Capture the flag infrastructure
The aim of this project is automating an infrastructure for an existing capture the flag challenge. The challenge is fully developed, but is currently manually deployed and all participants play on the same targeted web sites. Additionally some manual steps are required in order for the challenges to work. Lastly if an error occurs, manual steps are needed in order to restore an older working snapshot of the challenge.

The tasks of this project will be to automate the deployment of the targeted sites such that when a user will register for the challenge he will receive a set of targeted sites deployed only for him and automate all the manual work needed for the challenges to run.

The code for the challenges is in nodejs and all the infrastructure is based on docker.

Phases
1. Automate a docker deployment of the target web sites per user registration for the challenge. Update the challenge web application to reflect the unique URL’s of the target web sites for that user. Set up of DNS infrastructure may be required for this step.
2. Automate the manual steps needed for the XSS and CSRF challenges to work which imitate a user logging in to the target web sites. This can be done with headless browsers such as splash or phantom.
3. Enable the capability of the registered user to restore the state of the target web sites to a point in history if an error occurs due to his attacks.

Deliverables
1. The final code for the entire system
2. A report stating the changes done in the code and the documentation of operation of the infrastructure

Aviv Ron
rona@il.ibm.com
058-5810200