EXSS: Um Emulador Educativo de Ataques *Cross-Site Scripting*

Bianca Domingos Guarizi[1], Isabela Maira Mendite Alves[1], Júlia Abbud Fernandez e Souza[1], Guilherme Oliveira Pimentel[2], João André Campos Watanabe[2], Dalbert Matos Mascarenhas[1], Ian Vilar Bastos[3], Marcelo Gonçalves Rubinstein[3], Igor Monteiro Moraes[2]

[1]Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ
Petrópolis - RJ - Brasil

[2]Laboratório MidiaCom – IC/TCC/PGC
Universidade Federal Fluminense (UFF), Niterói – RJ – Brasil

[3]Universidade do Estado do Rio de Janeiro (UERJ) – Rio de Janeiro, RJ, Brasil

{bianca.guarizi,isabela.alves,julia.fernandez}@aluno.cefet-rj.br,
{guilherme_pimentel,jwatanabe}@id.uff.br, dalbert.mascarenhas@cefet-rj.br,
ian.bastos@eng.uerj.br, rubi@uerj.br, igor@ic.uff.br

Abstract. *This paper proposes an emulator for Cross-Site Scripting (XSS) attacks for learning in cybersecurity. The emulator allows users to identify websites vulnerable to XSS attacks in a controlled environment. The identification of vulnerabilities is achieved through activities that consist of a theoretical introduction to the topic, followed by practical procedures for conducting XSS vulnerability tests on a web server running on a virtual machine. Activities are developed for different levels of knowledge. The particularity of the proposed emulator is its educational approach, and its goal is to raise awareness among undergraduate students and professionals to develop less vulnerable websites.*

Resumo. *Este artigo propõe um emulador de ataques* Cross-Site Scripting *(XSS) para o aprendizado em cibersegurança. O emulador permite que usuários identifiquem sítios Web vulneráveis a ataques XSS em um ambiente controlado. A identificação de vulnerabilidades se dá pela realização de atividades que são compostas por uma introdução teórica sobre o assunto da atividade, seguida de procedimentos práticos para a realização de testes de vulnerabilidade XSS em um servidor Web executado em uma máquina virtual. São desenvolvidas atividades para diferentes níveis de conhecimento. A particularidade do emulador proposto é a sua abordagem educativa e seu objetivo é conscientizar alunos de graduação e profissionais a desenvolver sítios Web menos vulneráveis.*

1. Introdução

Um relatório produzido pela CyCognito [CyCognito, 2023] mostra que 70% das aplicações Web são desenvolvidas com brechas de segurança severas e que 30% estão vulneráveis a alguma das 10 categorias de ataques mais realizados e identificados pela *Open Worldwide Application Security Project* (OWASP) [OWASP, 2021]. Dentre os ataques mais realizados, encontra-se o *Cross-Site Scripting* (XSS) [Grossman, 2007, Gupta e Gupta, 2017, Rodríguez et al., 2020, Liu et al., 2019]. O ataque XSS explora

campos de entrada de dados para inserir conteúdos não-confiáveis em uma aplicação Web legítima, na qual não há uma codificação ou validação apropriada das entradas de dados fornecidas [Kaur et al., 2023]. O ataque XSS é um dos principais responsáveis pelo roubo e violação de dados privados em grandes organizações. Em 2018, a empresa aérea British Airways sofreu um roubo de aproximadamente 380.000 registros devido a uma vulnerabilidade XSS em seu módulo de pagamento [Reuters, 2018, BBC, 2018].

Os ataques XSS podem ser classificados em três categorias: (i) XSS refletido ou não-persistente; (ii) XSS armazenado ou persistente; (iii) XSS baseado no modelo de documento por objetos (*Document Object Model* - DOM). No ataque XSS refletido, o atacante gera um *Uniform Resource Locator* (URL) que contém um código malicioso, como parte da requisição HTTP. O código malicioso é inserido em campos de entrada da aplicação Web, como barras de busca, seções de comentários e caixas de texto de autenticação. Ao receber um URL da página Web servida e executá-la em seu navegador, o usuário legítimo executa um código malicioso presente no URL que foi enviado pelo atacante. No XSS armazenado, o atacante gera um código malicioso que é armazenado persistentemente em um servidor vulnerável, geralmente através de um banco de dados. Um exemplo deste tipo de ataque pode ser encontrado em aplicações Web que servem como fóruns de discussão ou redes sociais. Este tipo de ataque não necessita um URL para que seja executado e pode afetar um número maior de usuários, visto que qualquer usuário que navegue pela aplicação Web poderá executar o código malicioso servido pela página comprometida. No XSS baseado em DOM, o atacante também usa um URL para inserir o código malicioso. Entretanto, o URL neste tipo de ataque altera dinamicamente a estrutura dos objetos que compõem a página HTML para inserir duas novas estruturas, uma fonte e um sorvedouro. A estrutura de objetos alterada na página HTML só ocorre no momento que a página é processada pelo navegador do usuário legítimo, sem que o servidor da página HTML esteja ciente da modificação. Com a página Web alterada, o elemento fonte inserido recupera informações sensíveis do usuário legítimo e as direciona ao elemento sorvedouro, no qual o atacante coleta as informações sensíveis.

