FIT2093 Introduction to Cybersecurity - 2023

Assignment 3: Web hacking Challenge

Purpose	Your goal is to do security testing of a mini web application to identify web application vulnerabilities in it, using the techniques covered in our Web and database security lectures. Then, the goal is to demonstrate how to exploit the vulnerabilities discovered to break the app's security.
Your task	This assignment is an individual assessment. Apply your penetration testing techniques in assessing web application and SQL vulnerabilities.
Value	**10**% of your total marks for the unit
Page / Time Limit	**ONE** Individual video**:** Presentation **up to 10 minutes** **Note:** mark deductions will apply for presentations over the 10 minutes limit
Due Date	**9 June 2023 11:55 pm Melbourne time**
Submission	Individual video as a **mp4** for Part A-D via Moodle assignment submission Individual video slides as a **ppt** via Moodle assignment submission
Assessment Criteria	*Please see the assessment criteria as given in sections below.*
Late Penalties	● 10% deduction per calendar day or part thereof for up to one week ● Submissions more than 7 calendar days after the due date will receive a mark of zero (0) and no assessment feedback will be provided.
Feedback	Feedback will be provided on student work via: ● general cohort performance ● specific student feedback ten working days post submission

Overview of the assignment

The assignment is worth 10% of your total unit mark.

In **Part A** of the assignment (weight: 2.5% of your unit mark), you will demonstrate your understanding of XSS security vulnerabilities by testing the web application such vulnerabilities and assessing whether any vulnerabilities you find can potentially be exploited by an attacker.

In **Part B** of the assignment (weight: 2% of your unit mark), you will demonstrate your understanding of client-side penetration testing techniques to attempt to bypass the web application's mechanism for enforcing access control to private documents to authorised users.

Part C of the assignment (weight 2.5% of your unit mark) requires you to demonstrate your skills in testing for SQL injection vulnerabilities in a part of the web application that makes queries to an SQL database, and exploit any vulnerabilities you discover to breach gain unauthorised access to the database.

Part D of the assignment (weight 2% of your unit mark) requires you to explain the relation of parts A-C to individual privacy and ethics.

You will prepare and submit an individual **10 minute video presenting** your tests, results and explanations for tasks A-D. Your video presentation slides (in powerpoint format) should also be submitted.

The clarity of your video and slides presentation will count towards 1% of your total mark for the assignment. Please ensure your voice during the video presentation is clearly audible.

Assessment Details

Task	**Rubric**
Part A	2.5% ■ Task A.1 (1.0%): list of potential XSS vulnerability points (0.6%) and (0.4%) ■ Task A.2 (1.5%): for testing techniques (0.3%), tests results (0.6%) and explanation for each result (0.3%), vulnerability (0.15%) and mitigation (0.15%)
Part B	2% ■ Task B.1 (2%): testing(s) techniques (0.5%) and interpretation (0.5%), exploit/vulnerabilities' explanation (1%)
Part C	2.5% ■ Task C.1 (2%): for list of users testing (0.5%), results and interpretation, for table and fields testing results and interpretation) (1.5%) ■ Task C.2 (0.5%): for modifying a non phone no. field testing, results and interpretation (0.5%)
Part D	2% ■ Privacy implications discussion (1%) ■ Ethics implications discussion (1%)
Presentation	1% ■ Clarity of presentation

