New issue

Jump to bottom

A file upload vulnerability exists in the background #1

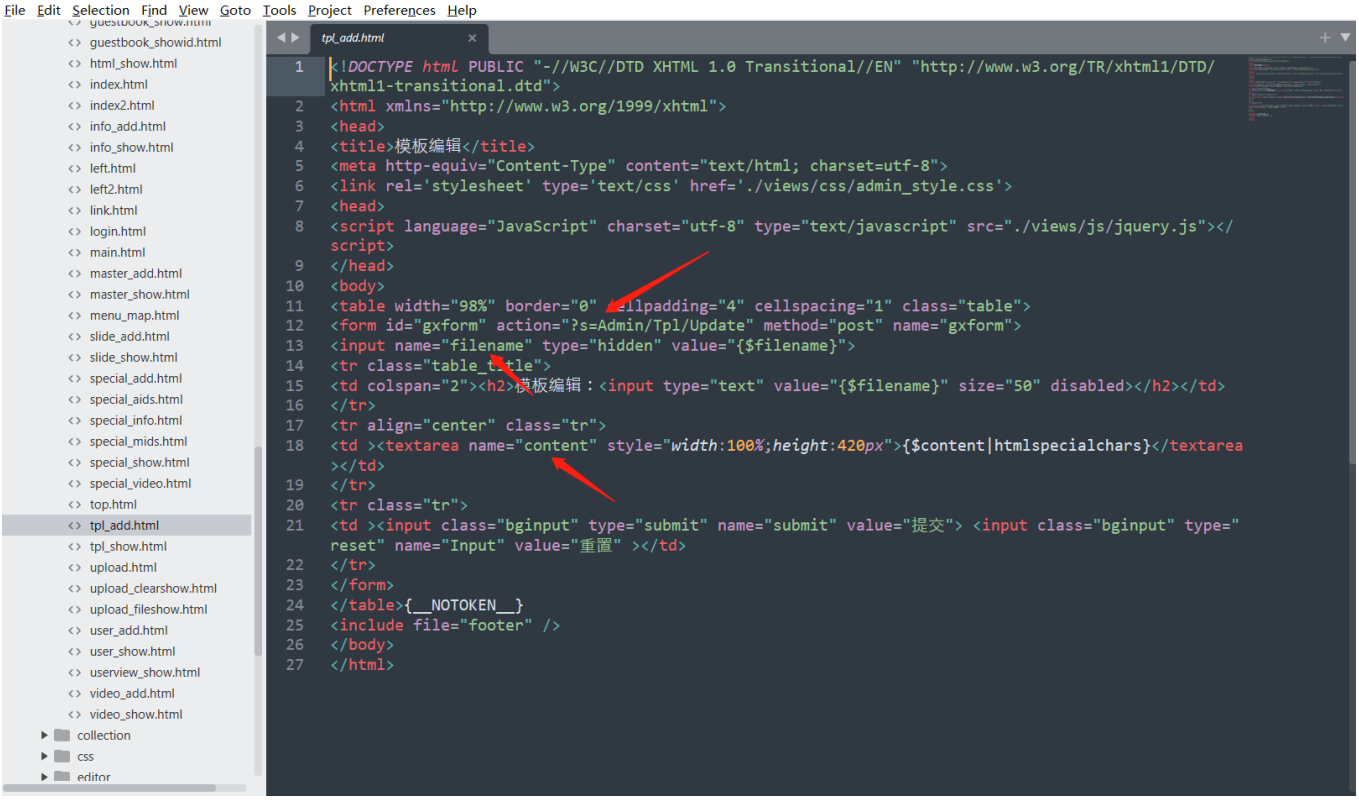
Open **Zack-Huang** opened this issue on Apr 25 · 1 comment

Zack-Huang commented on Apr 25

1、Vulnerability code Audit

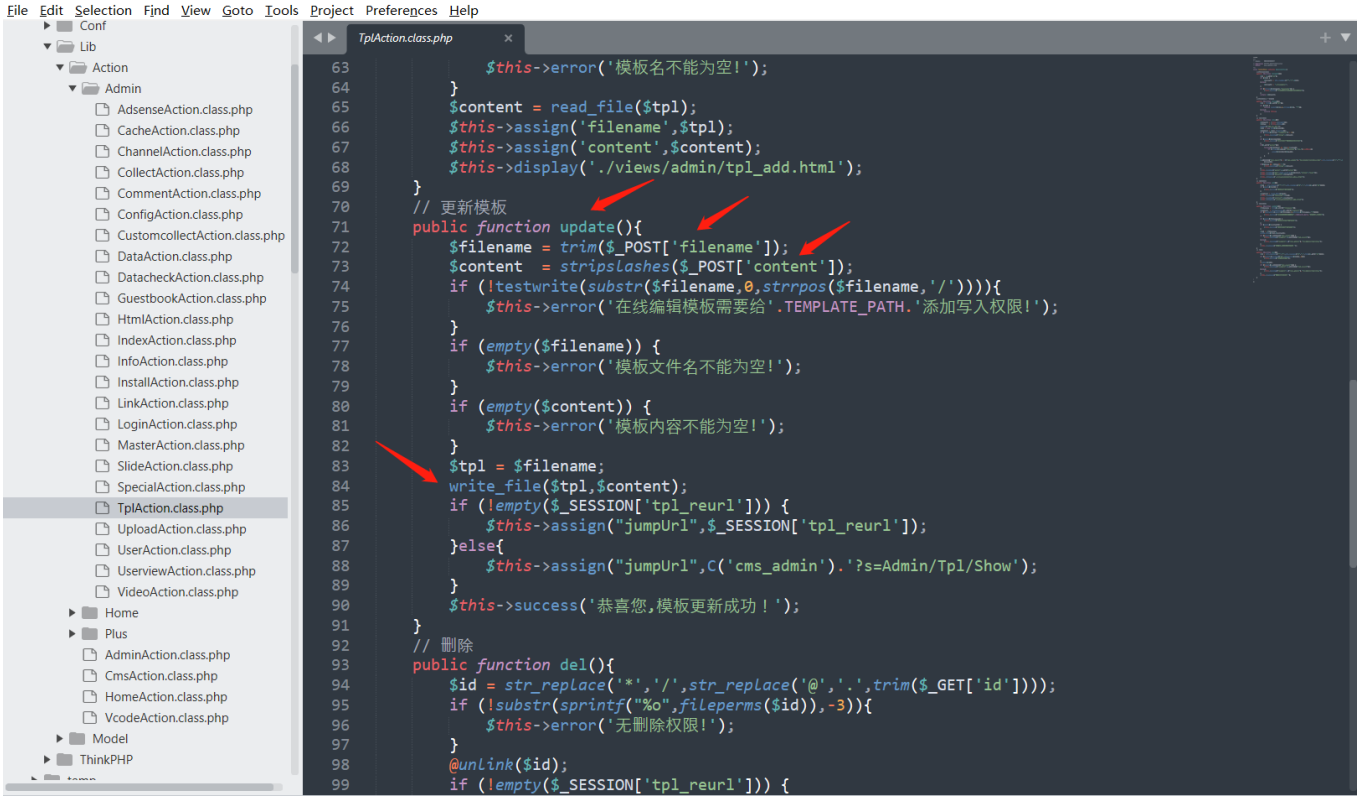
The vulnerability appears in the template management page in the background:

/views/admin/tpl_add. HTML file is received by filename, content is received by content, and then the data is sent to? S =Admin/Tpl/Update



Track? S = Admin/Tpl/Update page source/core/Lib/Action/Admin/TplAction class. PHP file, see the Update function to receive the filename and the content variables, only after receiving the two variables for judging whether it is empty, Data is written to the file directly using the write_file function without dangerous

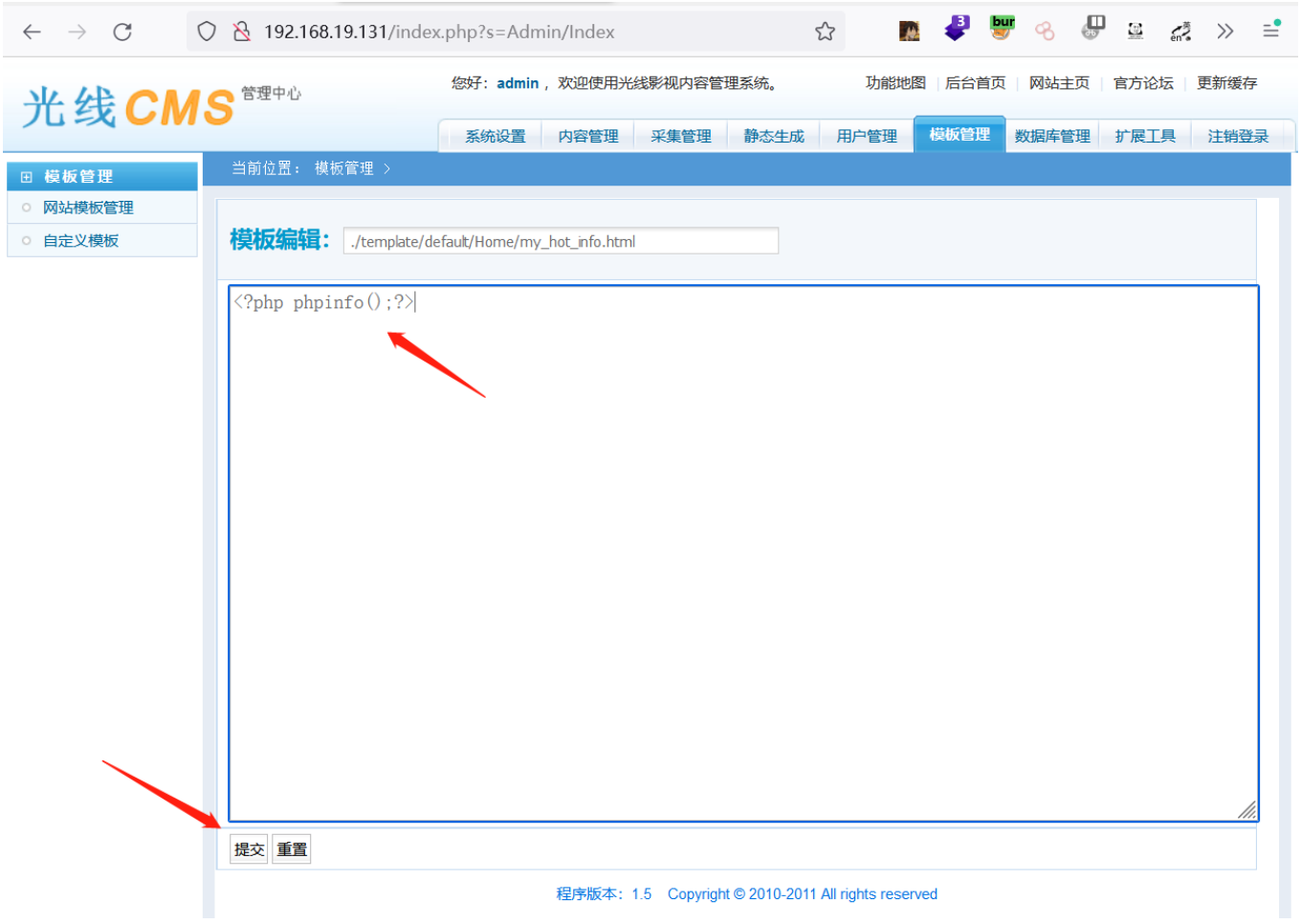
character detection for file names and contents, which means there is any file upload vulnerability.



2、The exploit

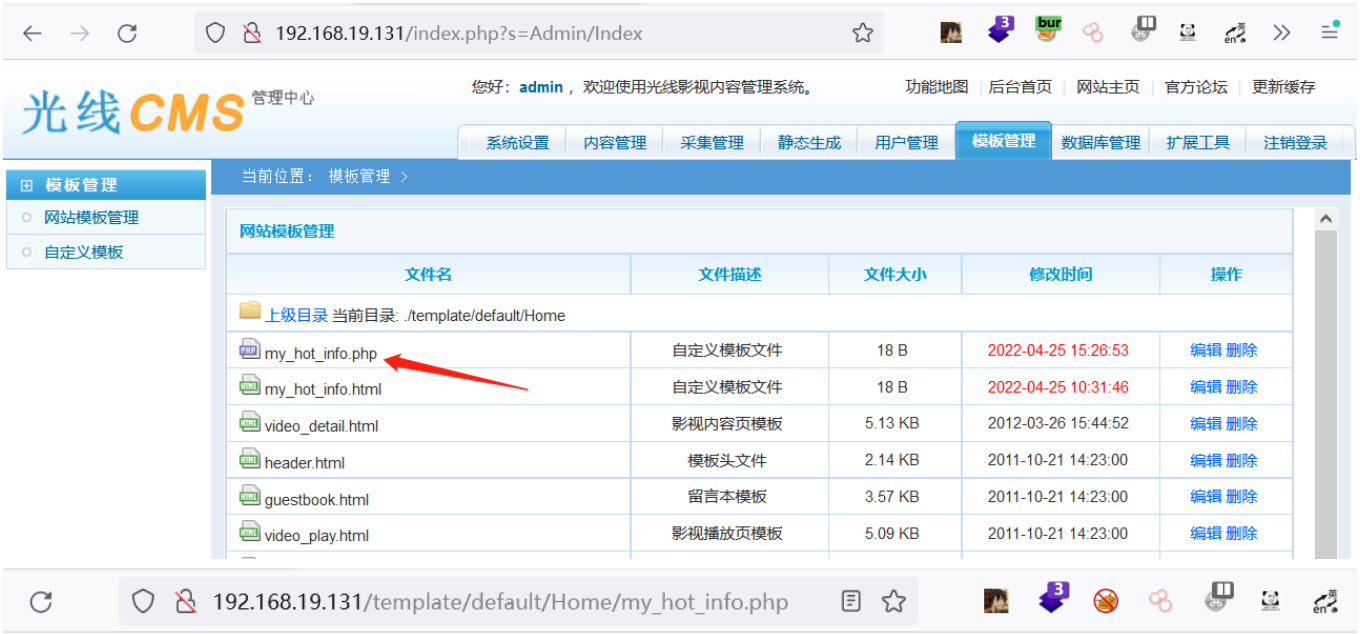
Log in to the background of the target website by admin default password admin888 or password blasting or even phishing, click Template Management to enter the /template/default/Home directory, select any file and click Edit:

Enter the EDIT page, enter the PHP test code in the file content form, start the BurpSuite tool to capture packages, and click Submit:



After BurpSuite catches the package, change the filename suffix to PHP and click "Put the package" :

My_hot_info.php file was created successfully, and the PHP test code was successfully executed.



Zack-Huang commented on May 17 — Author

This vulnerability has been fixed in the new version, please visit the link to download the latest version of V1.7: http://www.gxcms.org/

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant