RMIT UNIVERSITY

School of Science

INTE1070/1071 Secure Electronic Commerce

Assignment 1

	Assessment Type: Individual assignment; no group work. Submit online via Canvas→Assignments→Assignment 1. Marks awarded for meeting requirements as closely as possible. Clarifications/updates may be made via announcements/relevant discussion forums.
	Due date: **Week 4, Friday the 14th Aug 2020 11:59pm** Deadlines will not be advanced, but they may be extended. Please check Canvas→Syllabus or via Canvas→Assignments→Assignment 1 for the most up to date information. As this is a major assignment in which you demonstrate your understanding, a university standard late penalty of 10% per each working day applies for up to 5 working days late, unless special consideration has been granted.
	Weighting: **30 marks (Contributes 30% of the total Grade)**

1. Overview

The objective of Assignment 1 is evaluating your knowledge on the topics covered in Lecture 1-4. Topics include an overview of the E-Commerce system, common security attacks on E-Commerce websites, protecting E-commerce sites using well-known approaches, and some fundamentals of crypto protocols that are used for securing electronic commerce. Assignment 1 will focus on developing your abilities in identifying security flaws in an e-commerce website and securing the e-commerce application using some of the well-known approaches. Assignment 1 contains several problems related to the topics mentioned above. You are required to prepare the solutions with the description of the step-by-step processes as a single PDF or MS Word file and necessary codes.

There are 4 (four) questions in Assignment-1. Q1 is related to different security attacks that can be performed on an e-commerce website. On the other hand, Q2 to Q4 are related to some of the popular protection methods that are used in e-commerce applications. Protection methods include Google's ReCaptcha V2 and V3, email and SMS based multifactor authentication, and Google's two factor authentication (2FA) framework.

Develop the solution of this assignment in an iterative fashion (as opposed to completing it in one sitting). You should be able to start preparing your answers immediately after the Lecture-1 (in Week-1). At the end of each week starting from Week-1 to Week-4, you should be able to solve at least one question.

If there are questions, you must ask via **the relevant Canvas discussion forums** in a general manner.

Submission instructions are detailed in Section 2.

2. Submission Instructions

Overall, you must follow the following special instructions:

- You must fulfil the requirements in the questions.
- For the questions that require implementation, you must implement the functionalities stated in the questions. Any change in a user interface is acceptable if the functionality is there.
- In your solution, you must show all of the steps with necessary code segments and screenshots for each question.
- Please note that you are required to record the steps in a video and post it in the CANVAS or YouTube whenever asked. Provide the link in your solution.
- Upload your solution as a single PDF or Word document in CANVAS. Also, upload codes as a single ZIP file in the CANVAS.

- Do not put the PDF withing the ZIP file.

3. Assessment Criteria

This assessment will determine your ability to:

- Follow requirements provided in this document and in the lessons.
- Independently solve a problem by using cryptography and cryptanalysis concepts taught over the first four weeks of the course.
- Meeting deadlines.

4. Learning Outcomes

This assessment is relevant to the following Learning Outcomes:

- CLO 1: Explain the range of threats to e-commerce security.
- CLO 2: Explain how cryptography can be, and is, used to achieve security.
- CLO 3: Describe the different standards in use for secure electronic commerce, such as certificates, MACs, etc.
- CLO 6: Describe the different protocols in use for secure electronic commerce, such as SSL / TLS.

5. Assessment details

Please ensure that you have read **Section 1** to **3** of this document before going further. Assessment details (i.e. question Q1 to Q4) are provided in the **next page**.

Q1. Security Attacks on E-Commerce Websites (9 Marks)

Alice owns a computer store in Melbourne city. In order to increase the sales, she has developed an E-Commerce application for her computer store. Some of the well-known attacks on E-commerce websites are as follows:

- Cross-Site Scripting (XSS)
- SQL injections
- Hidden field manipulation
- Fishing Attack
- Cookie poisoning
- Web scraping
- Layer 7 DoS attacks
- Parameter tampering
- Buffer overflow
- Backdoor or Debug options
- Stealth commanding
- Forced browsing
- Third-party misconfigurations

Alice realizes that the E-Commerce application must be secured before it becomes online. From that realization, she hires you and your team as a security consultant to identify the security risks of her developed E-Commerce application.