Este artigo propõe um emulador de ataques XSS para promover a conscientização e o aprendizado prático na área de cibersegurança. O emulador proposto, chamado de EXSS, permite que usuários identifiquem sítios Web vulneráveis a ataques XSS em um ambiente controlado. A identificação de vulnerabilidades se dá através da realização de atividades pelos usuários, visto que o principal objetivo do emulador proposto reside em fornecer uma abordagem educacional para lidar com os ataques XSS. As atividades são compostas por uma introdução teórica sobre o assunto da atividade, seguida de procedimentos práticos para a realização de testes de vulnerabilidade XSS em um servidor Web executado em uma máquina virtual. Os ambientes de laboratório emulam um pequeno *e-commerce* que contém vulnerabilidades a serem exploradas. Desse modo, os usuários verificam a existência de vulnerabilidades fazendo testes de inserção de caracteres e *scripts*. O usuário é guiado passo-a-passo pelo emulador durante a execução desses testes. São definidas atividades para diferentes níveis de conhecimento que abordam os três tipos de ataques XSS. O diferencial do emulador proposto é ser totalmente gratuito, executar sem necessidade de acesso à Internet e ter suporte ao português. O EXSS está sendo desenvolvido no contexto dos Grupos de Trabalho do Programa Hackers do Bem.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta a

arquitetura do emulador proposto, citando as tecnologias escolhidas para implementação dos módulos que compõem tal arquitetura. A Seção 3 descreve as funcionalidades do emulador proposto e a demonstração a ser realizada. A Seção 4 descreve ferramentas similares ao emulador proposto. A Seção 5 conclui o artigo e destaca implicações e recomendações estratégicas para o emulador proposto.

2. A Arquitetura do Emulador EXSS

O emulador EXSS possui quatro módulos, como ilustra a Figura 1: Interface do Usuário, Catálogo de Atividades, Análise de Vulnerabilidades e Relatório Técnico.

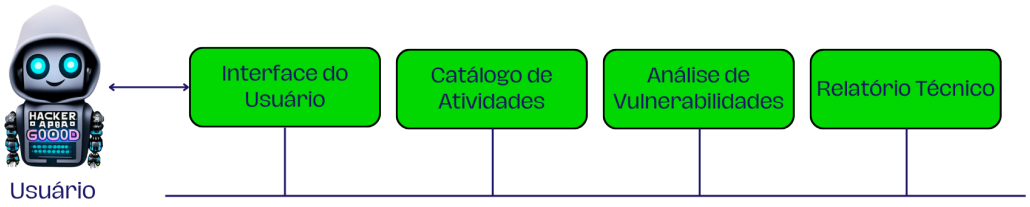

Figura 1. Um diagrama de blocos dos módulos do emulador de ataques.

O módulo Interface do Usuário corresponde a uma interface Web amigável com os usuários, com foco na usabilidade e na acessibilidade. A interface é intuitiva e visa atender a usuários de diferentes níveis de habilidade, oferecendo orientações claras e recursos explicativos. Possui uma usabilidade aprimorada por meio do uso de técnicas de *design* centradas no usuário e utiliza gamificação. Há diferentes páginas Web em função da atividade. Cada atividade é composta por diferentes tarefas, desde a leitura de um texto explicativo até a realização de um ataque. Essa abordagem permite que o aluno acesse facilmente todo o curso de forma iterativa, explorando o conteúdo e os níveis conforme avança. A interface gráfica inclui uma página principal, na qual o usuário escolhe o nível de suas atividades.Além disso, há uma aba lateral expansível que facilita a navegação do usuário por todas as atividades propostas.

