

Threat Name: SQL_Injection_Attack

Threat Category: Web Application Exploitation

Threat Description: The YARA rule SQL_Injection detects common SQL injection payloads, which can be used to bypass authentication or extract database records.

Indicators of Compromise (IoCs):

' OR 1=1

' OR '1'='1

OR 1=1--

Detection Mechanism: Matches SQL injection strings found in logs or scripts.

Possible Attribution & Use Cases: Used in web application penetration testing and exploitation attempts.

Recommended Actions: Implement input validation and prepared statements to prevent SQL injections.