Lab 1

Chetan Sahrudhai Kimidi - ckimidi

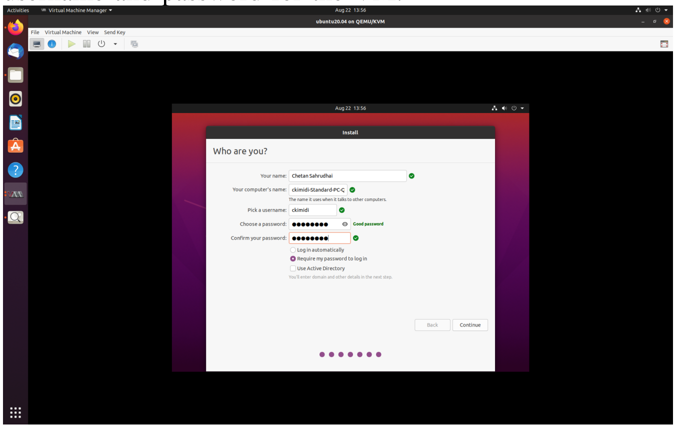
***Abstract*—Environment and required technical setup, along with installation of OWASP Webgoat, WebWolf and a DefendTheWeb find-the-password challenge.**

I. Introduction

OWASP, the Open Worldwide Application Security Project, is a part of the OWASP Foundation, which creates tools and specializes in web application security.[1] The application we installed into the virtual machines we created, in this lab, WebGoat, is one of their products, which is intentionally insecure, used primarily for educational purposes. Apart from this, we have also created a GitHub repository, setup remote desktop access and solved one of the introductory challenges.

II. VM Installation

Prior to WebGoat, I installed Ubuntu 20.04.6 LTS on the Ubuntu lab machine allocated to me. I customized the installation, as I wanted to tweak with the resources allocated to the VM. I allocated 2 CPUs, 4GB of RAM, 50GB of storage, chose NAT for the network and setup my username and password for the VM.



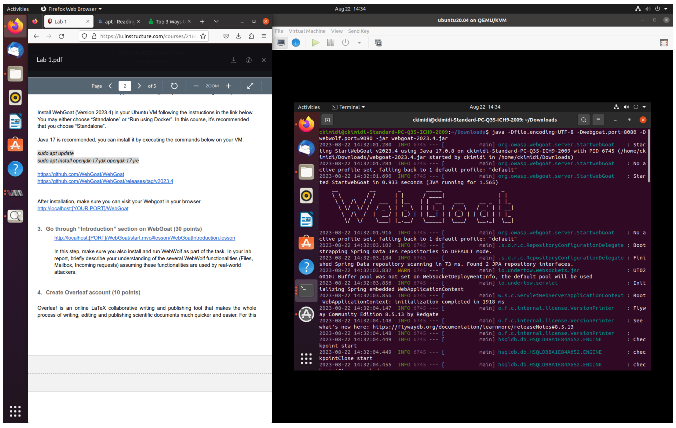
Who are you?

Your name: Chetan Sahrudhai
Your computer's name: ckimidi-Standard-PC-Q
The name it uses when it talks to other computers.
Pick a username: ckimidi
Choose a password: ●●●●●●●● Good password
Confirm your password: ●●●●●●●●
○ Log in automatically
● Require my password to log in
□ Use Active Directory
You'll enter domain and other details in the next step.

III. WebGoat Installation

As recommended in this course, I chose to install the Standalone version of WebGoat 2023.4 in my VM. This program is a demonstration of common server-side application flaws. The exercises are helpful in learning about application security and penetration testing techniques.[2] Since WebGoat installation requires Java on the VM, I installed Java and later WebGoat, using these commands:

```
sudo apt update
sudo apt install openjdk-17-jdk openjdk-17-jre
java -Dfile.encoding=UTF-8 -Dwebgoat.port=8080 -
Dwebwolf.port=9090 -jar webgoat-2023.4.jar
```



Install WebGoat (Version 2023.4) in your Ubuntu VM following the instructions in the link below. You may either choose “Standalone” or “Run using Docker”. In this course, it's recommended that you choose “Standalone”.

