University of Roehampton London

School of Arts, Humanities and Social Science

Module title and code: 2023.24 Security Testing - CMP020N211S

Title of coursework: Portfolio 01

Learning outcomes:	Add all that apply, e.g. • LO3: Apply appropriate practices, tools, and techniques in the context of a given security testing scenario. • LO4: Synthesise, analyse and present the outcomes of a given security testing engagement, as a report or presentation.LO1: Investigate and apply measures that can be taken to prevent or mitigate the undesirable effects of cyber-crime.
Assessment weighting	20%
Maximum mark	100
Submission details (e.g. submission link)	In-class Demonstration Moodle Submission Link
Word limit (if applicable)	N/A
Date set	23/02/2024
Deadline	19/02/2024
Feedback and marks	Verbal and Rubric by: 19/02/2024
Assessment setter's name	Dr Charles Clarke

Academic Misconduct:

"Academic integrity and honesty are fundamental to the academic work you produce at the University of Roehampton. You are expected to complete coursework which is your own and which is referenced appropriately. The university has in place measures to detect academic dishonesty in all its forms. If you are found to be cheating or attempting to gain an unfair advantage over other students in any way, this is considered academic misconduct, and you will be penalised accordingly."

Further details about "Student Code of Conduct" and "Disciplinary Regulations" can be found at:

https://www.roehampton.ac.uk/corporate-information/policies/

Assessment introduction (if applicable):

IMPORTANT: This is a “live” document and will be subject to changes and updates during the life cycle of the lab portfolio. Therefore, it is imperative that you check this document regularly!! This portfolio includes both assessment and employability learning journeys.

The focus of this portfolio is developing your individual security testing skillset and practical knowledge of web security vulnerabilities and how to exploit them. This maps to stages 3 (Identify vulnerabilities) and 4 (Exploit weaknesses) in the CREST Penetration Testing process we have discussed.

You are learning to think like an attacker, building your awareness and practical experience with offensive security tools, and learning to applying these skills to a selection of problems.

You are going to focus on web application security testing. This is a very large and complex area of security testing. Therefore, you are going to focus on a small subset of the most common and most impactful vulnerabilities. This will enable you to build your knowledge and skills in a structured and progressive manner.

1. Deploy a vulnerable web application (OWASP Juice Box) using VirtualBox.
2. Deploy a virtual machine for security testing using VirtualBox.
3. Learn about and practice using security testing tools.
4. Learn about, discover, and exploit common web vulnerabilities.

A diagram of what you will deploy is shown in Figure 1.

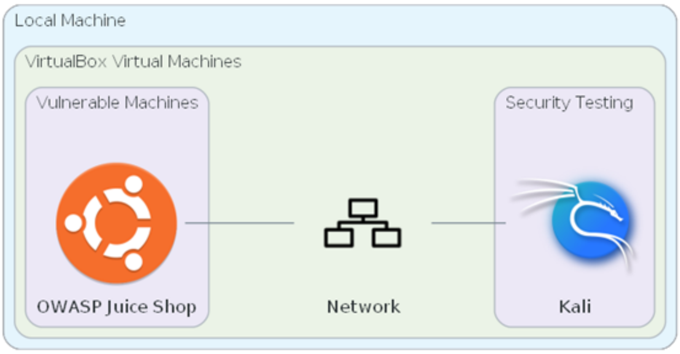

Figure 1. Deployment Concept

5. You will also complete a job search employability activity that relates to the skills and technologies that you will use in this portfolio.

Resources Required for this Portfolio Lab

This lab requires two virtual machines. You therefore need a type 2 hypervisor available (e.g., VirtualBox, UTM, Hyper-V). For Windows machines, Macs with Intel processors and Linux PCs, we recommend VirtualBox. For Macs with Apple Silicon (e.g., M1, M2, M3 processors), we recommend UTM.

Using a Lab PC?

VirtualBox has already been installed in the DB117.

Using your own Laptop or PC?

If you plan to run this lab portfolio on your own laptop, you will need to have a minimum of 8 GB of RAM.

Requirements

Requirement 1. Setup your security testing environment

Getting Started

1) Deploy an OWASP Juice Shop virtual machine. This will be made available to you via USB or you can choose to install OWASP Juice Shop for yourself.

