema proposto tem como objetivo criar um ambiente virtual para que estudantes e entusiastas de área da segurança digital possam aprender e testar suas habilidades.

1.1 Considerações iniciais

A segurança da informação tem se consolidado, nas últimas décadas, como um dos pilares das empresas, governos e sociedade em um mundo cada vez mais conectado com o meio digital. Quando surgiu a ARPANET, no final da década de 1960, inicialmente desenvolvida para fins militares, até a sua popularidade comercial na década de 1990, o meio digital trouxe inúmeros benefícios para a população, mas também abriu espaço para a proliferação de ameaças cibernéticas (CASTELLS, 2003). A popularização da World Wide Web, junto ao crescimento do comércio eletrônico e das redes sociais, ampliou consideravelmente os vetores de ataque, fazendo com que a cibersegurança tenha se tornado uma área estratégica para organizações e indivíduos (STALLINGS, 2019)

Por volta de 1980 já existiam estudos e a difusão dos primeiros vírus e softwares maliciosos, impulsionando o surgimento dos antivírus comerciais. Nos anos de 1990 e 2000, as ameaças começaram a evoluir, ataques direcionados a sistemas corporativos, bancos de dados sensíveis e infraestruturas críticas passaram a ser visados por cibercriminosos (KASPERSKY, 2020). Com isso, surgiram formas de prevenir e remediar essas vulnerabilidades, surgiram ferramentas como firewalls, sistemas de detecção e prevenção de intrusão, além de leis cada vez mais rígidas, como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e, no Brasil, a Lei Geral de Proteção de Dados (LGPD) que reforçam a necessidade de proteger o sistema e seus usuários (União Europeia, 2016; BRASIL, 2018).

Nos dias de hoje, fatores como a popularização da Internet das Coisas (IoT) e o cenário da segurança da informação se tornaram cada vez mais importantes. Impulsionada pela pandemia de COVID-19, desencadeou-se a tendência do trabalho remoto e do comércio online. A proteção de dados tornou-se cada vez mais importante para indivíduos, empresas e governos. Relatórios como OWASP Top Ten (OWASP Foundation, 2021) evidenciam que vulnerabilidades como SQL Injection, Cross-Site Scripting (XSS) e upload de arquivos maliciosos permanecem entre as mais exploradas em ataques reais, reforçando a necessidade de mecanismos eficazes de prevenção e mitigação.

Empresas recorrem ao **teste de penetração** (pentest), um teste de segurança cibernética que tem como principal objetivo simular um ataque para encontrar vulnerabilidades em um sistema. Este teste é feito de maneira legal e com contrato, garantindo que nenhuma vulnerabi-

lidade explorada causará danos para os clientes da empresa e garantindo que o sistema está seguro (IBM, 2025). Além disso, a prática possui caráter educacional, sendo replicada em laboratórios controlados e plataformas específicas que oferecem ambientes seguros e éticos para estudantes e profissionais desenvolverem suas habilidades. Dessa forma, é possível praticar técnicas ofensivas sem riscos jurídicos ou danos a sistemas de terceiros, em conformidade com o Marco Civil da Internet e a Lei Carolina Dieckmann (BRASIL, 2014; BRASIL, 2012).

Existem diversas iniciativas internacionais, como as plataformas Hack The Box (HTB) e TryHackMe, que têm desempenhado um papel importante no ensino de segurança ofensiva e defensiva. No entanto, essas ferramentas apresentam barreiras relacionadas ao idioma, custos de acesso e falta de contextualização com a realidade brasileira. Além disso, são direcionadas prioritariamente ao mercado global, o que reforça a carência, no Brasil, de soluções didáticas acessíveis, em português, capazes de facilitar o aprendizado individual e de atender tanto a ambientes acadêmicos quanto corporativos.

Devido a isso, é importante investir em metodologias inovadoras de ensino em cibersegurança. A segurança digital não é somente um diferencial competitivo entre as empresas, mas uma necessidade. Laboratórios controlados podem ajudar estudantes, entusiastas e profissionais a entenderem as técnicas ofensivas de exploração de vulnerabilidades, e ao mesmo tempo permiti-los a desenvolver habilidades defensivas para proteger sistemas. Tendo isso em vista, a OwnedBox será desenvolvida como uma solução gratuita e de código aberto, voltada ao aprendizado e à capacitação de profissionais em cibersegurança ofensiva. A plataforma permitirá que instituições de ensino e organizações adaptem os laboratórios às suas necessidades específicas e colaborem com a evolução da aplicação web.

1.2 Objetivos

Nesta seção será apresentado o objetivo geral deste trabalho.

1.2.1 Objetivo geral

Desenvolver uma aplicação web denominada **OwnedBox**, que funcione como um laboratório de ensino em cibersegurança ofensiva e defensiva, possibilitando a exploração prática de vulnerabilidades web comuns em um ambiente controlado, seguro e didático.

