SECURITY INNOVATION

Bot Security

Level 3 - Data Flow Diagram and Threat Model for Create Inquiry bot

---

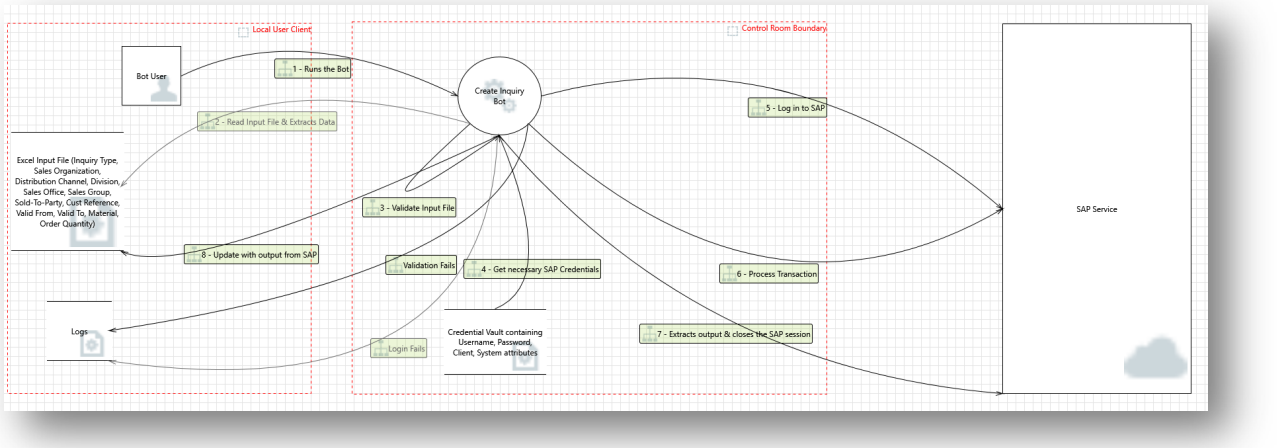
Bot Details

Bot Name: Create Inquiry
Bot Version: **1.0.0**
Report Prepared by: Satish S – Senior Security Team Lead, Security Innovation
Report Prepared for: **Spectar**
Date: 28/02/2020

Data Flow Diagram

The SAP Create Inquiry bot simplifies the process of creating inquiries in SAP. It is a reusable, fast and effective solution to cater most of the users and process the sales order with least manual intervention.

The following data flow diagram describes the operation and interactions of the **Create Inquiry** bot and its associated components.



Data flow Description

The following steps outline the bot's interactions as displayed in the data flow diagram.

1. The Bot User invokes the bot to start its processes.
2. The SAP Create Inquiry bot reads excel "Input File" and extracts the required data ("Order Type", "Sales Organization", "Distribution Channel", "Division", "Sales Office", etc.).
3. The SAP Create Inquiry bot validates the data.
4. The following actions are taken depending on the results of data validation.
    a. If data validation succeeds, the Create Sales Order bot gets necessary SAP credentials from Credential Vault.
    b. If data validation fails, the Create Sales Order bot writes logs to the "Error Log" folder and stores the error Snapshot to logs folder.
5. SAP Create Inquiry bot logs in to SAP Service. If login fails, it creates an entry in "Error Log" and creates the snapshots in "Snapshot" folder.
6. The SAP Create Inquiry bot processes the transaction based on the "Input File".
7. The SAP Create Inquiry bot extracts output and closes the SAP session.
8. The SAP Create Inquiry bot updates the status in the "Input Excel File" with output from SAP.

List of Identified Threats

The following threats to the Create Inquiry bot were generated in consultation with the data flow diagram, Create, Read, Update and Delete (CRUD)[1], Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege(STRIDE)[2], and other brainstorming activities.

Threat	Description	Asset	Impact
An attacker can read, update or delete data stored in the application binaries	An attacker can read, update or delete data stored in the application binaries.	Create Sales Order	Information Disclosure, Tampering
An attacker can update the business logic in the application scripts	An attacker can modify the business logic in the application scripts and modify the workflow of the bot.	Create Sales Order atmx scripts	Tampering
An attacker can create, read or update data between the bot and SAP service	A MiTM attack allows for the modification of traffic between SAP services and Create Sales Order bot.	SAP services	Spoofing, Tampering
An attacker can redirect the bot to an invalid SAP account	An attacker can trick the Create Sales Order bot to communicate with a fake SAP account resulting in false results.	SAP	Spoofing
SAP User excessive privileges	A SAP user with excessive privileges is used for the SAP Create Sales Order bot.	SAP	Elevation of Privilege, Tampering, Information Disclosure
The application performs insufficient Input Validation	An attacker can provide malformed input resulting in malformed input being processed by bot.	Input File	Repudiation, Denial of Service, Elevation of Privileges
An attacker can create a fake input file	A rogue operating system process, application, or user might create a fake input file and reconfigure the bot to use this file instead. The result would be that output file information would be based on the fake input file, not the real data.	Input File	Spoofing, Tampering, Denial of Service
An attacker can read the input file	An attacker that can read the input file via compromised OS process, application, or user account would gain SAP credentials and could use this information to further launch attacks against known company assets.	Input File	Information Disclosure
An attacker can update the input file	An attacker that can update the input file via compromised OS process, application, or user account.	Input File	Denial of Services
An attacker can delete the input file	An attacker that can delete the input file may disrupt the bot from regular operation resulting in the bot being unable to update the input file with accurate information.	Input File	Denial of Services
An attacker can delete contents in the SAP account.	An attacker who can delete the contents in the SAP account can disrupt the ability of the bot to perform its duties.	SAP Data	Tampering , Denial of Service