Java 17 is recommended, you can install it by executing the commands below on your VM:

sudo apt update
sudo apt install openjdk-17-jdk openjdk-17-jre

https://github.com/WebGoat/WebGoat
https://github.com/WebGoat/WebGoat/releases/tag/v2023.4

After installation, make sure you can visit your Webgoat in your browser
http://localhost:[YOUR PORT]/WebGoat

3. Go through “Introduction” section on WebGoat (30 points)

http://localhost:[PORT]/WebGoat/start.mvc#lesson/WebGoatIntroduction.lesson

In this step, make sure you also install and run WebWolf as part of the task. In your lab report, briefly describe your understanding of the several WebWolf functionalities (Files, Mailbox, Incoming requests) assuming these functionalities are used by real-world attackers.

4. Create Overleaf account (10 points)

Overleaf is an online LaTeX collaborative writing and publishing tool that makes the whole process of writing, editing and publishing scientific documents much quicker and easier. For this

```
ckimidi@ckimidi-Standard-PC-Q35-ICH9-2009:~/Downloads$ java -Dfile.encoding=UTF-8 -Dwebgoat.port=8080 -D
webwolf.port=9090 -jar webgoat-2023.4.jar
2023-08-22 14:32:01.280  INFO 6745 --- [           main] org.owasp.webgoat.server.StartWebGoat    : Star
ting StartWebGoat v2023.4 using Java 17.0.8 on ckimidi-Standard-PC-Q35-ICH9-2009 with PID 6745 (/home/ck
imidi/Downloads/webgoat-2023.4.jar started by ckimidi in /home/ckimidi/Downloads)
2023-08-22 14:32:01.284  INFO 6745 --- [           main] org.owasp.webgoat.server.StartWebGoat    : No a
ctive profile set, falling back to 1 default profile: "default"
2023-08-22 14:32:01.690  INFO 6745 --- [           main] org.owasp.webgoat.server.StartWebGoat    : Star
ted StartWebGoat in 0.933 seconds (JVM running for 1.565)

2023-08-22 14:32:01.916  INFO 6745 --- [           main] org.owasp.webgoat.server.StartWebGoat    : No a
ctive profile set, falling back to 1 default profile: "default"
2023-08-22 14:32:03.102  INFO 6745 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Boot
strapping Spring Data JPA repositories in DEFAULT mode.
2023-08-22 14:32:03.184  INFO 6745 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Fini
shed Spring Data repository scanning in 73 ms. Found 2 JPA repository interfaces.
2023-08-22 14:32:03.832  WARN 6745 --- [           main] io.undertow.websockets.jsr               : UT02
6010: Buffer pool was not set on WebSocketDeploymentInfo, the default pool will be used
2023-08-22 14:32:03.856  INFO 6745 --- [           main] io.undertow.servlet                      : Init
ializing Spring embedded WebApplicationContext
2023-08-22 14:32:03.856  INFO 6745 --- [           main] w.s.c.ServletWebServerApplicationContext : Root
 WebApplicationContext: initialization completed in 1918 ms
2023-08-22 14:32:04.147  INFO 6745 --- [           main] o.f.c.internal.license.VersionPrinter    : Flyw
ay Community Edition 8.5.13 by Redgate
2023-08-22 14:32:04.148  INFO 6745 --- [           main] o.f.c.internal.license.VersionPrinter    : See
what's new here: https://flywaydb.org/documentation/learnmore/releaseNotes#8.5.13
2023-08-22 14:32:04.148  INFO 6745 --- [           main] o.f.c.internal.license.VersionPrinter    :
2023-08-22 14:32:04.449  INFO 6745 --- [           main] hsqldb.db.HSQLDB8A1E84A652.ENGINE        : Chec
kpoint start
2023-08-22 14:32:04.449  INFO 6745 --- [           main] hsqldb.db.HSQLDB8A1E84A652.ENGINE        : chec
kpointClose start
2023-08-22 14:32:04.455  INFO 6745 --- [           main] hsqldb.db.HSQLDB8A1E84A652.ENGINE        : chec
```

I downloaded the necessary JAR from the release repo [3]. After successful installation of WebGoat, I noted down the port was 8080, from the log, and then opened it in the browser using the link, http://localhost:8080/WebGoat.