Create an E-commerce website (with a database as back-end and other necessary tools such as HTML, PHP, Javascript, CSS files etc.) for yourself to demonstrate the chosen attacks. However, for the sake of convenience, a sample code of Alice's E-Commerce application (includes HTML, PHP, JavaScript, and CSS source files) and the database (as SQL file) are uploaded in the **CANVAS** under **Assignment-1** home page. You should add or edit pages to whenever required.

Create a group of 3 people. Then, you are required to configure Alice's E-Commerce application in your personal computer or any free websites (where you can host your website) using the knowledge you have learnt from **Tutorials 1 to 4**.

Once you have configured the application, you are required to demonstrate **at least three types of attacks** that can be performed on Alice's E-Commerce application. For each of the attack, you need to do the followings:

a) Write down all the necessary steps to launch each attack with screenshots.
b) Record the steps in a video and post it in the CANVAS or YouTube (as a private video). Provide the link. You should not share the link of the video any of your peer groups.

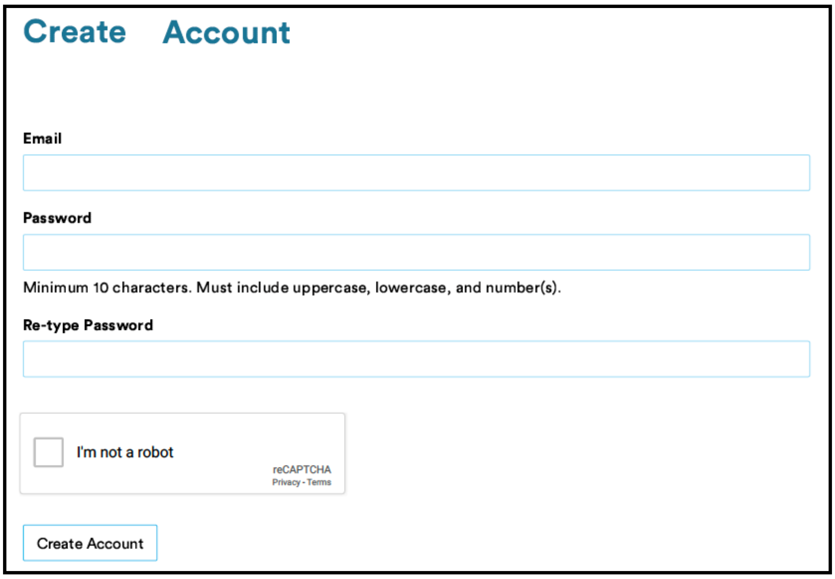
Provide the above items mentioned in (a) and (b) as a group.

Q2. Securing E-Commerce Website from spam and abuse (2+3 = 5 Marks)

In the E-Commerce application that has been provided in the CANVAS in relation to **Q1**, only registered users should be authorized to login to the Ecommerce application and trade. A registered user can be either a seller or buyer who needs to create a user account. It is possible that several fake users are created by human attackers or software bots for hampering the operation of the E-Commerce application. To protect the E-Commerce application from spam and abuse, Alice requests you to integrate CAPTCHA in her E-Commerce application.

Considering the security strength of Google's **reCAPTCHA** service, you have decided to integrate it in Alice's application.

a) From the knowledge you have learnt in Tutorial, implement Google's **reCAPTCHA version 2:**
   i. Design a form similar to the one given in **Figure-2.1** to create user account with Google's **reCAPTCHA version 2**.
   ii. Show step by step processes, with appropriate code segments and screenshots, how Google's **reCAPTCHA version 2** can be applied in the E-Commerce application to prevent creating fake user accounts. Also, record the steps in a video and post it in the CANVAS or YouTube (as a private video) and provide the link. You should not share the link of the video any of your peer groups.



Create Account

Email

Password

Minimum 10 characters. Must include uppercase, lowercase, and number(s).

