**Cybersecurity 401**

**Module 8 - Web Application Security**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 39 - SQLi with Burp Suite, Web Goat**

## 

## 

**| Rodrigo Brasil 01/2024 |**

## **Tasks**

### **Part 1: Staging**

This lab requires Web Security Dojo VM with an internet connection (NAT mode is recommended).

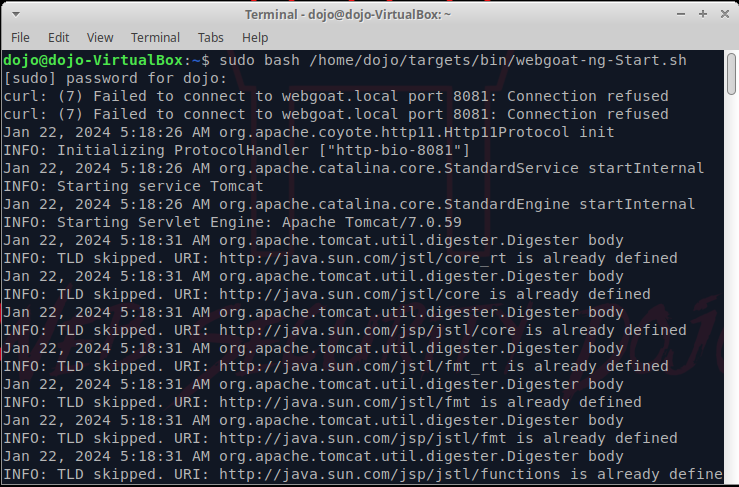


### 

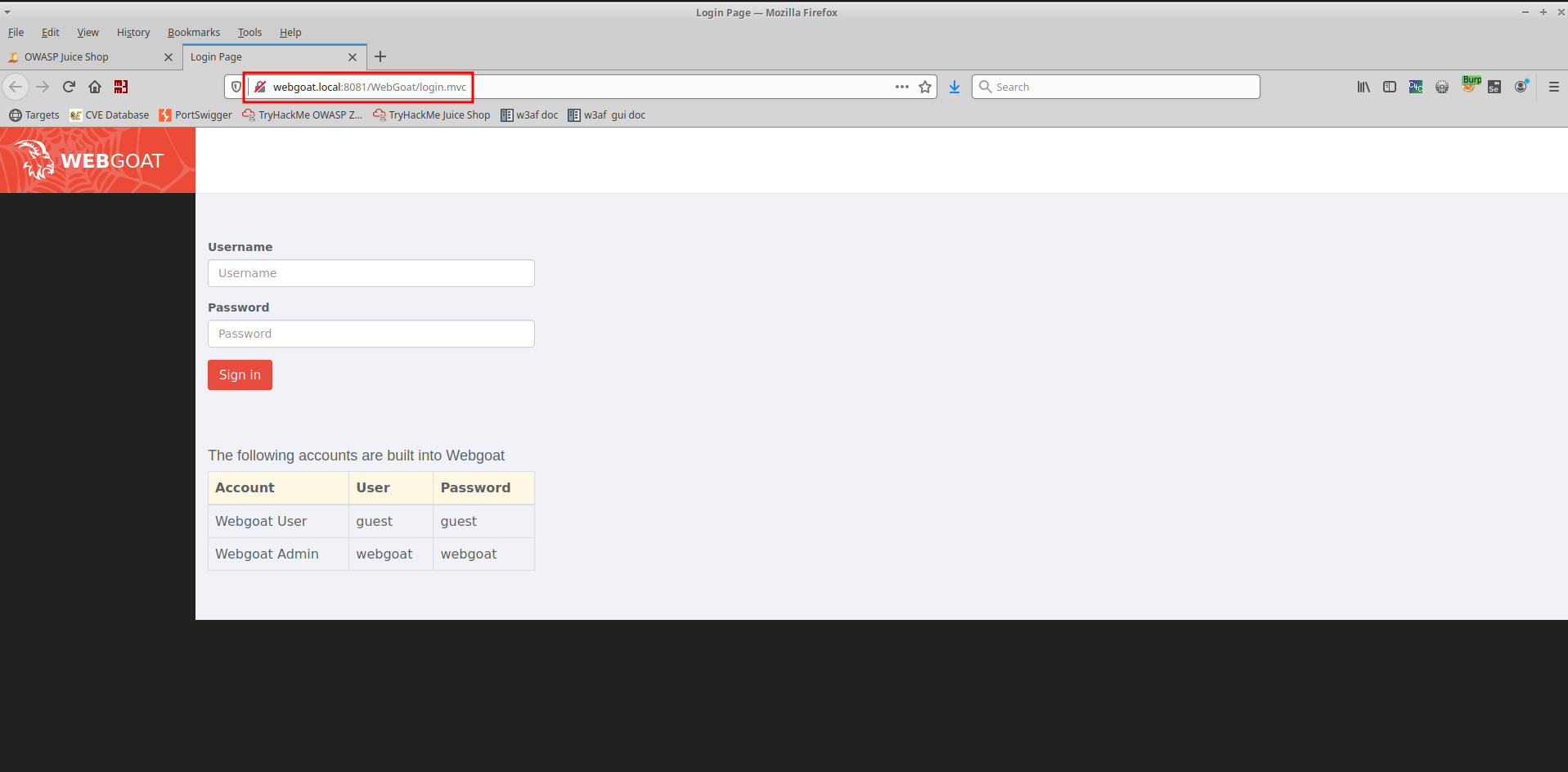
### **Part 2: OWASP Web Goat**

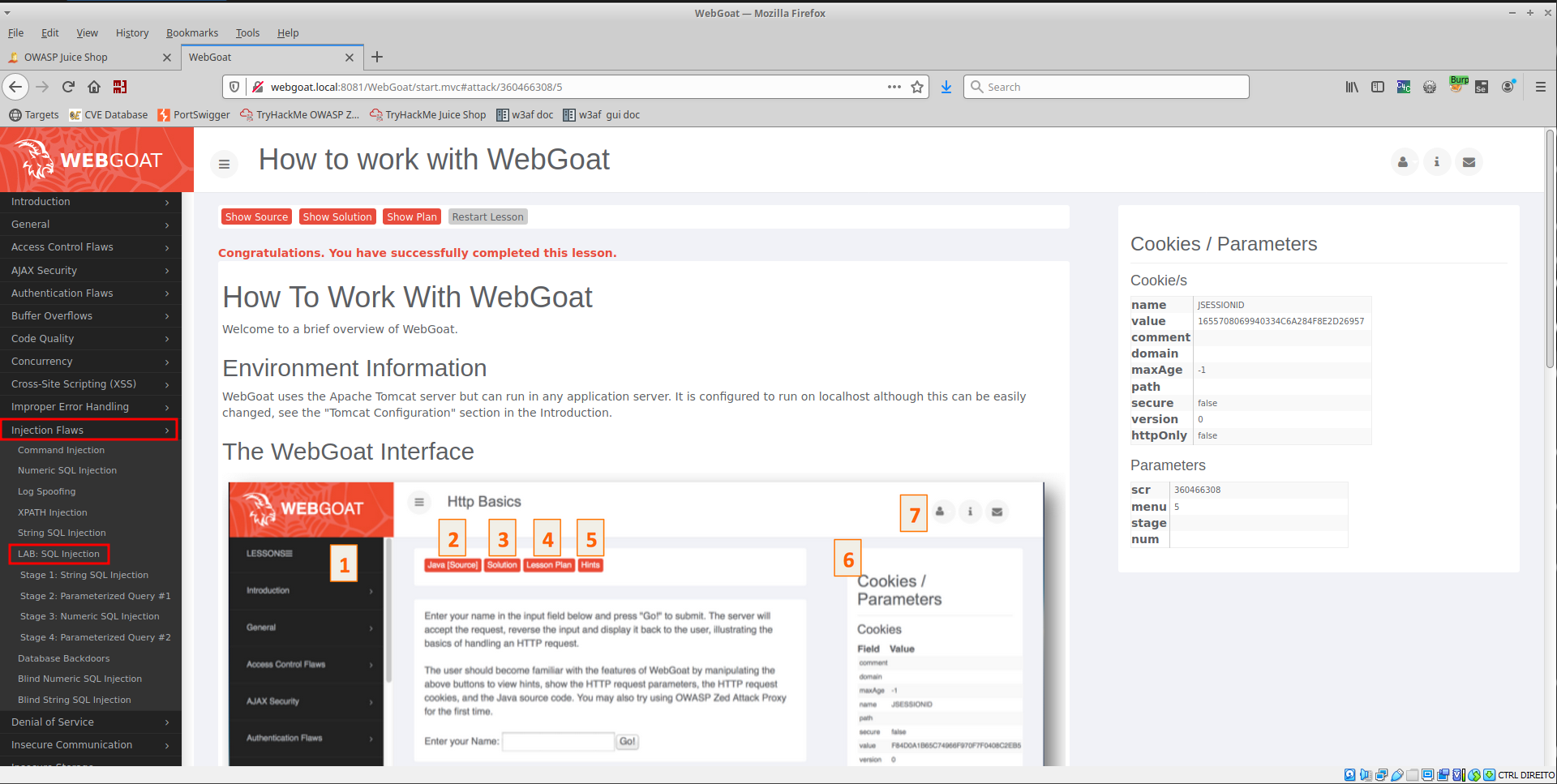
OWASP Web Goat comes preinstalled on Web Security Dojo.