IV. ”Introduction” section and WebWolf

After signing up on the WebGoat application, I read the Introduction section and about how I can poke, prod or hack my own scapegoat a.k.a. WebGoat, and learn all the essential techniques.

Then, I ran and signed up on WebWolf, as seen in Fig. 1, while WebGoat is already running, by clicking on the appropriate icon in the top-right area.

WebWolf is a separate web application which simulates an attackers machine. Using this, we can learn what takes place on the attacked site and the actions we need to do as an attacker.[4]

WebWolf primarily offers functionalities such as file uploads, mailbox facility and access to incoming requests. Usually, 9090 is the default port. The following is my brief understanding of each functionality, assuming they are used by real-world attackers:

1. Attackers can upload files in a hosted URL.
2. The attacker has a mailbox, to which all the user's mails are redirected to.
3. A simple httpd server (no need of local installation) functionality is offered, which logs the incoming requests, which can then be accessed on the webwolf/landing/ page.

V. GitHub Repo and Overleaf Setup

I already have an Overleaf account, which I am currently using to write this report, so I skipped the account creation step. I downloaded the suggested report template, for further usage.

I created a repository on IU GitHub, to save all my lab reports, following the required naming conventions, and also added both the professor and the AI as collaborators to it. The repository can be found here.

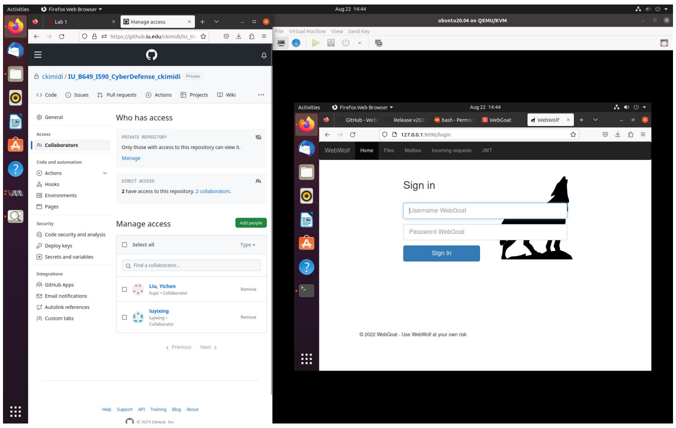
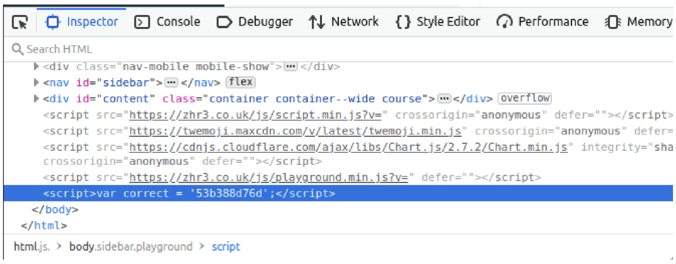


Fig. 1. GitHub repo creation and WebWolf signup successfully.

VI. Stretch Goals

In this optional/bonus task, I was given a challenge, where I had to find out the password, while landing on a login page. My approach to solve this was searching out the password phrase, using the Inspect element browser feature, since the code of the page we view is accessible there. Once I pressed F12 and scrolled to the bottom, I came across the correct password phrase, from the JavaScript code present i.e. the script tag, as in Fig. 2.



```
▸ <div class="nav-mobile mobile-show">⋯</div>
▸ <nav id="sidebar">⋯</nav> flex
▸ <div id="content" class="container container--wide course">⋯</div> overflow
  <script src="https://zhr3.co.uk/js/script.min.js?v=" crossorigin="anonymous" defer=""></script>
  <script src="https://twemoji.maxcdn.com/v/latest/twemoji.min.js" crossorigin="anonymous" defer=
  <script src="https://cdnjs.cloudflare.com/ajax/libs/Chart.js/2.7.2/Chart.min.js" integrity="sha
  crossorigin="anonymous" defer=""></script>
  <script src="https://zhr3.co.uk/js/playground.min.js?v=" defer=""></script>
  <script>var correct = '53b388d76d';</script>
 </body>
</html>
html.js > body.sidebar.playground > script
```

