Security lab Manager

Developed by Simon Owens
Security Engineer

Advisor/Sponsor: Mr. Mark Randall
University of Evansville

ABSTRACT

The Security Lab Manager is a web application that manages vulnerable virtualization machines for users to practice hacking on. Users can start hacking in their own virtual environment. Administrators can view completed exercises and send grades to users.

Features

- ❑ Launch exercises via GUI
- ❑ Automatic grading/emailing
- ❑ Configure all data via GUI
- ❑ Secure web portal
- ❑ Four full virtual exercises
- ❑ Scales to performance needs

Software

- ❑ Front End – JavaScript, JQuery, HTML5, CSS
- ❑ Back End – Django Framework, Python, Docker SDK, Bash, PostgreSQL
- ❑ Platform – Docker Linux Containers: Can run and develop on Windows or Linux if Docker is installed

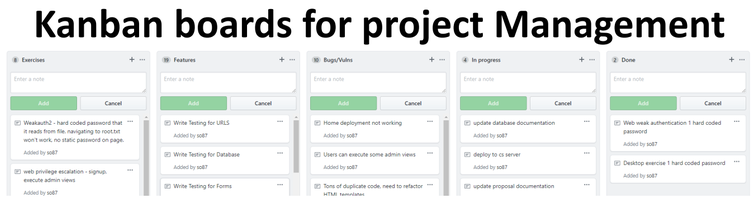
PROBLEM

Security training is desired in all parts of industry: secure coding for developers, Q/A Testers, and Security Engineers. There are several virtual machines to practice security, but none have a student-teacher model. Students can now easily begin learning security with just this application. The table below compares current options for learning security, bring your own device(BYOD), using VMware virtual machines, or this application.

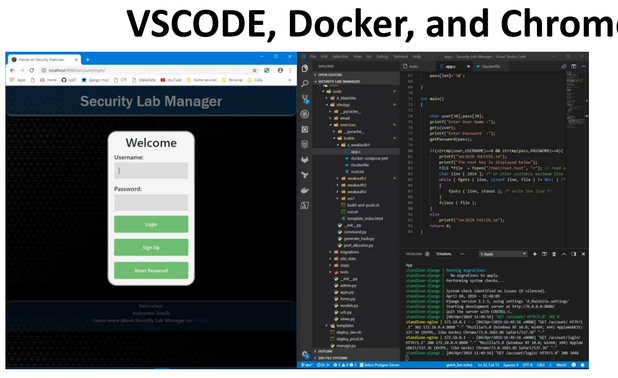
Features	BYOD	Virtual Machines	Security Lab Manager
Configured vulnerable exercises	✖	Some	✓
Downloaded/Configured debuging tools	✖	Some	✓
Cross-platform	✖	✓	✖
Exercise completion results in grade	✖	✖	✓
Unique answers to exercises	✖	✖	✓
Access Control	✖	✖	✓
Low computing resource requirements	✖	✖	✓
Requires only an internet browser	✖	✖	✓
Manage and email grades	✖	✖	✓

DEVELOPMENT

Kanban boards for project Management



VSCODE, Docker, and Chrome for development



Docker SDK for Python

A Python library for the Docker Engine API

Navigation

...

Docker SDK for Python

A Python library for the Docker Engine API. It lets you do anything the docker command does, but from within Python apps – run containers, manage containers, manage Swarms, etc.

For more information about the Engine API, see its documentation.

Django documentation

Everything you need to know about Django.