[1] https://en.wikipedia.org/wiki/Create,_read,_update_and_delete
[2] https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzZWN1cmVwcm9ncmFtbWluZ3xneDo0MTY1MmM0ZDI0ZjQ4ZDMy

Threat	Description	Asset	Impact
Insecure Logging	The bot writes sensitive data to logs or snapshots.	Logs	Information Disclosure

Threat Ranking

This section provides the results of the risk analysis performed for the **Create Inquiry** bot based on the data flow diagram and identified threats. Threats were reviewed, and the following impact categories were used to identify the risk for each threat: Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability (DREAD)[3].

The Average total is calculated by adding up all the values of the categories and dividing by 5 (number of categories).

Threat	Impact	Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Average Total
An attacker can read, update or delete data stored in the application binaries.	Information Disclosure, Tampering	5	8	5	5	9	6.8
Logs stores excessive/sensitive information or logs are not handled properly.	Information Disclosure	6	7	6	7	7	6.6
An attacker can create a fake input file	Spoofing, Tampering, Denial of Service	8	7	5	5	8	6.6
An attacker can update the input file	Tampering	8	6	5	5	8	6.4
An attacker can delete the input file	Denial of Services	7	6	5	5	8	6.2
An attacker can read the input file	Information Disclosure	6	6	5	5	8	6
An attacker can delete contents in the SAP account.	Tampering, Denial of Service	9	7	3	5	5	5.8
An attacker can modify the business logic in the application scripts and modify the workflow of the bot.	Tampering	8	6	3	5	6	5.6
A MiTM attack allows for the modification of traffic between SAP services and Sales Order bot.	Spoofing, Tampering, Elevation of Privileges	10	4	3	5	3	5

[3] https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers#the-dread-approach-to-threat-assessment

Threat	Impact	Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Average Total
An attacker can trick the Sales Order bot to communicate with a fake SAP account resulting in false results.	Spoofing	6	5	3	5	5	4.8
Excessive Privileges for the SAP user used by the bot.	Elevation of Privilege, Tampering, Information Disclosure	8	4	4	5	3	4.8
An attacker can provide malformed input resulting in malformed input being processed by bot.	Repudiation, Denial of Service, Elevation of Privileges	7	5	3	5	3	4.6

Summary of Top Threats

This section summarizes the top threats to the **Create Inquiry** bot and its associated assets. It also combines some of the threats listed is section three into an easily managed grouping. The risk rankings were also re-assessed for the grouped threats.

Threat	Impact	Average Risk Ranking
An attacker can read, update or delete data stored in the application binaries.	Information Disclosure, Tampering	6.8
Logs store excessive/sensitive information or logs are not handled properly.	Information Disclosure	6.6
An attacker can create a fake input file	Spoofing, Tampering, Denial of Service	6.6

Static Analysis

Bot Details

Bot Name: **Create Inquiry**
Bot Version/Build: **1.0.0**
Report Prepared by: **Satish S – Senior Security Team Lead, Security Innovation**
Report Prepared for: **Spectar**
Date: **February 24, 2020**

Application Source Code Scanning

Tool Details

Tool Used: Veracode
Tool version information: VERACODE Engine Version - 20200218164746

Tool Configuration

VERACODE

Veracode Detailed Report prepared for Automation Anywhere – Feb 24, 202

Policy Evaluation

Policy Name: Veracode Recommended High

Revision: 1

Policy Status: Pass

Description

Veracode provides default policies to make it easier for organizations to begin measuring their applications against policies. Veracode Recommended Policies are available for customers as an option when they are ready to move beyond the initial bar set by the Veracode Transitional Policies. The policies are based on the Veracode Level definitions.

Rules

Rule type	Requirement	Findings	Status
Minimum Veracode Level	VL4	VL4 + SCA	Passed
(VL4) Min Analysis Score	80	100	Passed
(VL4) Max Severity	Medium	Flaws found: 0	Passed

Scan Requirements

Scan Type	Frequency	Last performed	Status
Static	Quarterly	2/24/20	Passed

Remediation

Flaw Severity	Grace Period	Flaws Exceeding	Status
Very High	0 days	0	Passed
High	0 days	0	Passed
Medium	0 days	0	Passed
Low	0 days	0	Passed
Very Low	0 days	0	Passed
Informational	0 days	0	Passed

Type	Grace Period	Exceeding	Status
Min Analysis Score	0 days	0	Passed

Tool coverage

Static Code Analysis was performed on the *SapGUIScript1.dll*.

Scope of Static Scan

The following modules were included in the static scan because the scan submitter selected them as entry points, which are modules that accept external data.

Engine Version: 20200218164746

The following modules were included in the application scan:

Module Name	Compiler	Operating Environment	Engine Version
LicenseIntegrationHelper.dll	MSIL_MSVC14_X86	Win32	20200218164746
SapGUIScript1.dll	MSIL_MSVC14_X86	Win32	20200218164746