O módulo Catálogo de Atividades é responsável pela definição das atividades. Cada atividade é composta por diferentes tarefas: uma introdução teórica sobre o assunto da atividade, seguida de procedimentos práticos para realização de testes de vulnerabilidade XSS. Esse módulo se comunica com o módulo Interface do Usuário para apresentar a lista de atividades disponíveis e carregar a atividade. Também se comunica com os módulos Análise de Vulnerabilidades e Relatório Técnico para a execução das atividades. Essas comunicações estão ilustradas na Figura 1. O emulador EXSS provê quatro atividades. Três atividades abordam os três tipos mais comuns de ataques XSS e a quarta atividade é dedicada ao treinamento de boas práticas em Desenvolvimento Seguro. As atividades são: Atividade 1: XSS Refletido; Atividade 2: XSS Armazenado; Atividade 3: XSS baseado em DOM; Atividade 4: Desenvolvimento Seguro.

É importante ressaltar que cada atividade oferece uma base teórica para a compreensão dos diferentes tipos de XSS, seguida por tarefas de laboratório. Os tutoriais estão disponíveis para orientar os usuários na aplicação dos conceitos aprendidos, visando a facilitar a resolução das atividades práticas. Cada atividade é associada a um nível de conhecimento necessário para o usuário realizá-la. Há atividades para três níveis: iniciante, intermediário e avançado. No nível iniciante, o objetivo é familiarizar os usuários com o

emulador EXSS e os conceitos dos diferentes tipos de ataques XSS. Já os usuários com conhecimentos intermediários e avançados têm a oportunidade de experimentar *scripts* que explorem a vulnerabilidade XSS. Adicionalmente, estes usuários mais avançados podem aplicar correções nos códigos das páginas, a fim de avaliar a eficácia em eliminar ou mitigar as vulnerabilidades de XSS identificadas. Isso permite a aplicação prática dos conhecimentos adquiridos em cenários reais de cibersegurança.

O Módulo Análise de Vulnerabilidades contém o núcleo do emulador, pois nesse módulo são executadas as tarefas práticas. Esse módulo hospeda sítios Web e executa o Apache 2 como servidor Web. Os ambientes das atividades estarão integrados a um pequeno *e-commerce* desenvolvido especificamente para este emulador, Figura 2.

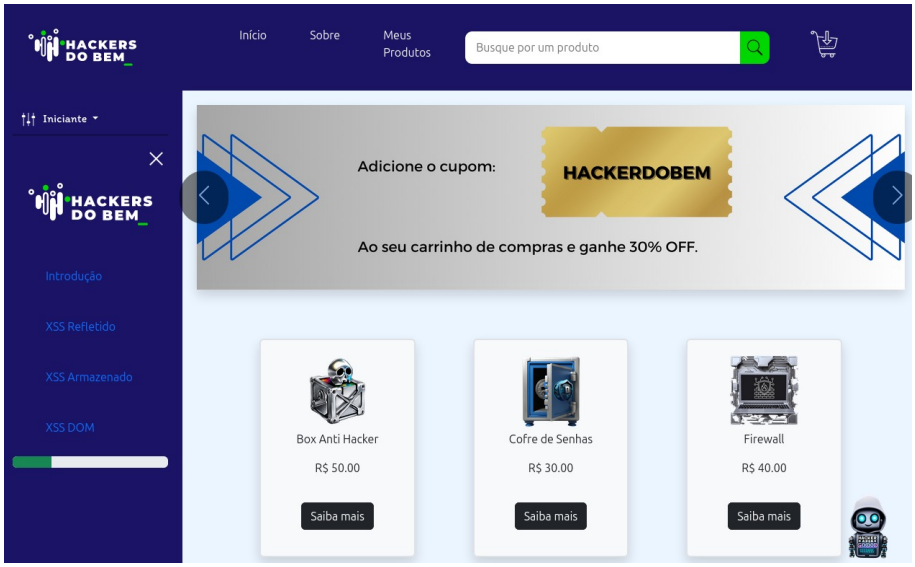

Figura 2. O *e-commerce* desenvolvido para o emulador EXSS.

O Módulo Relatório Técnico tem uma abordagem gamificada para facilitar a aprendizagem do usuário. Após interagir com o laboratório, o usuário receberá um *feedback* sobre a atividade concluída. Para proporcionar uma experiência interativa e didática, os usuários são recompensados com medalhas de conclusão como parte da experiência gamificada.