2 TRABALHOS RELACIONADOS

Existem diversas plataformas voltadas para o ensino de segurança da informação, inclusive no âmbito ofensivo. Essas ferramentas permitem que estudantes tenham acesso a ambientes simulados para a exploração de vulnerabilidades. No entanto, apresentam barreiras como idioma, custo ou dificuldade de adaptação ao contexto acadêmico brasileiro. Nesse cenário, destacam-se algumas soluções bastante populares, cujas características, pontos positivos e limitações justificam a necessidade e a proposta da plataforma **OwnedBox**.

Entre as plataformas existentes, uma das mais reconhecidas no ramo de segurança ofensiva é o **Hack The Box**. Criado em 2017, o qual disponibiliza laboratórios que simulam diferentes tipos de vulnerabilidades e níveis de dificuldade, oferecendo aos alunos a oportunidade de praticar técnicas de exploração em um ambiente controlado e constantemente atualizado (Hack The Box Ltd., 2025). Outra iniciativa relevante é o **TryHackMe**, que se destaca pelo foco em atividades do tipo *Capture The Flag* (CTF), modalidade competitiva em que os participantes exploram falhas em laboratórios virtuais para conquistar pontos e melhorar sua posição em rankings globais (TRYHACKME, 2025).

Além dessas plataformas, é importante citar também o **Damn Vulnerable Web Application** (DVWA), uma aplicação web desenvolvida intencionalmente com vulnerabilidades para fins educacionais. O DVWA é amplamente utilizado em cursos de segurança ofensiva, pois permite que os estudantes treinem em um ambiente simples, acessível e adequado para o aprendizado progressivo de conceitos e técnicas fundamentais da área (RandomStorm, 2025).

Assim, observa-se que, embora existam diversas iniciativas internacionais, há carência de soluções em língua portuguesa, gratuitas e com foco didático-acadêmico no contexto brasileiro, justificando a proposta da OwnedBox.

3 PROPOSTA

Este trabalho propõe o desenvolvimento da aplicação web **OwnedBox**, um ambiente de ensino gratuito de código aberto voltado para a prática de segurança web ofensiva e defensiva. O sistema será disponibilizado como um **protótipo funcional *Produto Mínimo Viável, do inglês Minimum Viable Product* (MVP)**, contemplando três vulnerabilidades web entre as mais recorrentes segundo o OWASP Top 10 (OWASP Foundation, 2021): *SQL Injection*, *Cross-Site Scripting* e *upload de arquivos maliciosos*. Cada vulnerabilidade será apresentada em um módulo específico, permitindo que o estudante explore a falha ofensivamente, receba um **token de validação** ao concluir o desafio e, em seguida, visualize contramedidas defensivas que demonstrem como corrigir o problema.

A aplicação será distribuída como **código aberto no GitHub**, acompanhada de *snapshots* das máquinas de laboratório, possibilitando que qualquer usuário instale o sistema em seu próprio ambiente local ou servidor. Para viabilizar essa instalação, será incluída uma **página de instruções com os requisitos necessários**, de modo a facilitar a configuração mesmo por usuários com pouca experiência em implantação de aplicações web. Essa escolha elimina a necessidade de manter a plataforma publicada em um domínio público, reduz riscos de segurança e reforça o caráter acadêmico e didático do projeto.

Por se tratar de um projeto de **código aberto**, os utilizadores poderão contribuir ativamente com a evolução da aplicação, propondo melhorias, corrigindo falhas e desenvolvendo **laboratórios personalizados** que atendam a demandas específicas. Essa abertura à colaboração amplia o potencial educacional da plataforma, tornando-a um recurso dinâmico e em constante aperfeiçoamento pela comunidade.

Além disso, a aplicação contará com uma **página de estatísticas do usuário**, no qual será possível acompanhar o progresso individual, visualizar os tokens coletados e obter uma visão clara do desempenho durante os estudos.

3.1 Perfis de usuários

A aplicação web contempla, nesta etapa de desenvolvimento, apenas um perfil de usuário: o **Estudante** (ou Usuário Comum). Esse perfil é responsável por realizar o cadastro e autenticação na plataforma, acessar os módulos de aprendizado, explorar as vulnerabilidades simuladas e visualizar os tokens de validação obtidos ao concluir os desafios propostos.

3.2 Funcionalidades Essenciais

As funcionalidades descritas a seguir representam os requisitos essenciais definidos para a aplicação web **OwnedBox**. Cada funcionalidade está apresentada no formato de História

de Usuário, identificada por um código no padrão HUxx (História de Usuário), como HU01, HU02, HU03, e assim por diante, o que possibilita uma melhor organização e referência ao longo do trabalho.