Re-type Password

Figure-2.1: Expected User Registration Page enabled with Google's reCAPTCHA version 2

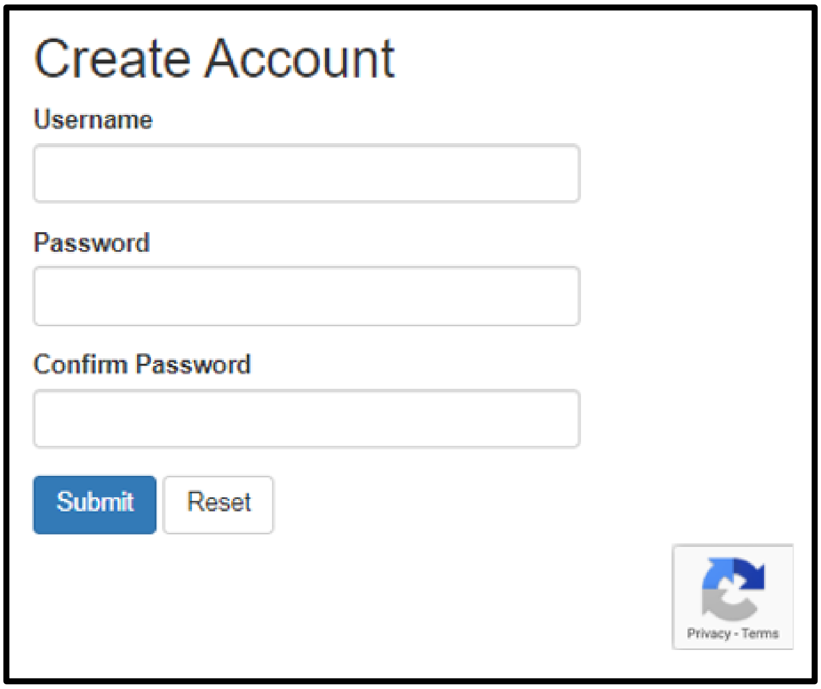
b) You have found that Google has a new version of its reCAPTCHA which is **reCAPTCHA version 3**. When you informed Alice about the **reCAPTCHA version 3**, she is convinced that reCAPTCHA version 3 is better.

To make Alice happy:

i. Design a form similar to the one shown in **Figure-2.2** to create user accounts with Google's **reCAPTCHA version 3**.

ii. Show step by step processes, with appropriate code segments and screenshots, how Google's **reCAPTCHA version 3** can be applied in the E-Commerce application to prevent creating fake user accounts. Also, record the steps in a video and post it in the CANVAS or YouTube (as a private video) and provide the link. You should not share the link of the video any of your peer groups.

iii. What are the advantages of using **reCAPTCHA version 3**?



Create Account

Username

Password

Confirm Password

Figure-2.2: User Registration Page enables with Google's reCAPTCHA version 3

Q3. Simple Multi-Factor Authentication (4 Marks)

Once user accounts have been created, only valid users should be allowed to login and trade using Alice's E-Commerce application. However, attackers can still compromise the login system with the aid some sophisticated software. So, you have decided to integrate the **multi-factor authentication** in Alice's E-Commerce application.

Develop an **Email-based multi-factor authentication** for Alice's E-Commerce application that has the following requirements. Also, record the steps in a video and post it in the CANVAS or YouTube (as a private video) and provide the link. You should not share the link of the video any of your peer groups.

Requirements:

i. Create a simple login form as shown in **Figure-3.1**. When a user provides a valid email (your RMIT student email) and password (e.g. 1234), the user should receive a **6-digit** random number in his/her email address as shown in **Figure-3.2** and the page to be shown as presented in **Figure-3.3.**

ii. Once the verification code is provided in the form shown in **Figure-3.3**, the code should be verified, and the **Success Page** is shown (see **Figure-3.4**). Otherwise, the **Failure Page** is shown (see **Figure-3.5**).

