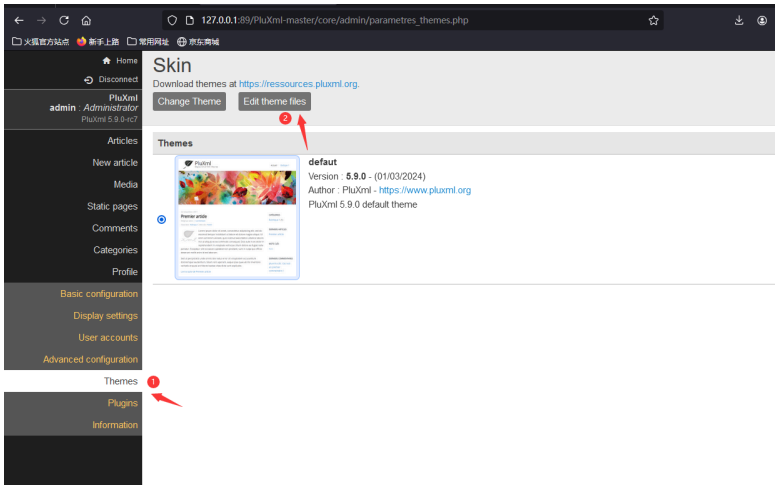
In PluXml v5.8.16 or lower, after logging in to the backend, there are any file modifications that can cause a Trojan to be written, causing RCE and posing a great threat to the server. #829

New issue

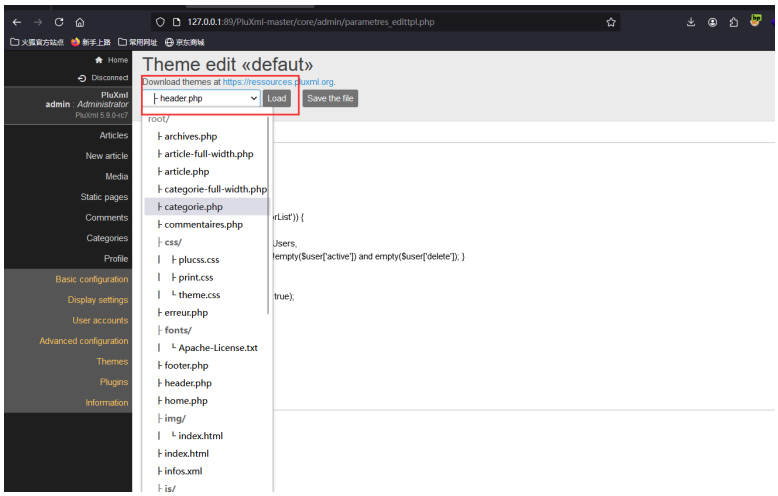
Open **4everwl** opened this issue on Sep 12 · 4 comments

4everwl commented on Sep 12

Software Link :https://github.com/pluxml/PluXml
Website : https://pluxml.org/After
the installation is complete, log in as admin, open the page



Here you can modify the theme code in the theme folder.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

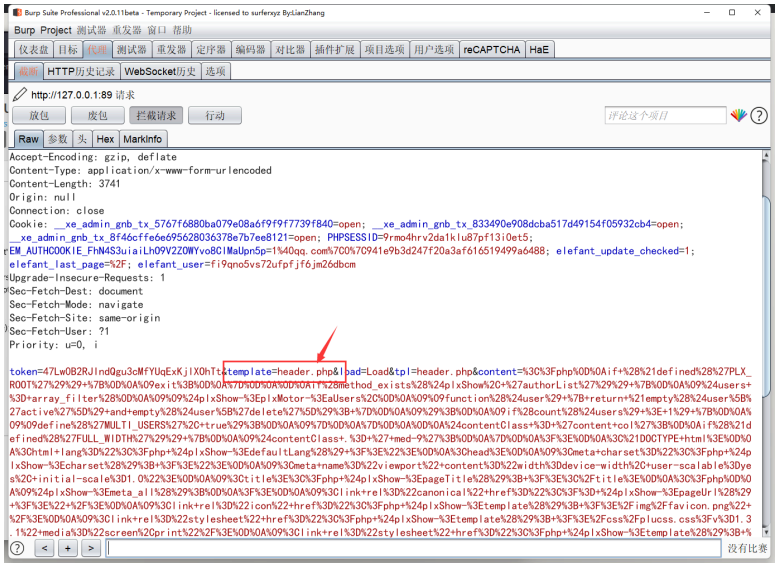
No milestone

Development

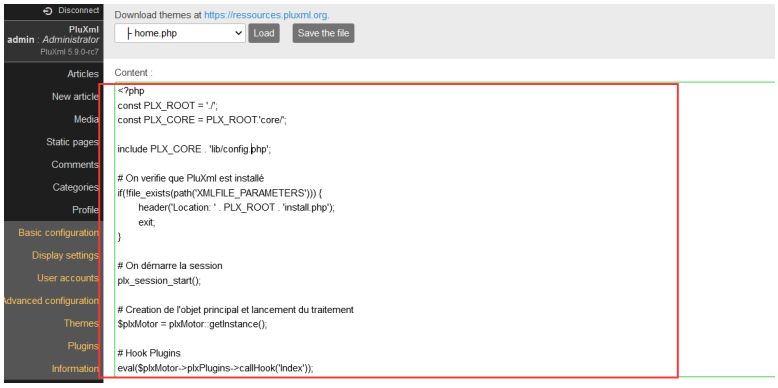
No branches or pull requests

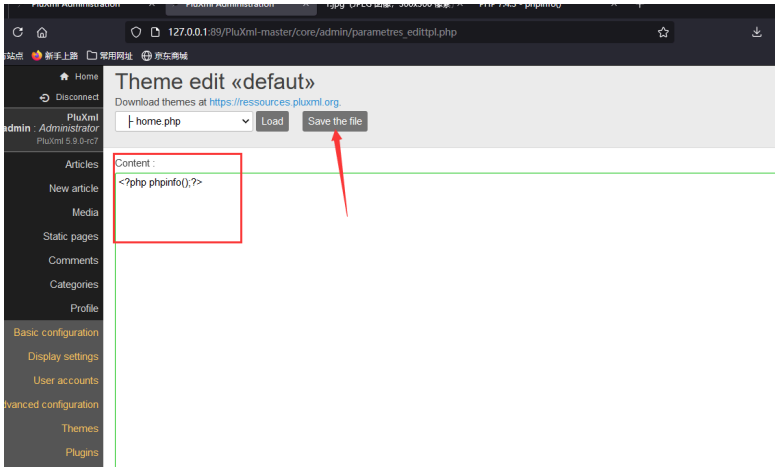
2 participants

Request packet capture, try to modify the parameter template to: ../../index.php

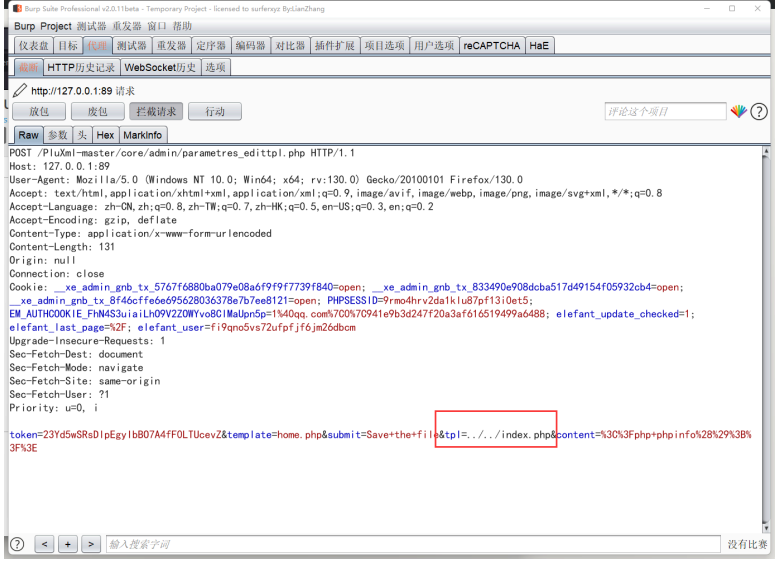


What is returned at this time is the content of index.php. We try to modify the file content.

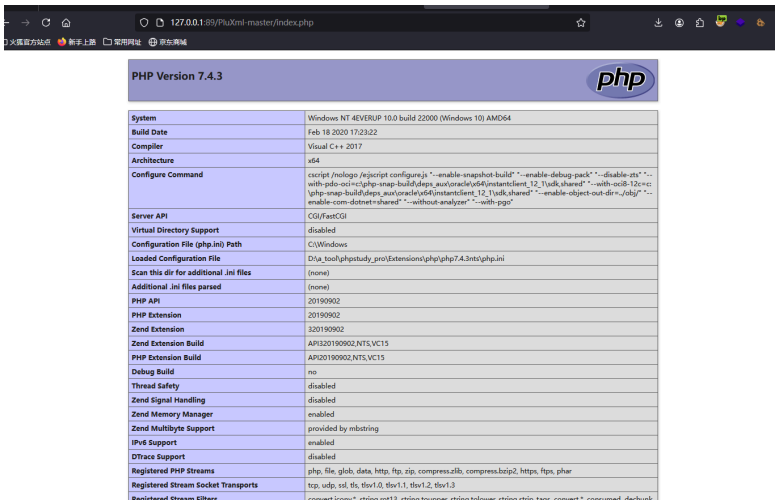




Request packet capture and change the parameter tpl to: ../../index.php

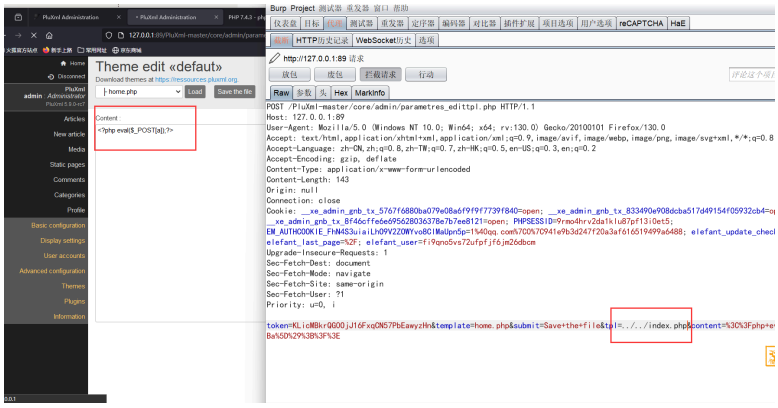


Successful echo.

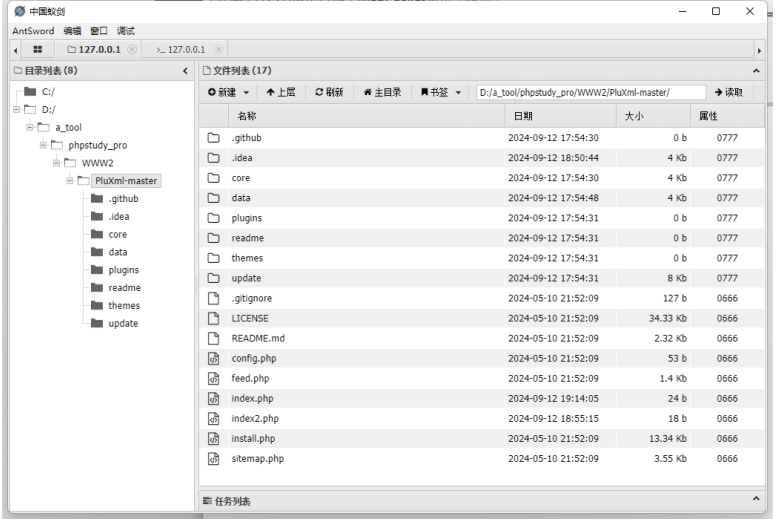


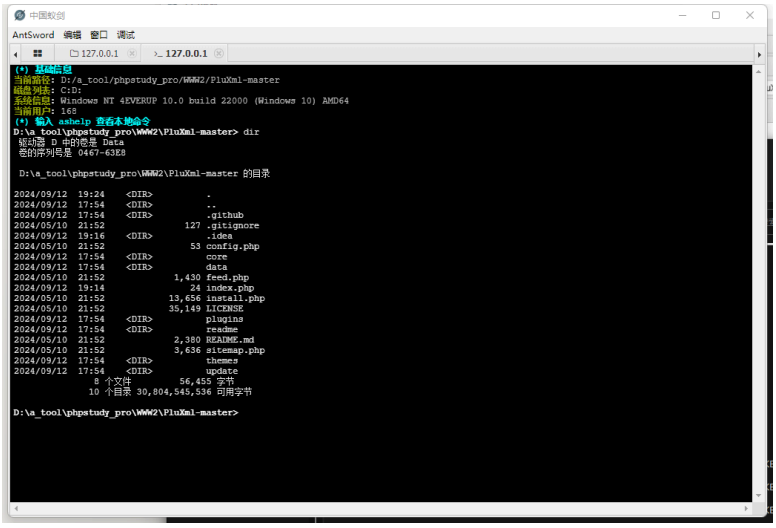
System	Windows NT 4EVERUP 10.0 build 22000 (Windows 10) AMD64
Build Date	Feb 18 2020 17:23:22
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\a_tool\phpstudy_pro\Extensions\php\php7.4.3nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS,VC15
PHP Extension Build	API20190902,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3

Write Trojan.

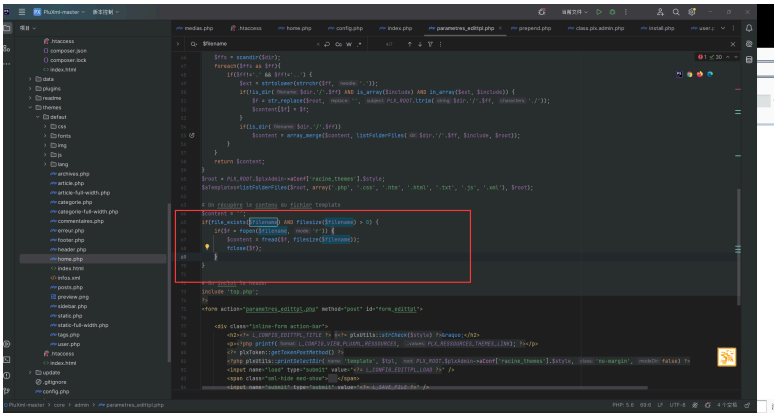


get shell.





The cause of this vulnerability is that $filename is not strictly judged in the project's core/admin/parametres_edittpl.php, which allows users to splice paths to read and modify arbitrary files.



gcyrillus commented 2 weeks ago • edited

Contributor

That is not a trouble, why would an administrator load a trojan in its own site ? Are you of that kind yourself ?
If we follow your way of thinking, the whole administration itself is dangerous, *hey, i can add a new article and even configure the CMS as I wish !*

4everwl commented 2 weeks ago — Author

What I mean is that after logging in, the attacker obtains the login backend of the website and can use social workers or weak passwords to take down the website shell

gcyrillus commented 2 weeks ago — Contributor

okay, i understand but this is not specific to PluXml and why the administrator would do such a thing? If the issue is about a weak password, again this is not PluXml, but the USER. Or like i like to say, *that weird thing standing in betwwen the chair and the keyboard* ;)
There is a plugin that can make it harder to login, even with a weak password :
https://kazimentou.fr/repo/index.php?plugin=kzOtPHP&download
But however , if both datas are stolen, or lost then found, there is nothing to be done to avoid someone else to log in. It can actually happen to any digital account one has. If i'm wrong or missed something, do not hesitate to tell me and forget my misunderstanding :)

4everwl commented 2 weeks ago — Author

OK, I understand. I think this Theme edit function should only be able to edit Theme files, not be able to modify other files across levels.