CSRF

User/Admin logs into website

Attacker posts an image or posts a linked comment with commands to edit the users account

USER/ADMIN

User/Admin clicks on illicit photo or linked message on website

Attacker

Users browser sends HTTP requests to target site which allows the attacker to make specific actions occur

XSS

User/Admin logs into website

Attacker injects a comment or image to inject malicious scripts on forum of website

Attacker

User interacts with the XSS attack and is forced to run the script causing the user/admin to be redirected
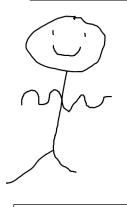
USER/ADMIN

SQL injection

USER/ADMIN

User/Admin logs into website

User/Admin uses site to post and add data

Data and user accounts are stored in a database

Attacker

SQL injection to run a query of the websites data base often returning the first user which is most often the administrator.

URL manipulation

USER/ADMIN

User/Admin logs into website

User/Admin has access to certain parts of the website that will redirect you on a homepage if you have a certain privilege described by your account. This may be a link to get you to a member only forum.

User/Admin access part of website that was made only for "them"

Attacker

The attacker in this case can manipulate the URL in order to gain access to parts of the website that they are not entitled too. This can be done if there is no added layer of security to see in the user is logged in or not.