Remote Code Execution (RCE)

Product: **CMS Made Simple v2.2.22**

SUMMARY

A Remote Code Execution (RCE) vulnerability exists in CMS Made Simple v2.2.22.
An authenticated CMS administrator can upload and execute arbitrary PHP files via the Content → File Manager module, because file type validation is not enforced and the `/uploads/` directory is executable by default.

This vulnerability escalates privileges from content administration to system command execution as the `www-data` user, which is not an intended capability of the CMS.

Because the `www-data` user is shared by other web applications on the same server, this could allow compromise of other CMS instances or websites hosted on the same server.

PREREQUISITES

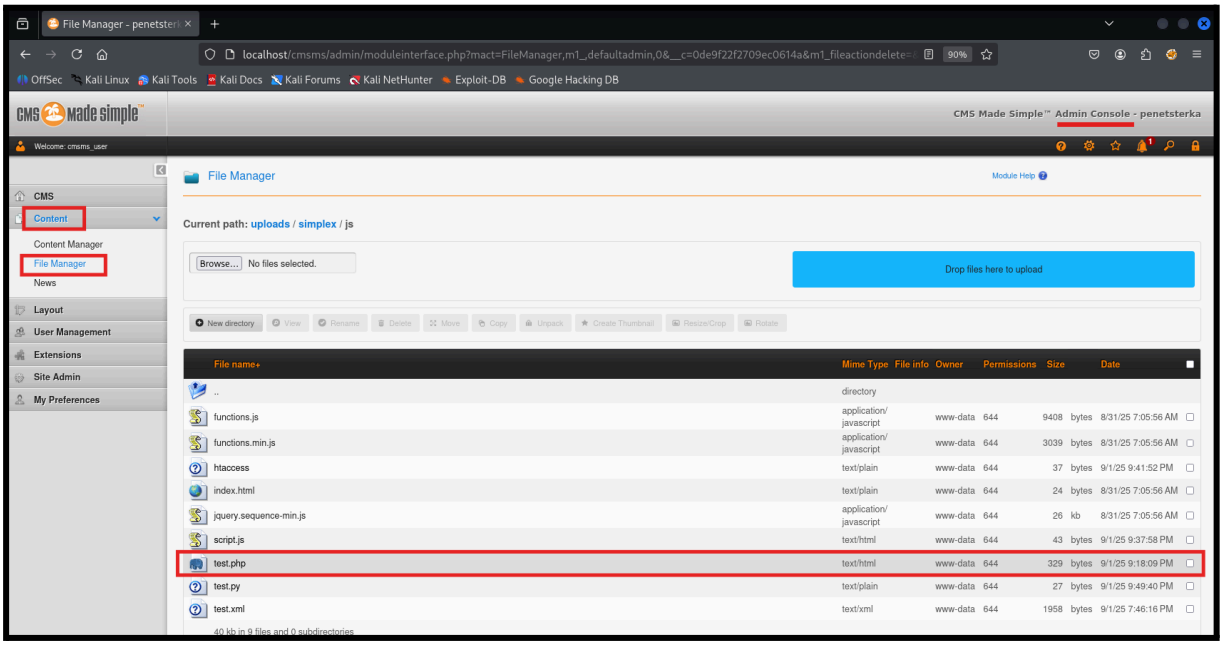
- Valid **administrator account** on CMS Made Simple v2.2.22
- Access to the **Content / File Manager** module
- Ability to upload files to the /uploads/ directory

LOCATION

- Administrator Panel
- Path: **Content → File Manager → uploads/simplex/js/**

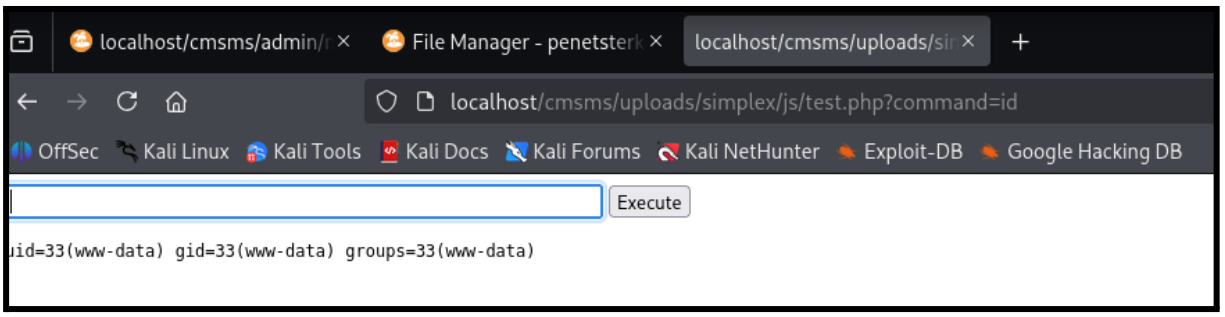
STEPS TO REPRODUCE

1. Log in as an administrator to **CMS Made Simple 2.2.22**
2. Create a shell.php file containing a simple web shell
3. Upload the shell.php file using the **Content / File Manager** upload form