- **HU01**: Como um usuário, quero realizar meu cadastro informando dados básicos (nome, e-mail e senha), para que eu possa acessar a aplicação web e participar dos módulos de aprendizado.
- **HU02**: Como **usuário cadastrado**, quero **efetuar login com minhas credenciais**, para **acessar meu perfil e os módulos de aprendizado**.
- **HU03**: Como **usuário autenticado**, quero **acessar meu perfil com informações de desempenho**, para **acompanhar meu progresso na aplicação web**.
- **HU04**: Como **estudante de cibersegurança**, quero **acessar laboratórios com vulnerabilidades simuladas**, para **praticar técnicas ofensivas em ambiente controlado**.
- **HU05**: Como **usuário da aplicação web**, quero **visualizar contramedidas para cada vulnerabilidade**, para **aprender como corrigir falhas e aplicar boas práticas defensivas**.
- **HU06**: Como **usuário que conclui um desafio**, quero **receber um token de validação**, para **comprovar que atingi o objetivo proposto**.
- **HU07**: Como **usuário da plataforma**, quero **acessar relatórios de desempenho**, para **acompanhar minha evolução ao longo do tempo**.
- **HU08**: Como **usuário da OwnedBox**, quero **ter garantia de que meus dados estão protegidos**, para **utilizar a aplicação web sem riscos**.
- **HU9**: Como **usuário**, quero ter acesso a uma página com instruções de instalação e requisitos do sistema, para que eu consiga configurar a aplicação web corretamente em meu ambiente local.

4 CONSIDERAÇÕES FINAIS

A crescente complexidade dos sistemas digitais e a intensificação dos ataques cibernéticos tornam indispensável a adoção de práticas avançadas de segurança da informação. Nesse contexto, o Pentest consolida-se como uma estratégia essencial para identificar vulnerabilidades e fortalecer defesas, desde que conduzido de forma ética, legal e controlada.

A disponibilidade de laboratórios virtuais e plataformas específicas, como ambientes de treinamento e aplicações vulneráveis intencionalmente, possibilita que estudantes, pesquisadores e profissionais desenvolvam suas habilidades sem infringir a legislação vigente. Dessa maneira, a formação prática em cibersegurança não apenas contribui para a capacitação técnica, mas também promove uma cultura de responsabilidade e conformidade legal.

Neste contexto, foi apresentada a proposta da plataforma OwnedBox, que busca oferecer um espaço controlado para o aprendizado prático em segurança web. Por meio de módulos que simulam vulnerabilidades comuns, como SQL Injection, Cross-Site Scripting (XSS) e Upload de Arquivos Maliciosos, onde os usuários poderão exercitar técnicas ofensivas, receber tokens de validação como comprovação de suas conquistas e, em seguida, compreender contramedidas defensivas aplicáveis. A OwnedBox pretende se apresentar como uma alternativa didática em potencial, capaz de apoiar a formação de profissionais mais preparados para lidar com os desafios de um cenário digital em constante transformação.

REFERÊNCIAS

BRASIL. **Lei n.º 12.737, de 30 de novembro de 2012 - Lei Carolina Dieckmann**. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 08 set. 2025.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014 - Marco Civil da Internet**. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 set. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD)**. 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 set. 2025.

CASTELLS, M. **A Galáxia da Internet: Reflexões sobre a Internet, os Negócios e a Sociedade**. Rio de Janeiro: Jorge Zahar Editor, 2003. Tradução de *La Galaxia Internet* (2001). ISBN 9788571107403.

Hack The Box Ltd. **Hack The Box**. 2025. https://www.hackthebox.com/. [Acesso em: 2025-09-09].

IBM. **O que é um teste de penetração (pentest)?** 2025. Acesso em: 08 set. 2025. Disponível em: https://www.ibm.com/br-pt/think/topics/penetration-testing.

KASPERSKY. **A Brief History of Computer Viruses What the Future Holds**. 2020. Acesso em: 08 set. 2025. Disponível em: https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds.

OWASP Foundation. **OWASP Top 10: The Ten Most Critical Web Application Security Risks**. 2021. https://owasp.org/Top10/. Acesso em: 11 set. 2025.

RandomStorm. **Damn Vulnerable Web Application (DVWA)**. 2025. https://github.com/digininja/DVWA. [Acesso em: 2025-09-09].

STALLINGS, W. **Cryptography and Network Security: Principles and Practice, 8th edition**. [*S.l.*]: Pearson, 2019. 832 p.

TRYHACKME. **TryHackMe - Plataforma de Aprendizado em Segurança Cibernética**. 2025. Acesso em: 08 set. 2025. Disponível em: https://tryhackme.com/.

União Europeia. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - Regulamento Geral de Proteção de Dados (GDPR)**. 2016. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 08 set. 2025.