Assignment Details

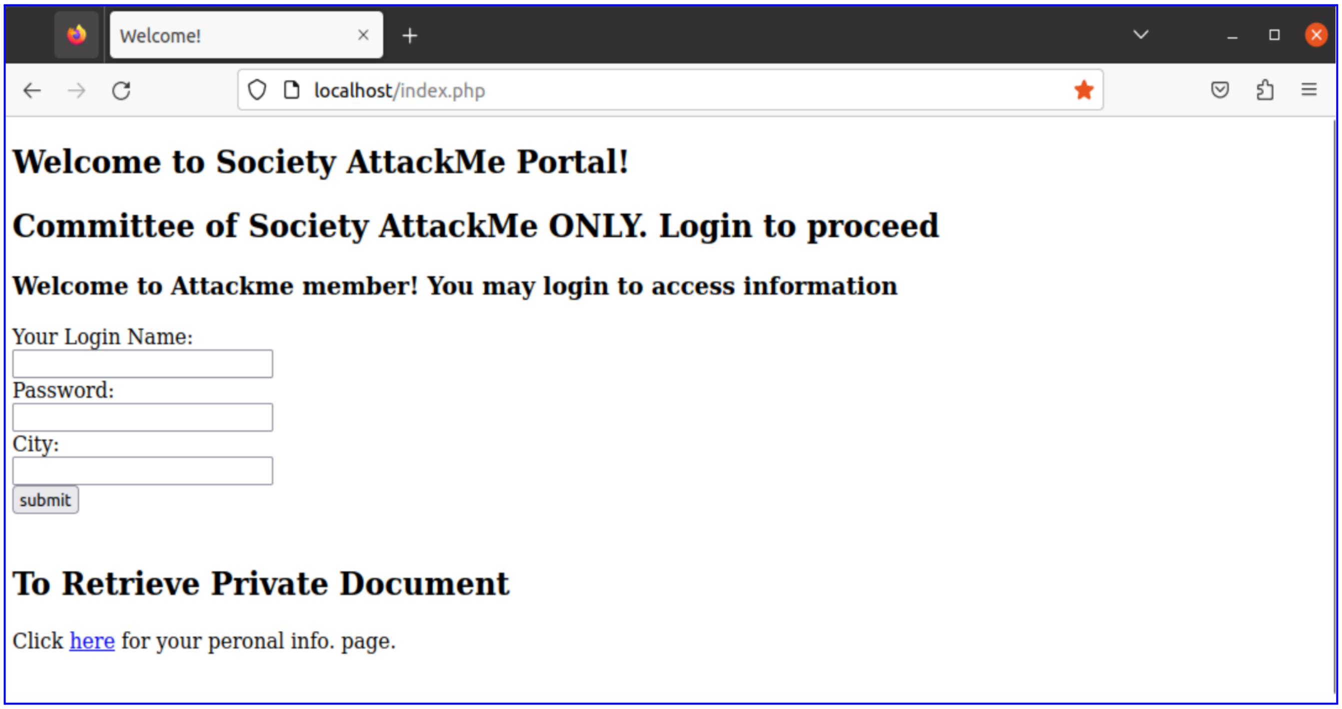
You can download the Asg3 VM .ova file from the link on the Moodle Assessments page (for Windows or Mac devices with Intel CPUs) or the Asg3 VM Zip file (for Mac devices with M1/M2 CPU; follow the "Asg3 VM Install Instructions - Mac M1/M2 Devices" to install the VM).

Once you run the VM, log in with the following credentials:

VM login name: student
VM password: student

Your task is to perform the following security tests on this web application. You should perform these tests using the Firefox or burpsuite built-in web browser installed in your Ubuntu lab VM, and the burpsuite tool installed in this VM.

Visit the homepage for the web application at the URL (http://attackme.com/index.php) using your web browser. If all is well, the browser should display a page that looks as in **Fig. 1**. (note: you can also use the URL http://localhost/index.php)



Welcome to Society AttackMe Portal!

Committee of Society AttackMe ONLY. Login to proceed

Welcome to Attackme member! You may login to access information

Your Login Name:

Password:

City:

To Retrieve Private Document

Click here for your peronal info. page.

Fig.1 *Login Page*

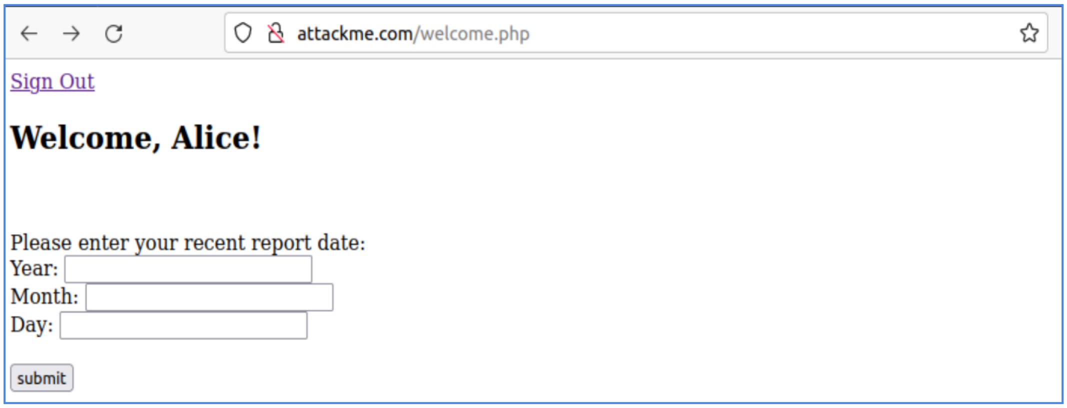
Part A: Member's Welcome Page Security Test (2.5 marks)

This web app allows members of Society AttackMe to access their personal documents.