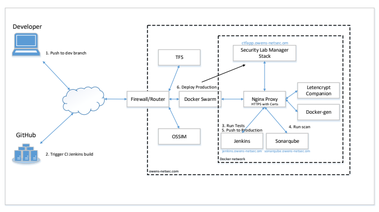
How the documentation is organized

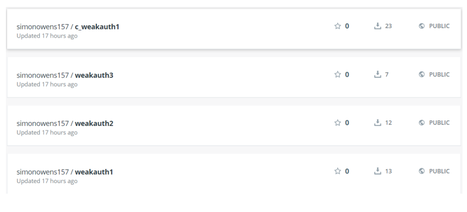
Django has a lot of documentation. A high-level overview of how it's organized will help you know where to look for certain things:

- Tutorials take you by the hand through a series of steps to create a Web application. Start here if you're new to Django or Web application development. Also look at the "First steps" below.
- Topic guides discuss key topics and concepts at a fairly high level and provide useful background information and explanation.
- Reference guides contain technical reference for APIs and other aspects of Django's machinery. They describe how it works and how to use it but assume that you have a basic understanding of key concepts.
- How-to guides are recipes. They guide you through the steps involved in addressing key problems and use-cases. They are more advanced than tutorials and assume some knowledge of how Django works.

Jenkins runs Anchore, Sonarqube, and ZAP scans

Store Security reports, push code and Docker images to source control, deploy to production





UNIVERSITY OF EVANSVILLE
EST 1854
Civic Mission…Sacred Trust

REQUIREMENTS

- ❑ Student interface for starting, stopping, and restarting exercises. There should also be a place to submit answers for exercises
- ❑ Instructor interface for creating, editing, deleting: classes, exercises, students, and managing application performance
- ❑ Instructors should be able to easily check and email grades
- ❑ Must contain one web security exercise
- ❑ Must contain one desktop security exercise
- ❑ Must be developed securely – scan for vulnerabilities and fix them
- ❑ Must be easily installed and enhanced by other developers

Secure

There are zero vulnerabilities in Anchore, Sonarqube, and ZAP

Efficient

The Docker Software Development Kit allows virtual machines to be built, started, and stopped in under 20seconds

