Database Administration Security

Cybersecurity Department

Course Code: ***CBS 214***

Theoretical Lecture 8: Input Validation & Information Leakage

Halal Abdulrahman Ahmed

Agenda

- What & Why of Input Validation
- How Attacks Work
- Attack Types (Buffer Overflow, Path Traversal, XSS, SQLi)
- Impact & Modern Relevance
- Loginsoft Perspective + Homework

Learning Outcomes

By the end, students will be able to:

- Define input validation and its security role.
- Identify common input validation attacks.
- Explain the consequences of poor validation.

What is Input Validation?

- An input validation attack occurs when an attacker sends malicious or unexpected data into an application that fails to properly verify user input. If the system trusts the data without checking format, size, or type, the attacker can exploit that weakness to access data, execute code, or disrupt the system.
- Every application receives input through forms, APIs, file uploads, or system integrations. Without validation, malicious input can manipulate application behavior.
- In simple terms, input validation ensures that only safe and expected data enters the system.

Why Input Validation Matters?

Without Validation	With Validation
Attackers can inject malicious commands	Only safe, expected data enters
Databases can be stolen or deleted	Data stays protected
Users' sessions can be hijacked	Users remain secure
System can crash or run attacker code	System behaves normally

Why Input Validation Matters? (cont.)

If that input isn’t verified, it becomes an entry point for attackers. Input validation ensures data matches expected rules such as:

- Correct format
- Allowed characters
- Proper length
- Valid data type

Without it, attackers can inject harmful commands instead of normal data.

How the Attack Works?

1. The attacker finds a form or parameter that accepts user input
2. They insert specially crafted malicious data
3. The application processes it as legitimate input
4. The system executes unintended actions

Instead of entering:

- username = Ahmed
- The attacker enters:
- username = Ahmed' OR '1'='1
- Now the system behaves differently than intended.

Types of Input Validation Attacks

1. Buffer Overflow

- The attacker sends extremely large input to exceed memory limits, corrupting memory and potentially executing malicious code.

2. Canonicalization (Path Traversal) Attack

- The attacker manipulates file paths to access restricted files.

Example:

The website lets you open files like /files/report.pdf. The attacker types ../../../../etc/passwd to climb up the folder tree and reach system files they should never see (like password files).

Types of Input Validation Attacks (Cont.)

3. Cross-Site Scripting (XSS)

- Malicious scripts are injected into web pages so they run in a victim's browser.
- Result:
- Cookie theft
- Session hijacking
- Account takeover

4. SQL Injection

- Database queries are altered using malicious input to:
- Read confidential data
- Modify records
- Delete information

Common Attacks Prevented by Input Validation

Improper input handling leads to serious vulnerabilities. Many of these attacks begin with unvalidated input. Common attacks prevented include:

- SQL injection
- Cross site scripting
- Command injection
- Buffer overflow
- Path traversal attacks

Impact of Poor Input Validation

- When input validation is weak or absent, attackers can manipulate databases, execute arbitrary commands, access restricted data, or crash systems.
- Poor validation is one of the most common root causes of application vulnerabilities.

Input Validation in Modern Cybersecurity

- With API driven architectures and cloud native applications, input validation extends beyond web forms. Microservices, third party integrations, and automated workflows must all validate incoming data.
- Secure coding practices and DevSecOps integration ensure validation is embedded into development lifecycles.

Loginsoft Perspective

At Loginsoft, Input Validation is treated as a foundational secure coding control. Through our Vulnerability Intelligence, Threat Intelligence, and Security Engineering services, we help organizations identify weaknesses caused by improper input handling. Loginsoft supports input validation security by

- Mapping vulnerabilities to root causes
- Identifying exploitable injection risks
- Prioritizing remediation based on threat intelligence
- Supporting secure development best practices
- Reducing recurring vulnerability patterns
- Our intelligence driven approach ensures applications remain resilient against input based attacks.

Research Tasks (Homework)

- Should input validation be done on the client side?
- What is the most secure validation approach?
- How does Loginsoft help improve input validation security?

References

- Loginsoft. (n.d.). Input validation in cybersecurity. In *Cybersecurity Glossary*. Retrieved May 10, 2026, from https://www.loginsoft.com/glossary/input-validation-in-cybersecurity


Any
Question