Local Command Execution (File Upload) in OpenCMS 11.0.2

Author: Daniel Moreno

First, you need to get valid JSESSIONID admin Cookie or admin login and password.

Version 11.0.2 is vulnerable to Open Redirect and CSRF vulnerability (Fig 1 and 2).

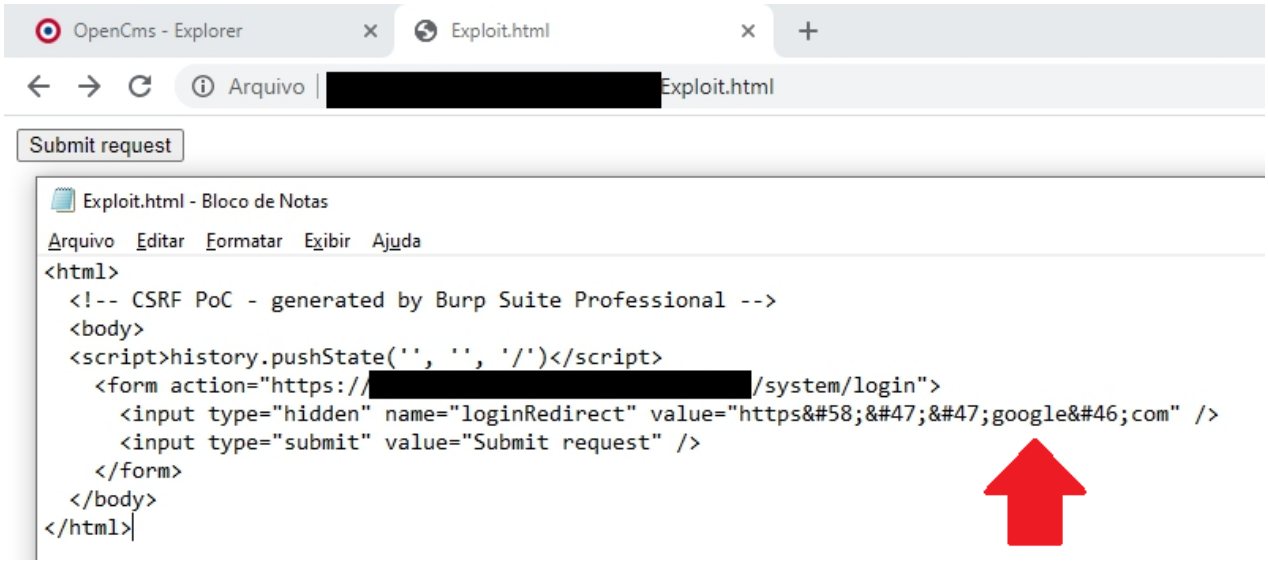

Fig 1 – CSRF vulnerability. Due to this vulnerability, Open Redirect is possible.

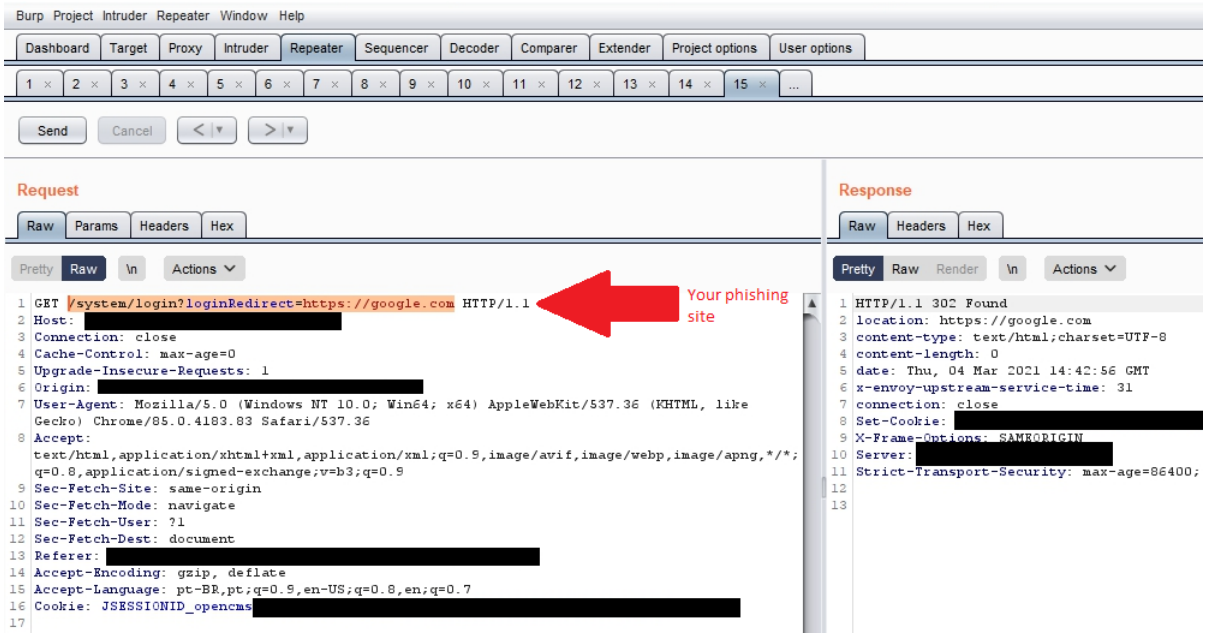

Fig 2 – Open Redirect in GET request. Send admin to your phishing page.

After obtaining the administrator password, upload malicious JSP (Fig 3).

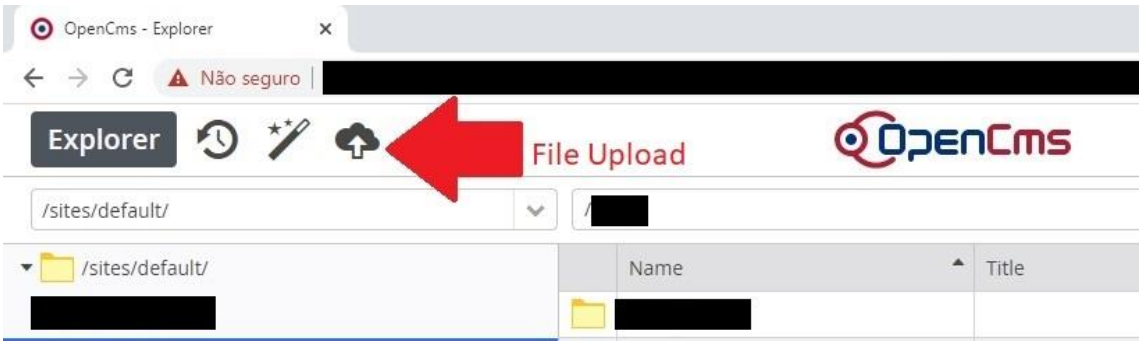

Fig 3 – File upload.

Malicious JSP (Fig 4)