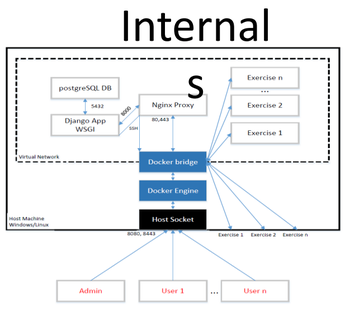
Functional

Student and instructor tasks can be easily done in seconds through the GUI

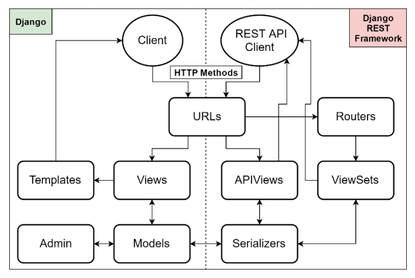
DESIGN

Components

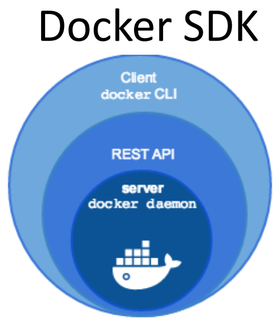
Internal



REST Framework

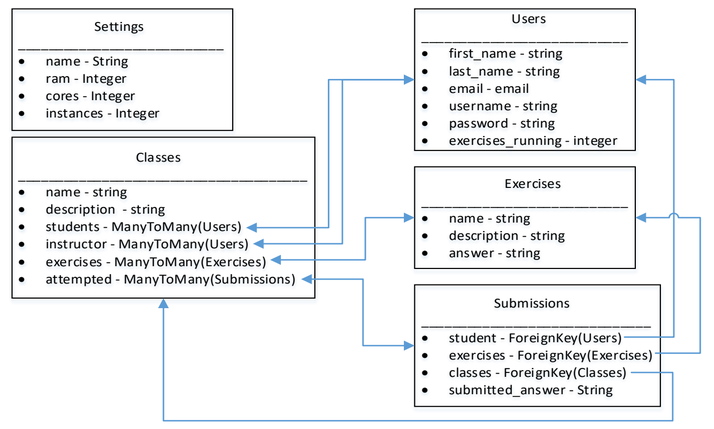


Docker SDK

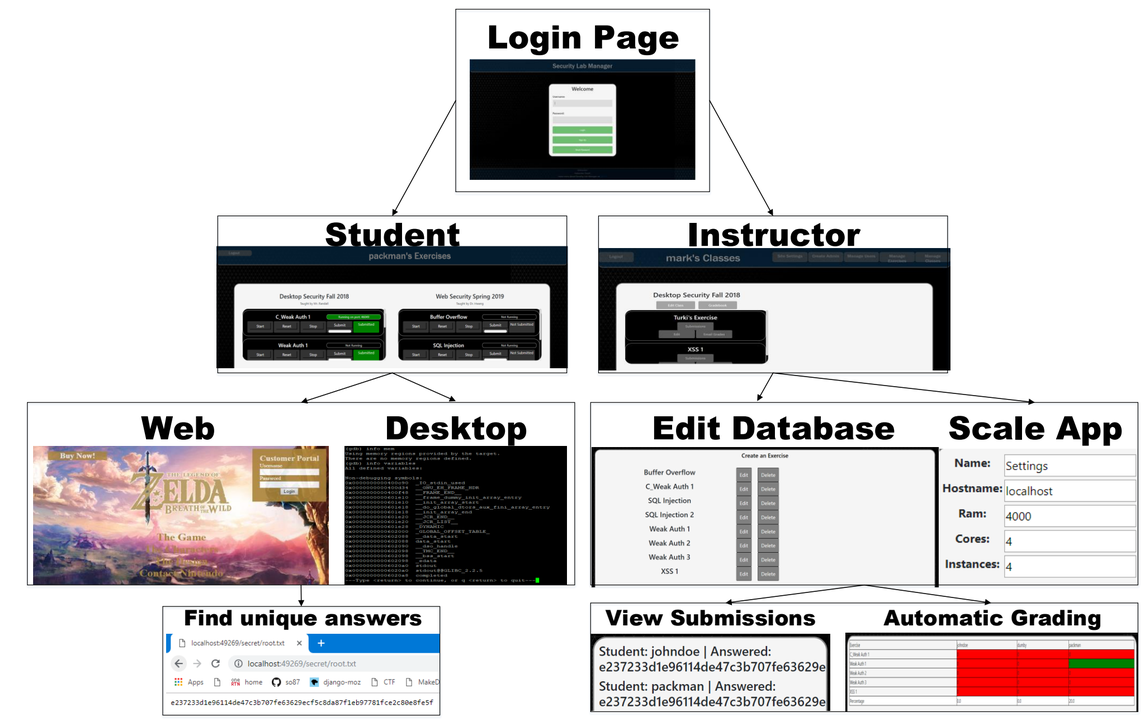


Database

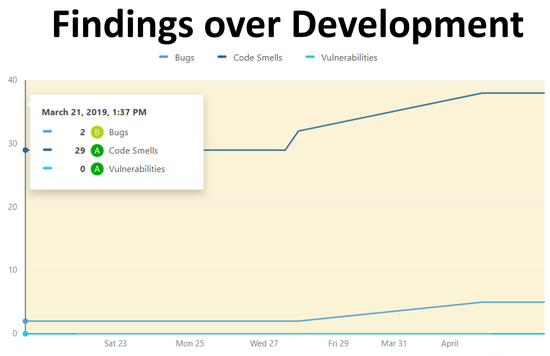
- ❑ Classes
- ❑ Exercises
- ❑ Submissions
- ❑ Users
- ❑ Settings



RESULT



Findings over Development



Codebase Size

New Lines	944
Lines of Code	2,740
Lines	3,112
Statements	586
Functions	44
Classes	35
Files	56
Comment Lines	82
Comments (%)	2.9%

Summary

The application met all requirements, is much more efficient than using virtual machines, and helps students learn security in a hands on way.