University of Massachusetts Dartmouth

A Secure Design Pattern Approach Toward Tackling Lateral-Injection Attacks

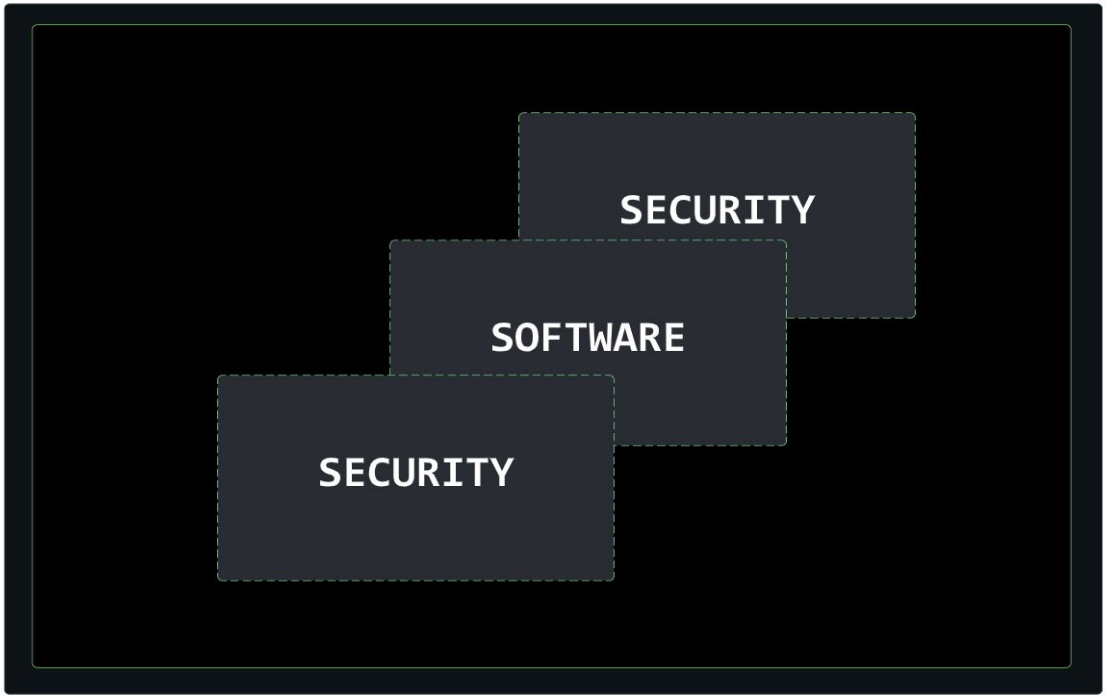
The 15th IEEE International Conference on Security of Information and Networks

Chidera “Chi” Biringa & Gokhan Kul

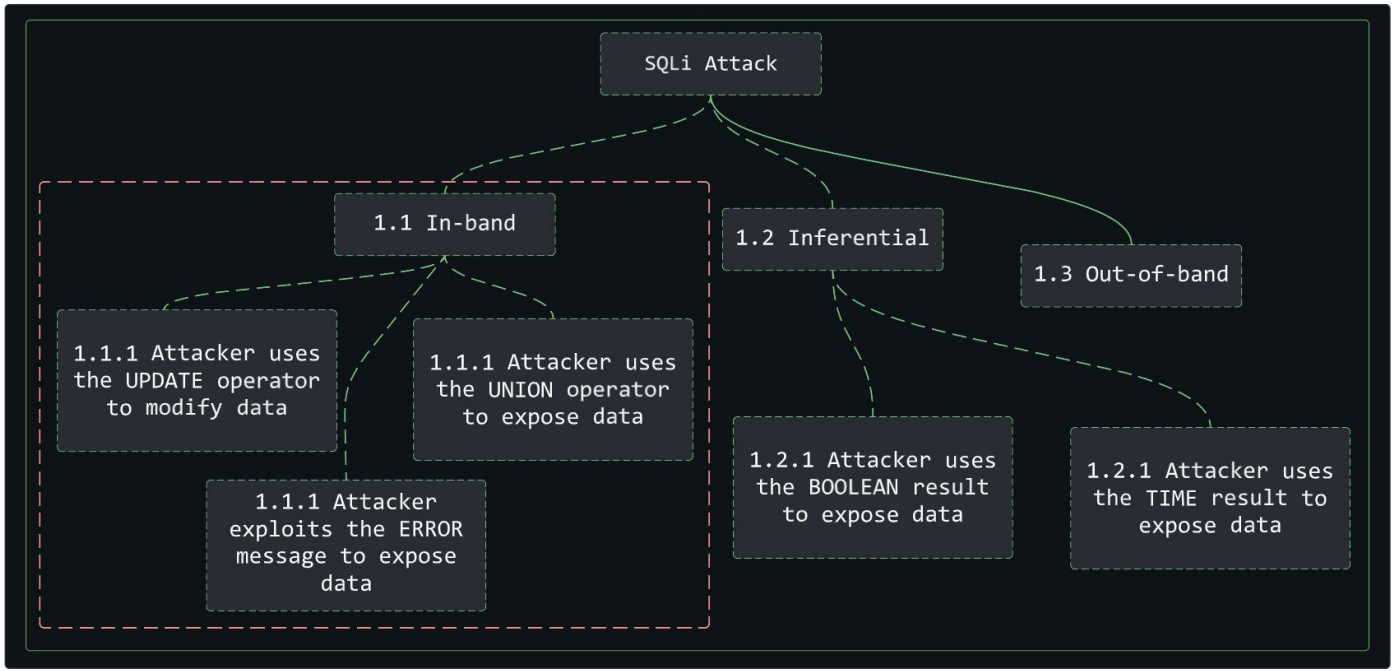
Outline

- Introduction: Security Design Patterns
- Problem: Lateral-SQL Injection Attacks
- SEAL Design
- Evaluating SEAL
- Conclusion