In this part, your aim is to do security testing of the **committee member** part of the web application, from the point of view of an outsider (non-member) attacker trying to reveal the secret committee information. To help you with this, you are given the login credentials of one of the registered committee members (however, note that an outsider attacker will **not** know these credentials):

Username: Alice
Password: alice
City: Sydney

After clicking the “submit” button with the above credentials, the browser should display a welcome page, as shown in **Fig. 2**.

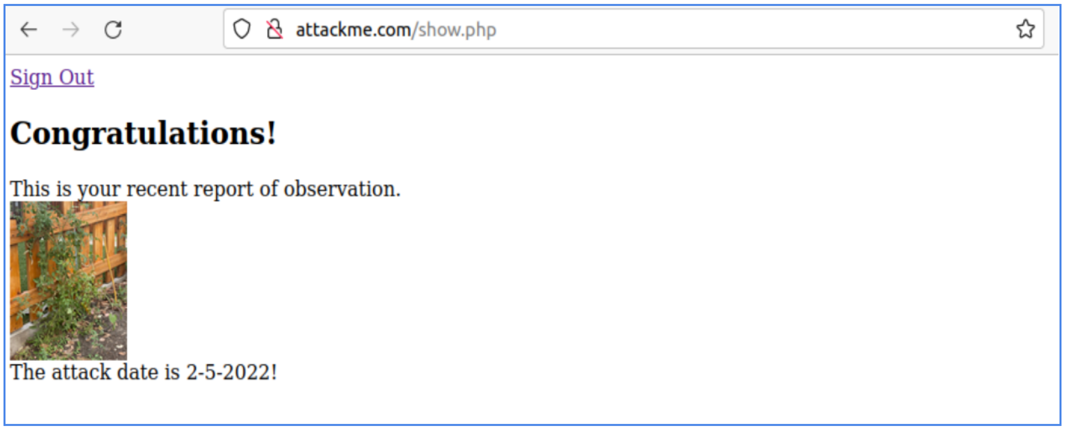


Welcome, Alice!

Please enter your recent report date:
Year:
Month:
Day:

Fig. 2. *Welcome page*

Then, after entering the report date (Date: 2 May 2022) into the and clicking the “submit” button, you should see the secret report of observation as shown in **Fig. 3**.



Congratulations!

This is your recent report of observation.

The attack date is 2-5-2022!

Fig. 3. *Secret report of observation.*

Complete the following tasks:

- **Task A.1 (1 mark)** Based on the application behavior for the given login and welcome pages above:
    - **List potential points** on the home and greeting pages where a **reflected XSS** input injection vulnerability **might** exist
    - **Explain** your reason(s) on why they are the potential XSS vulnerability points.

