The URL Cruise Missile

- The parameters of the URL can be manipulated to exploit a vulnerable back-end DB system.
- The path is what can be manipulated to cause a web server to dump the /etc/passwd file.
- Three threat agents that can pose a risk are:
    - Government
    - Individual
    - Group
- Weak, compromised credentials or broken authentication can act as attack vectors for injection.
- Injection attacks exploit the confidentiality part of the CIA triad.
- Mitigation methods that thwart injection attacks are input validation, input sanitation, query parameterization, and web application firewalls.

Web Server Infrastructure

- Client information, such as names, addresses, etc., is usually stored in databases.
- Applications like online forms, Gmail, and shopping carts are all web applications.
- A web server stores web files, images, and supports physical data interaction.
- The user interacts with the client.
- A firewall prevents intruders and filters appropriate traffic.

Server-Side Attacks

- Input sanitization cleans and scrubs user input in order to prevent it from exploiting security holes by proactively modifying user input.

- Input validation tests user and application-supplied input. The process is designed to prevent malformed data from entering a data information system by verifying user input meets a specific set of criteria (i.e. a string that does not contain standalone single quotation marks).
- Costs, issues with management, or utilization of firewalls might fail at producing secure web applications.
- The hacker can manipulate the URLs path/file to exploit a file on a web server.
- As a network defender, Server-Side validation is preferred over Client-Side validation because it's easier to defend against attacks.

Web Application Firewalls

- WAFs operate on layer 7 in the OSI the Application layer.
- A WAF helps protect web applications by filtering and monitoring web traffic in connection.

- A WAF based on the negative security model (Blacklisting) protects against known attacks, and a WAF based on the positive security model (Whitelisting) allows pre-approved traffic to pass.

Authentication & Access Controls

- 4 Factors of Multifactor Authentication
    - Biometrics: eye scan, fingerprint, etc.
    - Location: Physical location/GPS
    - Key cards: RFID cards
    - Authentication input: username & password
- A password and a pin ARE NOT 2FA, but a password and a Google authenticator app can be.
- Constrained user interface restricts what users are able view on interface.