**HTTP parameter pollution (HPP)**

It is a technique used to add extra/duplicate parameters in web request to check if the web application deviates from intended behavior. A web application parses all the parameters provided by the user. But the application may change the intended behavior if the input is not sanitized properly based on the web application technology at the server-side.

Following table shows us how the web technology parses the duplicate parameters:



Developers should sanitize the input and should be aware of the parsing mechanism of the respective web technology in use to avoid application errors.

Parameter pollution may or may not cause logical issue. For example, a password reset functionality in a web application (JSP and Apache) the first occurrence of parameter maybe parsed to produce the password reset link, but developer might by mistake parse the last occurrence to send the reset link thereby an attacker can takeover any account. Same issue was found by Avinash Jain and the link for his blog is <https://medium.com/@logicbomb_1/bugbounty-compromising-user-account-how-i-was-able-to-compromise-user-account-via-http-4288068b901f>

Few more HPP issues are documented below:

<https://hackerone.com/reports/105953> <https://hackerone.com/reports/114169>

Reference:

<https://www.acunetix.com/blog/whitepaper-http-parameter-pollution/>