looCiprian Added CVE-2022-28479, CVE-2022-28478, CVE-2022-28051 ... on Apr 28 History

..

Images	7 months ago
README.md	7 months ago

README.md

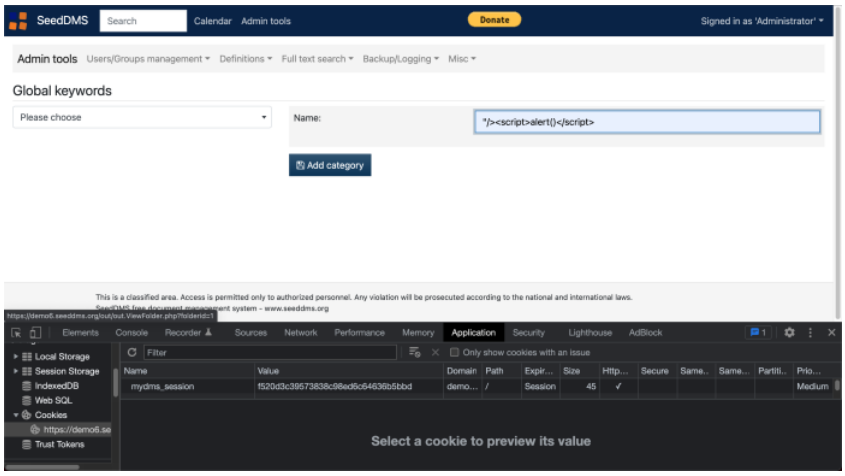
CVE

Description

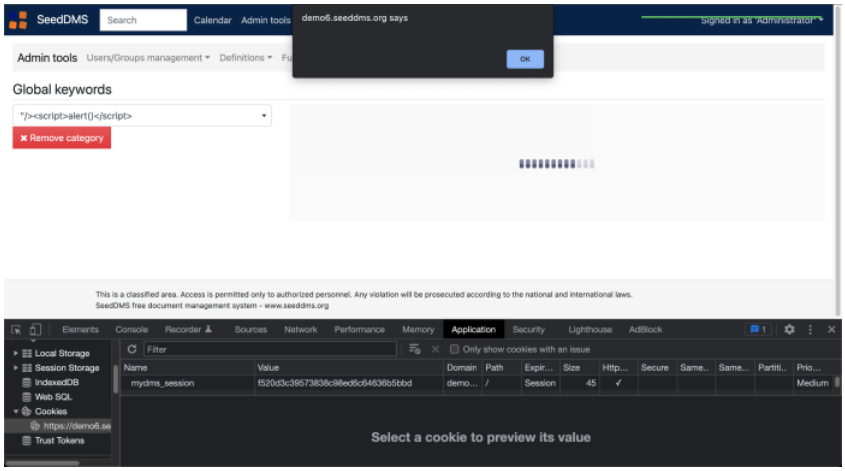
SeedDMS versions 6.0.18 and 5.1.25 are prone to stored XSS. The "Add category" functionality inside the "Global keywords" menu does not sanitize user input allowing javascript injection.

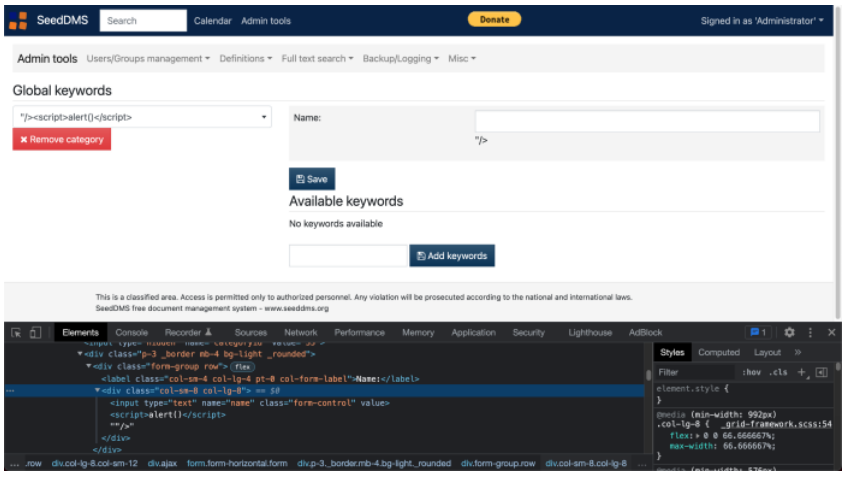
POC

Injecting the payload



By pressing the "Add category" button the malicious payload is saved and triggered by the application





Remediation

Escape user input by using "htmlspecialchars" php function

Reference

https://sourceforge.net/p/seeddms/code/ci/6fc17be5d95e8f00fbe5c124c4acd377fa2ce69d/

Timeline

- [22/03/2022] Vulnerability evidence sent to the vendor
- [23/03/2022] Vulnerability confirmed by the vendor
- [23/03/2022] Vulnerability fixed by the vendor

Notes

Thanks to the main developer of SeedDMS, Uwe Steinmann, that immediately acknowledged the vulnerability and fixed it.