# False Positive Documentation

Kindly provide the answers for the following queries regarding the vulnerability.

1. Name of the Application

| SetupAI |
| --- |

1. Package ID/Version ID/Listing ID

| 04tDp000000uQd2IAE |
| --- |

1. Partner Name

| SetupAI |
| --- |

1. Document Filing Date (YYYY-MM-DD)

| 2023-09-06 |
| --- |

1. Target URL (Optional)

|  |
| --- |

1. Review Date (In Case if app already undergone security review)

|  |
| --- |

#### Repeat Step 6 to 9 in case of multiple Vulnerability

1. Vulnerability Name

| Validate CRUD permission before SOQL/DML operation or enforce user mode |
| --- |

#### *Meant for the Internal Salesforce Security Team*

| Final Comment from Salesforce Team |  |
| --- | --- |
| Date of Review (YYYY-MM-DD) |  |
| Result |  |

1. Detected By

| * Chimera * PMD * Security Review * Others,   If case of others Please provide details : Code Analyzer |
| --- |

1. Detailed explanation for considering False Positive ( Elaborate as much as possible)

| I have a custom CRUD class that contains methods for checking user CRUD access to the Chat\_\_c and Message\_\_c objects so that all field and object access can be checked more succinctly.  The Code Analyzer picked up a violation on line 25 of Controller.cls where a new Message\_\_c is inserted. This insert statement is inside an if statement on line 21 that checks CRUD access on both Chat and Message.  2 more violations are on lines 42 and 43 of Controller.cls inserting a Chat\_\_c and a Message\_\_c. These are inside an if statement on line 40 checking CRUD access.  Finally, line 52 of Function.cls creates a Message\_\_c record. This is inside a CRUD check if statement on line 51. |
| --- |

1. Evidence (screenshots of the code, implementation, Command Output)

| **Controller.cls - lines 16-52**  **Function.cls - lines 50-56**  **CRUD.cls - entire class** |
| --- |