email class to read up on HTML, SQL

116: Web Security

① Assignment 2

② Why attack web apps?
- Juiciest + personal
- Business data
- Poorly trained devs (i.e. you)

② About the web stack
- HTTP → GET, POST
- HTML → content
- CSS → presentation, layout
- JavaScript → interactivity
- Server-side language + framework
- Database(s) → persistent data storage

④ The cardinal sins
- Input validation
- Input validation
- Input validation } lack thereof
- Misconfiguration
- Data exposure
- Access control

⑤ OWASP Top 10 and CWE / SANS Top 25

6. Our attack playground
7. Proxies
8. XSS
9. Exercise: MessageHub
10. Cookie thief
11. Prevention
    - Replace special characters, especially "<" and ">" with HTML encoded equivalents "<" and ">" respectively

10A. The effects of XSS:
- *Mangled & defaced content
- * Annoying popups
- * Fraud
- * Stolen cookies for the domain

The idea: present all users w/ fraudulent content where to attack: user input is echoed to other users, including yourself