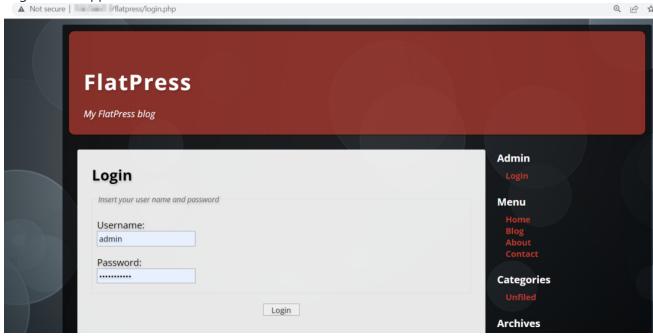
| <> Code | ○ Issues 61 | ?1 Pull requests | Actions | Projects | ₩iki | |
|--|--|---|--|---|---|---------|
| New issue | | | | | J | lump to |
| Flatpr | ess- 1.2.1 | - Reflected 2 | XSS on pa | age para | meter #1 | 53 |
| Open | | ened this issue on Sep | - | | | |
| _abels | security | | | | | |
| s4n-h4x | or commented on | n Sep 27 • edited ▼ | | | | |
| Severity | • | | | | | |
| - | • | | | | | |
| Medium | | | | | | |
| Medium Descript | | | | | | |
| Descript Cross-si | t ion : te scripting (XSS) v | vulnerabilities arise who | | | | |
| Descript Cross-sit victim's | t ion : te scripting (XSS) v browser, mostly u | sing JavaScript. A vulne | erable web appli | cation might em | bed untrusted | |
| Descript Cross-sir victim's data in t | ti on : te scripting (XSS) v browser, mostly us he output, withou | | erable web applionit. In this way, ar | cation might em attacker can inj | bed untrusted ect a malicious | e |
| Descript Cross-sir victim's data in t script in victim's | tion: te scripting (XSS) ventors to the seripting the seripting the seription withous to the application, browser. | sing JavaScript. A vulne t filtering or encoding and the script will be i | erable web applion it. In this way, ar returned in the re | cation might em attacker can inj esponse. This wil | bed untrusted ect a malicious Il then run on the | |
| Descript Cross-sir victim's data in t script in victim's | tion: te scripting (XSS) ventors to the seripting the seripting the seription withous to the application, browser. | sing JavaScript. A vulne t filtering or encoding | erable web applion it. In this way, ar returned in the re | cation might em attacker can inj esponse. This wil | bed untrusted ect a malicious Il then run on the | |
| Descript Cross-sirvictim's data in t script invictim's lt is obse attacks. | tion: te scripting (XSS) ventors to the seripting the seripting the seription withous to the application, browser. | sing JavaScript. A vulne t filtering or encoding and the script will be i | erable web applion it. In this way, ar returned in the re | cation might em attacker can inj esponse. This wil | bed untrusted ect a malicious Il then run on the | |
| Descript Cross-sir victim's data in t script in victim's It is obse attacks. Technica It is poss | tion: te scripting (XSS) vectors browser, mostly use the output, withou to the application, browser. browser that the page al Impact: sible to steal or mage | sing JavaScript. A vulne t filtering or encoding and the script will be a ge parameter does not anipulate customer ses | erable web applicit. In this way, and returned in the resamilize input prossions and cookies | cation might em attacker can inj esponse. This wil operly which lea es, which might b | bed untrusted ect a malicious Il then run on the ds to reflected X | |
| Descript Cross-sir victim's data in t script in victim's It is obse attacks. Technica It is poss | tion: te scripting (XSS) vectors browser, mostly use the output, withou to the application, browser. browser that the page al Impact: sible to steal or mage | sing JavaScript. A vulne t filtering or encoding and the script will be i se parameter does not | erable web applicit. In this way, and returned in the resamilize input prossions and cookies | cation might em attacker can inj esponse. This wil operly which lea es, which might b | bed untrusted ect a malicious Il then run on the ds to reflected X | |
| Descript Cross-sir victim's data in t script in victim's It is obse attacks. Technica It is poss imperso | tion: te scripting (XSS) vectors browser, mostly use the output, withou to the application, browser. browser that the page al Impact: sible to steal or mage | sing JavaScript. A vulne t filtering or encoding and the script will be a ge parameter does not anipulate customer ses | erable web applicit. In this way, and returned in the resamilize input prossions and cookies | cation might em attacker can inj esponse. This wil operly which lea es, which might b | bed untrusted ect a malicious Il then run on the ds to reflected X | |
| Descript Cross-sir victim's data in t script in victim's It is obse attacks. Technica It is poss imperso | tion: te scripting (XSS) vectors browser, mostly use the output, withou to the application, browser. erved that the page al Impact: sible to steal or manate a legitimate use the Remediation: | sing JavaScript. A vulne t filtering or encoding and the script will be a ge parameter does not anipulate customer ses | erable web applicit. In this way, and returned in the resamilize input prossions and cookies | cation might em attacker can inj esponse. This wil operly which lea es, which might b | bed untrusted ect a malicious Il then run on the ds to reflected X | |
| Descript Cross-sir victim's data in t script in victim's It is obse attacks. Technica It is poss imperso Suggest 1. App | tion: te scripting (XSS) vectors browser, mostly use the output, without to the application, browser. Berved that the page al Impact: Sible to steal or manate a legitimate used Remediation: | sing JavaScript. A vulne t filtering or encoding and the script will be a se parameter does not anipulate customer ses user, allowing the hack | erable web applicit. In this way, and returned in the research sanitize input pressions and cookies er to view or alternative. | cation might em attacker can inj esponse. This wil operly which lea es, which might b | bed untrusted ect a malicious Il then run on the ds to reflected X | |

1. Login to the application

2zr4da



2. Entre the below payload in the URL and observe XSS payload getting executed. Payload:

http://server/flatpress/admin.php? p=static&action=write&page=%22onfocus%3d%22alert%28document.cookie%29%22autofocus%3d%2



Opening issue here, Got no reply from [hello@flatpress.org] for 2 months

azett commented on Oct 2

Confirmed. Sorry for being late!



| Assignees |
|------------------------------|
| No one assigned |
| |
| Labels |
| security |
| Projects |
| |
| None yet |
| Milestone |
| No milestone |
| Development |
| No branches or pull requests |
| 2 participants |