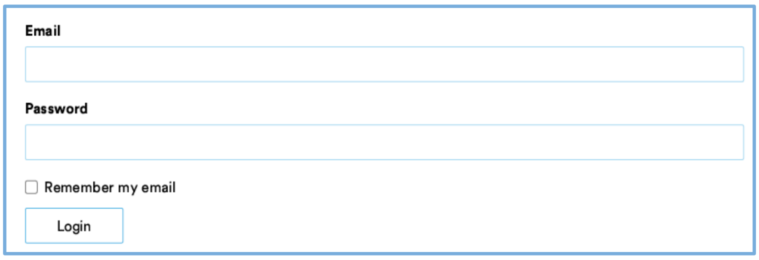
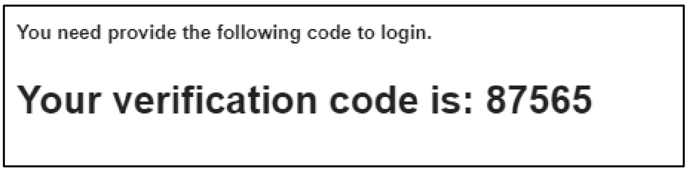


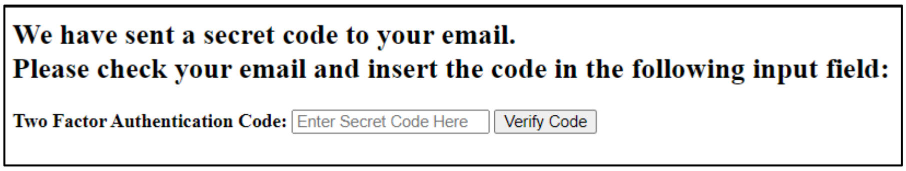
Figure-3.1: Login Form for Email-based Two Factor Authentication



You need provide the following code to login.

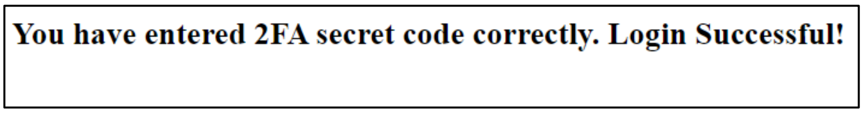
Your verification code is: 87565

Figure-3.2: Email containing the 6-digit Two Factor Authentication code



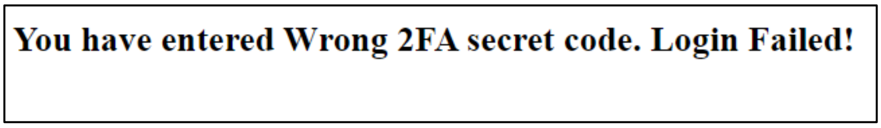
We have sent a secret code to your email.
Please check your email and insert the code in the following input field:

Figure-3.3: Form to Enter the Verification Code



You have entered 2FA secret code correctly. Login Successful!

Figure-3.4: Success Page shown if a valid code is entered



You have entered Wrong 2FA secret code. Login Failed!

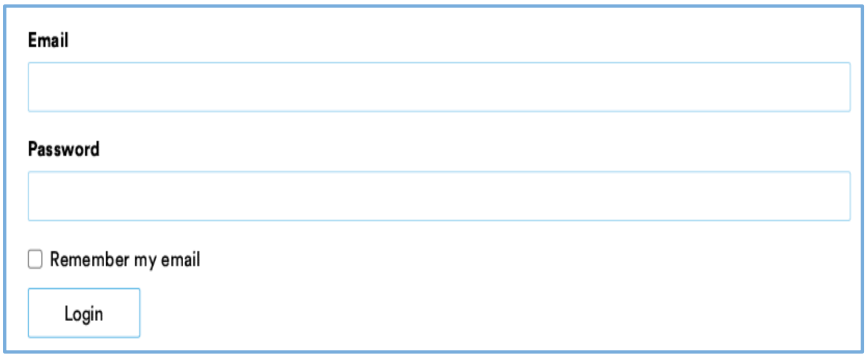
Figure-3.5: Failure Page shown if an invalid code is entered

