**Http Header Tampering/Http post**

In this document, we explain a scenario in which web application vulnerability is exploited by an attacker to elevate privileges.

**Description**

Privilege escalation occurs when a user gets access to more resources or functionality than they are normally allowed, and such elevation or changes should have been prevented by the application. This is usually caused by a flaw in the application. The result is that the application performs actions with more privileges than those intended by the developer or system administrator.

For example:

The following HTTP POST allows the user that belongs to grp001 to access order #0001:

**POST /user/viewOrder.jsp HTTP/1.1**

**Host: www.example.com**

**...**

**groupID=grp001&orderID=0001**

A malicious user that does not belong to grp001 can modify the value of the parameters ‘groupID’ and ‘orderID’ to gain access to that privileged data.

**REFERENCES:**

**[1]** <https://www.owasp.org/index.php/Testing_for_Privilege_escalation_(OTG-AUTHZ-003)>