New issue

Jump to bottom

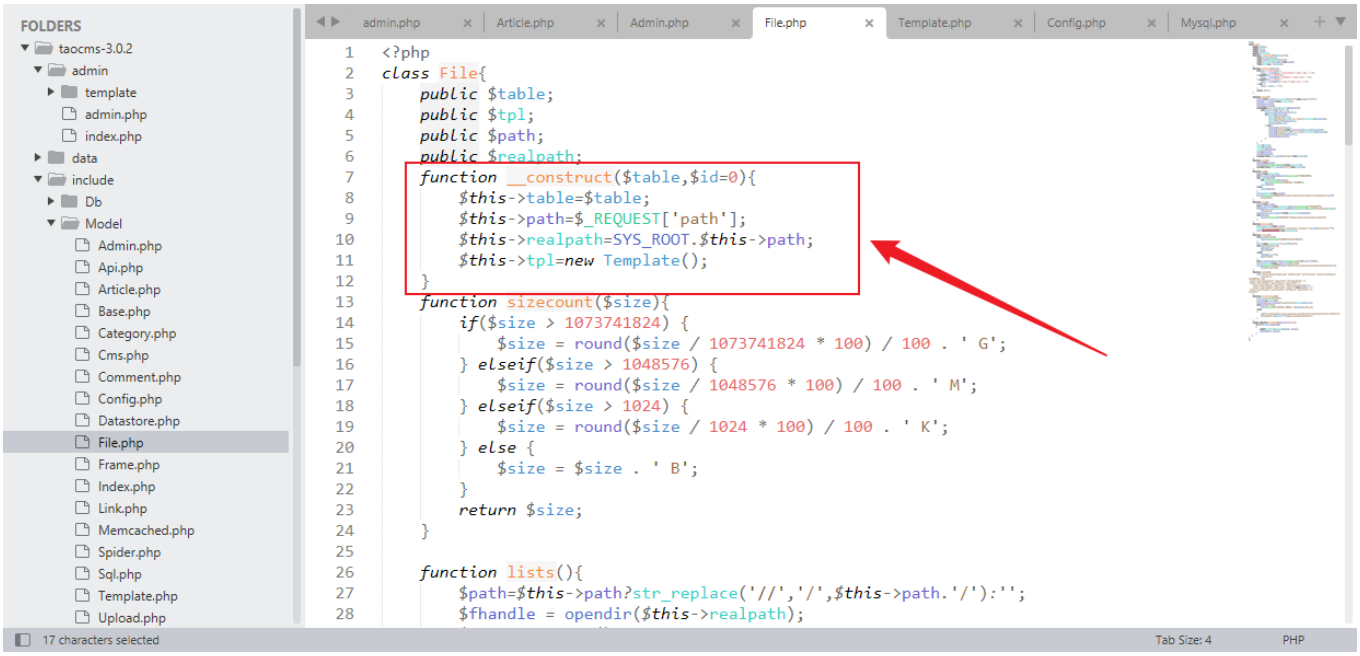
arbitrary file read vulnerability #15

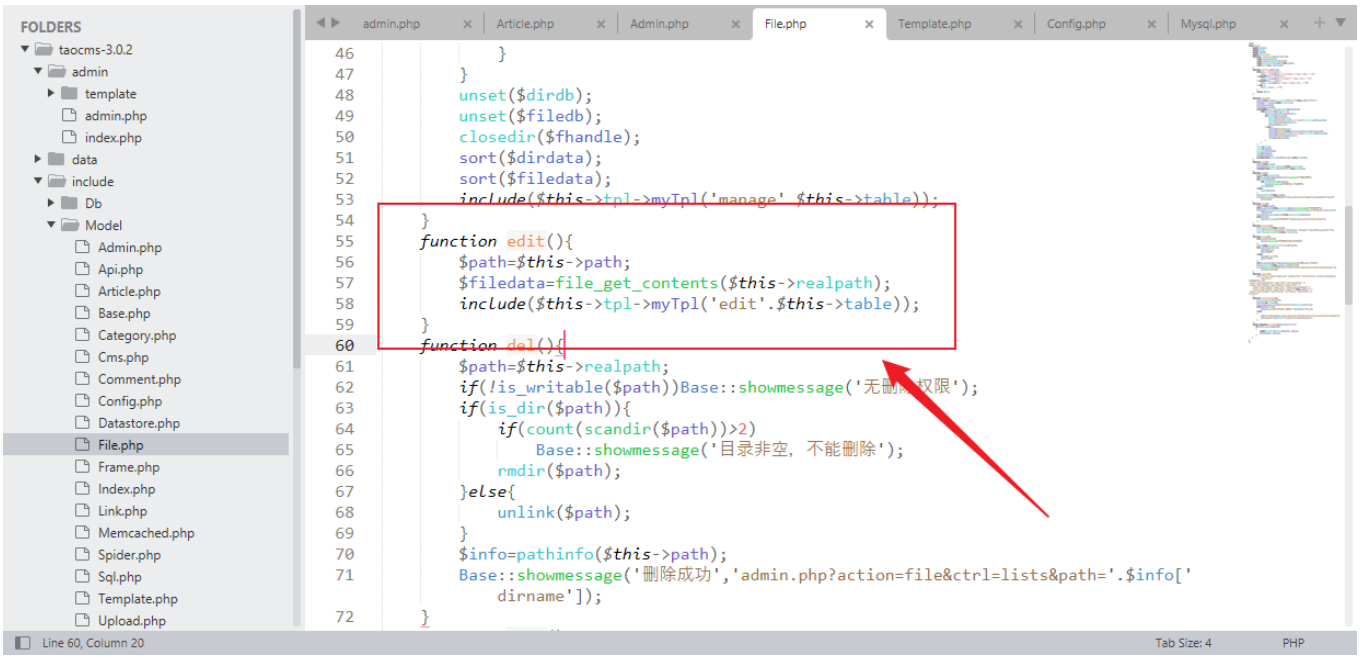
Open **destinypwd** opened this issue on Jan 10 · 0 comments

destinypwd commented on Jan 10

analysis

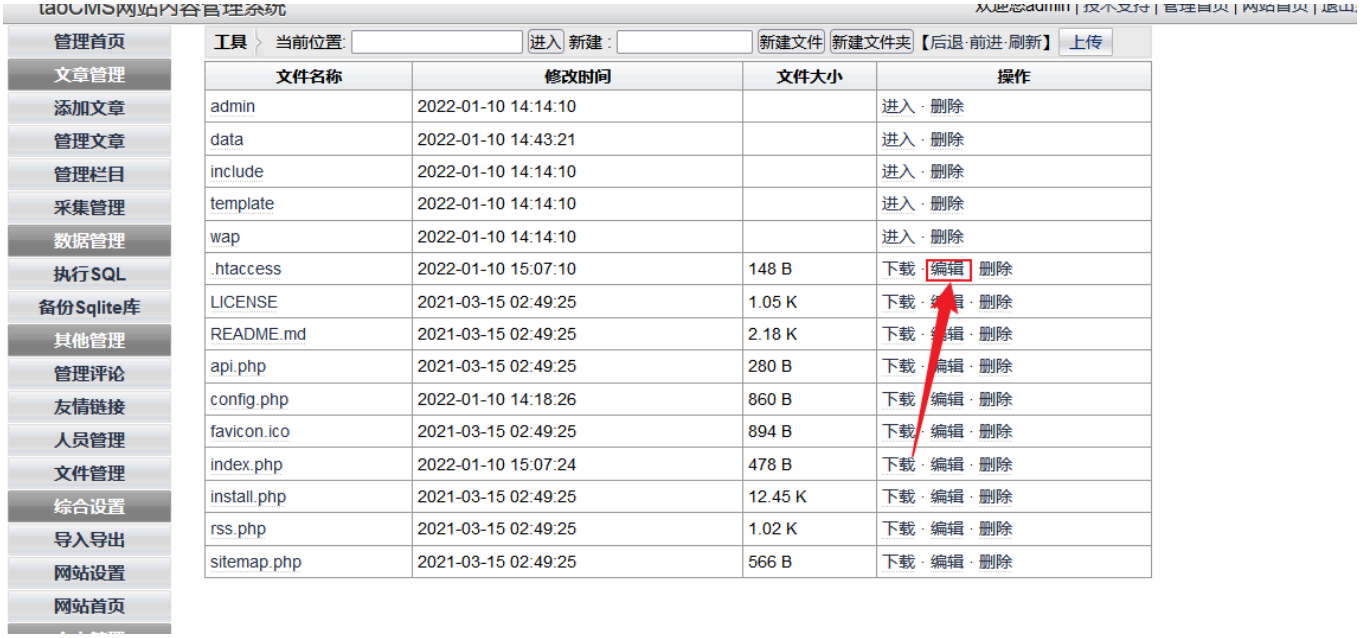
The location of the vulnerability is line 55 in \taocms\include\Model\File.php and we can see that the path parameter is passed directly to file_get_contents function without filtering



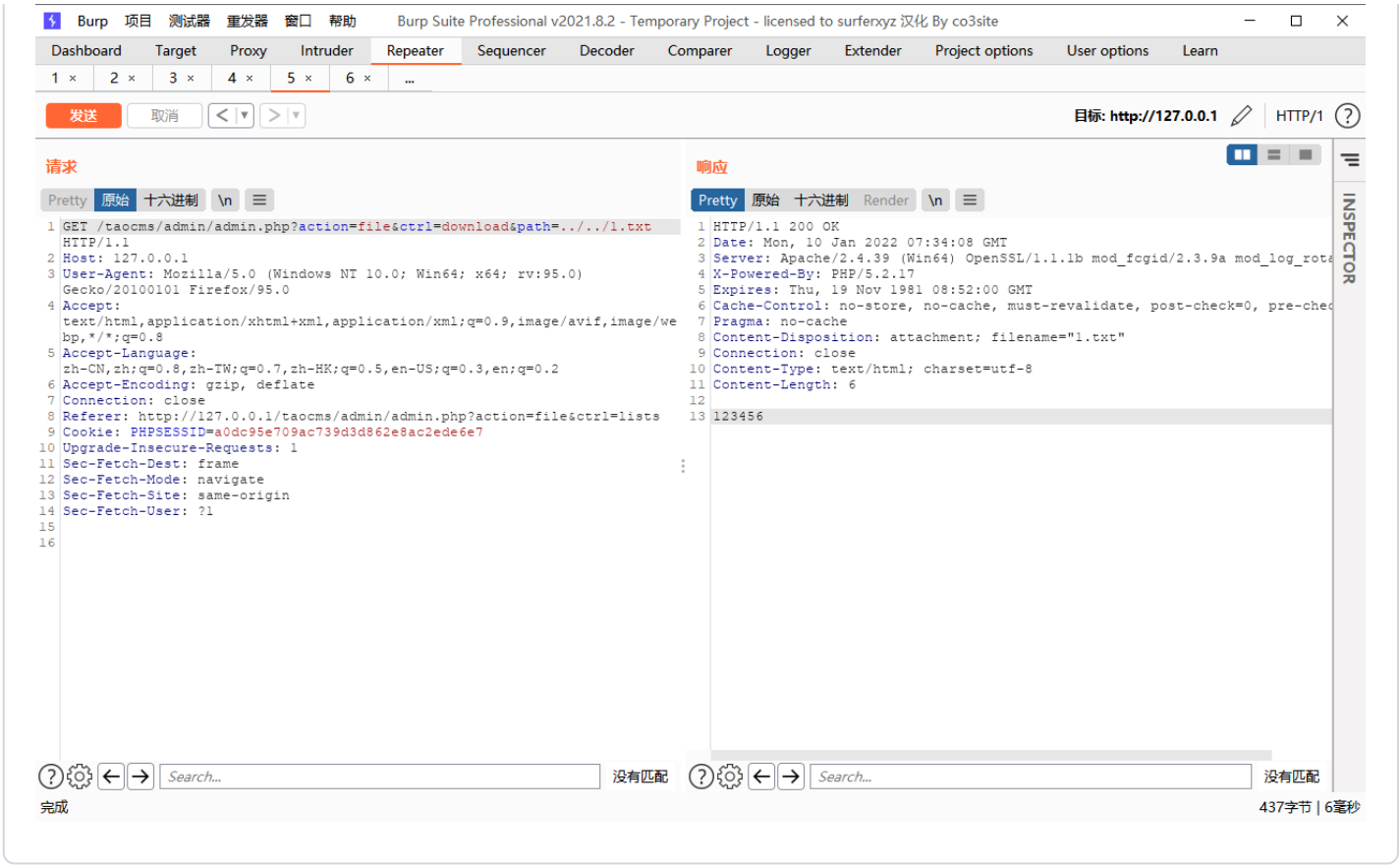


poc

After login as admin,Enter the file management interface and edit function



Get packets using brup
Any file can be read after changing the path parameter



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant