

[New issue](#)
[Jump to bottom](#)

/!\Security #114

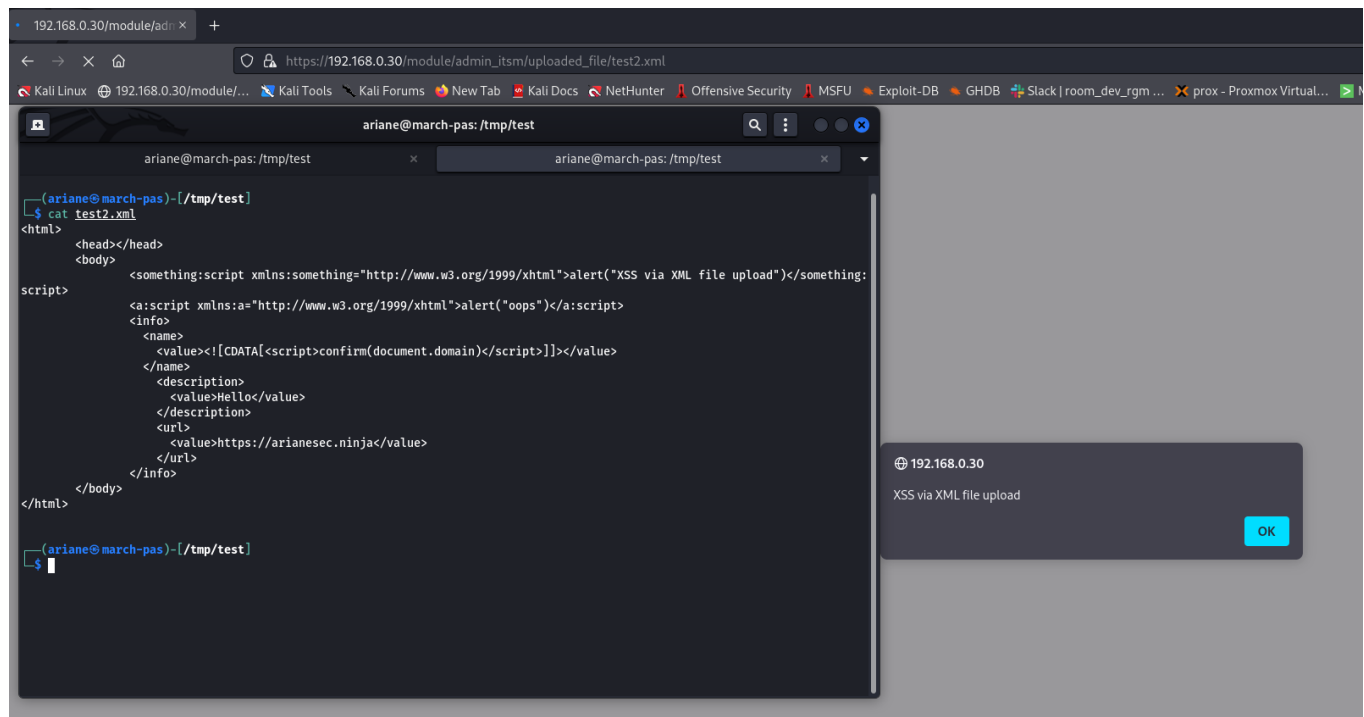
Open ArianeBlow opened this issue on Feb 2 · 2 comments

ArianeBlow commented on Feb 2

Hello,

Il y a un petit soucis dans le contrôle des fichiers uploadés via le file upload du module ITSM.

La possibilité d'uploader du format XML devrait se suivre d'un contrôle du dit fichier, en l'état il est possible d'uploader (via un user authentifié), un document XML contenant une XSS ou d'autres joyeusetées malicieuses.



ArianeBlow commented on Feb 3

Author

Dasn mon infini sagesse, je vous ait envoyé un mail avec "le reste". (PS: je n'ai pas essayé de fair du RCE via le file upload de XML, à savoir que c'est en thérorie possible via appel d'entité extern).

ArianeBlow commented on Mar 1

Author

Une CVE a été enregistrée pour cette XSS : <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24612>

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

