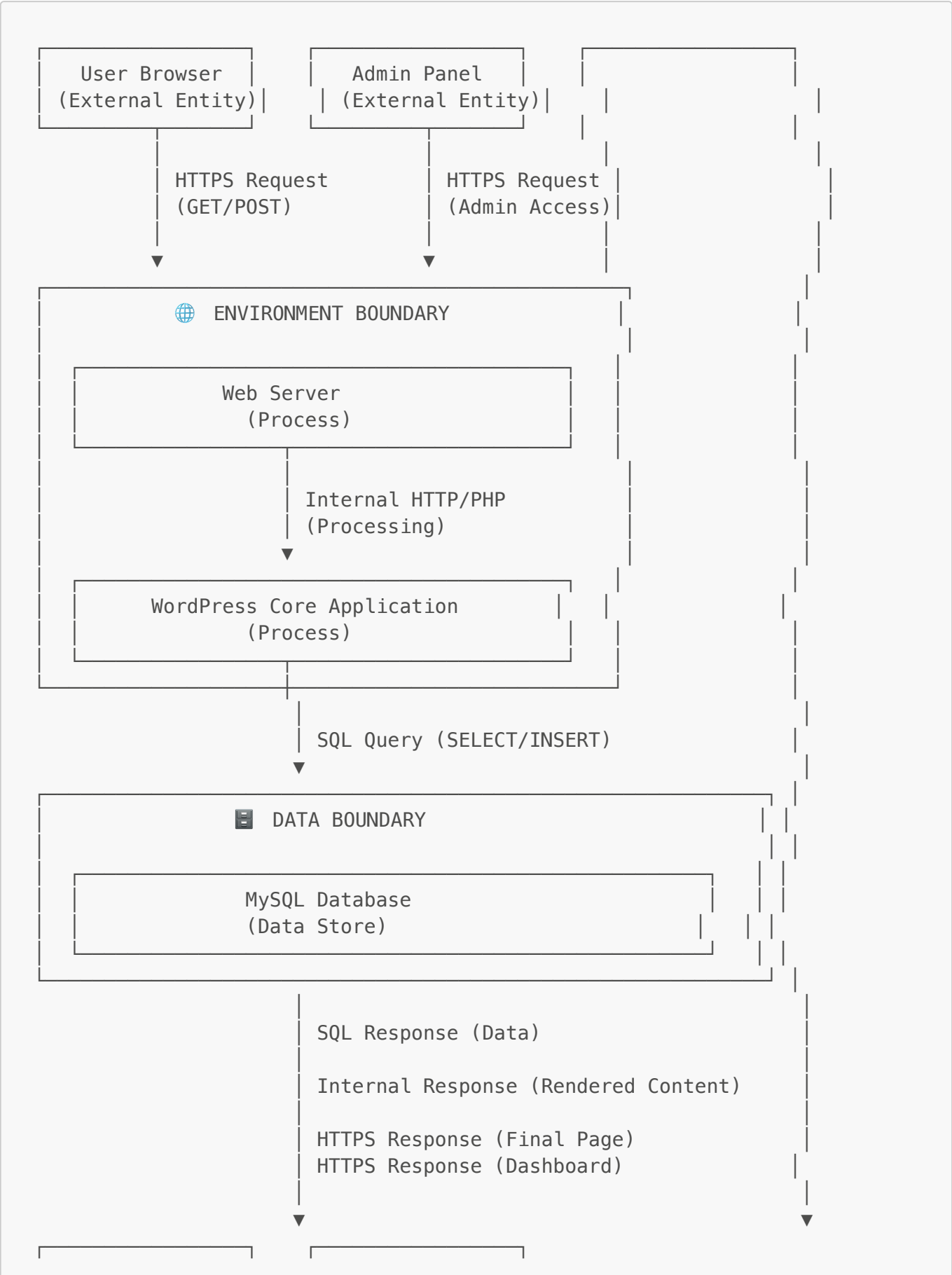
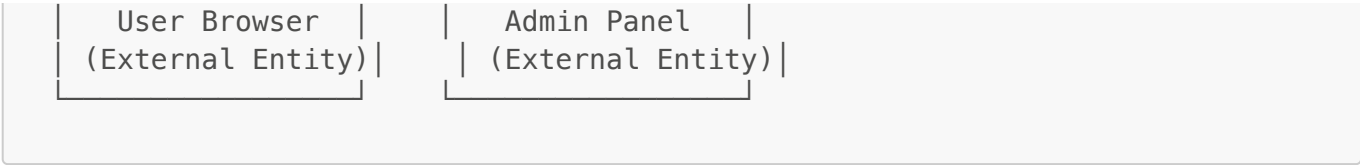


