

Unicesumar

Leonardo Lemes Pedrozo

Desafio Profissional

Curitiba

Maio, 2023

Sumário

1. INTRODUÇÃO -----	03
1.1. CONTEXTO E JUSTIFICATIVA DO TRABALHO PRÁTICO -----	03
1.2. OBJETIVOS -----	03
1.3. METODOLOGIA -----	03
2. AMBIENTE VIRTUAL -----	03
2.1. INSTALAÇÃO E CONFIGURAÇÃO DO VIRTUALBOX -----	03
2.2. INSTALAÇÃO E CONFIGURAÇÃO DO LINUX NA MÁQUINA VIRTUAL -----	03
2.3. INSTALAÇÃO E CONFIGURAÇÃO DO WEBGOAT -----	03
3. VISÃO GERAL DO WEBGOAT -----	04
3.1. DESCRIÇÃO E FUNCIONALIDADES DO WEBGOAT -----	04
3.2. COMO ACESSAR E NAVEGAR NO WEBGOAT -----	04
4. PRÁTICAS COMUNS DE SEGURANÇA EM APLICAÇÕES WEB -----	04
4.1. CONCEITOS BÁSICOS DE SEGURANÇA EM APLICAÇÕES WEB -----	04
4.2. IDENTIFICAÇÃO DE VULNERABILIDADES COMUNS EM -----	04
APLICAÇÕES WEB	
4.3. BOAS PRÁTICAS PARA MITIGAÇÃO DE VULNERABILIDADES EM -----	04
APLICAÇÕES WEB	
4.4. SQL INJECTION -----	05
5. CONCLUSÃO -----	05
5.1. SÍNTESE DOS RESULTADOS E CONCLUSÕES DO TRABALHO -----	05
PRÁTICO	
5.2. LIMITAÇÕES DO TRABALHO E SUGESTÕES PARA TRABALHOS -----	05
FUTUROS	
6. REFERÊNCIAS BIBLIOGRÁFICAS -----	05

## 1. INTRODUÇÃO

### 1.1. CONTEXTO E JUSTIFICATIVA DO TRABALHO PRÁTICO

Neste trabalho prático, será efetivamente o uso do WebGoat, um ambiente virtual que oferece laboratórios para o aprendizado de vulnerabilidades em aplicações web, como SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) e outros. O objetivo é compreender os conceitos de segurança em aplicações web e explorar a identificação e mitigação dessas vulnerabilidades.

### 1.2. OBJETIVOS

Os objetivos deste trabalho são práticos, aprender sobre conceitos de segurança em aplicações web, identificar vulnerabilidades comuns em aplicações web e aplicar boas práticas para mitigar vulnerabilidades em aplicações web.

### 1.3. METODOLOGIA

A metodologia adotada consiste em criar um ambiente virtual utilizando o VirtualBox com uma máquina virtual Linux. Em seguida, será realizada a instalação e configuração do WebGoat nesse ambiente. Será feita uma visão geral do WebGoat e suas funcionalidades, e serão exploradas as práticas comuns de segurança em aplicações web, com foco na identificação e mitigação de vulnerabilidades.

## 2. AMBIENTE VIRTUAL

### 2.1. INSTALAÇÃO E CONFIGURAÇÃO DO VIRTUALBOX

Para a instalação do virtualbox eu acessei o link disponibilizado pela professora para download e instalei e criei uma nova máquina virtual.

### 2.2. INSTALAÇÃO E CONFIGURAÇÃO DO LINUX NA MÁQUINA VIRTUAL

Depois de criar uma nova máquina virtual configurei para linux e em seguida baixei uma imagem do kali, instalei e configurei e iniciei a máquina virtual linux com o kali e fiz login no mesmo.

### 2.3. INSTALAÇÃO E CONFIGURAÇÃO DO WEBGOAT

Em seguida instalei e executei o webgoat, minha escolha de tema para o trabalho foi o SQL Injection (intro) e irei começar a responder as questões.

## 3. VISÃO GERAL DO WEBGOAT

### 3.1. DESCRIÇÃO E FUNCIONALIDADES DO WEBGOAT

O WebGoat é uma plataforma de treinamento projetada para desenvolvedores e profissionais de segurança sobre as vulnerabilidades mais comuns em aplicações web. O WebGoat oferece uma série de funcionalidades que permitem aos usuários explorar vulnerabilidades em aplicações web.

### 3.2. COMO ACESSAR E NAVEGAR NO WEBGOAT

Após iniciar o virtualbox realizei o download e iniciei o webgoat então acessei e escolhi um dos temas para a realização das atividades.

## 4. PRÁTICAS COMUNS DE SEGURANÇA EM APLICAÇÕES WEB

### 4.1. CONCEITOS BÁSICOS DE SEGURANÇA EM APLICAÇÕES WEB

A definição de segurança em aplicações web é o ato ou prática de proteger sites contra acesso, uso, modificação, destruição ou interrupção não autorizados.

### 4.2. IDENTIFICAÇÃO DE VULNERABILIDADES COMUNS EM APLICAÇÕES WEB

A identificação de vulnerabilidades em aplicações web é essencial para garantir a segurança adequada dos sistemas. Injeção de SQL: A vulnerabilidade de injeção de SQL ocorre quando um invasor consegue inserir comandos SQL maliciosos em entradas não filtradas ou validadas. Isso pode permitir que o invasor execute consultas não autorizadas no banco de dados, obtenha informações efetivas ou até mesmo modifique os dados. Para identificar essa vulnerabilidade, é importante examinar os pontos de entrada de dados na aplicação e verificar se eles estão sendo devidamente tratados.

### 4.3. BOAS PRÁTICAS PARA MITIGAÇÃO DE VULNERABILIDADES EM APLICAÇÕES WEB

Para mitigar vulnerabilidades em aplicações web, é importante seguir as seguintes boas práticas:

- 1- Validação e sanitização de dados: Valide e higienize todos os dados recebidos do usuário antes de usá-los, evitando injeção de código malicioso.
- 2- Controle de acesso: Implemente um sistema de autenticação segura para verificar a identidade dos usuários.

#### 4.4. SQL INJECTION

A SQL Injection é uma vulnerabilidade comum em aplicações web que permite que um invasor execute comandos SQL não autorizados através de campos de entrada não sanitizados ou validados. Isso ocorre quando a aplicação não filtra corretamente os dados fornecidos pelo usuário, permitindo que o invasor insira instruções SQL maliciosas. Essa vulnerabilidade pode ter consequências graves, como o acesso não autorizado ao banco de dados, roubo de informações, alteração ou exclusão de dados e até mesmo a execução de comandos no servidor de banco de dados. A identificação da SQL Injection pode ser feita por meio de técnicas de testes de penetração, onde entradas explícitas, como campos de pesquisa, formulários de login ou parâmetros de URL, são exploradores para inserção de comandos SQL maliciosos.

### 5. CONCLUSÃO

#### 5.1. SÍNTESE DOS RESULTADOS E CONCLUSÕES DO TRABALHO PRÁTICO

O trabalho prático de montagem de um ambiente virtual web vulnerável utilizando o WebGoat no VirtualBox Linux proporcionou uma oportunidade de aprendizado sobre vulnerabilidades em aplicações web. Durante o processo, foi possível compreender os conceitos de segurança em aplicações web e explorar práticas comuns de identificação e mitigação de vulnerabilidades.

#### 5.2. LIMITAÇÕES DO TRABALHO E SUGESTÕES PARA TRABALHOS FUTUROS

Tive dificuldades em instalar e configurar o kali na máquina virtual, talvez se tivesse um manual passo a passo detalhado de como fazer todo o processo desde criar uma máquina virtual até navegar no webgoat seria mais fácil, ou se fosse feito em sala de aula junto com o professor. Só consegui concluir esse trabalho com a ajuda de meus colegas para instalar ou configurar alguns sistemas, pois estava com dificuldades.

### 6. REFERÊNCIAS BIBLIOGRÁFICAS

OWASP. (2021). Projeto OWASP Top Ten. Disponível em: <https://owasp.org/www-project-top-ten/>

Oráculo. (2021). Diretrizes de codificação segura para Java SE. Disponível em: <https://www.oracle.com/java/technologies/javase/seccodeguide.html>

W3C. (2021). Política de Segurança de Conteúdo Nível 3. Disponível em: <https://www.w3.org/TR/CSP3/>

OWASP. (2021). Folha de dicas de prevenção de script entre sites (XSS). Disponível em: [https://cheatsheetseries.owasp.org/cheatsheets/Cross\\_Site\\_Scripting\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

OWASP. (2021). Folha de dicas para prevenção de falsificação de solicitação entre sites (CSRF). Disponível em: [https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site Request Forgery Prevention Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html)

OWASP. (2021). Teste de SQL Injection. Disponível em: [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/02-Web\\_Application\\_Security\\_Testing\\_Guidelines/01-Testing for SQL Injection](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Web_Application_Security_Testing_Guidelines/01-Testing_for_SQL_Injection)

