Government Secrets DB

"A CTF Extravaganza" – OPERATING GUIDE

Credentials:

- Windows_WebServer VM:
  - Uncle:P@ssedU1
  - Admin:@dm1n1sR00t
    - All security question answers are 'abc123'
- Government Secrets DB (The website)
  - Admin: @dmin5rul3Z

Instructions:

1. Restore VM to 'Good' snapshot for clean state. Boot up and log in to 'uncle' user. **DO NOT TOUCH ANYTHING AFTER LOGGING IN!**
   a. 'START_WEBPAGE.bat' is set to run upon log in and any clicks or keystrokes **WILL** mess this script up.
      i. If this script gets messed up, close all windows and click the 'START_WEBPAGE.bat' icon on Desktop.
   b. Everything is good to go once you see a Firefox window with the comments page ('Everyone's a Critic') auto refreshing every 5 seconds or so.
2. Confirm SentryHD is up by checking the HMI. It is running on ports 81 and 444.

Upkeep:

1. Keep an eye on the comments page and make sure that 'Admin' is constantly refreshing and loading ALL of the comments.
   a. If comments are not loading due to a disgruntled web user, click 'REFRESH_DB.bat' icon on Desktop.
      i. This will clear comments DB. You may need to re-input URL to 'localhost/comments' if XSS was clever enough to redirect you.
2. IF IP CHANGES link to backend of site will be broken
   a. Update 'server_ip' variable in C:\Users\uncle\HAVIC_XSS_2\react_front\constants.js and run 'yarn build' in C:\Users\uncle\HAVIC_XSS_2\react_front\ directory

Future work:

1. Admin bot is vulnerable to XSS manipulation. Alerts and redirects will break the script. I plan on implementing an autodetect feature that will wipe comments DB clean every time a user breaks the refreshing script.
2. I want to plant more hints.
   a. Flag 1: leave a comment stating that the Admin is currently on and checking the comments
   b. Flag 3: mention something about a UPS manager inside of the box