New issue

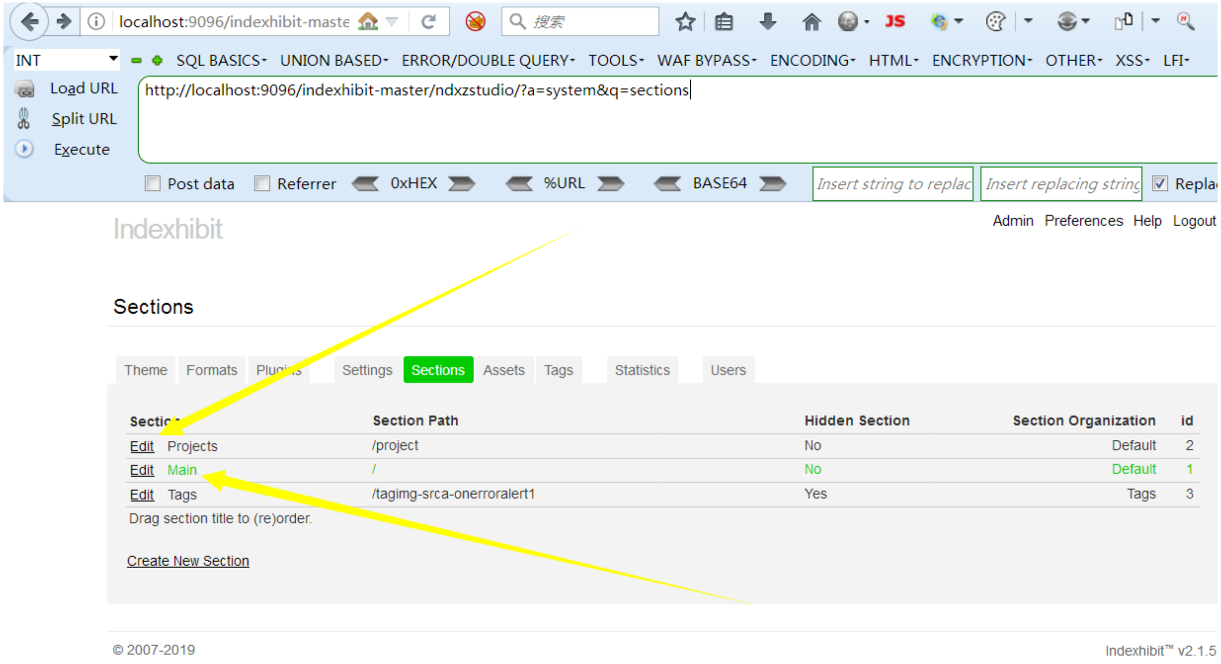
Jump to bottom

There are multiple cross-site scripting (XSS) vulnerabilities in the management panel #21

Closed zyfyc opened this issue on Feb 19, 2019 · 1 comment

zyfyc commented on Feb 19, 2019 • edited

There are two Stored-XSS Vulnerabilities in the backstage
We can make the Stored-XSS via edit the Projects or Main
poc:


localhost:9096/indexhibit-maste
搜索
INT
SQL BASICS· UNION BASED· ERROR/DOUBLE QUERY· TOOLS· WAF BYPASS· ENCODING· HTML· ENCRYPTION· OTHER· XSS· LFI·
Load URL
Split URL
Execute
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replac
Insert replacing string
Repla
Indexhibit
Admin Preferences Help Logout
Theme Formats Plugins Settings Sections Assets Tags Statistics Users
© 2007-2019
Indexhibit™ v2.1.5

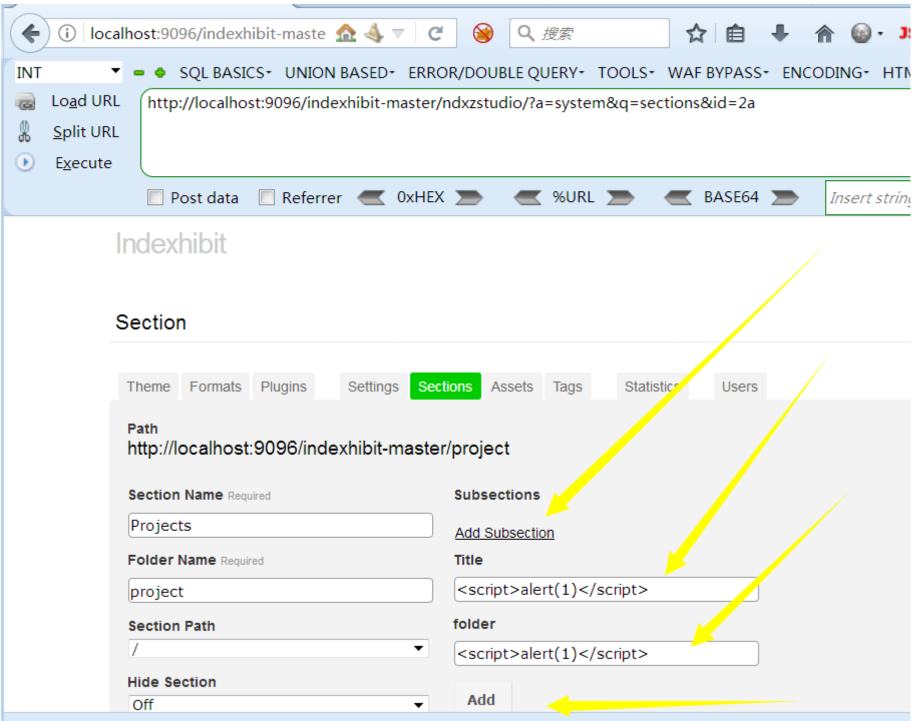
http://localhost:9096/indexhibit-master/ndxzstudio/?a=system&q=sections

