Misuse cases

**Brute Force**

Requirements: User is not logged in.

1. A malicious agent tries to get access to the system by using many different usernames and passwords.

2. After a number of failed login attempts, the system blocks further tries for a period of time.

**Vandalism**

Requirements: User is logged in and has at least moderator privileges.

1. A malicious/careless agent deletes/corrupts the data in the member registry from the administration interface.

2. Actions on the registry are logged and can be traced to specific users.

## Cross Site Scripting

Requirements: User is creating a post on the forum.

1. A malicious agent tries to post script to the forum.

2. The post is sanitized before it is inserted into the database. Tags are escaped.

## Injection Attack

Requirements: User is supplying input through a form or url.

1. A malicious agent attempts an injection attack through some means of input on the site.

2. All data that is inserted into the database is parameterized. Data is validated before it is used and exceptions are thrown if it falls outside the expected parameters.