COMPSCI5104/5093: Assessed Exercise 2 Secured Software Engineering

Due Date: 20-03-2023 @16:30 GMT

Marking Scheme

There is a Task given in this assessment which is worth a total of 40 marks. It counts for overall 20% weightage in the course.

Deliverable Instructions

You are to submit a pdf via the Moodle coursework submission link. You may annotate this document if you wish, or create a new document from scratch if you prefer. You are free to use whatever software/tools you require to create the document, just ensure that your solutions are clear. Your file name must follow the format "**sse_1_*<your_GUID>***".

Deadline

Your submission is due on **20-03-2023 at 16:30**. In accordance with the university Code of Assessment Policy, late submissions will be accepted. However, any late submissions will be penalised by 2 bands for each additional day up to 5 working days; Any late submission after 5 working days will receive the grade H (with a band value of 0). Also note that all submissions will be checked against the university plagiarism monitoring system.

Task (40 Marks)

Consider you are building a website for a Journal that publishes previously unpublished research articles. The system consists of different kind of users such as Authors, Editor, Editorial Staff, Reviewers and Admin. Following are the main requirements of the system:

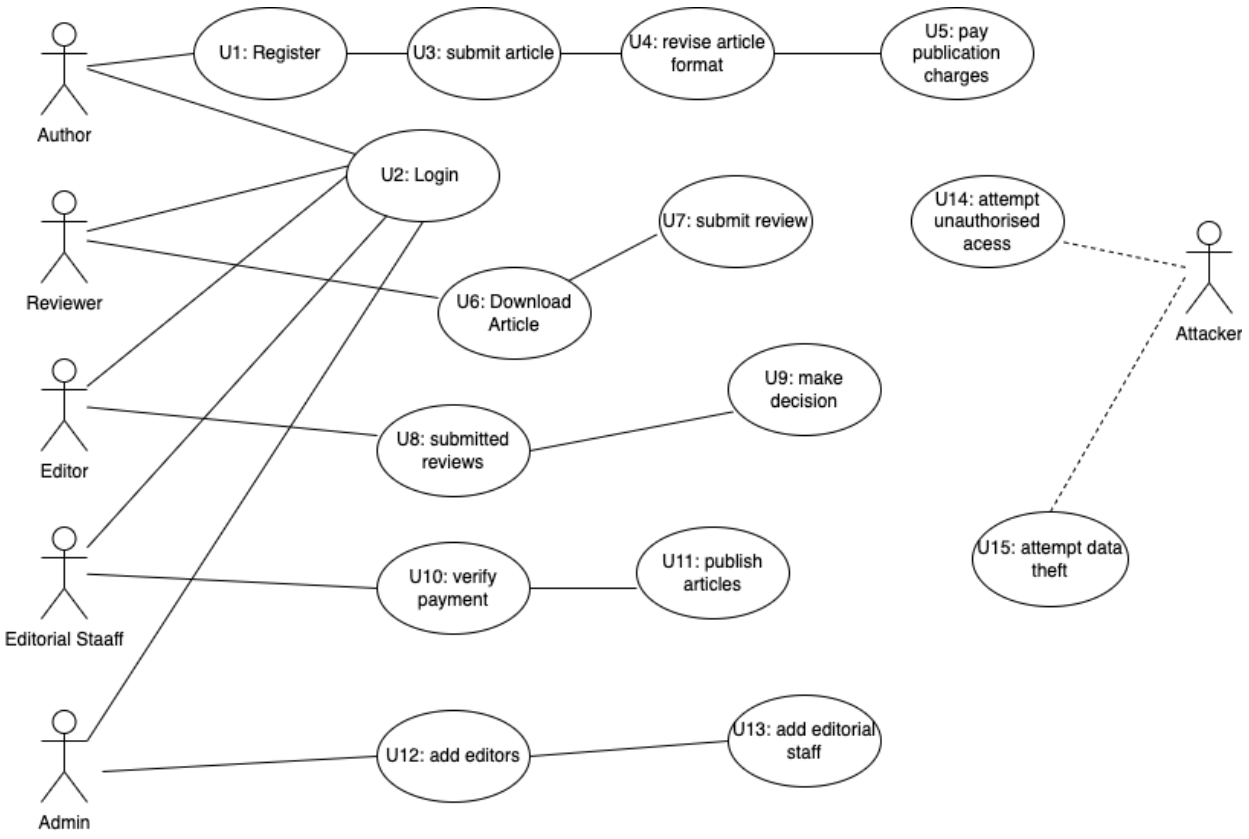
- Authors should be able to upload their articles to the system
- Reviewer can download the articles and submit the review against the paper
- Editor can review the received reviews and make a decision on the acceptance/rejection of the paper (notified to the author via email)
- Authors have to pay article publication charges through 3rd party payment gateway in case of acceptance of their papers
- Accepted and paid articles are published on the website by the Editorial Staff after verifying the payment information. If the paper is not formatted according to the journal's format, the editorial staff asks the Authors to format it accordingly
- Editors and Editorial Staff are added to the system by the Admin whereas the reviewers are added to the system by the Editor
- Authors can create their accounts directly on the website

Following security implementations are already considered in the requirements stage:

- SSL and TLS is enabled for data communication
- Prevention for Cross-site scripting and Sql-injection

⇒ a) Create a Use Case overview diagram for the case study with at-least 15 main use cases of the system. Include the legitimate actors, attackers, user cases and their interactions in the diagram. (15 marks)

NOTE: You can create use case and mis use case diagrams for formulating your solution, but it is not part of the solution to be included in your submission.



⇒ b) Threats identification: List down 10 high-level threats to the system e.g., T1, T2 etc. (10 marks)

list of high-level threats to the system:

Threats Identifications:

T1. unauthorized access to user account
T2. data tamper by attackers
T3. brute force attacks on user accounts
T4. privilege escalation by attackers
T5. inside threats from malicious users
T6. inadequate logging and monitoring
T7. sensitive data theft
T8. denial of service attacks
T9. phishing attacks
T10. insecure 3rd party integrations

⇒ c) Threats mitigation: what would be your policies for threat mitigation against each identified threat e.g., T1, T2 etc. Briefly explain, do not write more than 100 words for each threat mitigation. (10 marks)

T1. unauthorized access to user account:

Implement strong ussr authentication mechanisms to give access to legit users like using multi factor authentication and enforcing the strong password policies.

T2. data tamper by attackers

Use secured data storage practices to avoid data tamper and make sure data integrity by having strong cryptographic techniques.

T3. brute force attacks on user accounts

Implement user account lockout policies and also using CAPTCHA to get prevented from brute force attacks.

T4. privilege escalation by attackers

Enforce the principle method of least privilege and also do regular review on user permissions.

T5. inside threats from malicious users

Always monitor the user activities and have proper alarming procedures with the code of conduct.

T6. inadequate logging and monitoring

Implement perfect logging and monitoring systems and do regular audits

T7. sensitive data theft

Always protect the sensitive data with good encryption techniques, legit access controls.

T8. denial of service attacks

Having network defenses, rate limiting and load balancing to protect against DoS attacks.

T9. phishing attacks

Give good user training about phishing attacks to recognize the kind of those attacks and always use email filtering systems.

T10. insecure 3rd party integrations

Always examine the 3rd party security systems and always work with trusted providers.

⇒ d) One of the aspects in this task is to identify the threats and requirements negotiation. After identifying the threats and mechanisms to mitigation, what new use cases would be included in the system? List down the list of new identified use cases. List name only if the name is meaningful to understand otherwise include a maximum of 2 lines description with the use case. (5 marks)

new use cases would be included in the system are:

1. Implement multi-factor authentication
2. Implement CAPTCHA login page
3. Implement code of conduct principle
4. Perform 3rd party integrations security
5. Implement logging and monitoring systems