2) Deploy a Kali Linux virtual machine as your security testing workstation. You might also want to try using ParrotOS Security Edition. You can download it here.

3) Configure both virtual machines in accordance with the minimum specifications shown in Tables 1 and 2.

Virtual Machine Specifications

Property	Value
Use case	OWASP Juice Shop server
CPUs	2
RAM	2 GB
Operating System	Ubuntu 22.04
Network Adaptor 1	NAT
Network Adaptor 2	192.168.123.1 (Internal Network)
Source	Pre-built, cloned or ISO
Install	nodejs version 16, npm, git
Source for OWASP Juice Shop	git clone https://github.com/juice-shop/juice-shop.git –depth 1
Useful Link(s)	https://owasp.org/www-project-juice-shop/
Credentials	User: student Password: Student1

Table 1: OWASP Juice Shop Virtual Machine

Property	Value
Use case	Security Testing workstation
CPUs	2
RAM	4 GB
Operating System	Kali Linux
Network Adaptor 1	NAT
Network Adaptor 2	192.168.123.10 (Internal Network)
Source	Pre-built, cloned or ISO
Credentials	User: kali Password: kali

Table 2: Security Testing workstation Virtual Machine

Requirement 2. OWASP Juice Shop Functionality Testing

When conducting a security test, you will need to understand what and how the application normally works. Therefore, you should be able to answer the following questions:

- What are the features and functions of the application?
- What are the inputs and outputs of the application?
- What are the expected and unexpected behaviours of the application?

To help you answer these questions, you will need to conduct a functionality test. This is a manual process that involves interacting with the application and observing the outcomes. You will need to document your findings in your lab notebook.

1) Visit the following URL: https://pwning.owasp-juice.shop/part1/happy-path.html and work through the advice presented.

2) Map out the functionality of the website. For example, using a mind map, table, or site map from within Burp Suite or OWASP Zed Attack Proxy.

3) Complete the Scope template for the site you are planning to test and add it to your git repository.

4) Demonstrate your functionality testing and your scope agreement to your instructor for approval to proceed.

Note: Ensure you capture your work in your lab notebook.

Requirement 3. Exploit a Cross-Site Scripting vulnerability

1) Research Cross Site Scripting here: https://owasp.org/www-community/attacks/xss/.
2) Visit https://pwning.owasp-juice.shop/part2/xss.html (and any other resources that may be helpful to you). Implement an example of a Cross-Site Scripting Attack against your OWASP Juice Shop virtual machine.

3) Note: Ensure you capture your work, including failed attempts, in your lab notebook.

Requirement 4. Exploit a SQL injection vulnerability.

1) Research SQL Injection attacks here: https://owasp.org/www-community/attacks/SQL_Injection.

2) Visit https://pwning.owasp-juice.shop/part2/injection.html (and any other resources that may be helpful to you). Implement an example of an SQL injection attack against your OWASP Juice Shop virtual machine.

Note: Ensure you capture your work, including failed attempts, in your lab notebook.

Requirement 5. Exploit a Broken Access Control vulnerability.

1) Research Broken Access Control here: https://owasp.org/www-community/Broken_Access_Control.

2) Visit https://pwning.owasp-juice.shop/part2/broken-access-control.html (and any other resources that may be helpful to you). Implement an example of a Broken Access Control exploit against your OWASP Juice Shop virtual machine.

Note: Ensure you capture your work, including failed attempts, in your lab notebook.

Requirement 6. Exploit an Authentication Bypass vulnerability.

1) Research Broken Authentication here: https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication.

2) Visit https://pwning.owasp-juice.shop/part2/broken-authentication.html (and any other resources that may be helpful to you). Implement an example of an Authentication Bypass exploit against your OWASP Juice Shop virtual machine.

Note: Ensure you capture your work, including failed attempts, in your lab notebook.

Requirement 7. Exploit an Improper Input Validation vulnerability.

1) Research Improper Input Validation here: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html.

2) Visit https://pwning.owasp-juice.shop/part2/improper-input-validation.html (and any other resources that may be helpful to you). Implement an example of an Improper Input Validation exploit against your OWASP Juice Shop virtual machine.

