data sanitization/ validation

- problems with our app as is?

data sanitization/ validation

- problems with our app as is?
  - vulnerable to tags (including XSS)
  - length limits
  - valid email addresses

sanitization

- strip away bad things
- <script> becomes script
- assume input is malicious

validate

- make sure data is in valid ranges
  - eg, email addresses, dates, # of items to place in shopping cart
  - help the user get it right

data sanitization/ validation

- sanitize data
- validate data after sanitization
- store validation errors
- don’t take action
- present errors to user
  - offer pre-filled forms