# Title: FreshSales - Software Assurance Maturity Model for Q2

|  |  |  |
| --- | --- | --- |
| **Level 1** | **Level 2** | **Level 3** |
| 1. SAST and DAST scans are performed for all release in the security staging environment.    2. Security bugs with priorities P0 and P1 reported through security assessments and responsible disclosure programs are tracked to closure based on agreed SLA. | 1. Bug audit framework with SAST and SCA capability is integrated in the product's CI to identify and track security bugs to closure in Freshrelease.    2. P0 vulnerabilities are not introduced into production.  3. Security bugs with priorities P0, P1, and P2 reported through security assessments and responsible disclosure programs are tracked to closure based on agreed SLA. | 1. Bug audit framework with SAST and SCA capability is integrated in the product's CI to identify and track security bugs to closure in Freshrelease.  2. DAST is integrated in the product's CD pipeline to identify and track security bugs to closure in Freshrelease.    3. P0 and P1 vulnerabilities are not introduced into production.  4. Security bugs with priorities P0, P1, P2, and P3 reported through security assessments and responsible disclosure programs are tracked to closure based on agreed SLA.    5. Threat modelling / security design review are conducted by the respective product teams for features or functionalities that requires security considerations. |

**P0 Vulnerabilities:**

1) Remote Code Execution

2) SQL Injection

**P1 Vulnerabilities:**

1) Cross Site Scripting

2) Vulnerable third party components

3) Broken Access Control

**Product Team Action Items:**

1. Need to adhere the defined SLA to track and closure the issues
2. Provide the necessary information and access to security engineering team, to implement the model.

**Current Progress & Updates:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Activity | Status | Ownership | Action Items |
| 1. | Initial communication & SPOC identification | Completed | Product Maven |  |
| 2. | Initial SLA, Secure-SDLC, SAMM policies communication | Completed | Product Maven |  |
| 3. | Acceptance of SLA, Secure-SDLC, SAMM policies | Completed | Product SPOC |  |
| 4. | Understanding Architecture and Security design elements | Completed | Product SPOC |  |
| 5. | Understanding SDLC process across all squads | Completed | Product SPOC |  |
| 7. | Secure Architecture | Completed | Product SPOC | * Identify and prioritise third party components, platform services and external libraries used in the product |
| 8. | SAST implementation | Completed | Product Maven | * "Security Bug" type workflow agreement and configuration in Freshrelease - Completed * Import "Security Bug" type workflow for Freshsales project in Freshrelease - Completed * Brakeman and Bundler audit configuration in Security CI - Completed * Brakeman and Bundler audit configuration in Product pipeline - Completed |
| 9. | DAST implementation | In Progress | Product Maven | * ZAP integration in Security CI - Completed * ZAP integration in Product pipeline - In Progress |
| 10. | Security Testing - External VAPT | Completed | Product Maven | * Stack Creation - Completed * Paladion environment issue resolution - Completed * Issue Validation & Triaging - Completed * Brainstorming triaged issue - Completed * Fix verification and reporting re-open issues - Completed   **Reference:** [FreshSales & FreshID Open Issues](https://docs.google.com/spreadsheets/d/16Yxan5eRF5J3hISPImb81tCf-6mWZ9nYiEX4Q96mVWw/)   * ETA for triaged issues - Completed * Risk Rating Criteria & Mutual agreement on triaged issues - Completed * Confirmatory assessment - Completed * Confirmatory-Final report from Paladion - Completed |
| 11. | Security Testing - Internal VAPT | In Progress | Product Maven |  |
| 12. | Issue Management | In Progress | Product Maven | * SPOCs - [Swati Sharma](https://confluence.freshworks.com/display/~swati.sharma) [Sudharshan Jayasampath](https://confluence.freshworks.com/display/~sudharshan.jayasampath) [Vijayaragavan Venkatarathinam](https://confluence.freshworks.com/display/~vijayaragavan) [Manikandan S](https://confluence.freshworks.com/display/~manikandan) * Bi-Weekly catch-up meeting scheduled to prfioritize 'Open Security Issues'- Alternate Tuesday between 4.30 p.m. and 5.00 p.m |