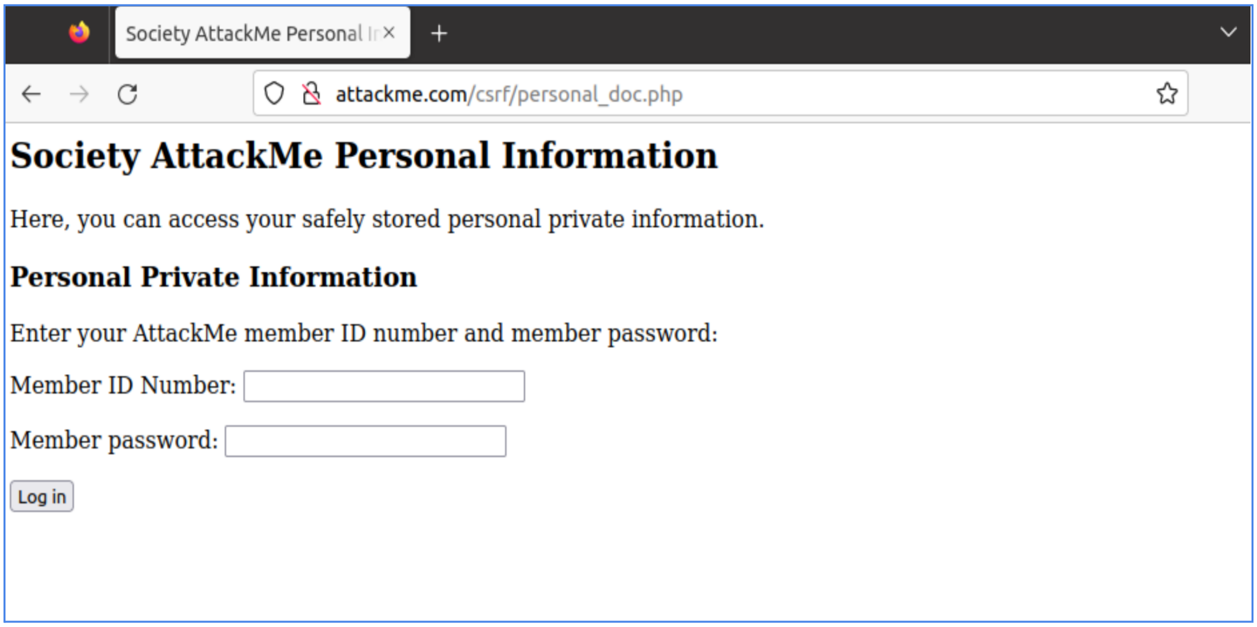
- **Task A.2** (**1.5 mark)** Experiment with the home page login and welcome member, and examine the behavior of these pages to different inputs. In particular:
    - For each of the **potential** XSS vulnerability points listed in Task A.1, perform tests to see if XSS vulnerabilities **actually exist** at these points.
    - Explain
        - your tests,
        - your test results,
        - your interpretation/conclusions on why or why not such XSS vulnerabilities exist at each point, and
        - for the points where XSS vulnerabilities exist, explain whether you think those vulnerabilities can be exploited by an outsider attacker to steal secret information (note: you don't need to actually carry out an exploit) and how to mitigate it.

Part B: Personal Information Security Test

In this part, your aim is to do security testing of the organization members' personal information part of the web app. For this, you are given one of the organization members' name and password, namely:

Member Name: Bob
Member ID Number: 1
Member password: Ro4mvSemq45xfepvaEr24

Use Bob's **member ID number** and **Member password** to log in to the Personal Private Information login page shown in **Fig. 4**.



Society AttackMe Personal I
attackme.com/csrf/personal_doc.php

Society AttackMe Personal Information

Here, you can access your safely stored personal private information.

Personal Private Information

Enter your AttackMe member ID number and member password:

Member ID Number:

Member password:

Fig. 4. *Personal Private Information login page.*

Complete the following tasks:

Task B.1 (2 marks)