Q4. Advanced Multi-Factor Authentication (8+4 = 12 Marks)

Once user accounts have been created, only valid users should be allowed to login and trade using Alice's E-Commerce application. However, attackers can still compromise the login system by performing the password guessing attack. To prevent an attacker getting access to the application by simply knowing the password, you have decided to integrate the **multi-factor authentication** in Alice's E-Commerce application.

a) Apply **Google's 2-step verification** (e.g.2FA, also called **2 Factor Authentication** or **2FA**) to user accounts of the E-Commerce application. You need to perform the followings:

   i. Create a **login form** (as shown in **Figure-4.1**) that would allow you to enter Email and password. Next, provide steps with necessary code segment and screenshots how you have integrated Goggle's **2FA** in Alice's E-Commerce application. Also, record the steps in a video and post it in the CANVAS or YouTube (as a private video) and provide the link. You should not share the link of the video any of your peer groups.



Email

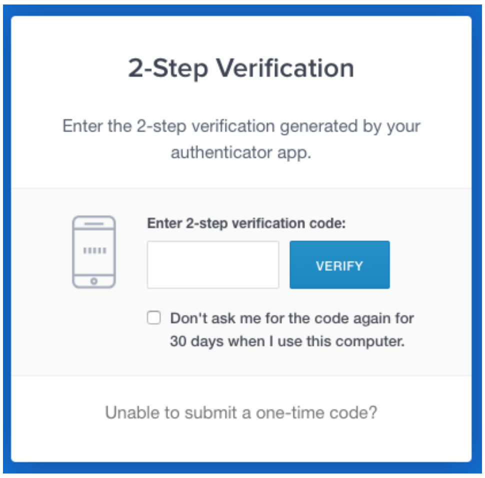
Password

□ Remember my email

Login

Figure-4.1: Login Form with Google's 2 Factor Authentication

   iii. Once a user enters correct email and password, a screen (like **Figure-4.2 or 4.3**) should prompt the user to enter 2-step verification code as follows:



2-Step Verification

Enter the 2-step verification generated by your authenticator app.

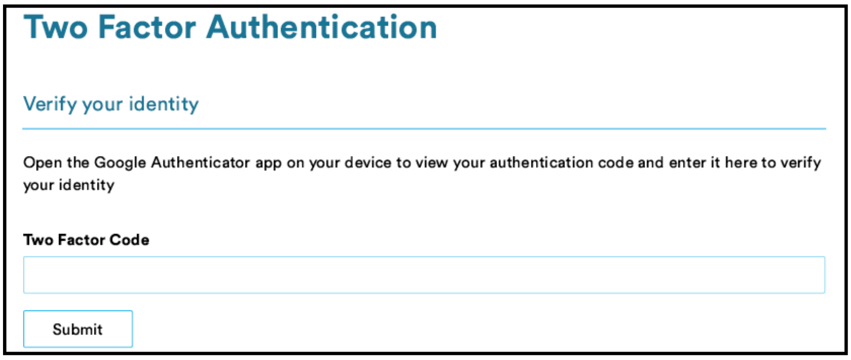
Enter 2-step verification code:

VERIFY

□ Don't ask me for the code again for 30 days when I use this computer.

Unable to submit a one-time code?

Figure-4.2: Google's Form to enter verification code in Google's 2 Factor Authentication



