

# Attacking Model Context Protocol and Tool Surfaces