[1\_XSS]

Payload: \"onload=alert(1)//

Description:

The payload works because the "replace()" function in PHP do not properly replace the input.

The first replacement works fine replace('\"', ''). But when it later replace('\\', '\\\\').

Issue:

The issue is that the replacement for '"' is first and coverted to '\"'. When the other replace

statment is called it sees '\"' and replace the '\' with a duel backslash '\\' but this in fact destroy the filter itself.

Example:

value = "\\"<outbreak>"