Fig. 2. Solution to the DefendTheWeb challenge

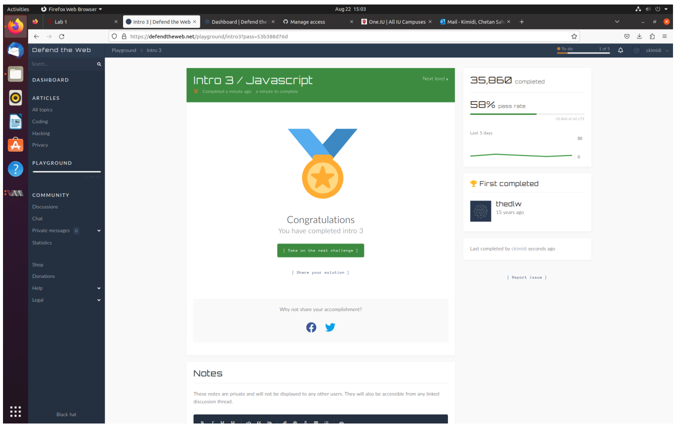
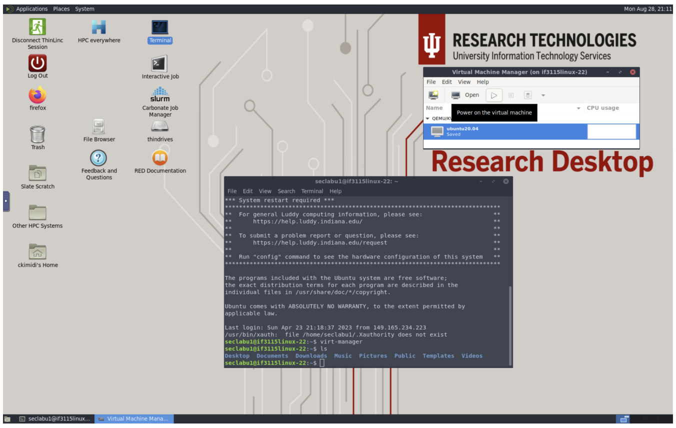


Fig. 3. Intro3 Challenge SOLVED!

VII. Remote Desktop Setup

To access my VM from home, I created my Carbonate account in class. After an hour, I logged into RED and accessed the lab machine using ssh. From the command line, I checked if I was able to access the VM, and it was working as expected.

Then, I resumed the VM, which I had saved in its state, as seen in Fig. 4.


RESEARCH TECHNOLOGIES
University Information Technology Services
Research Desktop
Virtual Machine Manager (on if3115linux-22)
Power on the virtual machine
ubuntu20.04
Saved

```
*** System restart required ***
******************************************************************************
**  For general Luddy computing information, please see:                    **
**      https://help.luddy.indiana.edu/                                     **
**                                                                          **
**  To submit a problem report or question, please see:                     **
**      https://help.luddy.indiana.edu/request                              **
**                                                                          **
**  Run "config" command to see the hardware configuration of this system   **
******************************************************************************

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Apr 23 21:18:37 2023 from 149.165.234.223
/usr/bin/xauth:  file /home/seclabu1/.Xauthority does not exist
seclabu1@if3115linux-22:~$ virt-manager
seclabu1@if3115linux-22:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
seclabu1@if3115linux-22:~$ 
```

Fig. 4. Remotely accessing my lab machine and the VM

VIII. Conclusion

In summary, I have successfully installed a new VM, and then installed WebGoat and WebWolf onto it, in this lab. I solved the Intro3 challenge (bonus task), as well. I have also created a GitHub repository for accessing all my lab reports easily, and also setup my remote desktop, to continue any unfinished lab work or to access my VM at home.

References

[1] OWASP Foundation
[2] GitHub Repository of WebGoat
[3] WebGoat 2023.4 Release JAR
[4] WebWolf Docs