UNICESUMAR

RENATO DE ALMEIDA MENDES

TRABALHO PRÁTICO MONTAGEM DE UM AMBIENTE VIRTUAL WEB VULNERÁVEL

CURITIBA

2023

UNICESUMAR

RENATO DE ALMEIDA MENDES

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

Sumário

CURITIBA

2023

INTRODUÇÃO

As aplicações hoje em dia estão cada vez mais vulneráveis, assim através do software VirtualBox, que executa uma máquina virtual, nela podemos acessar o site WebGoat que é uma aplicação desenvolvida pela Open Web Application Security Project (OWASP), ela ensina os desenvolvedores sobre as vulnerabilidades que se pode ter em uma aplicação web e como resolvê-las, ou seja, é um site que de treinamento na prática de teste de invasões em aplicações webs.

OBJETIVO

O WebGoat fornece um ambiente educacional para que os usuários possam aprender sobre vulnerabilidades e técnicas de segurança em aplicações web. Ele é projetado para ajudar desenvolvedores e profissionais de segurança a aprimorarem suas habilidades na identificação e exploração de falhas comuns em aplicações web. Ele faz com que os usuários identifiquem e explorem vulnerabilidades, e a como se prevenir sobres esses problemas.

METODOLOGIA

WebGoat oferece aos usuários a oportunidade de aprenderem na prática sobre vulnerabilidades e técnicas de segurança em aplicações web. Ele incentiva a experimentação, o erro e a compreensão dos conceitos subjacentes, permitindo que os usuários adquiram habilidades em testes de segurança e desenvolvimento seguro.

AMBIENTE VIRTUAL

INSTALAÇÃO E CONFIGURAÇÃO DO VIRTUALBOX

Acessei o site oficial da VirtualBox https://www.virtualbox.org/ a baixei a versão mais recente, e executei o arquivo, segui os passos padrões de instalação, após a instalação comecei a configurar, para poder abrir a maquina virtual fiz o donwload da iso do Kali no site https://www.kali.org/docs/virtualization/import-premade-virtualbox/.

Com a iso do Kali a baixada, abri ela pelo VirtualBox, quando mandei iniciar deu um erro de SVM. Onde ele pedia para que acessasse a BIOS do meu computador e ativasse o SVM. Após isso mandei iniciar a máquina virtual e deu tudo certo.

INSTALAÇÃO E CONFIGURAÇÃO DO LINUX NA MÁQUINA VIRTUAL

Após acessar a máquina virtual abri o cmd e coloquei os seguintes códigos:

sudo apt-get install default-jre;

wget https://github.com/WebGoat/WebGoat/releases/download/v2023.4/webgoat-2023.4.jar;

java -jar webgoat-2023.4.jar;

Com esses códigos o Linux está configurado, e com a instalação do WebGoat feita também.

CONFIGURAÇÃO DO WEBGOAT

Com a instalação do WebGoat feita no tópico passado, agora é só configurar. Acesse o site http://localhost:8080/WebGoat/ e nele você vai fazer o seu cadastro, com o cadastro feito, o site já está liberado para poder estudar e aprender sobre as vulnerabilidades.

VISÃO GERAL DO WEBGOAT

DESCRIÇÃO E FUNCIONALIDADES DO WEBGOAT

O WebGoat é um software de código aberto que fornece um ambiente educacional e interativo para aprender sobre vulnerabilidades e técnicas de segurança em aplicações web. Ele foi criado para ajudar desenvolvedores, estudantes e

profissionais de segurança a adquirirem conhecimentos práticos em testes de segurança e identificação de falhas em aplicações web.

COMO ACESSAR E NAVEGAR NO WEBGOAT

Você faz o acesso através de uma máquina virtual, pois como você vai fazer testes de vulnerabilidades em sites é importante você estar em uma máquina virtual permitindo que você faça uso de um computador sem estar vinculado a um lugar físico.

PRÁTICAS COMUNS DE SEGURANÇA EM APLICAÇÕES WEB

CONCEITOS BÁSICOS DE SEGURANÇA EM APLICAÇÕES WEB

A segurança em aplicações web é essencial para proteger dados e informações em um ambiente online. Alguns conceitos básicos incluem autenticação, autorização, criptografia, injeção de código, XSS, CSRF, gerenciamento de sessão. Esses conceitos visam garantir a integridade e a privacidade dos usuários, protegendo contra ameaças e vulnerabilidades.

IDENTIFICAÇÃO DE VULNERABILIDADES COMUNS EM APLICAÇÕES WEB

Vulnerabilidades comuns em aplicações web incluem injeção de código, cross-site scripting, cross-site request forgery, vazamento de informações sensíveis, redirecionamento e encaminhamento a sites não confiáveis.

BOAS PRÁTICAS PARA MITIGAÇÃO DE VULNERABILIDADES EM APLICAÇÕES WEB

Implementar autenticação e autorização de duas etapas, utilizar criptografias, limitar a exposição de informações sensíveis e ensinar para os usuários sobre segurança de sites e informações. Utilizando essas medidas de segurança, vai te proteger contra ameaças e vai garantir a sua integridade de dados e a usa privacidade.

SQL INJECTION

Injeção de SQL é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que trabalham com bases de dados realizando ataques com comandos SQL.

CONCLUSÃO

SÍNTESE DOS RESULTADOS E CONCLUSÕES DO TRABALHO PRÁTICO

Depois de ter executado toda a instalação do software para acessar a máquina virtual e ter feita a configuração dela, realizei tarefas de falhas na criptografia, onde eu compreendi melhor como são feitos as criptografias e os métodos utilizados para fazer. Percebi que tem todo um sistema lógico para cada tipo de criptografia, dificultado o acesso do invasor.

LIMITAÇÕES DO TRABALHO E SUGESTÕES PARA TRABALHOS FUTUROS

Teve links que estavam expirados, deixando com a dificuldade a instalação da máquina virtual, como também a sua configuração. Mas em si o trabalho foi interessante, pois mexemos com coisas diferentes, por exemplo a última vez que abri uma máquina virtual foi em 2019, fazer isso de novo foi interessante, pois pude reaprender o processo e a prender algumas vulnerabilidades do sistema. Como sugestão para futuros trabalhos deixar explicar mais algumas etapas, e utilizar links que estejam funcionado.

REFERÊNCIAS

https://developer.mozilla.org/pt-BR/docs/Learn/Server-side/First_steps/Website_security

https://www.cloudflare.com/pt-br/learning/security/what-is-web-application-security/

https://blog.4linux.com.br/conheca-as-10-principais-vulnerabilidades-web-de-2021/

https://trello.com/c/HorbZjhM/31-aula-7-dia-10-05-2023-seguran%C3%A7a-em-aplica%C3%A7%C3%B5es-web

https://trello.com/c/HorbZjhM/31-aula-7-dia-10-05-2023-seguran%C3%A7a-em-aplica%C3%A7%C3%B5es-web

CURITIBA

2023