* Web Goat does not start automatically in Security Dojo. You’ll need to start it manually from command line. Open a terminal in Security Dojo and enter **sudo bash /home/dojo/targets/bin/webgoat-ng-Start.sh** to initialize Web Goat.

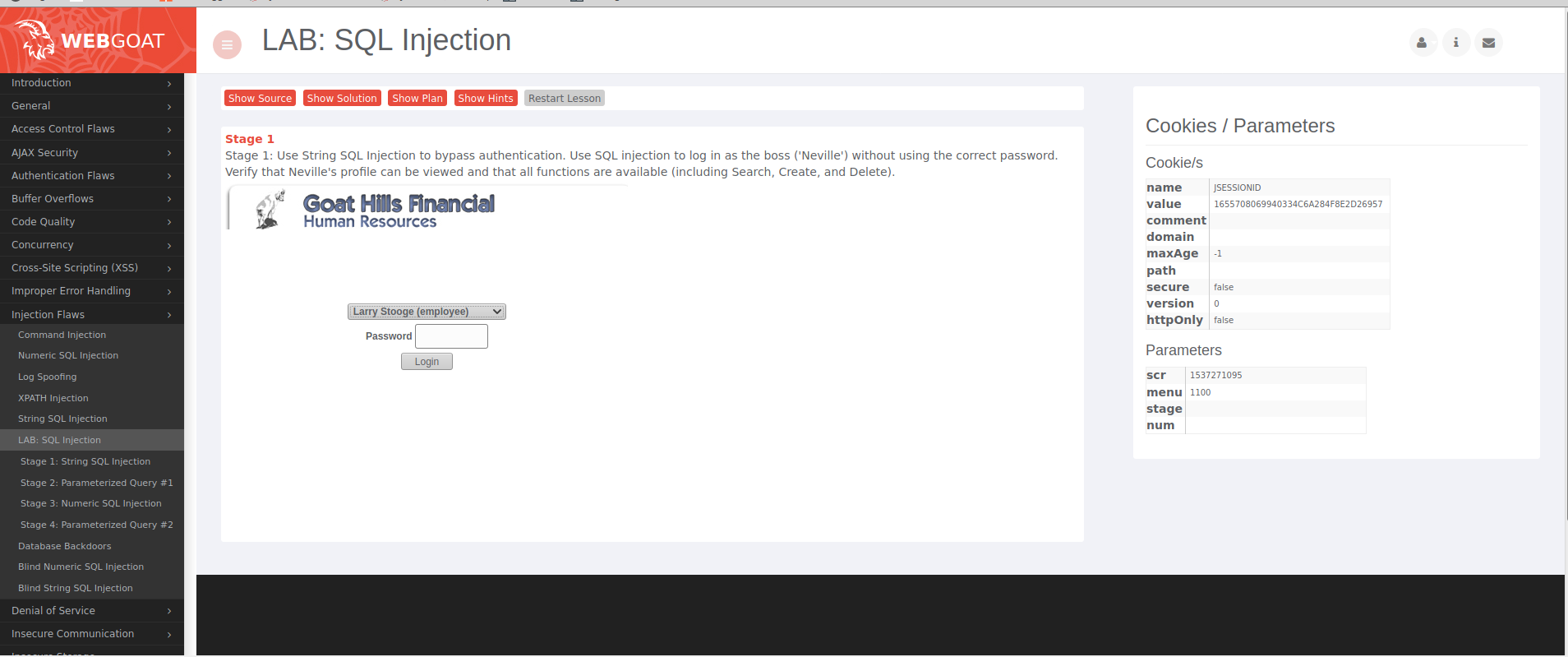


* In Firefox browse to **http://webgoat.local:8081/WebGoat/** and login as **guest**, password **guest**. If you encounter an “Unable to connect” error in Firefox, it means either Web Goat did not initialize correctly or the address was incorrectly typed.

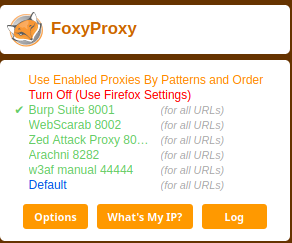


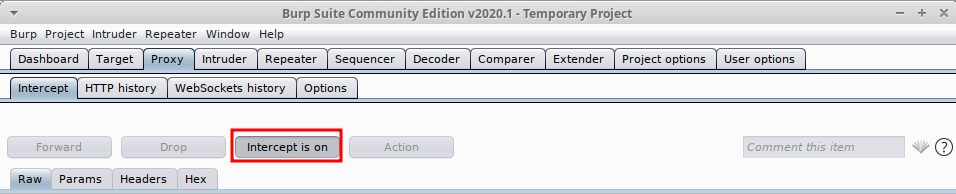


* On the left pane you’ll see various topics to explore (if you do not, Web Goat did not initialize correctly and you’ll need to **sudo reboot now** and try the above launch steps again). Navigate to Injection Flaws and complete the following sections:
  + String SQL Injection
  + LAB: SQL Injection
    - Stage 1: String SQL Injection
    - Stage 3: Numeric SQL Injection



* Turn on your proxy in your browser, and make sure **Intercept is on** in Burp Suite.





* If you get stuck, click “Show Hints” and click the arrow button repeatedly to view additional hints.
* Summarize what you did and learned in your submission.

### 

### **Part 3: Portswigger**

Portswigger is the company that created Burp Suite. They also happen to have a free training resource for web security students.

* Access [Portswigger Academy](https://portswigger.net/web-security/all-labs) and complete at least three of the SQL labs.
* Answer any questions/prompts in your submission doc, as well as explain the concept and what you did in each lab in detail.
* Clearly indicate why and how your solution works for the lab.

### 

### **Part 4: Reporting**

Answer the below questions in your own words:

* What is SQL injection?
* How is SQL injection detected?
* How can a web app developer defend against SQL injection?