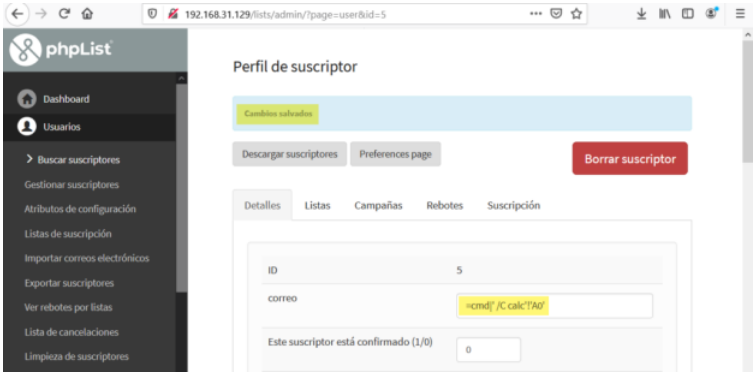
CSV INJECTION VULNERABILITY IN PHPLIST V3.6.0

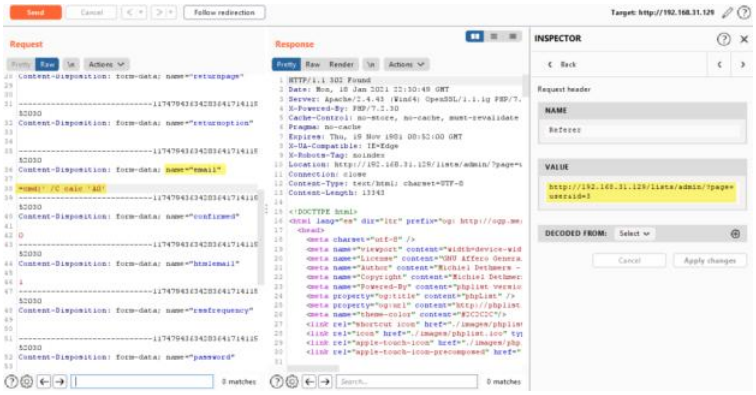
Software	PhpList	**Status**	Open
Version	3.6.0	**Severity**	Medium
Publication	19 – January – 2021	**CVSS Score**	6.5
Credits	Rafael Murillo Mercado | WeHackMX	**CVE**	CVE-2021-3188

Vulnerability Details

The phpList v3.0.6 application is vulnerable to CSV injection, an attacker can inject malicious code into the email parameter when registering a user to execute remote code on a user's computer. As shown in the following screenshot the applications do not validate the entity.

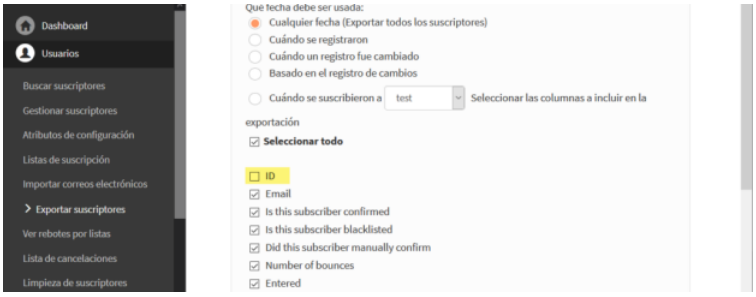


When the application sends the variable the special characters are not encoded in the frontend and the server-side input fields are not validated, this allows to enter special characters as "=cmd| ' /C calc 'A0'".



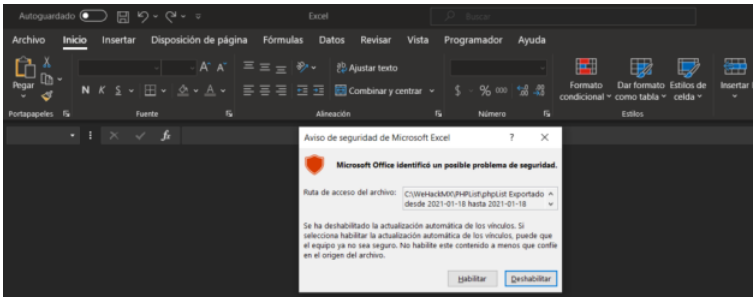
As shown below the application does not modify the input string and it allows download the content in CSV File.

The ID box must be unchecked for the payload to be interpreted, so that it takes the email string as the first value.



As show in the following screenshot the application allows download the CSV File.

When the user opens the CSV document, Excel will show a protection alert message, however if the user enables the macros, the payload will be executed.



As show in the following screenshot the payload is intercepted and the calculator is displayed as PoC, however an attacker can generate more sophisticated attacks.