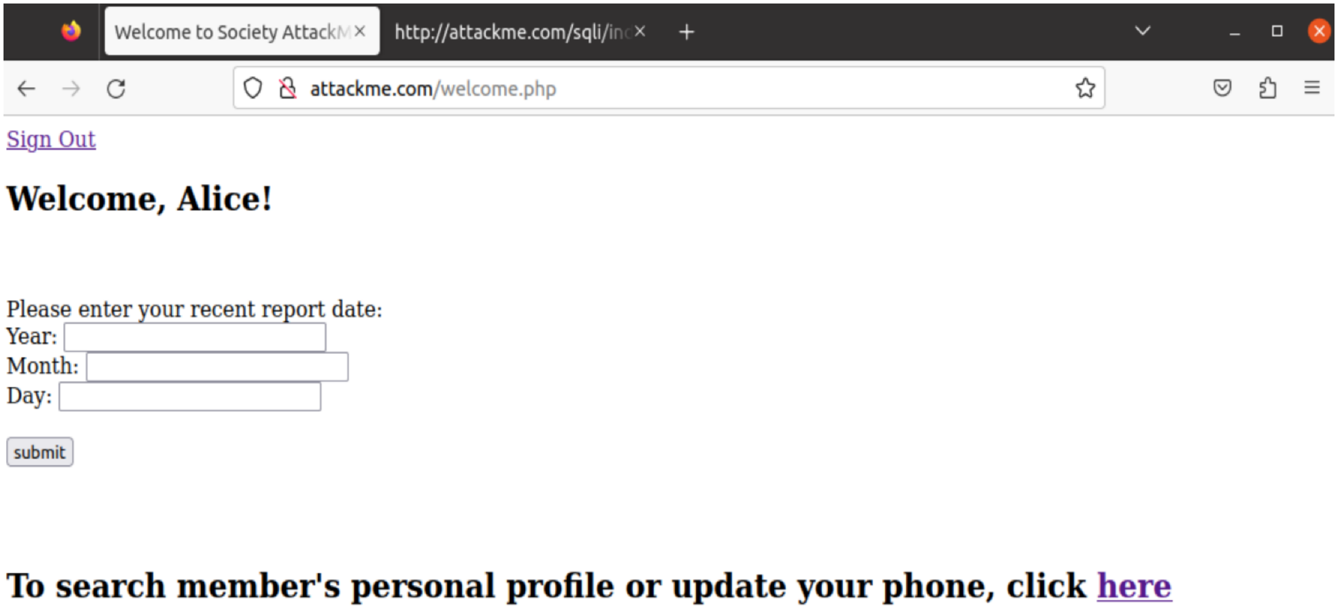
Bob has two private documents stored in his account with document IDs 1 and 2. Your goal in this task is to test the application against attacks by **Bob** (Member ID: 1) who is curious to learn about another member **Charlie**'s (Member ID: 2) private information.

- Can Bob gain unauthorised access to Charlie's personal private data?
  - If you think it is possible, explain the vulnerability you found and how Bob can exploit it, and show any private data of Charlie you managed to expose by the attack.
  - If you think it is not possible, explain why.
  - In any case, explain the tests you did, the results, and your interpretation of them.

Hints: experiment with the personal private information part of the web app to see how it behaves with **different inputs** from Bob. Use the burpsuite tool (see week 10 lab) to help with your experiments and try out potential attacks.

Part C: Attack on the database (2.5 marks)

In this part, your aim is to test for potential database SQL injection vulnerabilities in the committee's **personal profile** page**.** To do so, click the "here" link at the bottom of the "Welcome" page (see **Fig. 5**) after logging in as the user Alice as explained in Task A.



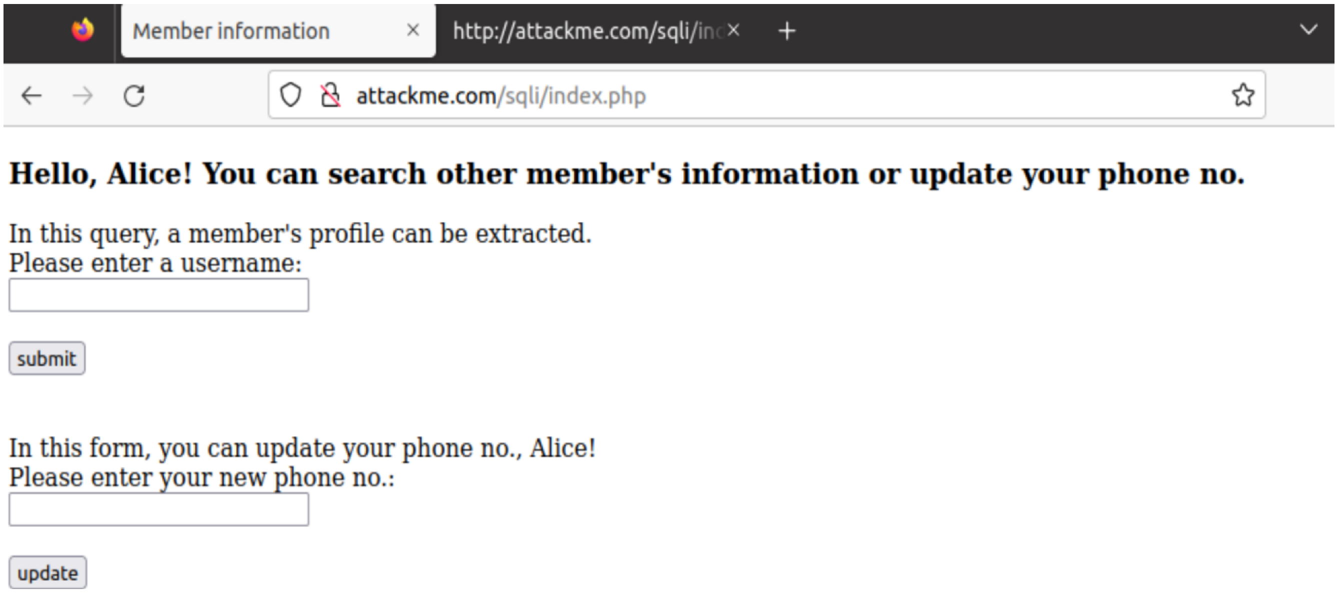
Welcome, Alice!

Please enter your recent report date:

To search member's personal profile or update your phone, click here

Fig. 5. *Member welcome page with link to personal profile at bottom.*

Alice's personal profile search page should appear as in Fig.6.



Hello, Alice! You can search other member's information or update your phone no.

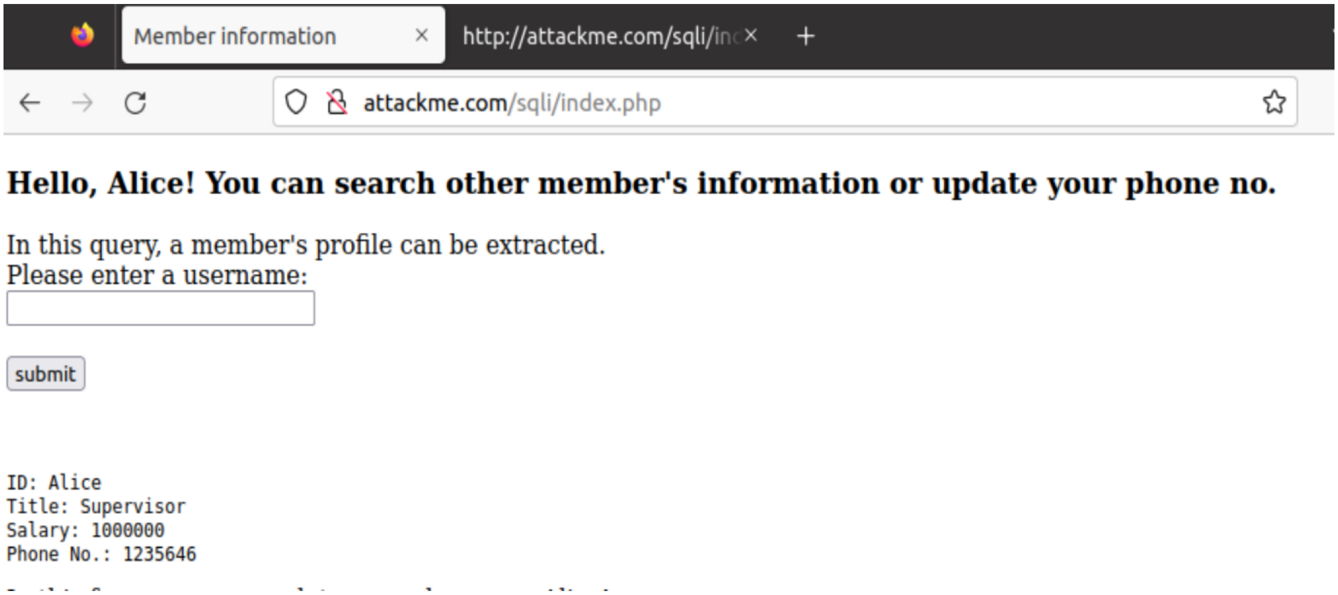
In this query, a member's profile can be extracted.
Please enter a username:

In this form, you can update your phone no., Alice!
Please enter your new phone no.:

Fig. 6. *Member personal profile search page.*

When you type in a username in the textbox under "Please enter a username:" in the search page, the personal details of the member user (**title, salary and phone no.)** will be shown in the website.

For example, if you submit the form with username = “Alice”, the information will be as shown in Fig. 7.



