SECURITY INNOVATION

Bot Security

Level 3 - Data Flow Diagram and Threat Model for
Salesforce Mass Transfer Records

Bot Details

Bot Name: Salesforce Mass Transfer Records
Bot Version: **1.0.0**
Report Prepared by: Satish S – Senior Security Team Lead, Security Innovation
Report Prepared for: **Thirdware Solution**
Date: February 25, 2020

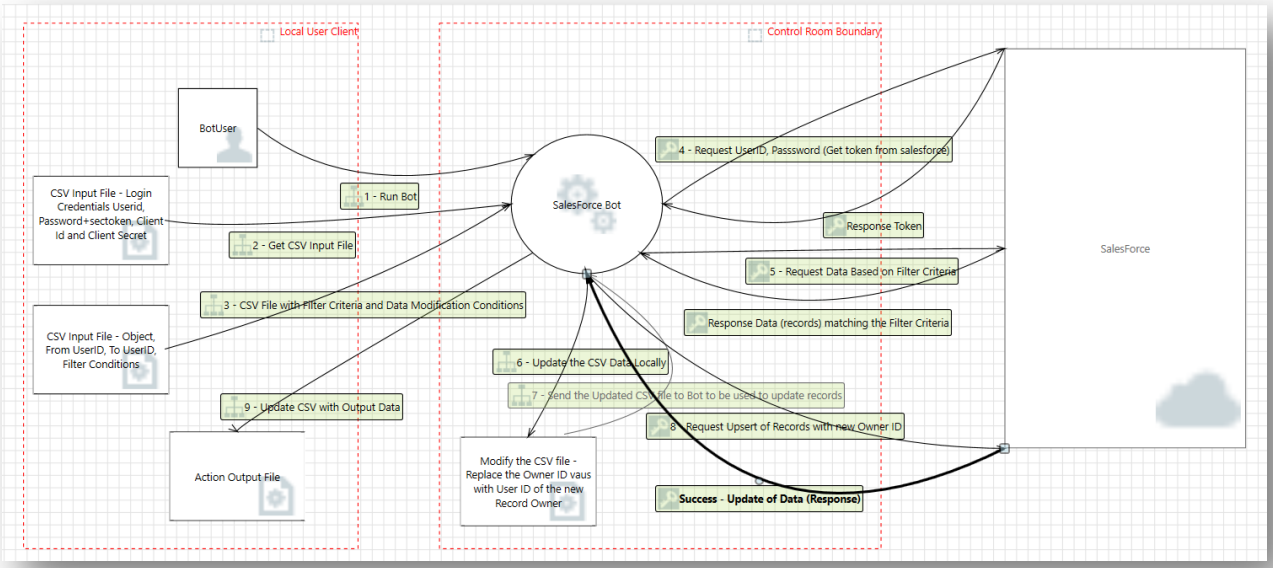
SECURITY INNOVATION

Data Flow Diagram

The Salesforce Mass Transfer Records bot simplifies the process of Transfer of Ownership in bulk which is not possible with the Mass Transfer tool of Salesforce.

Salesforce administrators are responsible for tasks ranging from helping users develop reports and resetting passwords to maintaining data quality, adding fields, and running backups, among many others. One of the key tasks of Salesforce administrators is to transfer record ownerships due to changes in job responsibility or territory coverage. Salesforce has an option to mass transfer records, but that's a very tedious and time-consuming job. The Salesforce Mass Transfer Records Bot helps Salesforce admins to easily manage the transfer ownership of records.

The following data flow diagram describes the operation and interactions of the **Salesforce Mass Transfer Records** and its associated components.



Data flow Description

The following steps outline the bots interactions as displayed in the data flow diagram.

1. The BotUser invokes the bot to start its processes.
2. The Salesforce MassTransferRecords Bot retrieves and processes CSV input file containing Login Credentials (Userid, Password+Security Token, ClientID, Client Secret).
3. A second CSV file is retrieved by the MassTransferRecords Bot containing the values for ‘Object’, ‘From UserID’, ‘To UserId’, and ‘Filter Conditions’.
4. The MassTransferRecords Bot makes a request to Salesforce and retrieves the necessary ‘Security Token’.
5. The MassTransferRecords Bot uses the security token and retrieves the data (records) matching the criteria provided in the filter conditions and stores the file as a CSV.
6. The MassTransferRecords Bot updates the CSV file by changing the ‘Owner Id’ to the new ‘UserId’ provided by the user.
7. The updated CSV file is sent to the MassTransferRecords Bot.
8. The MassTransferRecords Bot requests the UPSERT of new data provided to Salesforce.
9. Response data on successful (or failure) completion of action performed on Salesforce instance is returned to the MassTransferRecords Bot.
10. MassTransferRecords Bot creates a CSV file with output data including: ‘Id’, ‘Name’, ‘OwnerID’ .

List of Identified Threats

The following threats to the **Salesforce Mass Transfer Records** 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 modify the workflow of the bot	An attacker can intercept the application function calls and modify the workflow of the bot.	Salesforce Mass Transfer Records bot	Tampering
An attacker can change the business logic of the bot	An attacker can modify the bot atmx scripts and modify the business logic of the bot.	Salesforce Mass Transfer Records bot	Tampering, Denial of Service
An attacker can intercept the bot and perform Man-in-the-Middle attacks (MitM)	A MiTM attack allows for the modification of traffic between Salesforce services and Mass Transfer Records bot.	Salesforce services	Spoofing, Tampering, Elevation of Privilege
An attacker can redirect the Bot	An attacker can trick the Mass Transfer Records bot to communicate with a fake Salesforce account resulting in false results.	Salesforce	Spoofing
Salesforce User Excessive privileges	A user with excessive privileges is used for the Mass Transfer Records bot.	Salesforce	Tampering, Information Disclosure, Elevation of Privilege
Weak Salesforce configuration	An unauthenticated attacker can access Salesforce services and potentially gain access to sensitive salesforce data.	Salesforce	Tampering, Information Disclosure, Denial of Service, Elevation of Privilege.
Insufficient input validation	An attacker can provide malformed input resulting in malformed output files or reports.	Output File	Repudiation, Denial of Service, Elevation of Privilege
Network Disruption	An invoked action against Salesforce is not properly reported to output file.	Salesforce	Repudiation
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 access to the credentials stored in the input file.	Input File	Information Disclosure
An attacker can update the input file	An attacker that can read the input file via compromised OS process, application, or user account would modify the credentials stored in the input file.	Input File	Tampering

[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
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 Mass Transfer Records 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	Tampering, Denial of Service
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 output file with accurate information.	Input File	Denial of Service
An attacker can read the contents of the output file	An attacker that can read the contents of the output file through compromised process, application, or user account would gain access to sensitive salesforce data.	Output File	Information Disclosure
An attacker can update the contents of the output file	An attacker that can read the contents of the output file through compromised process, application, or user account would modify salesforce data stored.	Output File	Spoofing, Tampering
An attacker can delete the output file	An attacker that can delete the output file might disrupt the execution flow of the Mass Transfer Records bot, resulting in the bot not working. It may also result in the loss of historical status data if the data is not already backed up.	Output File	Repudiation
An attacker can read, update or modify the Salesforce token.	An attacker that can modify the token stored by the bot which would result in the integrity of the output results being compromised.	Session Token	Spoofing, Tampering, Elevation of privilege
An attacker can delete contents in the Salesforce account.	An attacker who can delete the contents in the Salesforce account can disrupt the ability of the bot to perform its duties.	Salesforce Data	Tampering , Denial of Service

Threat Ranking

This section provides the results of the risk analysis performed for the **Mass Transfer Records** 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 modify the Salesforce token.	Spoofing, Tampering, Elevation of Privilege	8	10	3	5	8	6.8
An attacker can create a fake input file	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 Service	7	6	5	5	8	6.2
An attacker can read the contents of the output file	Information Disclosure	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 Salesforce account.	Tampering, Denial of Service	9	7	3	5	5	5.8
An unauthorized attacker can access Salesforce services and potentially create, read, update salesforce data.	Tampering, Information Disclosure, Denial of Service, Elevation of Privilege.	10	5	4	5	4	5.3

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

An attacker can modify the bot atmx scripts and modify the business logic of the bot.	Tampering, Denial of Service	8	6	6	5	6	5.1
An attacker can intercept the application function calls and modify the workflow of the bot.	Tampering	5	6	4	5	5	5
An attacker can modify the traffic between Salesforce services and MassTransferRecords Bot. (MiTM)	Spoofing, Tampering, Elevation of Privilege	10	4	3	5	3	5
An invoked action against Salesforce is not properly reported to output file.	Repudiation	3	6	4	4	8	5
An attacker can update the contents of the output file	Spoofing, Tampering	4	6	5	5	5	5
An attacker can delete the output file	Repudiation	4	6	5	5	5	5
An attacker can redirect the Bot to communicate with a fake Salesforce account resulting in false results.	Spoofing	6	5	3	5	5	4.8
An attacker can provide malformed input resulting in malformed output files or reports.	Repudiation, Denial of Service, Elevation of Privilege	7	5	3	5	3	4.6
Excessive Privileges for the Salesforce user used by the Bot	Tampering, Information Disclosure, Elevation of Privilege	8	3	3	5	2	4.2

Summary of Top Threats

This section summarizes the top threats to the **Mass Transfer Records** 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 modify the Salesforce token.	Spoofing, Tampering, Elevation of Privilege	6.8
An attacker can create a fake input file	Tampering, Denial of Service	6.6
An attacker can update the input file	Tampering	6.4

Static Analysis

Bot Details

Bot Name: **Mass Transfer Records**
Bot Version/Build: **1.0.0**
Report Prepared by: **Satish S – Senior Security Team Lead, Security Innovation**
Report Prepared for: **Thirdware Solution**
Date: **February 21, 2020**

Application Source Code Scanning

Tool Details

Tool Used: VERACODE
Tool version information: VERACODE Engine Version - 20200124175904

VERACODE

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	2/18/20	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 *String_to_upper_case.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: 20200124175904

The following modules were included in the application scan:

Module Name	Compiler	Operating Environment	Engine Version
String_to_upper_case.dll	MSIL_MSVC14_X86	Win32	20200124175904

File Differences Between Scans

The uploaded modules for this scan do not match the modules you uploaded for the previous scan. This disparity can affect the scan results even if Veracode did not find flaws in the files with differences. See appendix for more details.