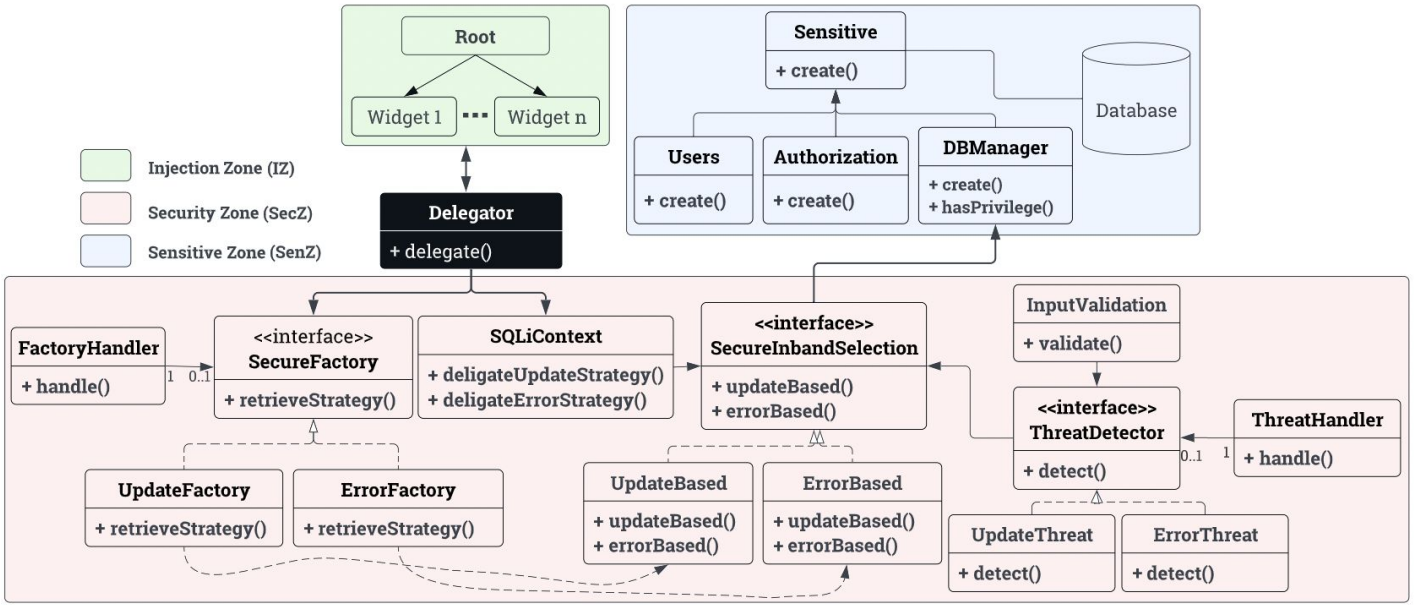
Introduction: Security Design Patterns



Lateral SQL-Injection Attack: Inband Variant



SEAL: Secure DEsign Pattern Approach Towards Tackling Lateral-Injection Attacks



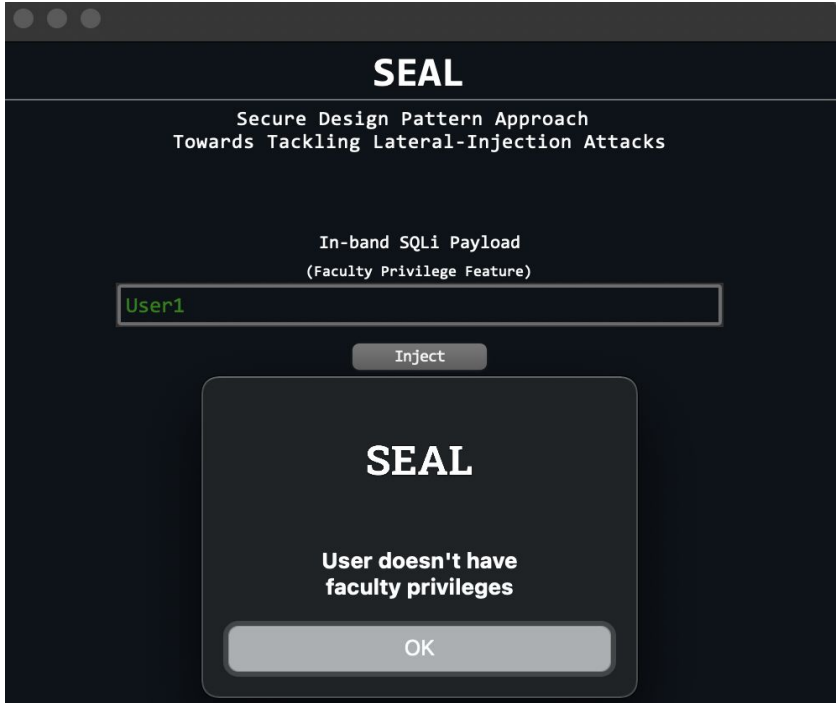
Threat Model

We designed in-band SQLi exploits (E) to demonstrate the utility of our proposed design in tackling injected attacks by permitting the integration of concrete secure strategies.