Sections

	Section	Section Path	Hidden Section	Section Organization	id
Edit	Projects	/project	No	Default	2
Edit	Main	/	No	Default	1
Edit	Tags	/tagimg-srca-onerroralert1	Yes	Tags	3

Drag section title to (re)order.

Create New Section


localhost:9096/indexhibit-maste
搜索
INT
SQL BASICS· UNION BASED· ERROR/DOUBLE QUERY· TOOLS· WAF BYPASS· ENCODING· HTM
Load URL
Split URL
Execute
Post data
Referrer
0xHEX
%URL
BASE64
Insert strin
Indexhibit
Theme Formats Plugins Settings Sections Assets Tags Statistics Users
Add Subsection
Add

http://localhost:9096/indexhibit-master/ndxzstudio/?a=system&q=sections&id=2a

Section

Path
http://localhost:9096/indexhibit-master/project

Section Name Required: Projects

Folder Name Required: project

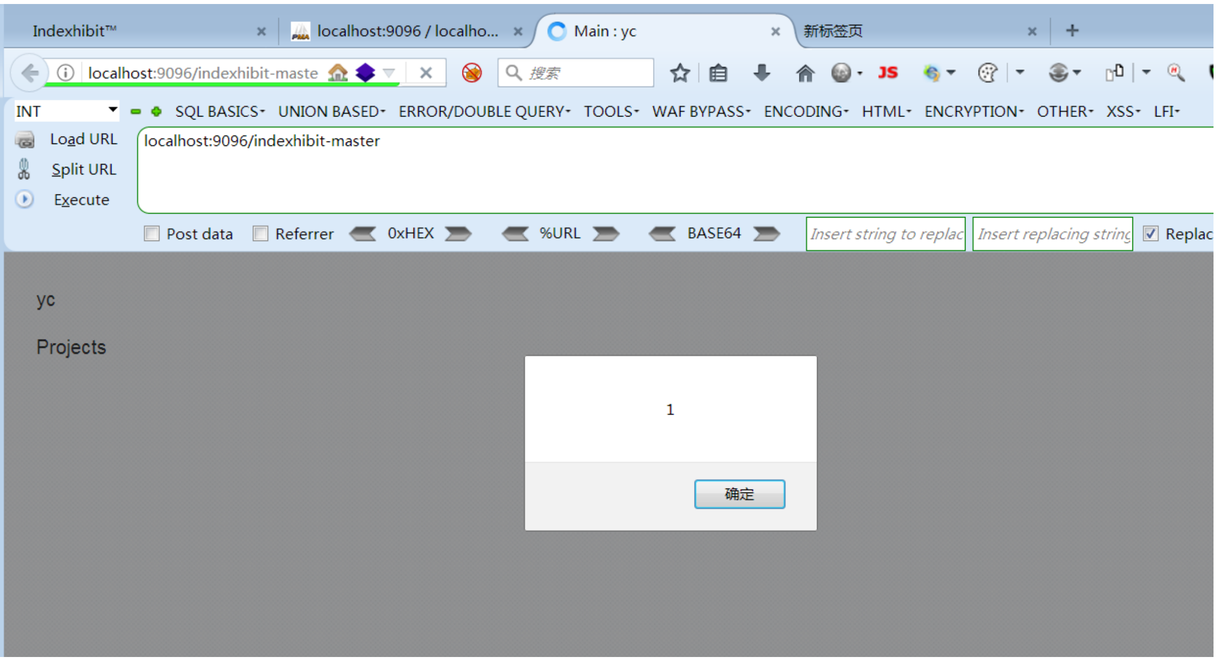
Section Path: /

Hide Section: Off

Subsections

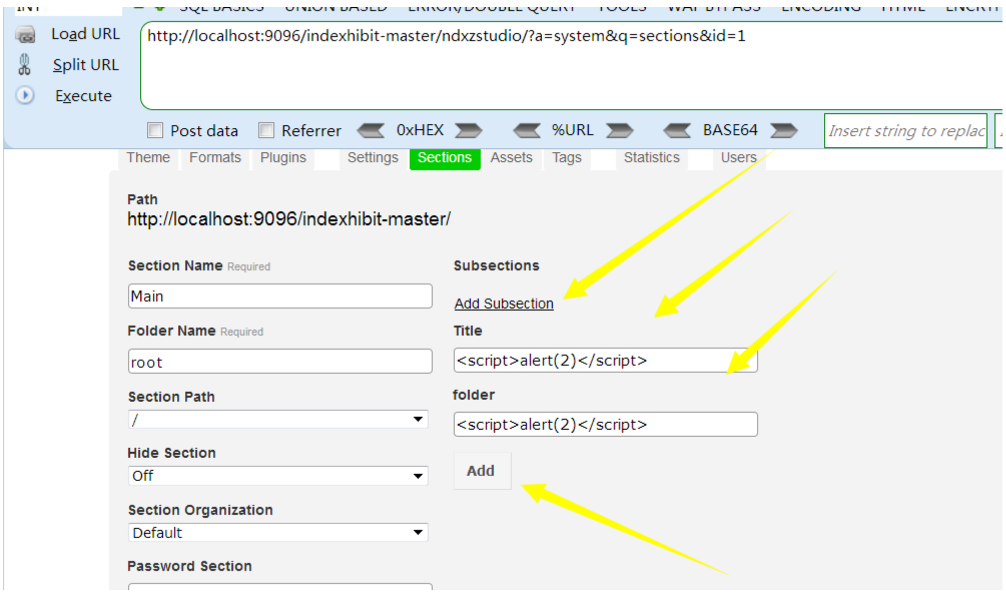
Title: <script>alert(1)</script>

folder: <script>alert(1)</script>



localhost:9096/indexhibit-master

1



http://localhost:9096/indexhibit-master/ndxzstudio/?a=system&q=sections&id=1

Path
http://localhost:9096/indexhibit-master/

Section Name Required: Main

Folder Name Required: root

Section Path: /

Hide Section: Off

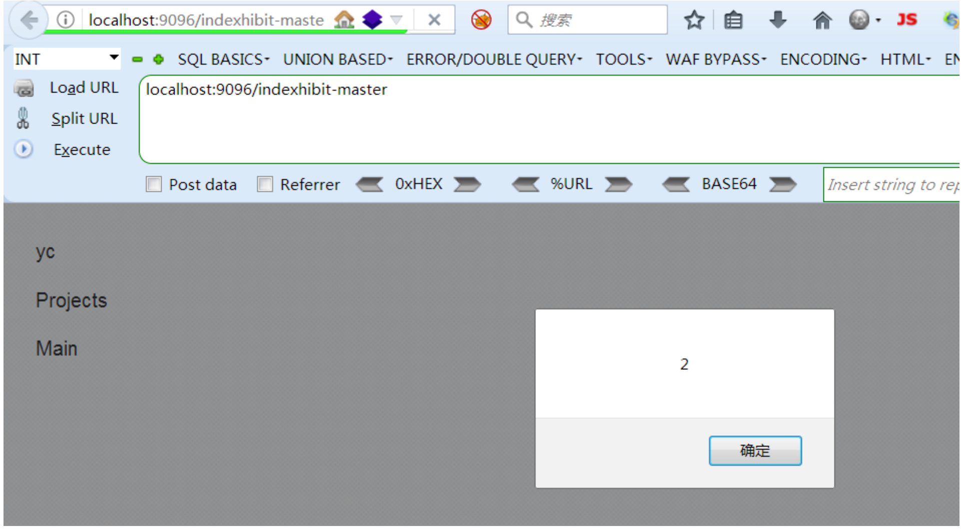
Section Organization: Default

Password Section

Subsections

Title: <script>alert(2)</script>

folder: <script>alert(2)</script>



localhost:9096/indexhibit-master

2

fix:
Strictly verify user input, you must perform strict checks and html escape escaping on all input scripts, iframes, etc. The input here is not only the input interface that the user can directly interact with, but also the variables in the HTTP request in the HTTP request, the variables in the HTTP request header, and so on.

Vaska commented on Feb 20, 2019 Collaborator

I understand this, but you are logged in to the cms - of course, if you are logged in you can do much damage to any site.

Vaska closed this as completed on Jul 27

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants