

WebGoat的安装和使用

（郭苏越、游伟 中国人民大学）

webgoat是什么？

WebGoat是OWASP组织研制出的用于进行web漏洞实验的应用平台，用来说明web应用中存在的安全漏洞。WebGoat运行在带有java虚拟机的平台之上，当前提供的训练课程有30多个，其中包括：跨站点脚本攻击（XSS）、访问控制、线程安全、操作隐藏字段、操纵参数、会话cookie、SQL盲注、数字型SQL注入、字符串型SQL注入、web服务、Open Authentication失效、危险的HTML注释等等。WebGoat提供了一系列web安全学习的教程，某些课程也给出了视频演示，指导用户利用这些漏洞进行攻击。

owasp中关于webgoat的介绍：<http://www.owasp.org.cn/owasp-project/websec-platform/>

Github：<https://github.com/WebGoat/WebGoat>

安装过程

（注：我们提供的虚拟机里已经安装好了WebGoat，无需执行第1-4步，从第5步开始即可）。

1. 下载webgoat

地址：<https://github.com/WebGoat/WebGoat/releases>

05 Sep 2021

github-actions

v8.2.2

675cfbe

Compare

v8.2.2

Latest

Version 8.2.2

New functionality

- Docker image now supports nginx when browsing to <http://localhost> a landing page is shown.

Bug fixes

- [#1039 jst-7-Code review](#)
- [#1031 SQL Injection \(intro\) 5: Data Control Language \(DCL\) the wiki's solution is not correct](#)
- [#1027 Webgoat 8.2.1 Vulnerable_Components_12 Shows internal server error](#)

Assets

webgoat-server-8.2.2.jar	91.9 MB
webwolf-8.2.2.jar	51.3 MB
Source code (zip)	
Source code (tar.gz)	

14

3

3

17 people reacted

2. 检测Java环境

kali中已经预装Java环境

执行 下面指令

```
java --version
```

3. 创建一个新的文件夹webgoat，并把第一步下载的文件拖入文件夹中

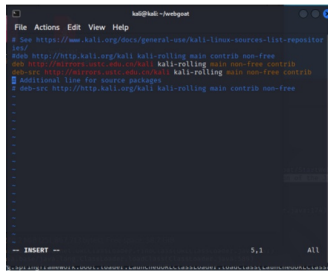
4. 升级java

换源：

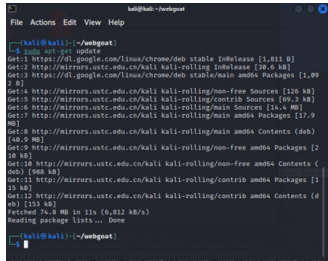
```
sudo vim /etc/apt/sources.list
```

把之前的源用#注释，并添加下面两个源：

```
deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
```



执行sudo apt-get update更新一下



java下载地址: https://download.oracle.com/java/17/latest/jdk-17_linux-x64_bin.tar.gz

下载之后拖入虚拟机中, 执行下面命令:

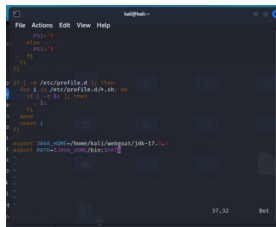
```
tar -zxvf jdk-17_linux-x64_bin.tar.gz
```

配置环境变量

```
sudo vim ~/.zshrc
```

把下面两句话粘贴到最后

```
export JAVA_HOME="/home/kali/webgoat/jdk-17.0.2"
export PATH=$JAVA_HOME/bin:$PATH
```

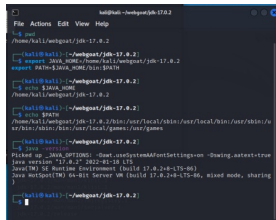


配置完成之后需要重启执行以下命令:

```
source ~/.zshrc
```

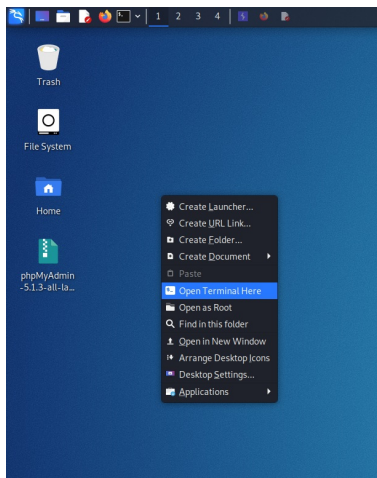
重新查看Java版本:

```
java --version
```



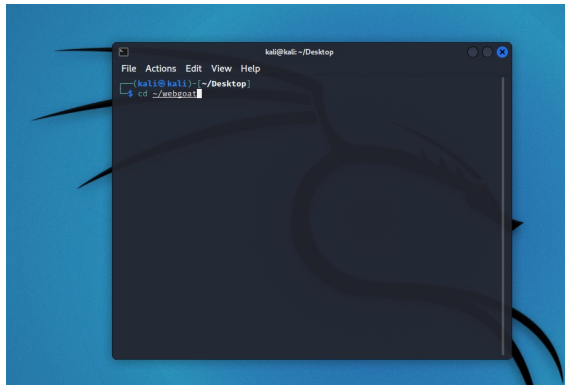
5. 启动webgoat

在桌面单击鼠标右键, 在弹出的右键菜单中选择"Open Terminal Here", 打开终端。



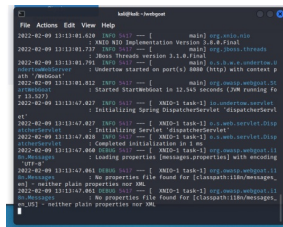
在终端中，执行以下命令进入webgoat文件夹：

```
cd ~/webgoat
```



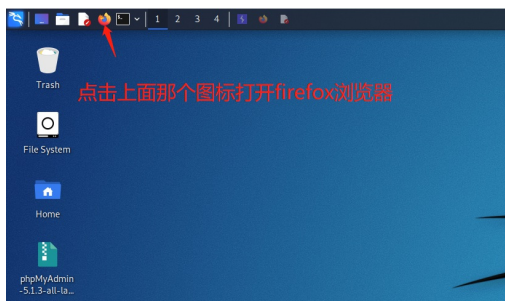
在终端中，执行以下命令启动webgoat:

```
java -jar webgoat-server-8.2.2.jar
```