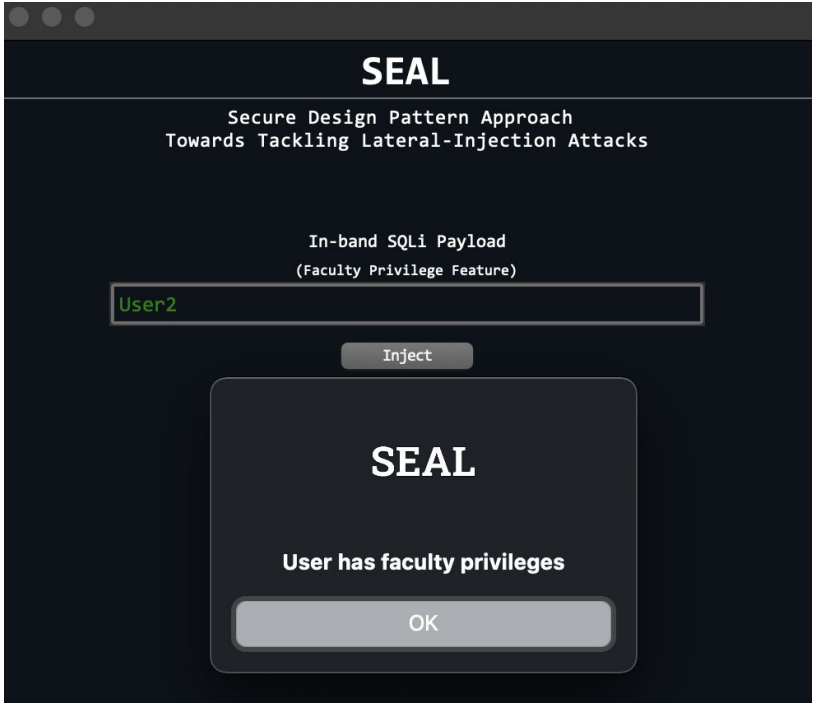
Attack Vectors Employed in this Work

- E_1 : UPDATE-based In-band SQLi
- E_2 : ERROR-based In-band SQLi

Evaluating SEAL

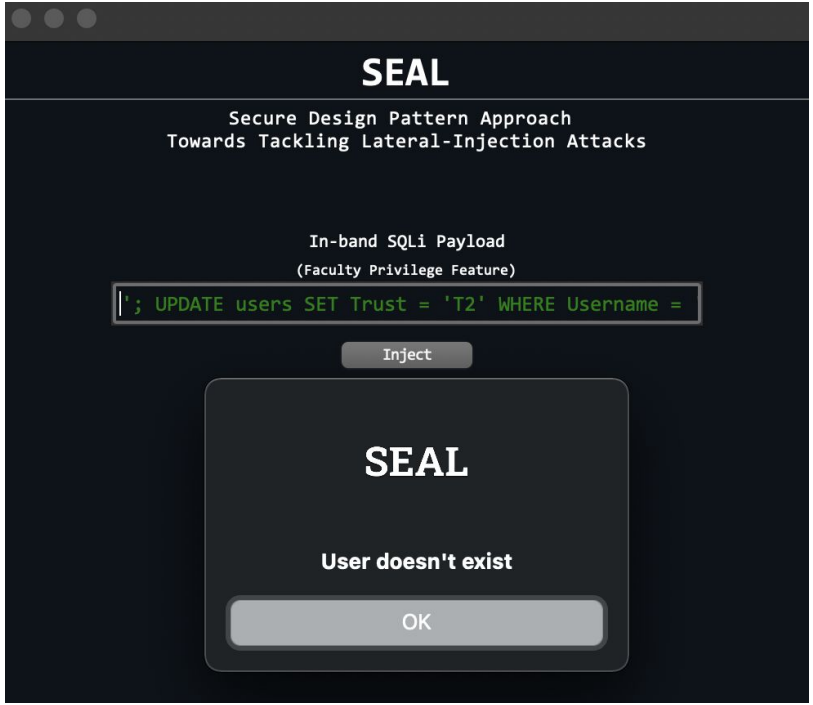


Case 1: “User1” Benign Injection

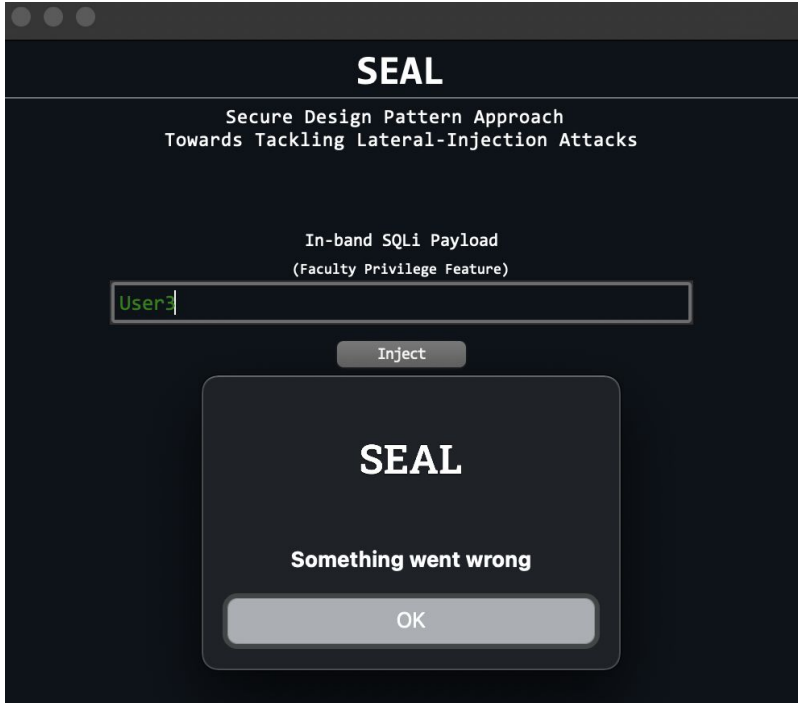


Case 2: “User2” Benign Injection

Evaluating SEAL Cont’d



Case 3: UPDATE-based Malicious Injection



Case 4: ERROR-based Malicious Injection

Conclusion

To reproduce the results used in this paper, visit: https://github.com/biringaChi/SEAL

Thanks