Abuse Case: Person injects SQL

Resource: Unlimited. Has backing from the Chinese government.

Actor: David.

Skills: Very experience at injecting SQL. Trained by the best of the best.

Objective: Wants to inject SQL to gain access to our database.

Abuse Case Description

David will try inject SQL

David will try to inject SQL once he enters the webpage. He will do method to do so. He first tries this method in the search bar. Then he tries to do this in any other access point he can type into. After this is completed, he will have access the database and be able to take everything away.

Misuse Case: Person accidently buys too many tickets

Resource: Only has a laptop.

Actor: Kneecomepoop(KCP)

Skills: Only uses the computer once a week.

Objective: Wants to buy tickets.

Abuse Case Description

Kcp tries to buy tickets from website, but when prompted to selected amount he accidently enters 30 rather then 3. The system proceeds to sell Kcp without a payment notification letting him know how much he is purchasing.

Operation: Sanitized(SEBydate(StartDate,endDate)),Sanitized(SEByCategory(categoryTxt))

Cross Reference: Abuse Case Person Injects SQL.

Precondition: SEBydate() and SEByCategory() must be sent first

Postcondition: It’ll scrub for any contamination of any SQL injection. It’ll check if SQL is being typed and sent it.

Operation: finalizeOrder(totalCost,tickets)

Cross Reference: Misuse Case Person accidentally buys too many tickets.

Precondition: must have tickets.

Postcondition: confirmation() is sent back to cart, confirming order. Showing amount of tickets purchased.



