New issue

Jump to bottom

Stored XSS in "Title" field #3255

Open **xoffense** opened this issue on Mar 3, 2021 · 1 comment

Labels 01 type: bug 13 prio: normal 21 status: confirmed

xoffense commented on Mar 3, 2021 • edited

Hi Team,

Description: Stored XSS, also known as persistent XSS, is more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.

Vulnerable Parameter: form.widgets.site_title

Affected version: 5.2.3

XSS payload: <ScRiPt>alert(1)</ScRiPt>

Steps to reproduce the issue:
1- Goto https://localhost/ where Plone 5.2.3 version is installed.
2- Click on "Log in now" and Login as "Manager"
3- Navigate to Manager=>Site Setup=>Site
4- Edit "Site title" field to "xyz<ScRiPt>alert(1)</ScRiPt>"

Video POC: https://drive.google.com/file/d/1J6ZFYmM9dpl2aPQP43fRIqe9N-uR4BIe/view?usp=sharing

Impact:
XSS can use to steal cookies, password or to run arbitrary code on a victim's browser

Reference:
https://hackerone.com/reports/485748
https://hackerone.com/reports/484434
https://hackerone.com/reports/643908

Regards,
Piyush Patil

mauritsvanrees added 01 type: bug 13 prio: normal 21 status: confirmed labels on Mar 3, 2021

mauritsvanrees commented on Mar 3, 2021 Member

Thanks.
For clarity for others reading this: Piyush first reported this to the Plone Security Team. We concluded it was not a vulnerability, because this is done by a Manager, and Managers can use the Web statistics field on the same form to include Javascript, which is what that field is intended for. So we advised Piyush to create a public issue.

Apparently you can also put Javascript in the site title field. This field is definitely *not* intended for that. It would be good if we either prevent storing this, or do not show it in places where the title is shown. (Likely we currently have a `tal:content="structure title"` in a template.)

Assignees
No one assigned

Labels
01 type: bug 13 prio: normal 21 status: confirmed

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants