Remote Code Execution (RCE)

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

SUMMARY

A **Remote Code Execution (RCE)** vulnerability in **CMS Made Simple v2.2.22** allows an authenticated CMS administrator to upload and execute arbitrary PHP files via the **Content / File Manager** module.

Due to the lack of enforced file-type validation and the /uploads/ directory (e.g. /uploads/simplex/js/shell.php) being executable by default, this results in arbitrary code execution as the www-data user.

This vulnerability escalates privileges from content administration to system command execution, which is not an intended capability of the CMS.

Because the code executes as the www-data user (shared by other web applications on the same server), this vulnerability could be used to compromise 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

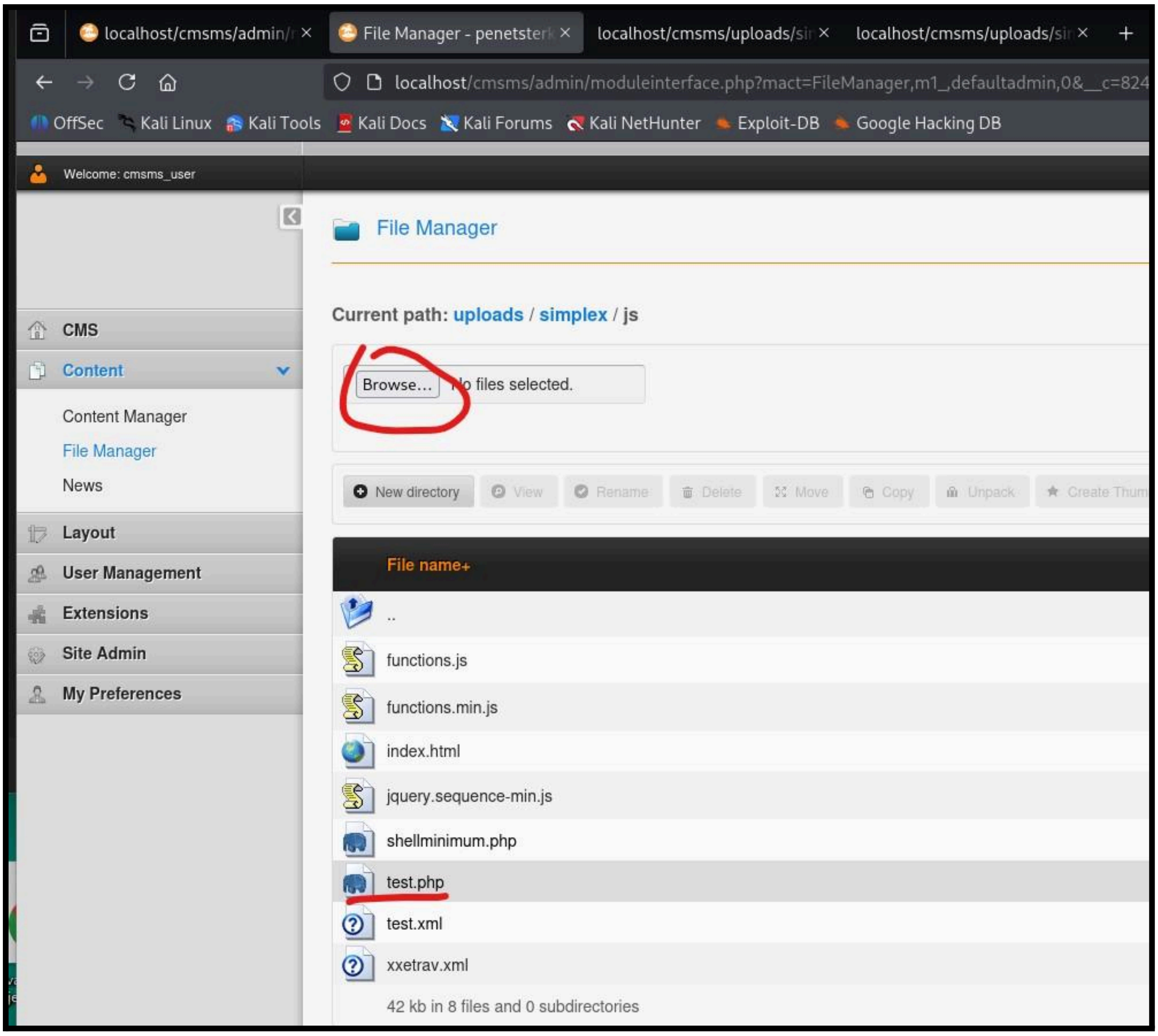
- Administrator Panel
- Path: **Content → File Manager → uploads/simplex/js/**

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



Current path: uploads / simplex / js

No files selected.

File name+

..
functions.js
functions.min.js
index.html
jquery.sequence-min.js
shellminimum.php
test.php
test.xml
xxetrav.xml

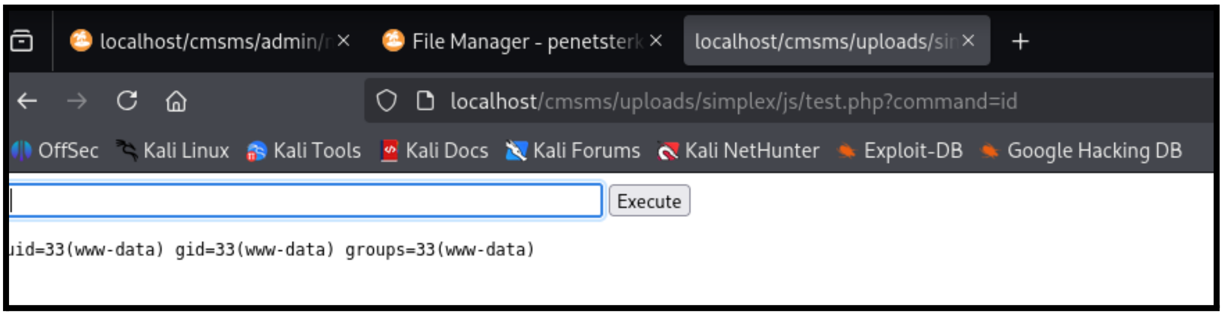
42 kb in 8 files and 0 subdirectories

4. In a browser, visit the uploaded shell at:

http://localhost/cmsms/uploads/simplex/js/shell.php

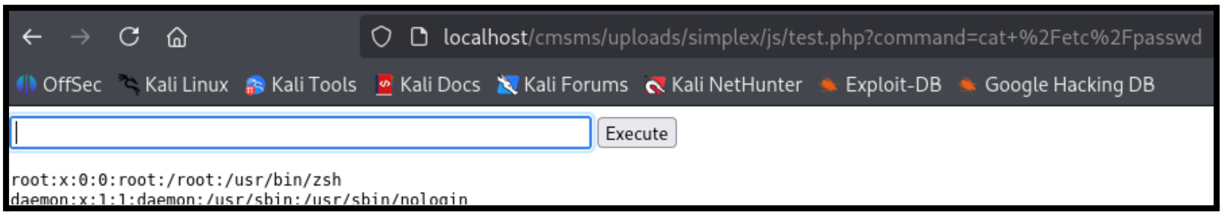
5. Execute the id command from the web shell. The output will confirm code execution as the www-data user:

uid=33(www-data) gid=33(www-data) groups=33(www-data)



```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

6. Execute further system commands (e.g. cat /etc/passwd) to demonstrate full RCE:



```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

PROOF OF CONCEPT

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

RECOMMENDATIONS

To prevent this vulnerability, it is recommended to:

- **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/
- **Separate upload directories from executable directories**

Referer: Kasia Sok