UNICESUMAR

THIAGO ROGERIO BASSETE DE ARAUJO

TRABALHO PRÁTICO MONTAGEM DE UM AMBIENTE VIRTUAL WEB VULNERÁVEL

CURITIBA

2023

UNICESUMAR

THIAGO ROGERIO BASSETE DE ARAUJO

TRABALHO PRÁTICO MONTAGEM DE UM AMBIENTE VIRTUAL WEB VULNERÁVEL

Trabalho apresentado à disciplina de Desafio profissional apresentada a disciplina de Desafio profissional III por solicitação da professora Ana Paula Costacurta.

CURITIBA

2023

Sumario

INTRODUÇÃO

O contexto deste trabalho prático está relacionado à instalação, configuração e uso do VirtualBox, Linux e WebGoat. Essas tecnologias são amplamente utilizadas no desenvolvimento e segurança de aplicações web. A justificativa para realizar esse trabalho prático é proporcionar aos usuários a oportunidade de aprender e praticar habilidades relacionadas à configuração de ambientes virtuais, instalação de sistemas operacionais e exploração de vulnerabilidades em aplicações web. Essas habilidades são essenciais para profissionais de segurança da informação e desenvolvedores que desejam entender melhor as ameaças e proteger seus sistemas contra ataques.

Os objetivos deste trabalho prático são demonstrar o processo de instalação e configuração do VirtualBox, guiar a instalação do Linux em uma máquina virtual e explorar o WebGoat para aprender sobre vulnerabilidades em aplicações web.

A metodologia adotada envolve a instalação e configuração do VirtualBox, incluindo a criação de uma nova máquina virtual, a instalação do Linux nessa máquina virtual e a exploração do WebGoat para aprender sobre vulnerabilidades em aplicações web. Os usuários seguirão um guia passo a passo para realizar essas etapas.

CURITIBA

2023

DESENVOLVIMENTO DO TRABALHO

2.1. Instalação e configuração do VirtualBox:

- Faça o download do VirtualBox no site oficial e siga as instruções do assistente de instalação.

- Crie uma nova máquina virtual, definindo nome, tipo e versão do sistema operacional, quantidade de memória RAM e tamanho do disco.

- Inicie a máquina virtual e instale o sistema operacional seguindo as instruções.

2.2. Instalação e configuração do Linux na máquina virtual:

- Obtenha uma imagem ISO do Linux kali.

- Crie uma nova máquina virtual no VirtualBox, definindo nome, tipo e versão do sistema operacional, quantidade de memória RAM e tamanho do disco.

- Inicie a máquina virtual e selecione a imagem ISO do Linux para instalar o sistema operacional.

- Siga as instruções do assistente de instalação do Linux e configure-o conforme necessário.

2.3. Instalação e configuração do WebGoat:

- Baixe e instale um servidor web, como o Apache Tomcat.

- Acesse o site oficial do WebGoat e baixe a versão mais recente.

- Instale o servidor web e copie o arquivo do WebGoat para o diretório de implantação.

- Inicie o servidor web e acesse o endereço do WebGoat em um navegador.

- Explore as lições disponíveis e siga as instruções para aprender sobre as vulnerabilidades.

3.1. Descrição e funcionalidades do WebGoat:

- O WebGoat é um aplicativo web de treinamento inseguro para aprender sobre vulnerabilidades.

- Oferece lições interativas que abrangem diversas categorias de vulnerabilidades.

- Proporciona um ambiente seguro e controlado para explorar vulnerabilidades.

- Fornece explicações detalhadas sobre as vulnerabilidades e suas correções.

- Suporta diferentes tecnologias e frameworks usados em aplicações web.

- Mantido pela comunidade OWASP.

3.2. Como acessar e navegar no WebGoat:

- Baixe e instale o WebGoat conforme as instruções do site oficial.

- Inicie o WebGoat e acesse-o em um navegador usando o endereço fornecido.

- Navegue pelas categorias e lições disponíveis.

- Siga as instruções em cada lição para explorar as vulnerabilidades.

- Leia as explicações e progrida nas lições para aprimorar suas habilidades de segurança.

4.1. Conceitos básicos de segurança em aplicações web:

- Incluem autenticação, autorização, criptografia, validação de entrada e gerenciamento de sessão.

4.2. Identificação de vulnerabilidades comuns em aplicações web:

- Vulnerabilidades de injeção de SQL, cross-site scripting (XSS), entre outras.

- Identificação por meio de testes de penetração, auditorias de segurança e análise de código.

4.3. Boas práticas para mitigação de vulnerabilidades em aplicações web:

- Codificação segura, autenticação e controle de acesso adequados, criptografia, atualizações regulares e monitoramento.

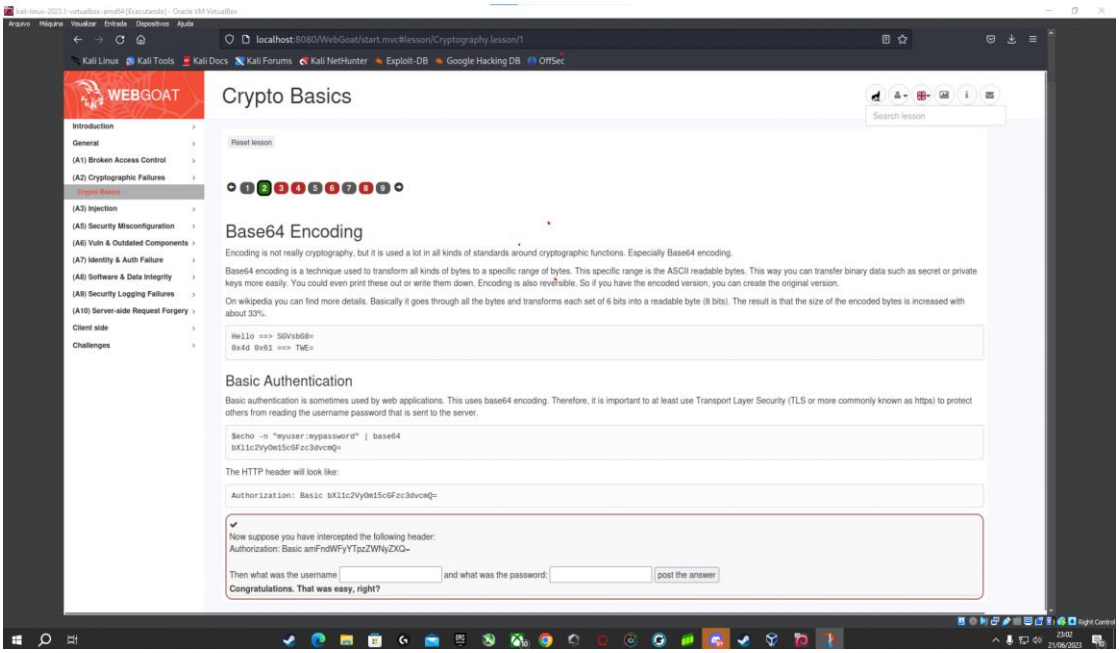
4.4. SQL Injection:

- Vulnerabilidade em que dados não sanitizados são inseridos

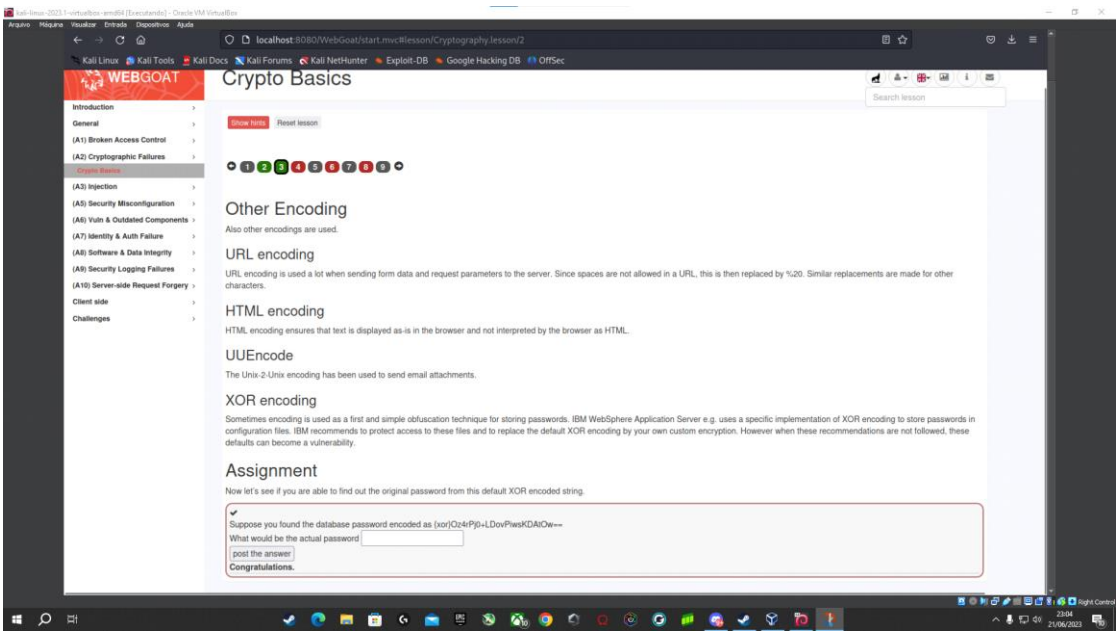
5.1 Atividades realizadas foram as de criptografia

atividades em que precisamos entrar e abrir os códigos e de criptografá-los e tambem transformar de ras para outros módulos 256

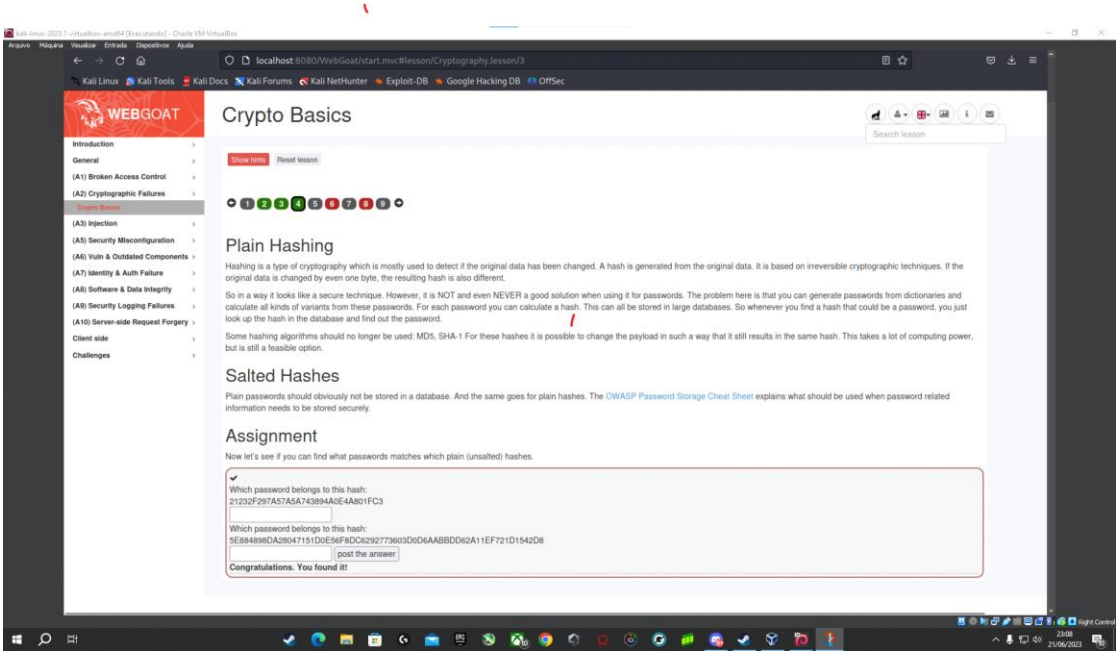
atividade número 2:



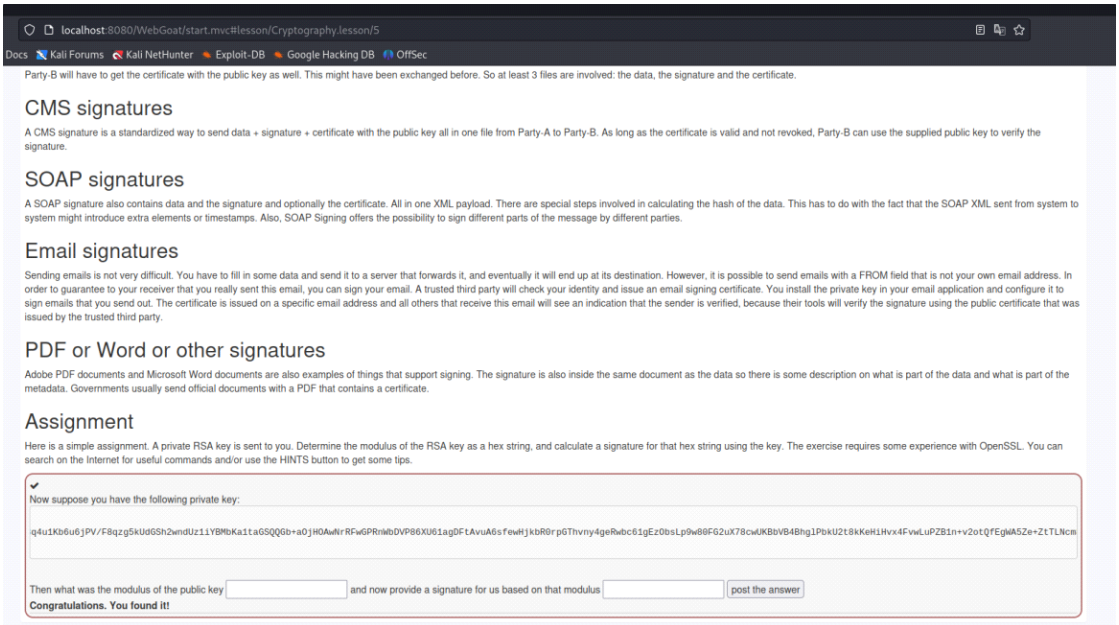
Atividade número 3:



Atividade número 4:



Atividade número 6:



CONCLUSÃO

este trabalho prático abordou a instalação e configuração do VirtualBox, Linux e WebGoat, um aplicativo web de treinamento inseguro para aprender sobre vulnerabilidades. Foram explorados conceitos básicos de segurança em aplicações web, identificação de vulnerabilidades comuns e boas práticas para mitigação. O WebGoat proporcionou um ambiente controlado para explorar vulnerabilidades, com lições interativas e explicações detalhadas. Através dessa abordagem prática, os participantes puderam aprimorar suas habilidades de segurança e se tornarem mais conscientes das ameaças em aplicações web.

CURITIBA

2023

REFERÊNCIAS

Site oficial do VirtualBox: https://www.virtualbox.org/

Documentação do VirtualBox: https://www.virtualbox.org/wiki/Documentation

Site oficial do Linux: https://www.linux.org/

Distribuições Linux populares:

Ubuntu: https://ubuntu.com/

CentOS: https://www.centos.org/

Fedora: https://getfedora.org/

Site oficial do WebGoat: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Documentação do WebGoat: https://github.com/WebGoat/WebGoat/wiki

Site oficial do OWASP (Open Web Application Security Project): https://owasp.org/

OWASP Top 10: https://owasp.org/top10/

CURITIBA

2023