O *framework* Bootstrap e as tecnologias HTML, CSS, JavaScript, JQuery, PHP e MySQL são usados para o desenvolvimento dos módulos do emulador. Ainda, o emulador EXSS precisa ser executado em um ambiente computacional com recursos isolados para que as atividades práticas que envolvam a exploração de vulnerabilidades não afetem os recursos computacionais de produção. Por isso, o uso da virtualização é imperativo. O ambiente virtualizado reproduz cenários de sítios Web vulneráveis a ataques XSS e as vulnerabilidades são emuladas para reproduzir cenários de ataque específicos. Os usuários podem explorar esses ambientes virtuais, aplicar técnicas de detecção e implementar contramedidas sem riscos. Isso proporciona uma experiência prática e valiosa para a aprendizagem em cibersegurança. A opção escolhida para prover isolamento é usar máquinas virtuais com a tecnologia do VirtualBox que executam o sistema operacional Ubuntu. O uso de máquinas virtuais através do VirtualBox permite emular diversos ambientes operacionais e de rede, facilitando a prática de ataques XSS em um contexto seguro

e isolado, sem riscos ao sistema de produção do usuário.

3. As Funcionalidades do Emulador EXSS e a Demonstração Planejada

A principal funcionalidade do emulador EXSS é a realização de atividades para os diferentes tipos de ataques XSS e os diferentes níveis de conhecimento do usuário. A Figura 3 ilustra a tela inicial do emulador. Nessa tela, o usuário é recebido pelo Hacker Good, um avatar desenvolvido para o emulador que auxilia o usuário durante o seu percurso nas atividades. O usuário também seleciona o nível das atividades que irá realizar: iniciante, intermediário ou avançado. Esses níveis são desbloqueados à medida que o nível anterior é concluído. Na lateral esquerda da tela, há um indicador de nível, um menu de acesso às atividades de cada tipo de ataque XSS e uma barra de progresso das atividades.

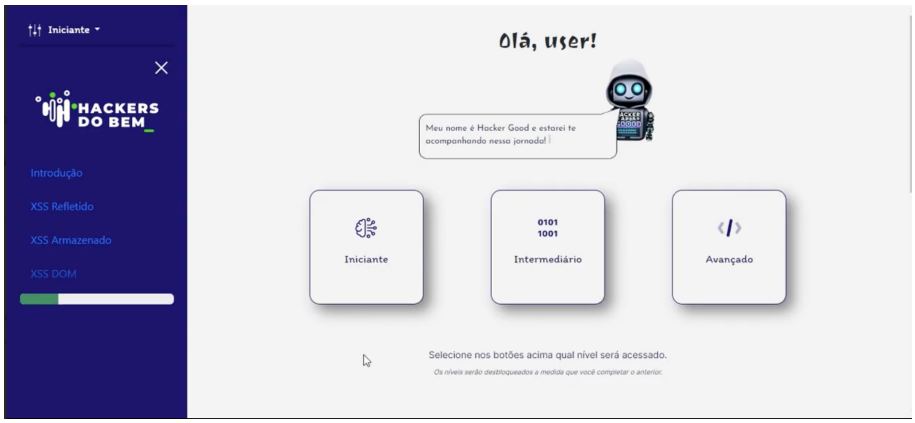

Figura 3. A tela inicial do emulador EXSS.

Ao clicar no botão correspondente ao nível de atividades desejado, o usuário vê uma tela com a documentação sobre a atividade. No nível iniciante, por exemplo, ele acessa a Introdução, na qual vê a motivação para se estudar o tema e a definição dos ataques XSS e seus diferentes tipos. Para passar à Atividade 1, é preciso clical no botão "Entedido".

A Atividade 1, por exemplo, trata do ataque XSS Refletido. A primeira tela da atividade contém um texto explicativo sobre tal ataque. Ao clicar no botão "Entedido", o usuário passa a explicação do Laboratório 1, na qual o Hacker Good retorna para explicar, passo-a-passo, o que deve ser feito. A Figura 4(a) ilustra uma tela de passo-a-passo, na qual o Hacker Good "fala"o que deve ser feito e apresenta o ambiente emulado do *e-commerce*. O usuário pode avançar e retornar clicando nos botões disponíveis. Em seguida, o usuário executa a atividade de laboratório e visualiza o seu resultado. No caso, do Laboratório 1 da Atividade 1, sobre XSS Refletido, o resultado do ataque é uma mensagem em um *pop-up*, como ilustra a Figura 4(b).

Cada atividade é composta por dois laboratórios. No nível iniciante, cada laboratório trata de um efeito do ataque, mensagens em *pop-up* ou redirecionamento de páginas, implementados de diferentes formas, refletido, armazenado ou baseado em DOM. Ao fim da atividade de laboratório, o usuário recebe um conjunto de perguntas que deve ser respondido e, só então, pode passar para a próxima atividade. Ao fim de todas a atividades de um mesmo nível, o usuário recebe a mensagem de que concluiu o nível atual.

(a) Uma tela de passo-a-passo. (b) Uma tela de resultado de laboratório.

Figura 4. Exemplos de telas do emulador EXSS.

O emulador EXSS, sua documentação para instalação e uso e os vídeos de configuração e de demonstração, com os passos descritos anteriormente, estão disponíveis em `https://www.midiacom.uff.br/gt-exss`. Alternativamente, podem ser obtidos: a imagem da máquina virtual com o emulador instalado em `https://drive.google.com/drive/folders/1Dpi8TWZnwcbUaoh97W8wuYgVQ6S_fajf`, a documentação e o código fonte em `https://github.com/bguarizi/emuladorXSS-HackersdoBem` e os vídeos de configuração e demonstração em `https://drive.google.com/drive/folders/1P-I-tWrgNDREgSetLyICa3e28z4hrqby`.

A demonstração no SF é a execução das Atividades 1, 2 e 3 do nível iniciante. Para isso, é preciso de um computador pessoal ou portátil, com o VirtualBox instalado e acesso à Internet para que seja possível obter a imagem da máquina virtual com o emulador instalado. Após isso, o computador não precisa mais de acesso à Internet.

4. As Ferramentas Relacionadas

Algumas ferramentas com o mesmo propósito do emulador EXSS foram encontradas na literatura [PortSwigger, 2024b, Google, 2024, OWASP, 2024, OWASP, 2023, TryHackMe, 2024]. A PortSwigger através de sua Academia de Segurança Web [PortSwigger, 2024b] provê uma série de laboratórios que envolvem a realização de diferentes tipos de ataques, incluindo o XSS. São apresentados textos curtos genéricos contendo conceitos básicos, como explorar vulnerabilidades e formas de evitar os ataques, dentre outros. Cada atividade é acessada *online* via uma página Web fictícia que contém uma vulnerabilidade propositalmente associada. Além dos textos genéricos, não há material de apoio à realização da atividade, exceto uma breve descrição do que deve ser realizado e a solução para a atividade, que fica escondida em um primeiro momento. Outro problema está relacionado à dependência da versão paga da ferramenta Burp Suite [PortSwigger, 2024a] para a realização de algumas atividades.

O XSS Game da Google [Google, 2024] contém seis atividades que incluem a realização *online* de diferentes tipos de ataques XSS em páginas Web vulneráveis. Em cada atividade são apresentadas a descrição, o objetivo, o código-fonte da página e até três dicas para a resolução da atividade, sendo os dois últimos itens inicialmente escondidos. Não possui um material de apoio mais completo de forma a facilitar a realização das atividades mais avançadas.

A OWASP Juice Shop [OWASP, 2024] corresponde a uma aplicação na qual pode-

se explorar vulnerabilidades do OWASP Top Ten [OWASP, 2021] e outras falhas de segurança de aplicações do mundo real, dentre as quais o XSS. A aplicação emula uma loja virtual com produtos vulneráveis e contém uma seção de pequenos tutoriais sobre diferentes tópicos. Usa gamificação através da contabilização e da exibição das interações do usuário em um sistema de pontuação interno com recompensas. Exige o uso de node.js, Docker ou Vagrant para instalação em ambiente Windows, Mac ou Linux, o que poder ser uma dificuldade para usuários inexperientes.

A OWASP Webgoat [OWASP, 2023] é outra aplicação propositalmente insegura para a realização de ataques comumente encontrados em aplicações baseadas em Java que utilizam componentes de código aberto comuns e populares, dentre os quais os ataques XSS. Os usuários interagem com o sistema por meio da interface do navegador com *host* local via contêineres para realizar as atividades e aprender sobre as diferentes vulnerabilidades. As aulas seguem um padrão simples de ensino: uma explicação teórica do conteúdo é acompanhada de uma aba restrita para teste e no fim há um pequeno questionário. Possui suporte à língua portuguesa. Durante a execução da aplicação, a máquina do usuário fica vulnerável a ataques e a própria OWASP recomenda que seja desconectada da Internet.

Por fim, a TryHackMe [TryHackMe, 2024] é uma plataforma de serviços *online* voltada ao aprendizado e desenvolvimento em cibersegurança, incluindo o estudo de XSS. A plataforma inclui materiais de leitura e avaliação, desafios e laboratórios. O progresso do usuário é armazenado de uma forma gamificada, com insígnias e títulos distribuídos internamente como forma de recompensa pelo avanço local. As atividades são realizadas em bibliotecas de salas, que são máquinas virtuais configuradas com cenários simulados de vulnerabilidades reais para que o usuário teste seus conhecimentos. Possui parte do conteúdo restrita para usuários assinantes.

O emulador EXSS reúne diversas vantagens das ferramentas anteriormente apresentadas, com algumas diferenças. Todas as atividades da ferramenta podem ser realizadas gratuitamente. O emulador trata particularmente de vulnerabilidades XSS, de forma a prover ao usuário um ensino que abrange desde atividades básicas até as avançadas. A abordagem educacional utilizada para lidar com os ataques XSS inclui uma introdução teórica sobre o assunto da atividade, seguida de procedimentos práticos para a realização de testes, de forma a guiar principalmente o usuário iniciante. Os testes são realizados em um ambiente controlado com o servidor Web executado em uma máquina virtual local, sem necessidade de uso da Internet durante a realização dos testes. Além disso, o EXSS possui suporte à língua portuguesa, algo significativo para muitos jovens cursando o ensino médio ou a graduação.

5. Conclusões e Trabalhos Futuros

Este artigo desenvolveu o emulador EXSS para ataque XSS. O emulador proposto permite que usuários identifiquem sítios Web vulneráveis a ataques XSS em um ambiente controlado. São definidas atividades compostas por uma introdução teórica e laboratórios experimentais que envolvem diferentes tipos de ataques XSS – refletido, armazenado e baseado em DOM – para diferentes níveis de usuários. O diferencial do emulador proposto é ser totalmente gratuito, executar sem necessidade de acesso à Internet e ter suporte ao português. No momento, o emulador proposto implementa as atividades do

nível iniciante. Os próximos passos incluem a implementação das atividades dos níveis intermediário e avançado e de uma trilha de progresso do usuário gamificada.

Agradecimentos

Este trabalho foi realizado com recursos da RNP, CNPq, CEFET/RJ, CAPES, FAPERJ e PGC/UFF.

Referências

BBC (2018). British Airways faces record £183m fine for data breach. Disponível em https://www.bbc.com/news/business-48905907 (18/04/2024).

CyCognito (2023). Web Apps are Leaving PII Exposed State of External Exposure Management Report. Relatório técnico.

Google (2024). XSS game. Disponível em https://xss-game.appspot.com/ (02/07/2024).

Grossman, J. (2007). *XSS attacks: Cross Site Scripting exploits and defense*. Syngress.

Gupta, S. e Gupta, B. B. (2017). Cross-site scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management*, 8:512–530.

Kaur, J., Garg, U. e Bathla, G. (2023). Detection of Cross-Site Scripting (XSS) attacks using machine learning techniques: a review. *Artificial Intelligence Review*, 56(11):12725–12769.

Liu, M., Zhang, B., Chen, W. e Zhang, X. (2019). A survey of exploitation and detection methods of XSS vulnerabilities. *IEEE Access*, 7:182004–182016.

OWASP (2021). OWASP Top 10. Disponível em https://owasp.org/Top10/ (18/04/2024).

OWASP (2023). OWASP webgoat | OWASP foundation. Disponível em https://owasp.org/www-project-webgoat/ (02/07/2024).

OWASP (2024). OWASP juice shop | OWASP foundation. Disponível em https://owasp.org/www-project-juice-shop/ (02/07/2024).

PortSwigger (2024a). Burp suite - application security testing software - PortSwigger. Disponível em https://portswigger.net/burp (02/07/2024).

PortSwigger (2024b). Web security academy: Free online training from PortSwigger. Disponível em https://portswigger.net/web-security (02/07/2024).

Reuters (2018). BA apologizes after 380,000 customers hit in cyber attack. Disponível em https://www.reuters.com/article/us-iag-cybercrime-british-airways/ba-apologizes-after-380000-customers-hit-in-cyber-attack-idUSKCN1LM2P6/ (18/04/2024).

Rodríguez, G. E., Torres, J. G., Flores, P. e Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: a survey. *Computer Networks*, 166:106960.

TryHackMe (2024). TryHackMe | cybersecurity training. Disponível em https://tryhackme.com/ (02/07/2024).