HTTP Method Override

Replicated the issue :

Graphical user interface, text, application, email

Description automatically generated

Problem: When X-HTTP or X-Method was set to PUT and allowed access to the server when it wasn’t supposed to. Also when manipulating the POST address, either adding extra characters to the front or back of the word “message”, it would allow malicious attacks to go in as well.

Solution:

Added an interceptor function that did not allow specific x-http or x-method request headers to go through. Solution works with the entire component of code, message, messageSummary, dailyRollup, dailyRollupSummary, monthlyRollup, monthlyRollupSummary, and specialSummary

Code : https://github.com/Travelport-Enterprise/TAHMS-MessageService/blob/TPSAB-616/src/main/java/com/travelport/soa/dms/message/util/Interceptor.java

HTML CORS Functionality Abuse

Replicated the issue:

Graphical user interface, text, application, email, website

Description automatically generated

Problem: different origin addresses could access the server

Solution: Only allowed Travelport domains to enter

allowedOriginPatterns("\*travelport.com\*", "\*.tvlport.net\*")

Solution works with the entire component of code, message, messageSummary, dailyRollup, dailyRollupSummary, monthlyRollup, monthlyRollupSummary, and specialSummary

Code: https://github.com/Travelport-Enterprise/TAHMS-MessageService/blob/TPSAB-616/src/main/java/com/travelport/soa/dms/message/CorsConfig.java