**Http Header Tampering/IP**

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

**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:

Some websites use IP address to limit the access or count the number of error login based on IP address.

For example:

**X-Forwarded-For: 8.1.1.1**

In this case, if the website uses the value of 'X-forwarded-For' as client IP address. An attacker can spoof the IP value of the 'X-forwarded-For' HTTP header to workaround the IP source identification.

**REFERENCES:**

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