Two Factor Authentication

Verify your identity

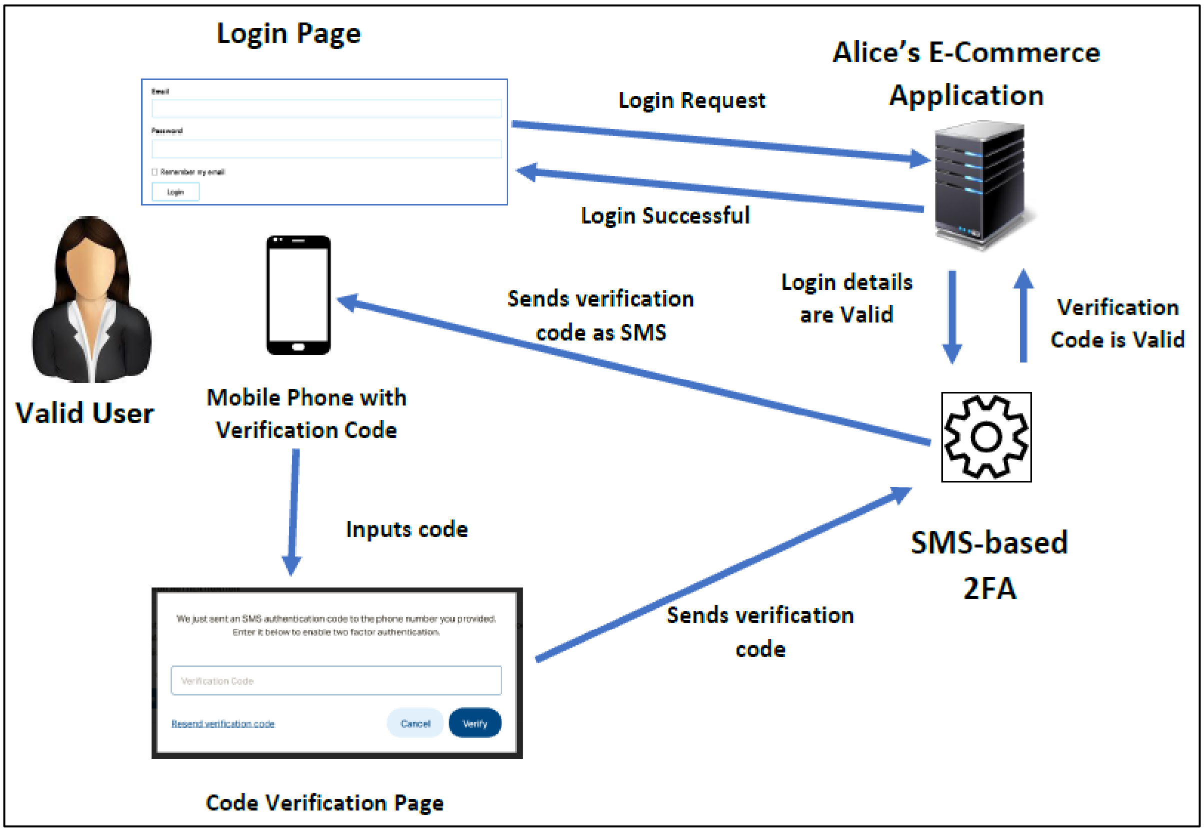
Open the Google Authenticator app on your device to view your authentication code and enter it here to verify your identity

Two Factor Code

Submit

Figure-4.3: Another Google's Form to enter verification code in Google's 2 Factor Authentication

b) Design an **SMS-based two factor authentication (2FA)** framework and show step-by-step process to implement it in Alice's E-Commerce application. In your designed 2FA framework, the E-commerce website should send an SMS to the verified user's mobile phone number each time a user provides valid username and password. The verification code should be a unique short-lived code. **Figure-4.4** shows an overview of the system. Show steps with necessary code segment and screenshots. Also, record the steps in a video and post it in the CANVAS or YouTube (as a private video) and provide the link. You should not share the link of the video any of your peer groups.



We just sent an SMS authentication code to the phone number you provided. Enter it below to enable two factor authentication.

Figure-4.4: Overview of SMS-based 2 Factor Authentication system

6. Academic integrity and plagiarism (standard warning)

Academic integrity is about honest presentation of your academic work. It means acknowledging the work of others while developing your own insights, knowledge and ideas. You should take extreme care that you have:

- Acknowledged words, data, diagrams, models, frameworks and/or ideas of others you have quoted (i.e. directly copied), summarized, paraphrased, discussed or mentioned in your assessment through the appropriate referencing methods,
- Provided a reference list of the publication details so your reader can locate the source if necessary. This includes material taken from Internet sites.

If you do not acknowledge the sources of your material, you may be accused of plagiarism because you have passed off the work and ideas of another person without appropriate referencing, as if they were your own.

RMIT University treats plagiarism as a very serious offence constituting misconduct. Plagiarism covers a variety of inappropriate behaviors, including:

- Failure to properly document a source
- Copyright material from the internet or databases
- Collusion between students

For further information on our policies and procedures, please refer to the University website.

7. Assessment declaration

When you submit work electronically, you agree to the assessment declaration.

8. Rubric/assessment criteria for marking

All of the computations must be correct and only provided values must be used. Instructions must be followed.

Criteria The characteristic or outcome that is being judged.						**Total**
Question 1 Security Attacks on E-Commerce Websites	3 different types of attacks are shown correctly and step-by-step processes are shown in the solution with necessary screenshots. The link of the video demonstration is provided. **9 Marks**	Any 1 of the followings is satisfied: 1) a. 3 different types of attacks are shown step-by-step with necessary screenshots. b. All of the attack methods are shown correctly. c. But, the link of the video demonstration is NOT provided **OR** 2) a. 2 different attacks are shown correctly, and step-by-step and step-by-step processes are shown with necessary screenshots. b. The link of the video demonstrations shows 2 attack methods. **6 Marks**	Any 1 of the followings is satisfied: 1) a. 3 different attacks are shown step-by-step without necessary screenshots. b. the link of the video demonstrations is NOT provided **OR** 2) a. 2 attack methods are shown step-by-step processes are shown in the solution with necessary codes. b. Only 2 attack methods are working correctly. c. The link of the video demonstrations shows 2 attack methods. **OR** 3) All of the three methods are partially shown, **3 Marks**		Not answered **0 Marks**	**9 Marks**
Question 2 Securing E-Commerce Website from spam and abuse	Both Q2(a) and Q2(b) are answered correctly with required description and screenshots. Video demonstration is provided. **5 Marks**	Any 1 of the followings is satisfied: 1) Only Q2(a) is answered correctly with required description and screenshots. Video demonstration is provided. **OR** 2) Both Q2(a) and Q2(b) are partially correct and a few description and screenshots are provided. Video demonstration is provided. **3 Marks**	Any 1 of the followings is satisfied: 1) Both Q2(a) and Q2(b) are correct, but inadequate description and screenshots are provided. Video demonstration is NOT provided. **OR** 2) Only Q2(b) is answered correctly with required description and screenshots. Video demonstration is NOT provided. **2 Marks**	Both Q2(a) and Q2(b) are attempted. But, answered are not correct and requirements are not fulfilled. Video demonstration is NOT provided. **1 Marks**	Not answered **0 Marks**	**5 Marks**

Question 3 Simple Multi-Factor Authentication	Answered correctly with detail step-by-step process. Explanations are excellent. Video demonstration is provided. **4 Marks**	Answer is partially correct, and detail step-by-step process is shown. Explanations are satisfactory. Video demonstration is NOT provided. **3 Marks**	Answer is correct but detail step-by-step process is NOT shown. Explanations are not satisfactory. However**,** Video demonstration is provided. **2 Marks**	Answer is partially correct, and detail step-by-step process is shown. Explanations are not satisfactory. Or, Video demonstration is NOT provided. **1 Marks**	Not answered **0 Marks**	**4 Marks**
Question 4 Advanced Multi-Factor Authentication	Both Q4(a) and Q4(b) are answered correctly with required description and screenshots. **12 Marks**	Any 1 of the followings is satisfied: 1) Only Q4(a) is answered correctly with required description and screenshots. **OR** 2) Both Q4(a) and Q4(b) are partially correct and a few description and screenshots are provided. **8 Marks**	Any 1 of the followings is satisfied: 1) Both Q4(a) and Q4(b) are correct, but inadequate description and screenshots are provided. **OR** 2) Only Q4(b) is answered correctly with required description and screenshots. **4 Marks**	Both Q4(a) and Q4(b) are attempted. But, answered are not correct and requirements are not fulfilled. **2 Marks**	Not answered **0 Marks**	**12 Marks**