SQL Injection				Severity: High
CVSS v3.1	8.8	**Vector**	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
Privileges	SAS Developer			
Version	SAS 9.4 for predictive performance management extension			

SQL injection attacks consist in inserting SQL queries through the usage of an input data field from the client application. This kind of attack allows to obtain access to the database which could then lead to the exfiltration, modify or deletion of existing data.

In this case, a SQL query is already present in a request sent during login process. By customizing this query and targeting specific SAS standard tables, the attacker could retrieve sensitive information regarding the application.

The vulnerable resource:

- https://<application-baseurl>/SASStudio/sasexec/sessions/{sessionID}/sql

Follow the steps below to replicate the results

The login flow presents a few POST requests which contains SQL commands, such as in **Error! Reference source not found.**

Figure 1: Original SQL query.

As visible in the image below, by modelling the query within the request and targeting a specific SAS standard table, *sashelp.VTABLE*, the application returns a 200 response along with sensitive information as output.

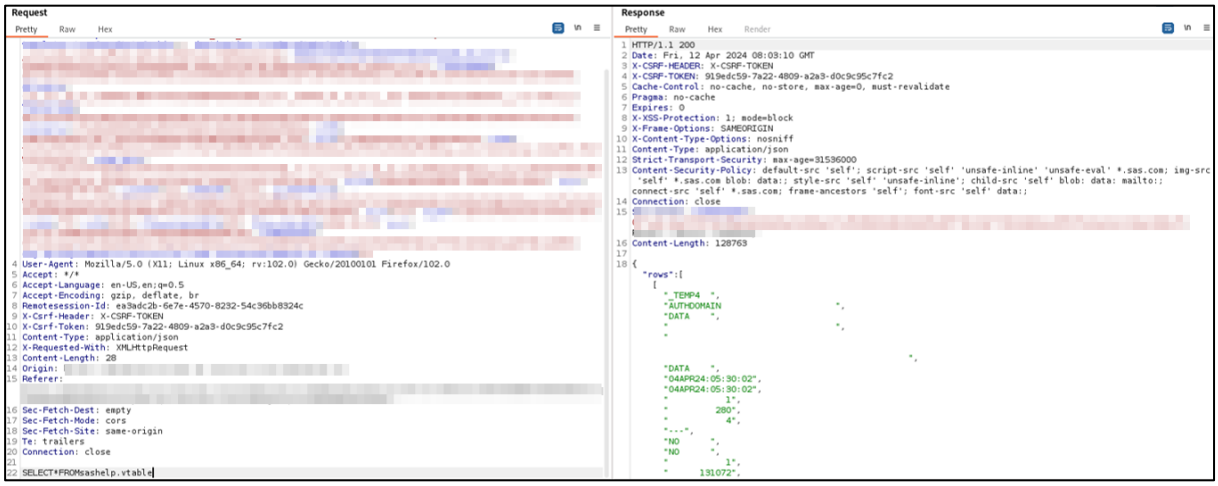

Figure 2: Modified query targeting sashelp.VTABLE.

As an example, it was also possible to retrieve sensitive information, like local server paths, by modeling the query and targeting sashelp.VEXTFL table.

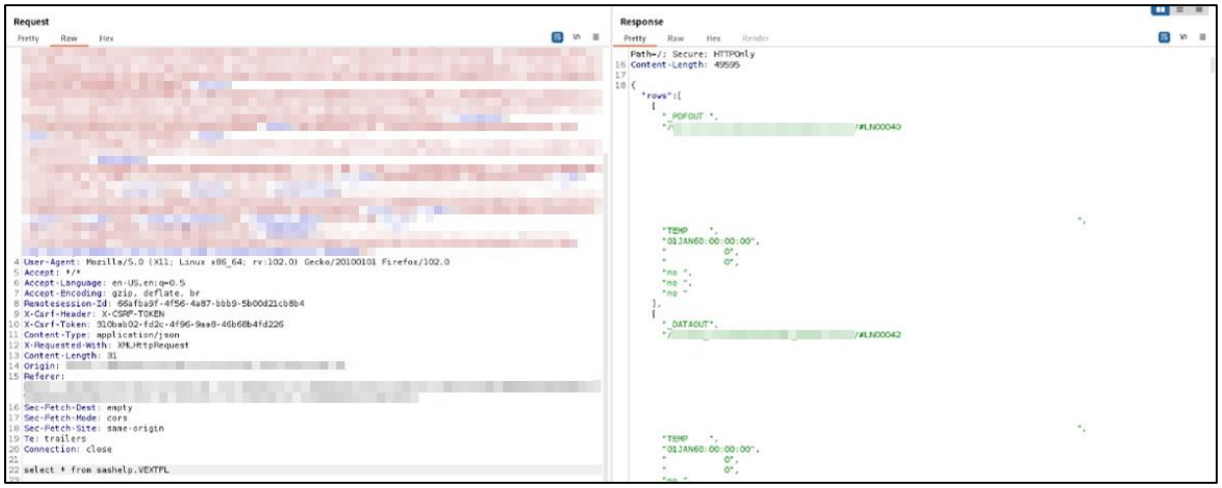

Figure 3: Modified query targeting sashelp.VEXTFL.

REMEDIATION:

SQL injection occur when user-controlled input is included into queries without prior sanitization. In order to prevent this, it is suggested to:

- Prefer the usage of prepared statements instead of concatenating user input into existing queries.
- Use properly constructed stored procedure.
- Sanitize and escape any user provided input.

For further information, please refer to:

- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html