flatpressblog / **flatpress** Public

Code   Issues 61   Pull requests   Actions   Projects   Wiki   ...

New issue   Jump to bottom

Flatpress- 1.2.1 - Reflected XSS on page parameter #153

Open **s4n-h4xor** opened this issue on Sep 27 · 1 comment

Labels   security

s4n-h4xor commented on Sep 27 • edited

Severity:
Medium

Description:
Cross-site scripting (XSS) vulnerabilities arise when an attacker sends malicious code to the victim's browser, mostly using JavaScript. A vulnerable web application might embed untrusted data in the output, without filtering or encoding it. In this way, an attacker can inject a malicious script into the application, and the script will be returned in the response. This will then run on the victim's browser.
It is observed that the page parameter does not sanitize input properly which leads to reflected XSS attacks.

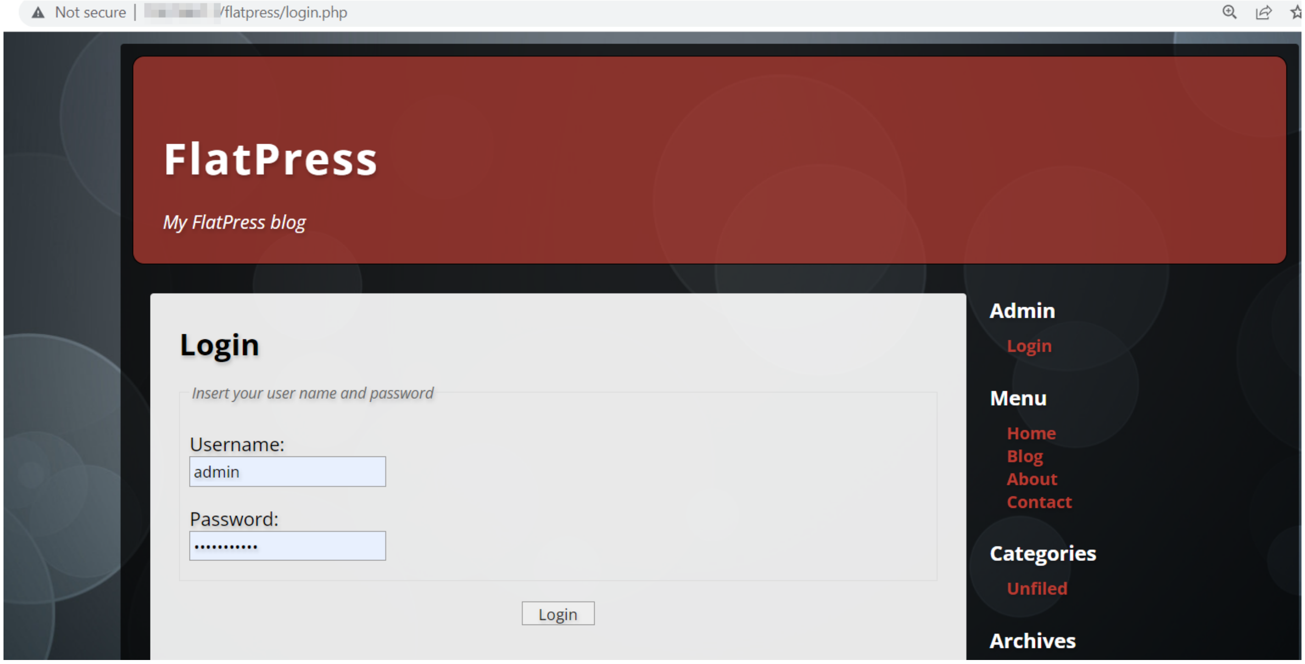
Technical Impact:
It is possible to steal or manipulate customer sessions and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter the blog.

Suggested Remediation:

1. Application should encode data on output.
2. Application should filter input on page parameters.

Steps to Reproduce:

1. Login to the application



Not secure | [redacted]/flatpress/login.php

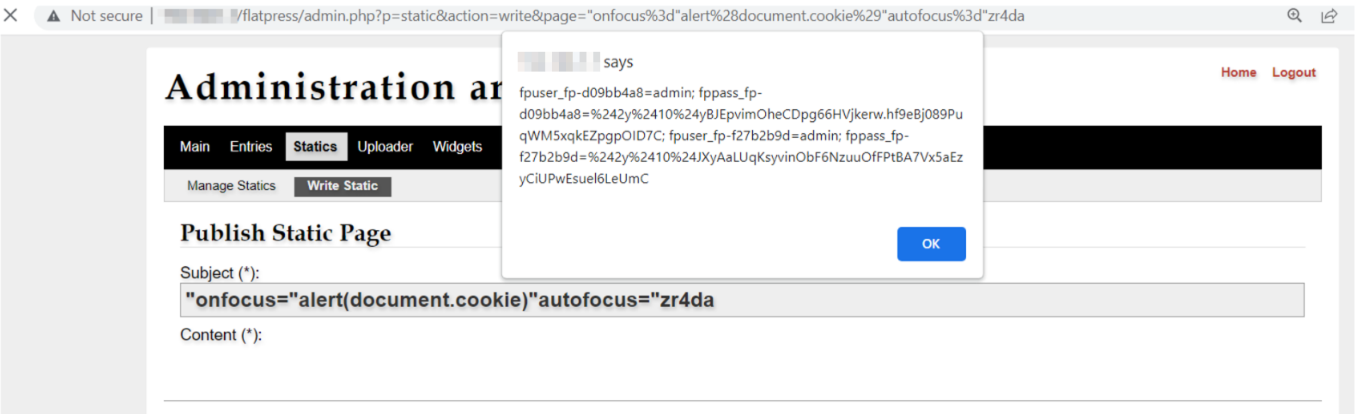
Login

Insert your user name and password

Username: admin

Password: ············

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%22zr4da



Not secure | [redacted]/flatpress/admin.php?p=static&action=write&page="onfocus%3d"alert%28document.cookie%29"autofocus%3d"zr4da

[redacted] says

```
fpuser_fp-d09bb4a8=admin; fppass_fp-d09bb4a8=%242y%2410%24yBJEpvimOheCDpg66HVjkerw.hf9eBj089PuqWM5xqkEZpgpOID7C; fpuser_fp-f27b2b9d=admin; fppass_fp-f27b2b9d=%242y%2410%24JXyAaLUqKsyvinObF6NzuuOfFPtBA7Vx5aEzyCiUPwEsuel6LeUmC
```

Publish Static Page

Subject (*): "onfocus="alert(document.cookie)"autofocus="zr4da

Content (*):

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

azett commented on Oct 2 Member

Confirmed. Sorry for being late!

azett added the security label on Oct 2

Assignees

No one assigned

Labels

security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants