UNIVERSIDADE FEDERAL DE SANTA CATARINA

Samuel Cardoso

Desenvolvimento de um Ambiente para Aprendizado e Prática de Técnicas de Segurança Ofensiva em Aplicações Web Vulneráveis

Florianópolis,
2022/1

Samuel Cardoso

Desenvolvimento de um Ambiente para Aprendizado e Prática de Técnicas de Segurança Ofensiva em Aplicações Web Vulneráveis

Proposta submetida ao Programa de Graduação em Ciência da Computação para obtenção do Grau de Bacharel.
Orientador: Profª. Carla Merkle Westphall

Florianópolis,
2022/1

FOLHA DE APROVAÇÃO DE PROPOSTA DO TCC

Acadêmico(s)	Samuel Cardoso
Título do Trabalho	Desenvolvimento de um Ambiente para Aprendizado e Prática de Técnicas de Segurança Ofensiva em Aplicações Web Vulneráveis
Curso	Ciências da Computação/INE/UFSC
Área de Concentração	**SEGURANÇA COMPUTACIONAL**

Instruções para preenchimento pelo *ORIENTADOR DO TRABALHO*:

- Para cada critério avaliado, assinale um X na coluna SIM apenas se considerado aprovado. Caso contrário, indique as alterações necessárias na coluna de Observação.

Critérios	**Aprovado**				**Observação**
	Sim	**Parcial**	**Não**	**Não se aplica**	
O trabalho é adequado para um TCC em CCO (relevância / abrangência)?	X				
O título é adequado?	X				
O Tema de pesquisa está claramente descrito?	X				
O problema/hipóteses de pesquisa do trabalho está claramente identificado?	X				
A relevância da pesquisa é justificada?	X				
Os objetivos descrevem completa e claramente o que se pretende alcançar neste trabalho?	X				
É definido o método a ser adotado no trabalho? O método condiz com os objetivos e é adequado para um TCC?	X				
Foi definido um cronograma coerente com o método definido (indicando todas as atividades) e com as datas das entregas (p.ex. Projeto I, II, Defesa)?	X				
Foram identificados custos relativos à execução deste trabalho (se houver)? Haverá financiamento para estes custos?				X	
Foram identificados todos os envolvidos neste trabalho?		X			
As formas de comunicação foram definidas?	X				
Riscos potenciais que podem causar desvios do plano foram identificados?	X				
Caso o TCC envolva a produção de um software ou outro tipo de produto e seja desenvolvido também como uma atividade realizada numa empresa ou laboratório, consta na proposta uma declaração (Anexo 3) de ciência e concordância com a entrega do código fonte e/ou documentação produzidos?				X	

Avaliação	☒ Aprovado	☐ Não Aprovado	
Professor Responsável:	Carla M. Westphall	18/07/2022	
Orientador Externo:			

RESUMO

Em um momento onde a tecnologia evolui tão rapidamente, novas vulnerabilidades em aplicações web são encontradas todos os meses enquanto outras são remediadas, isso faz com que o estado da arte da segurança computacional seja atualizado constantemente. Neste contexto, este trabalho se propõe a desenvolver um ambiente para aprendizado e prática de técnicas de segurança ofensiva em aplicações web com vulnerabilidades de alto risco nos últimos anos.
Palavras-chave: segurança computacional. vulnerabilidades. aplicações web. ambiente para aprendizado.

Sumário

1 Introdução

A democratização da Internet aumentou exponencialmente o uso de Internet no último século, afetando a vida cotidiana e corporativa das pessoas [**carneiro2022**], porém o aumento do uso da Internet contém consequências. Nos últimos anos problemas com ataques cibernéticos passaram a ser cada vez mais comuns ao redor do mundo e inclusive no Brasil [**avila2013brasil**]. Em contra ponto, políticas e leis tornam-se mais rigorosas quanto ao tratamento e a proteção de dados [**Neves_Lopes_Pavani_Sales_2021**], levando a segurança da informação e a segurança computacional a um novo nível de importância.

Para prevenção para infortúnios muitas empresas estão utilizando de técnicas de segurança ofensiva para monitorar o nível de segurança e aperfeiçoar suas defesas, já que é mais fácil corrigir uma vulnerabilidade ao ter o conhecimento dela [**vieira2018**]. Existem, porém, complicações e barreiras no aprendizado de segurança ofensiva, uma vez que há uma linha tênue entre legalidade e ilegalidade quando se realiza testes em sites de terceiros.

Visto a lacuna existente na área para aplicar o conhecimento teórico acerca de segurança ofensiva de forma prática, este trabalho se propõe a desenvolver de um ambiente para aprendizado e prática de técnicas de segurança ofensiva em aplicações web vulneráveis. Ambiente este que será desenvolvido em Docker para facilitar a execução do mesmo em múltiplos Sistemas Operacionais, permitindo o estudo dessas técnicas sem necessidade de alocar tantos recursos computacionais como outros mecanismos de virtualização fazem [**8528247**].

O ambiente proposto é constituído de uma imagem Docker contendo uma aplicação web que ficará disponível para acesso local, a aplicação conterá algumas falhas de segurança selecionadas, que em sua maioria podem ser encontradas no OWASP TOP 10:2021.

OWASP Top 10 que é um framework da OWASP, uma organização sem fins lucrativos, que traz informações sobre as falhas mais utilizadas em um determinado ano. Neste trabalho o OWASP Top 10 utilizado será do ano de 2021 [**url:OWASP**]. Desta forma serão selecionadas falhas da OWASP Top 10:2021, pois como são frequentemente encontradas falhas novas de segurança [**https://doi.org/10.48550/arxiv.2205.02544**], algumas técnicas passam a ser mais usadas e outras caem em desuso, se faz importante para quem estuda tais técnicas praticarem em falhas atuais.

2 Objetivos

2.1 Objetivos gerais

Este trabalho visa realizar a implementação de um ambiente em Docker contendo aplicações web vulneráveis para facilitar o aprendizado e a prática legal de técnicas de segurança ofensiva.

2.2 Objetivos específicos

Os objetivos específicos que podem ser descritos são os seguintes:

- Elencar o estado da arte das vulnerabilidades em aplicações web
- Selecionar as vulnerabilidades mais pertinentes para estudo por estudantes/profissionais interessados no atual estado da arte
- Projetar e decidir as tecnologias utilizadas no desenvolvimento do ambiente a fim de que tenha os recursos necessários à execução das vulnerabilidades selecionadas
- Desenvolver o ambiente de modo que sua instalação e uso por terceiros fique simplificada, deixando o foco da atividade no estudo das falhas propriamente dito

3 Método de Pesquisa

Primeiramente será realizado um estudo exploratório para uma maior compreensão do estado da arte da segurança ofensiva, tendo como foco tanto o entendimento de como é realizada a exploração da falha quanto quais ferramentas e ações são utilizadas para mitigar ou anular a falha.

Em um segundo momento, será realizado o planejamento do ambiente para dar suporte à exploração das vulnerabilidades enquanto o laboratório de estudo continue estável para novas tentativas. Em seguida, o desenvolvimento do ambiente em Docker é feito, buscando como objetivo implementar um ambiente de fácil usabilidade e boa estabilidade.

Por fim, todo o desenvolvimento e a seleção de vulnerabilidades apoiará a escrita da monografia, explicando em conjunto as falhas abordadas no trabalho e o laboratório desenvolvido para estudo.

4 Cronograma

Etapas	**2022**					**2023**				
	ago	**set**	**out**	**nov**	**dez**	**jan**	**fev**	**mar**	**abr**	**mai**
Desenvolvimento da solução										
Relatório projeto I										
Rascunho projeto II										
Defesa										
Ajustes e envio Final										

5 Recursos Humanos

Nome	Função
Samuel Cardoso	Autor
Carla Merkle Westphall	Orientador
Renato Cislaghi	Coordenador
a definir	Membro da banca I
a definir	Membro da banca II

6 Comunicação

O que precisa ser comunicado	Por quem	Para quem	Melhor forma de comunicação	Quando ou com que frequencia
Entrega da proposta de TCC	Autor	Coordenador	Sistema de TCC	única vez
Entrega do relatório I	Autor	Coordenador	Sistema de TCC	única vez
Entrega do relatório II	Autor	Coordenador	Sistema de TCC	única vez
Reuniões com o orientador	Autor	Orientador	Pessoalmente/videochamada	quando necessário

7 Riscos

Risco	Probabilidade	Impacto	Prioridade	Estratégia de resposta	Ações de Prevenção
Perda de dados	baixa	alto	alta	Recuperação da versão mais atual do código	manter o GitHub do projeto atualizado
Alteração do cronograma	baixa	médio	média	redefinição do croonograma	não se aplica