L04 Flowcharts - Clear Text Version

Diagram 1: Data Flow Diagram (DFD)

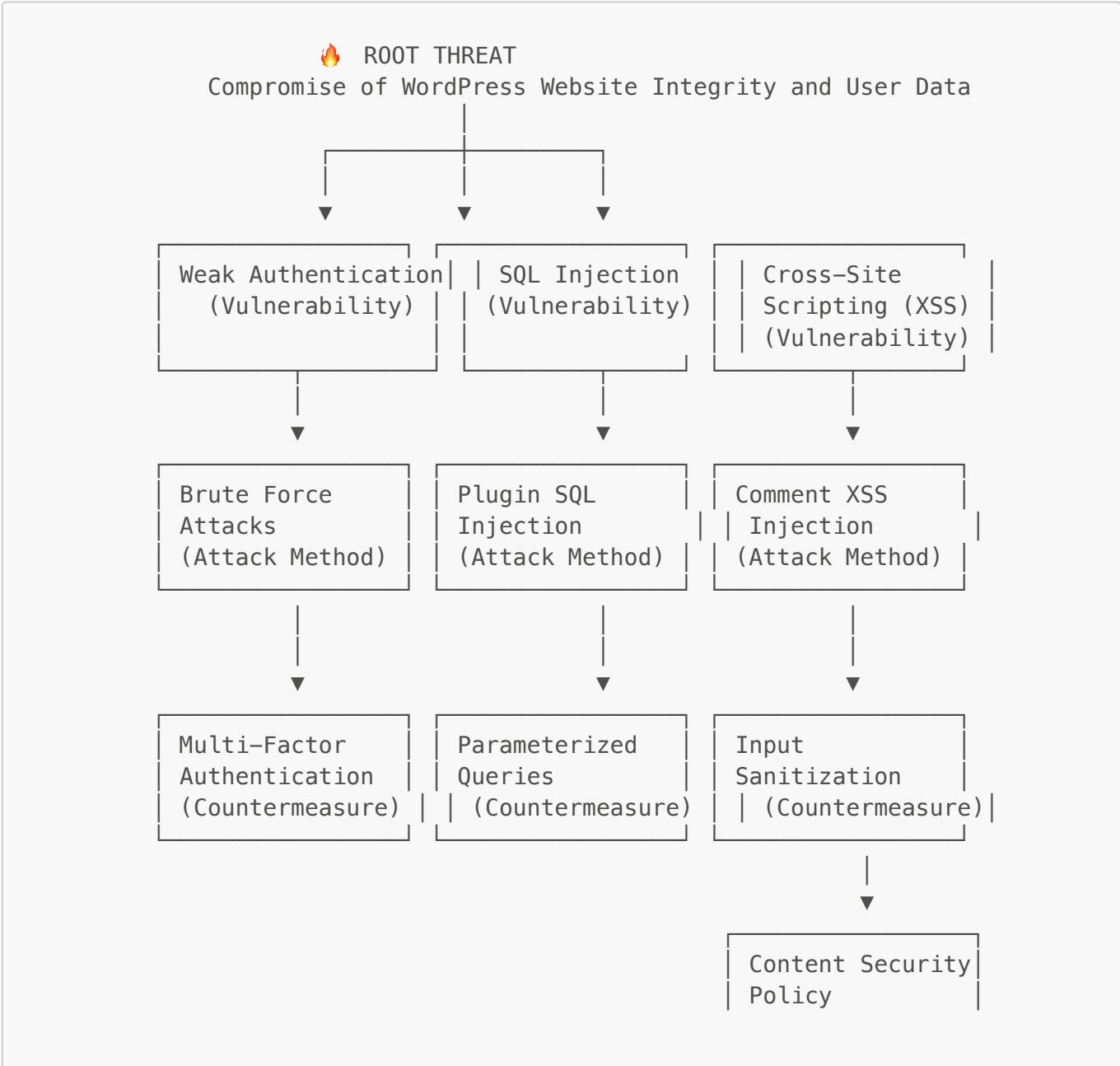




Data Flows (8 total):

