

Domain

Domain	Pros	Cons
School	<ul style="list-style-type: none">- Familiar CRUD operations- GDPR relevance- Realistic cyber threats	<ul style="list-style-type: none">- Complex privacy laws- Limited network complexity- May lack high-stakes elements
Online Retailer	<ul style="list-style-type: none">- Rich security requirements- Frequent target for attacks- Complex data	<ul style="list-style-type: none">- Extensive compliance needs- High scalability demands- Time constraints
International Space Station	<ul style="list-style-type: none">- High-stakes security- Advanced requirements- Unique challenges	<ul style="list-style-type: none">- Complexity may exceed scope- Hard to simulate realistic attacks- Steep learning curve

1. School Application Domain

Pros:

- **Clear Scope for CRUD Operations:** Schools require managing student, teacher, and staff records, which aligns well with CRUD (Create, Read, Update, Delete) functions.
- **GDPR and Data Sensitivity:** Schools handle sensitive data (e.g., student information) which aligns with GDPR requirements and provides a strong context for implementing data encryption and security.
- **Realistic Security Threats:** Schools are frequent targets for cyber attacks (e.g., ransomware), providing realistic scenarios for protecting against brute force, DoS, and injection attacks.

Cons:

- **Privacy Concerns and Regulatory Requirements:** Designing a system that fully adheres to privacy laws like GDPR for minors can be complex.
- **Less Complex Network:** Schools generally have simpler network setups than corporations or space stations, potentially making DoS attacks less impactful and limiting design options for certain security measures.
- **Moderate Technical Challenges:** The focus may lean heavily on data protection but offer less opportunity for testing advanced cybersecurity tactics like those required for high-stakes environments.

2. Online Retailer Application Domain

Pros:

- **Comprehensive Security Needs:** E-commerce applications demand strict security due to payment processing and sensitive customer data, making it an ideal domain for exploring advanced security measures like encryption and API protection.
- **Realistic Attack Vectors:** Online retailers are frequent targets for cyber-attacks, including brute force, DoS, and API injection, allowing the design to incorporate practical, real-world security defenses.

- **Complex Data Structure:** This domain typically has diverse data sets (e.g., customer, product, and transaction data) that align well with the requirement to use different data structures.

Cons:

- **Extensive Security Requirements:** Compliance requirements (e.g., PCI DSS for payment data) add complexity and might increase the workload for designing the system.
- **Performance and Scalability Considerations:** Online retailers typically require high scalability and performance efficiency, which could be challenging to implement within the project's scope.
- **Time Constraints:** The broad feature requirements and potential complexities could be hard to meet within the six-week project timeframe.

3. International Space Station (ISS) Application Domain

Pros:

- **High-Stakes Security Environment:** ISS systems require the highest level of security, giving the team a challenging and rewarding domain for implementing advanced security features, including unique responses to brute force and DoS attacks.
- **Complex System Requirements:** Space station systems have stringent access controls and operational monitoring, creating an opportunity to apply a sophisticated design with advanced encryption and monitoring.
- **Unique Domain-Specific Challenges:** The ISS offers a unique context for exploring security, especially for scenarios like off-Earth operations that require resilience against cyber threats.

Cons:

- **Complexity Beyond Project Scope:** The ISS may have extremely specialized requirements that could be challenging to replicate accurately in a classroom setting, potentially requiring resources or knowledge beyond the project's scope.
- **Difficulty of Simulating Attacks:** Simulating attacks like DoS on a space station system might lack realistic context without specialized network setups or access to relevant testing tools.
- **High Learning Curve:** Working within the space domain may require additional research, making it difficult for the team to complete the project within six weeks.