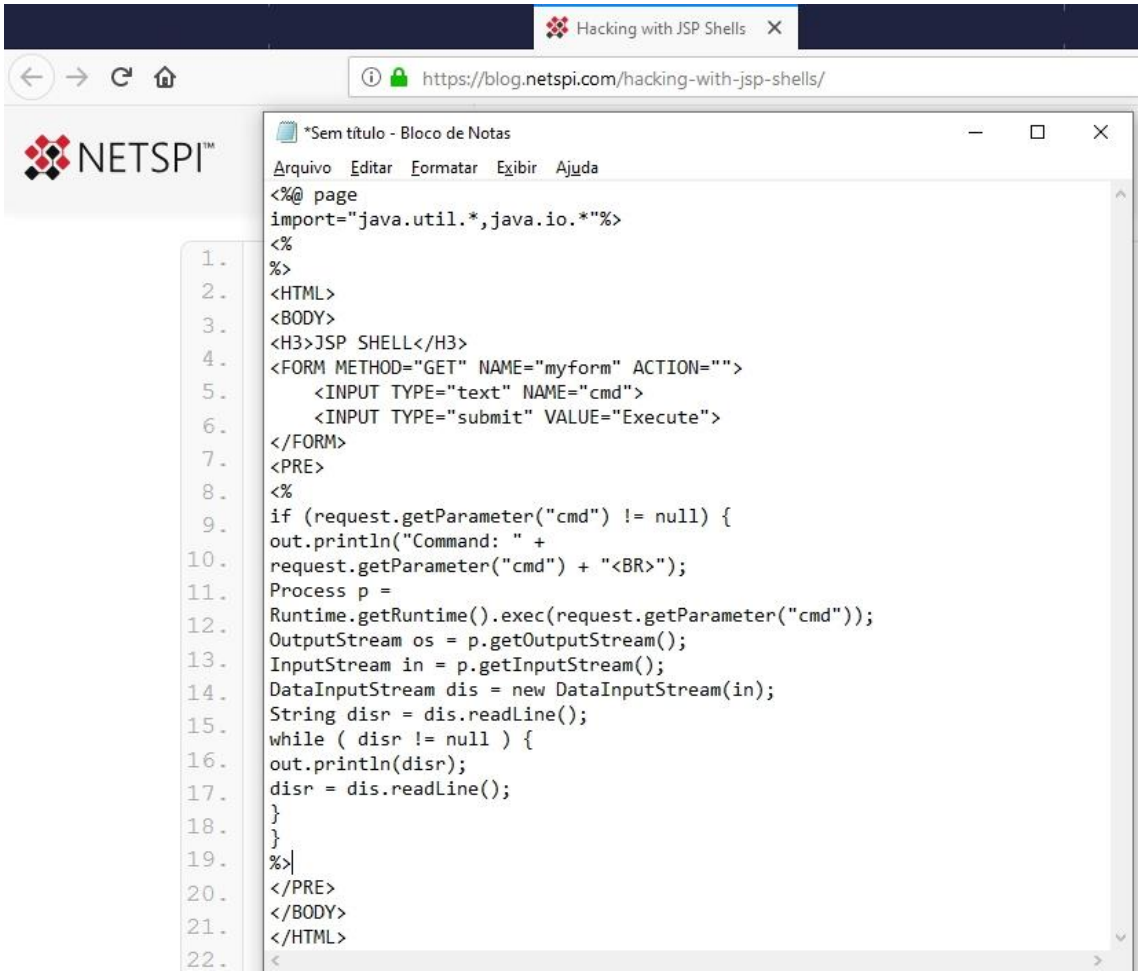

Fig 4 – Malicious JSP.

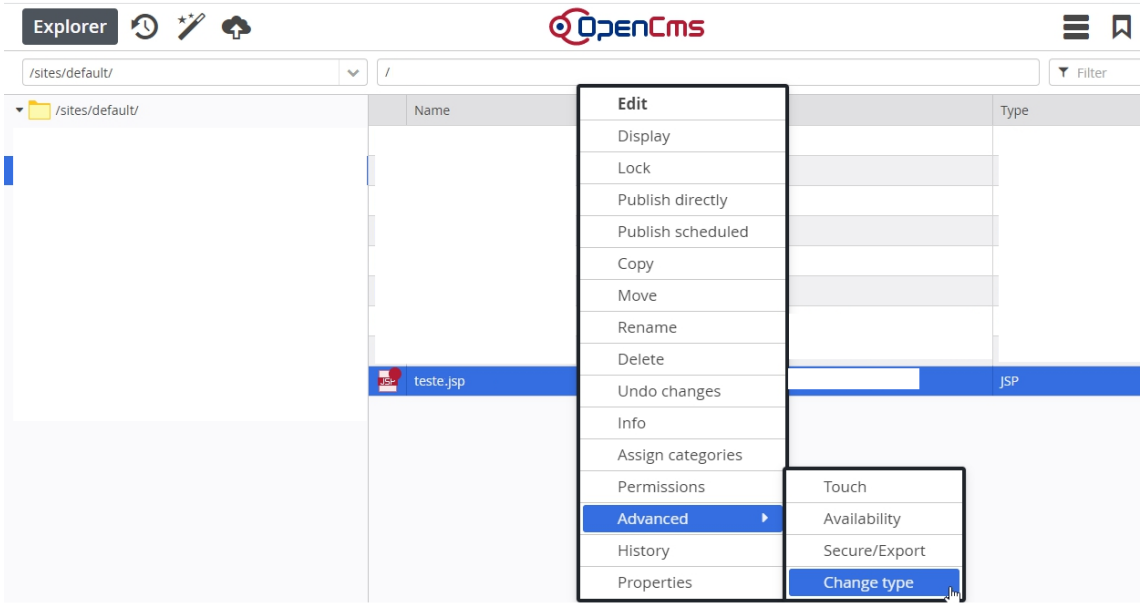

Fig 5 – Change file type to JSP.

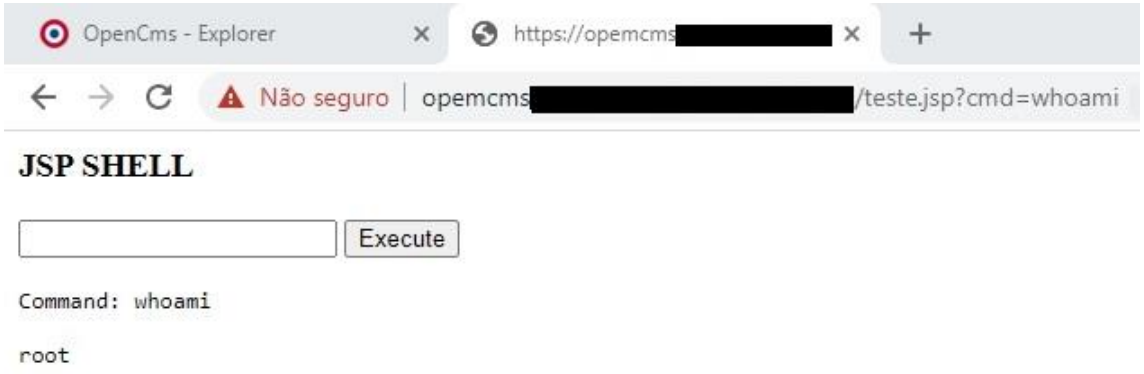

Fig 6 – Local command execution.