Note: Ensure you capture your work, including failed attempts, in your lab notebook.

Requirement 8. Exploit a Sensitive Data Exposure vulnerability.

1) Research Sensitive Data Exposure here: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.
2) Visit https://pwning.owasp-juice.shop/part2/sensitive-data-exposure.html (and any other resources that may be helpful to you). Implement an example of a Sensitive Data Exposure exploit against your OWASP Juice Shop virtual machine.

Note: Ensure you capture your work, including failed attempts, in your lab notebook.

Requirement 9. Maintain a lab notebook detailing your work.

An important part of any security test is recording what you have done and why as you go. It is important because you will need it when you come to write your report. You are going to create and maintain a lab notebook on your own **private GitHub** repository. You will use **markdown** to create your notebook.

Your lab notebook:

- Must be written in markdown and should be stored in a git repository.

- Is a mandatory document that you must use to record your work. It is not optional.

- Is a private document that you will use to record your work. It is not to be shared with others.

- Is a "living" document that you will update as you work through the lab. It is not a report.

- Is a personal document that you will use to record your thoughts, ideas, questions, and answers.

- Is not a formal document.

Here are some suggestions of what to include:

- The work you have done.
- The environment you used.

- The system under test.
- The vulnerabilities you discovered.
- How you exploited the vulnerabilities if you were able to.
- What you learned from this lab.
- Questions you have about the system.
- Your understanding of the system
- Commands you have run.
- Output from commands
- Diagrams (text, mermaid, photo of a paper sketch)
- Explanations of what you have done and why.
- Next steps you plan to take.

You may wish to use the template provided, but at a minimum we recommend that you include the following information:

```
# Lab Notebook

- **Student Name:** (name)
- **Student ID:** (id)
- **Lab:** (lab)
- **Date:** (date)

## Introduction

Describe the aim of this lab.

## Agreed scope

Summarise the agreed scope.

## Activity

Notes on your actions and observations.
```

Requirement 10: Complete the Job Search Employability Activity.

1) Visit one of the following job sites.
    - https://www.joblist.com/
    - https://www.totaljobs.com/
    - https://www.cwjobs.co.uk/
    - https://www.technojobs.co.uk/
    - https://wellfound.com/jobs
    - https://builtin.com/jobs
    - https://www.crunchboard.com/
    - https://www.dice.com/
    - https://jobspresso.co/
    - https://uk.indeed.com/q-uk-tech-jobs.html?vjk=d68ad7a6d5b165a2
    - https://www.reed.co.uk/jobs/technology-jobs

    - https://otta.com/
    - https://technet-it.co.uk/jobs/

2) Search for a job that interests you.

3) Read the job description and requirements.

4) Complete the survey required here: https://forms.office.com/e/HmBZM7Rkha

NOTE: You can submit to this survey as many times as you want to.

Wow factor suggestions.

It is feasible to pass this portfolio without completing any "wow factor." However, if you decide to take on this additional learning opportunity, the choice of what to contribute is yours. Here are some examples to consider:

- Perform and evidence a comprehensive functionality test.

- Research and discover hidden OWASP Juice Shop assets.

- Demonstrate the use of Zed Attack Proxy as an integral part of your security testing activities.

- Exploit additional vulnerabilities, either of the same type or different types.

- Approach a vulnerability with an alternative tool, for example:

    1. Burp Suite
    2. OWASP Zed Attack Proxy (ZAP)
    3. Charles Proxy
    4. mitmproxy

- Experiment with different tools, for example:
    - SQLMap for SQLi
    - XSStrike for XSS

- Deploy and test an additional vulnerable web application, for example:
    - OWASP WebGoat
    - OWASP Security Shepherd

    - Damn Vulnerable Web Application (DVWA)

Demonstration Tasks

To receive a mark for this work, you must:

1) demonstrate the extent to which you have completed the requirements and specifications of this portfolio, to your instructor. You must demonstrate Requirements 3, 4, 5, 6, 7 and 8.

2) upload your lab notebook to Moodle (Requirements 9 and 10).

NOTE: In order to ensure that instructor assessment time fairly distributed, each student is permitted one formal demonstration period in each lab session. After this, marks and an outcome will be published via a Moodle rubric.

End of Portfolio :-)