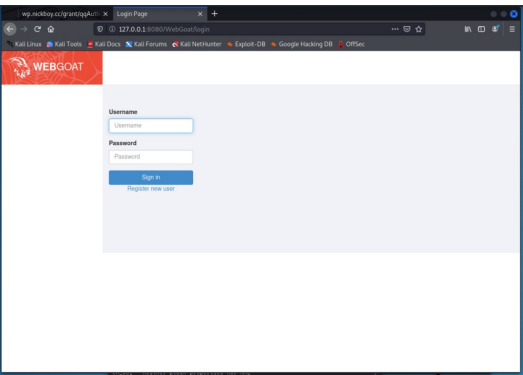


6. 浏览器直接访问WebGoat

点击屏幕上边栏中的firefox浏览器图标，打开firefox浏览器

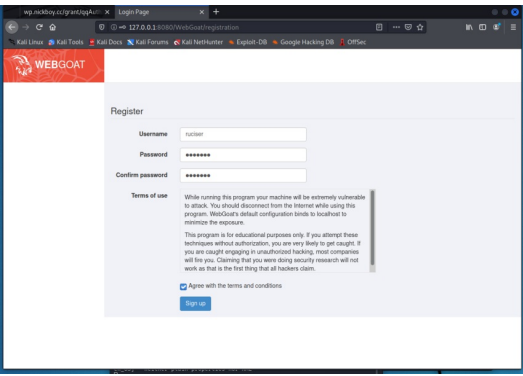


在浏览器的地址栏中输入地址<http://127.0.0.1:8080/WebGoat/login.html>

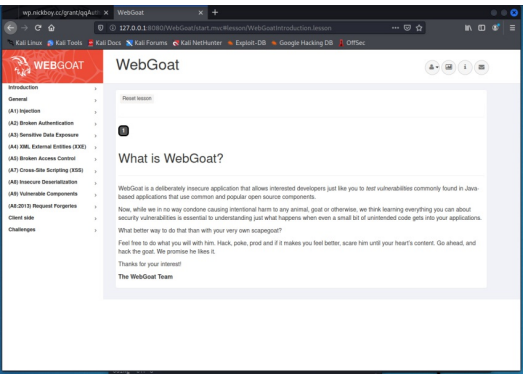


7. 注册新用户

注册一个account为ruciser, password为ruciser的账户

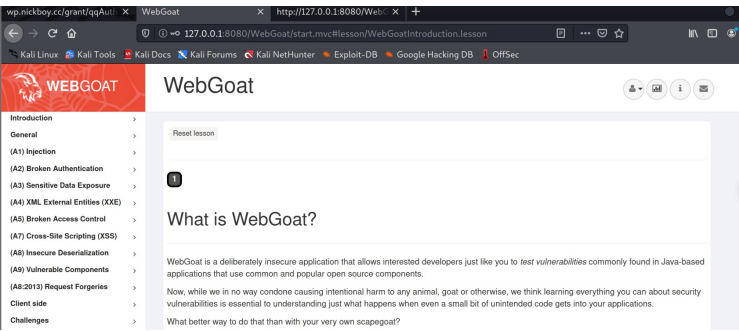


登录，下图为webgoat主界面

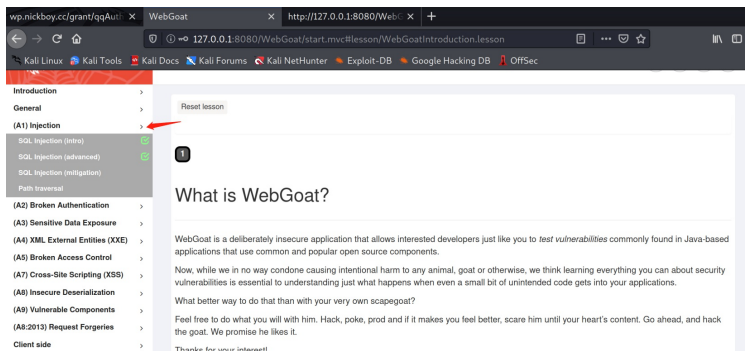


webgoat使用

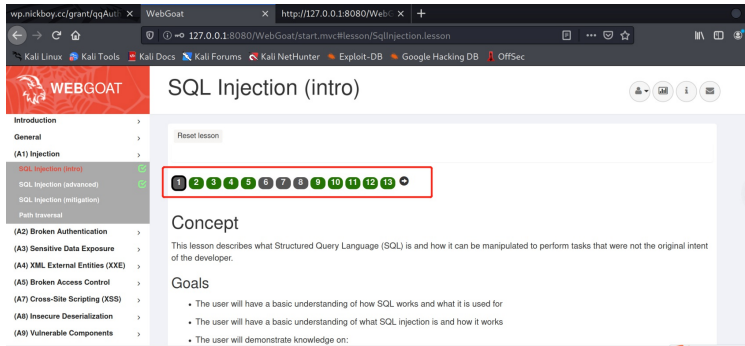
下图为webgoat初始界面



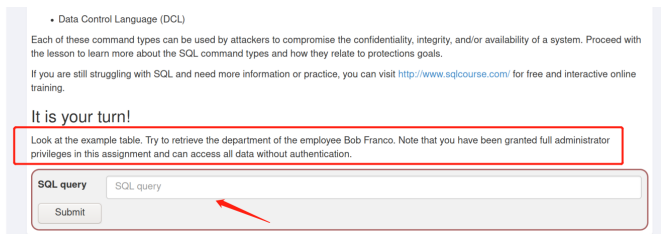
在界面左边是目录，webgoat提供了不同类型WEB漏洞的学习，点击相应的章节会显示章节的内容



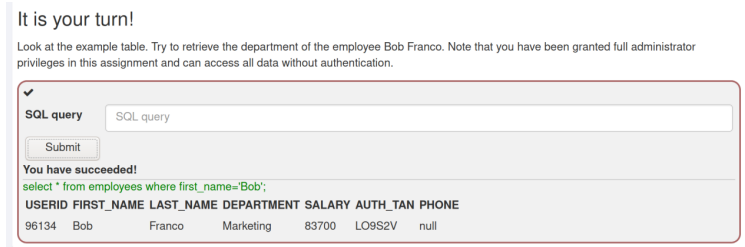
点击小标题进入到该小节中，每个小节有好几个关卡，如下图红框所示，灰色的部分是教学关卡，只需要阅读即可，绿色（红色）部分是实践关卡，完成练习之后按钮会从红色变为绿色



在每个实践关卡中，都会有任务说明（如下图红框），在箭头指示处填入答案



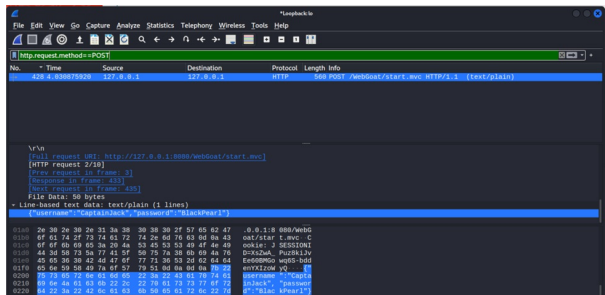
倘若答案正确，会有相应的提示



webgoat演示

insecure login

由于网络包中密码字段没有被加密，导致可以通过抓包获取用户名和密码



missing function level access control

通过阅读HTML源代码来获取隐藏功能