- 1. User → Web Server: HTTPS Request (GET/POST)
- 2. Admin → Web Server: HTTPS Request (Admin Access)
- 3. Web Server → WordPress: Internal HTTP/PHP (Processing)
- 4. WordPress → MySQL: SQL Query (SELECT/INSERT)
- 5. MySQL → WordPress: SQL Response (Data)
- 6. WordPress → Web Server: Internal Response (Rendered Content)
- 7. Web Server → User: HTTPS Response (Final Page)
- 8. Web Server → Admin: HTTPS Response (Dashboard)

Diagram 2: Threat Tree Diagram (TTD)



(Countermeasure) |

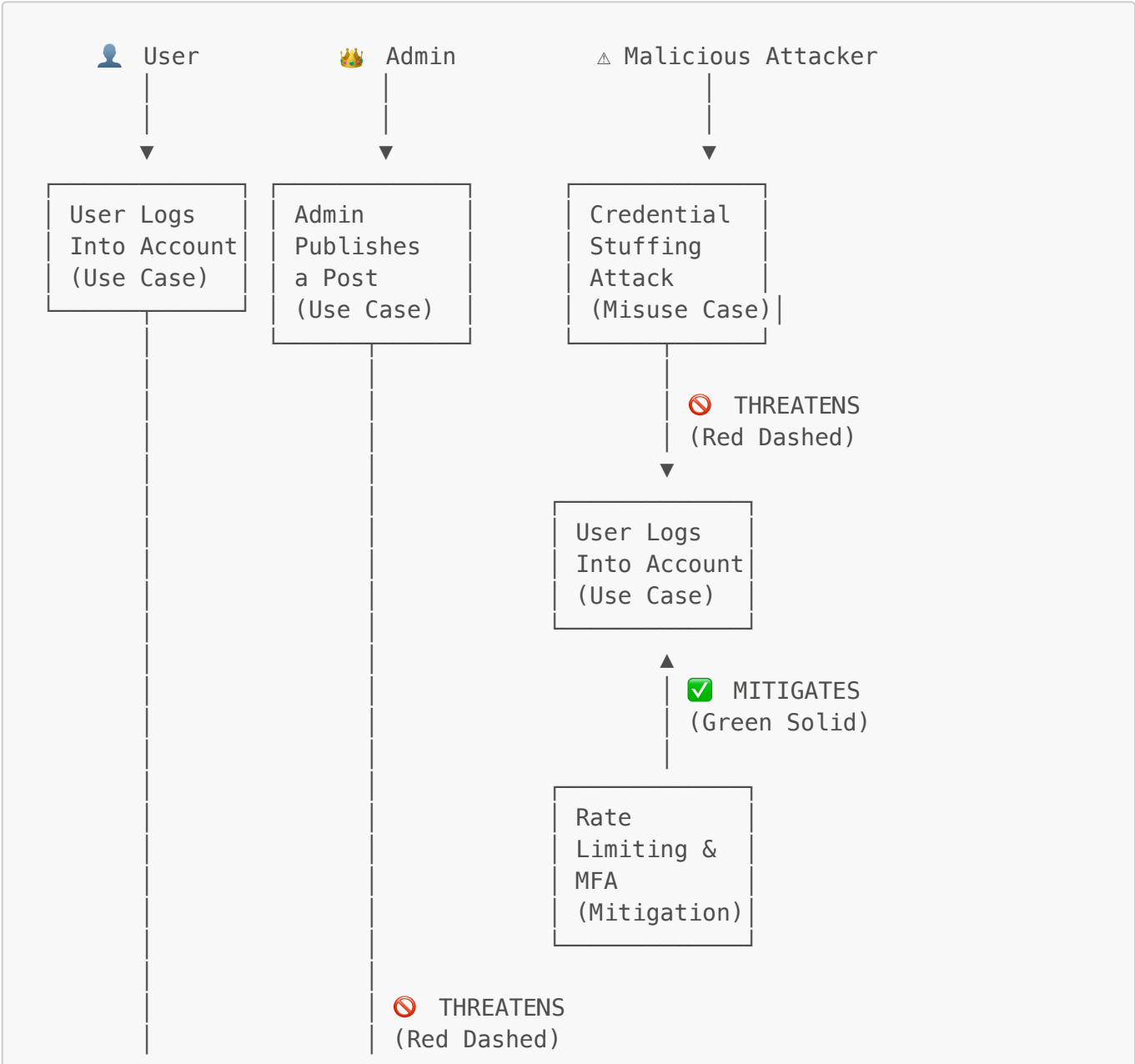
Vulnerabilities (3):

