Assignment 4

A small forum with roles

The application is described by the following functional requirements. To describe the applications security needs, misuse cases has been written. Security requirements are applied to the functional requirements on the following pages.

Functional requirements

F1. A user can register themselves on the forum.

F2. A user can login to the forum.

F3. A user can start a new topic (thread).

F4. A user can reply to existing topics (threads).

F5. A user can edit their own account data (Password etc.).

F6. Administrators can delete any topic and reply.

F7. Administrators can promote users to moderators.

F8. Administrators can demote moderators to users.

F9. Moderators can delete any topic and reply.

F10. A user's role determines what he/she is authorized to do in the application.

Use/Misuse cases

Registration

Use case

1. User wants to register themselves
2. System presents input fields for the required information.
3. User inputs the required information.
4. The system validates the input.
5. The user data is stored in the database.
6. User is redirected to the login page if registration was successful, else an error message will be presented.

Login

Use case

1. User wants to login.
2. System presents input fields for the required information.
3. User inputs the required information.
4. The system validates the input.
5. The input is checked against an existing user in the database.

Kevin Madsen km222ew
Hampus Karlsson hk222gn

6. The user will be sent to the forum page if the login was successful, else an appropriate error message will be displayed.

Misuse case

1. Misuser wants to login with a username he acquired but he doesn't have the password.
2. Misuser starts a dictionary attack.
3. The system counts attempted logins until a threshold is reached (5 attempts).
4. Misuser attempts the 5th login.
5. The system blocks the account the misuser was attempting to access for 15 minutes.

Misuse case Input fields.

1. Misuser wants to exploit the system using a script.
2. Misuser writes a script in the input field.
3. The system validates the input on both the client side and server side.
4. The system sanitizes the provided input data.
5. An error message is displayed.

Security requirements

Identification requirements

SI1

Reference functional requirement: F2

The system shall not force users to identify themselves multiple times during a single session.

Exception: F5

SI2

Reference functional requirement: F2

The system shall identify all users before allowing them to use the systems capabilities.

SI3

Reference functional requirement: F5

The system shall identify all users after they have edited their information

Authorization Requirements

SA1

Reference functional requirement: F10

The system shall not allow any user to access other users private account information.

SA2

Reference functional requirement: F6, F9, F10

The system shall not allow a user without authorized role to delete other users' posts or replies.

Kevin Madsen km222ew
Hampus Karlsson hk222gn

SA3

Reference functional requirement: F10

The system shall not allow an unauthorized user access to administrator or moderator rights.

Nonrepudiation Requirements

SN1

Reference functional requirement: F2

The system shall create and store records of login attempts with the following data:

- Timestamp
- Username
- Outcome of login attempt (fail or success)

SN2

Reference functional requirement: F5

The system shall create and store records of password change with the following data:

- Timestamp
- Username
- Ip address

SN3

Reference functional requirement: F6, F9

The system shall create and store records of topic removal with the following data:

- Timestamp
- Username
- Topic content

SN4

Reference functional requirement: F4, F5

The system shall create and store records of reply removal with the following data:

- Timestamp
- Username
- Reply content

Kevin Madsen km222ew
Hampus Karlsson hk222gn