Hello, Alice! You can search other member's information or update your phone no.

In this query, a member's profile can be extracted.
Please enter a username:

```
ID: Alice
Title: Supervisor
Salary: 1000000
Phone No.: 1235646
```

Fig. 7. *Search results for username “Alice”.*

Complete the following tasks:

Task C.1 (2 marks)

In this task, you should test for SQL injection vulnerabilities via user input of the query to achieve the following tasks. You should include your injection inputs and the screen captures of results in your presentation.

a) Attempt to list all the users in the database containing user information. **(0.5 marks)**

b) Attempt to determine the name of the database containing the user information and the corresponding fields (columns) in that table. **(1.5 marks)**

Task C.2 (0.5 mark)

In the bottom half of the member personal profile search page (see **Fig. 6**), user Alice can update her phone no. by entering a new phone no. Your task is to:

a) Attempt to make use of the fields found in Task C.1 to test for and exploit an SQL injection vulnerability in the phone update textbox to update some information other than phone no.

b) Include your SQL injection statement and screen captures before and after the changes by using a member profile search page query, and explain your interpretation of the test results.

Part D: Privacy and Ethics (2 marks)

Complete the following tasks:

- **Privacy**: discuss how the above vulnerabilities and/or attacks affects individual privacy, or give your reasons why privacy is not an issue
- **Ethics**: discuss how of each of Part A to C relates to ethical issues, or give reasons why ethics is not relevant

Submission

You must submit, via the link on the Moodle Assessments page:

- an individual **10-min video,** and
- the **video presentation slides (in powerpoint format) used in your video presentation.**

Your video presentation should present your answers to the tasks completed in Parts A-D above, including your test results, relevant screen captures/demonstrations and exploits.

The clarity of your video and slides presentation will count towards 1% of your total mark for the assignment. Please ensure your voice during the video presentation is clearly audible.

Appendices

WARNING (Academic integrity): It is an academic requirement that your submitted work be original. Zero marks will be awarded for the whole submission if there is any evidence of plagiarism or contract cheating (i.e. paying another person to complete the assessment task). It is fine to use code or other material from various sources in your report. However, any material that you obtain from some source (e.g. website, book, paper, article) **must be cited** in the appropriate place in your report and **listed in the references section** of your report. Please also note that students must work on this assignment individually, and significant similarities between assignments will be investigated for evidence of plagiarism.

REMARK (Guidelines on Use of AI tools in the Assignment): ChatGPT or other AI tools may be used for study purposes, to learn about your tasks, and to develop your assignment. However, similar to citation requirements for other references (see “Academic Integrity” statement above), you **must include a clear declaration of all generative AI tools used** (e.g. ChatGPT, DALL-E, Grammarly, voice-to-text), **how and where you have used them**. In particular, you should be aware that output of AI tools may not be factually correct and you should therefore critically evaluate the output generated by such tools for claim accuracy and appropriateness to the tasks, using reliable sources, before incorporating such output in your assignment (e.g. an example declaration may be: ‘ChatGPT was used to generate an initial structure, then I edit this to correct factual inaccuracies, add citations to support claims’).

Where to get help

What can you get help for?

English language skills

if you don't feel confident with your English.

- Talk to English Connect: https://www.monash.edu/english-connect

Study skills

If you feel like you just don't have enough time to do everything you need to, maybe you just need a new approach

- Talk to an academic skills advisor: https://www.monash.edu/learnhq/consultations

Things are just really scary right now

Everyone needs to talk to someone at some point in their life, no judgement here.

- Talk to a counsellor: https://www.monash.edu/health/counselling/appointments (friendly, approachable, confidential, free)

Things in the unit don't make sense

Even if you're not quite sure what to ask about, if you're not sure you won't be alone, it's always better to ask.

- Ask in the forums or email your tutor:

  Teaching team: https://lms.monash.edu/course/view.php?id=155649&section=1

  Consultation: https://lms.monash.edu/mod/resource/view.php?id=11630825

I don't know what I need

Everyone at Monash University is here to help you. If things are tough now they won't magically get better by themselves. Even if you don't exactly know, come and talk with us and we'll figure it out. We can either help you ourselves or at least point you in the right direction.

Change log

All changes to the assignment will be listed here with the time of the change (in Melbourne time):