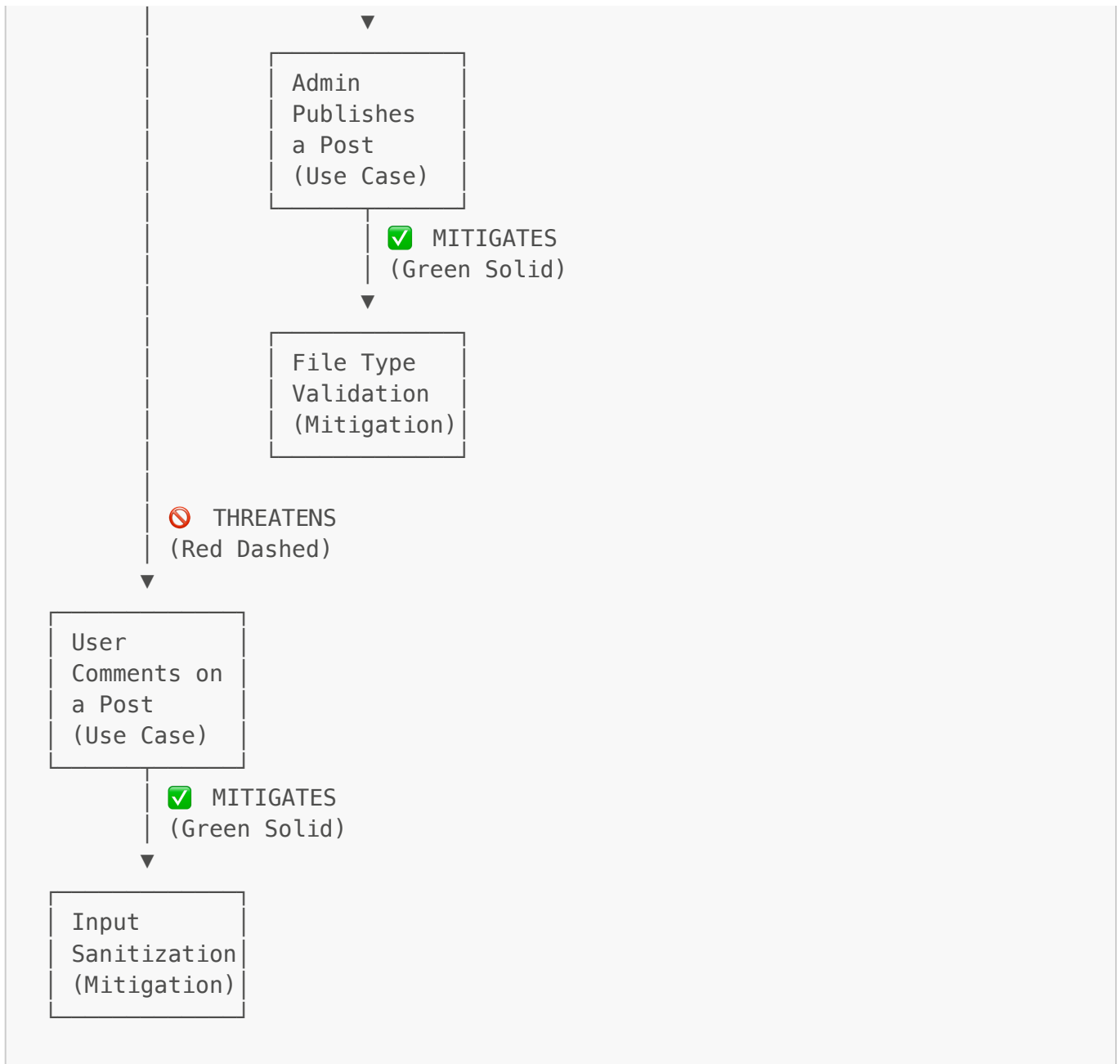
- Weak Authentication
- SQL Injection
- Cross-Site Scripting (XSS)

Countermeasures (4):

- Multi-Factor Authentication
- Parameterized Queries
- Input Sanitization
- Content Security Policy

Diagram 3: Use & Misuse Diagram (UMD)



**Actors (3):**

- User
- Admin
- Malicious Attacker

Use Cases (3):

- User Logs Into Account
- Admin Publishes a Post
- User Comments on a Post




Misuse Cases (3):

- Credential Stuffing Attack
- Malicious File Upload
- Comment XSS Injection

Mitigations (3):

- Rate Limiting & MFA
 - File Type Validation
 - Input Sanitization
-

Legend

-  THREATENS (Red Dashed Line)
-  MITIGATES (Green Solid Line)
-  NORMAL FLOW (Blue Solid Line)