L04 Flowcharts - Clear Text Version

Diagram 1: Data Flow Diagram (DFD)

```
┌──────────────────┐     ┌──────────────────┐     ┌──────────────────┐
│   User Browser   │     │   Admin Panel    │     │                  │
│(External Entity)│     │ │(External Entity)│     │                  │
└──────────────────┘     └──────────────────┘     │                  │
          │                        │                │                  │
          │ HTTPS Request          │ HTTPS Request  │                  │
          │ (GET/POST)             │ (Admin Access)│                  │
          │                        │                │                  │
          ▼                        ▼                │                  │
┌──────────────────────────────────────────────────┐                 │
│           🌐 ENVIRONMENT BOUNDARY                 │                 │
│                                                   │                 │
│  ┌──────────────────────────────────────────┐    │                 │
│  │            Web Server                    │    │                 │
│  │              (Process)                   │    │                 │
│  └──────────────────────────────────────────┘    │                 │
│                     │                             │                 │
│                     │ Internal HTTP/PHP           │                 │
│                     │ (Processing)                │                 │
│                     ▼                             │                 │
│  ┌──────────────────────────────────────────┐    │                 │
│  │      WordPress Core Application         │    │                │
│  │              (Process)                   │    │                 │
│  └──────────────────────────────────────────┘    │                 │
└──────────────────────────────────────────────────┘                 │
                      │                                               │
                      │ SQL Query (SELECT/INSERT)                     │
                      ▼                                               │
┌──────────────────────────────────────────────────────────────┐     │
│                 🗄 DATA BOUNDARY                             │  │
│                                                              │  │
│  ┌──────────────────────────────────────────────────────┐ │  │
│  │               MySQL Database                        │ │  │
│  │               (Data Store)                         │   │ │
│  └──────────────────────────────────────────────────────┘ │  │
└──────────────────────────────────────────────────────────────┘ │
                      │                                             │
                      │ SQL Response (Data)                         │
                      │                                             │
                      │ Internal Response (Rendered Content)        │
                      │                                             │
                      │ HTTPS Response (Final Page)                 │
                      │ HTTPS Response (Dashboard)                 │
                      │                                             │
                      ▼                                             ▼
┌──────────────────┐     ┌──────────────────┐
```

```
  │   User Browser  │      │   Admin Panel   │
  │ (External Entity)│      │ (External Entity)│
  └─────────────────┘      └─────────────────┘
```

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)

```
                       🔥 ROOT THREAT
              Compromise of WordPress Website Integrity and User Data
                                  │
                        ┌─────────┼─────────┐
                        │         │         │
                        ▼         ▼         ▼
          ┌─────────────────┐ ┌─────────────────┐ ┌─────────────────┐
          │ Weak Authentication│ │ SQL Injection   │ │ Cross-Site      │
          │   (Vulnerability) │ │ (Vulnerability) │ │ Scripting (XSS) │
          │                   │ │                 │ │ (Vulnerability) │
          └───────────────────┘ └─────────────────┘ └─────────────────┘
                    │                   │                   │
                    ▼                   ▼                   ▼
          ┌─────────────────┐ ┌─────────────────┐ ┌─────────────────┐
          │ Brute Force     │ │ Plugin SQL      │ │ Comment XSS     │
          │ Attacks         │ │ Injection       │ │ │ Injection       │
          │ (Attack Method) │ │ (Attack Method) │ │ (Attack Method) │
          └─────────────────┘ └─────────────────┘ └─────────────────┘
                    │                   │                   │
                    │                   │                   │
                    ▼                   ▼                   ▼
          ┌─────────────────┐ ┌─────────────────┐ ┌─────────────────┐
          │ Multi-Factor    │ │ Parameterized   │ │ Input           │
          │ Authentication  │ │ Queries         │ │ Sanitization    │
          │ (Countermeasure) │ │ (Countermeasure) │ │ (Countermeasure)│
          └─────────────────┘ └─────────────────┘ └─────────────────┘
                                                          │
                                                          ▼
                                                ┌─────────────────┐
                                                │ Content Security│
                                                │ Policy          │
```

```
                                                    │ (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)

```
      👤 User          👑 Admin              ⚠️ Malicious Attacker
         │                │                         │
         │                │                         │
         ▼                ▼                         ▼
  ┌─────────────┐  ┌─────────────┐       ┌─────────────┐
  │ User Logs   │  │ Admin       │       │ Credential  │
  │ Into Account│  │ Publishes   │       │ Stuffing    │
  │ (Use Case)  │  │ a Post      │       │ Attack      │
  └──────┬──────┘  │ (Use Case)  │       │ (Misuse Case)│
         │         └──────┬──────┘       └──────┬──────┘
         │                │                     │
         │                │                     │ 🚫 THREATENS
         │                │                     │ (Red Dashed)
         │                │                     ▼
         │                │              ┌─────────────┐
         │                │              │ User Logs   │
         │                │              │ Into Account│
         │                │              │ (Use Case)  │
         │                │              └─────────────┘
         │                │                     ▲
         │                │                     │ ✅ MITIGATES
         │                │                     │ (Green Solid)
         │                │                     │
         │                │              ┌─────────────┐
         │                │              │ Rate        │
         │                │              │ Limiting &  │
         │                │              │ MFA         │
         │                │              │ (Mitigation)│
         │                │              └─────────────┘
         │                │
         │                │ 🚫 THREATENS
         │                │ (Red Dashed)
```

```
       │                ▼
       │         ┌─────────────┐
       │         │ Admin       │
       │         │ Publishes   │
       │         │ a Post      │
       │         │ (Use Case)  │
       │         └─────────────┘
       │                │ ✅ MITIGATES
       │                │ (Green Solid)
       │                ▼
       │         ┌─────────────┐
       │         │ File Type   │
       │         │ Validation  │
       │         │ (Mitigation)│
       │         └─────────────┘
       │
       │ 🚫 THREATENS
       │ (Red Dashed)
       ▼
┌─────────────┐
│ User        │
│ Comments on │
│ a Post      │
│ (Use Case)  │
└─────────────┘
       │ ✅ MITIGATES
       │ (Green Solid)
       ▼
┌─────────────┐
│ Input       │
│ Sanitization│
│ (Mitigation)│
└─────────────┘
```

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)