**Condition Value**

**(using condition value for elevation of privilege)**

**Description 1**

Attacker can gain privileges by manipulating condition value in the http request. We present a concrete example: [1]

For example:

In an environment where the server sends an error message contained as a value in a specific parameter in a set of answer codes, as the following:

**@0`1`3`3``0`UC`1`Status`OK`SEC`5`1`0`ResultSet`0`PVValid`-1`0`0` Notifications`0`0`3`Command Manager`0`0`0` StateToolsBar`0`0`0`**

**StateExecToolBar`0`0`0`FlagsToolBar`0**

The server gives an implicit trust to the user. It believes that the user will answer with the above message closing the session.

In this condition, verify that it is not possible to escalate privileges by modifying the parameter values. In this particular example, by modifying the `PVValid` value from '-1' to '0' (no error conditions), it may be possible to authenticate as administrator to the server.

**REFERENCES:**

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