Screenshot 1: *CMS Made Simple 2.2.22 administrator panel – Content → File Manager – upload of* `test.php`

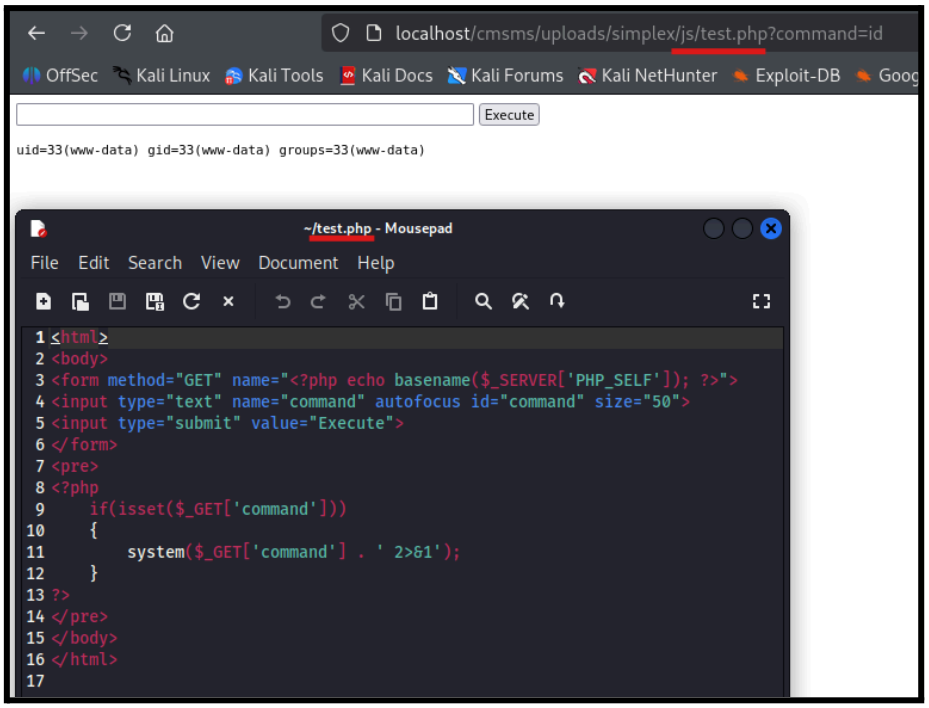
4. In a browser, visit the uploaded shell at:
http://localhost/cmsms/uploads/simplex/js/test.php
5. Execute the id command from the web shell. The output will confirm code execution as the www-data user:
uid=33(www-data) gid=33(www-data) groups=33(www-data)



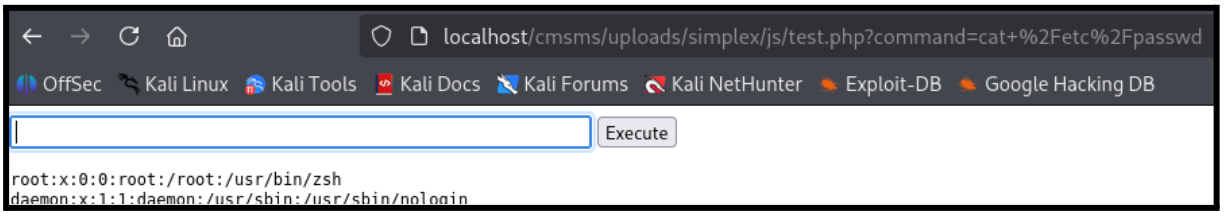
Screenshot 2: *Visiting* `/uploads/simplex/js/test.php?command=id` *returns* `uid=33(www-data) gid=33(www-data)`*, confirming arbitrary code execution on the server.*

PROOF OF CONCEPT

The output from the web shell confirms that it is possible to execute arbitrary system commands (Remote Code Execution — RCE).



Screenshot 3: *Source code of uploaded test.php (simple command execution shell)*



Screenshot 4: *cat /etc/passwd command*

RECOMMENDATIONS

- **Implement strict file type validation** (whitelist only safe file extensions such as .jpg, .png, .pdf)
- **Disable execution of uploaded files** by configuring the web server (e.g. .htaccess) to prevent code execution in /uploads/

Please assign a CVE ID for this issue and credit the discovery to **Kasia Sok**