# Service Problems

## During Preparation:

For each page, check the following things:

* Verify the inputs on the page aren’t SQL injectable.
  + The page should not allow for SQL injectable GET requests.
  + The page should not allow for SQL injectable PUT requests.
* Verify the inputs on the page aren’t XSS injectable.
  + The page should not allow for XSS injectable GET requests.
  + The page should not allow for XSS injectable PUT requests.
* Verify the inputs on the page don’t have persistent XSS vulnerabilities.
* Verify that unnecessary iframes are removed from the page.
* Abstract out any functionality that does not need to be provided to the user. For example an input box that could be converted into a dropdown menu because there is only a certain set of inputs that should be provided.
* Verify that there isn’t a buffer overflow vulnerability on the input fields. This will usually be indicated by a long input being cut off and then unexpected behavior following the submission of the input.
* Add try-catch loops throughout the event handlers to make sure that all error cases are caught by the program.

For the entire website, check the following things:

* Verify the website isn’t file traverable.
  + Verify that you can’t get the /etc/shadow from the website.
  + Verify that you can’t get the source code for the website from the website.
* Verify the website isn’t running as root.
* Verify that the website is running as a designated user for the website. Usually the website is ran as the www-data user.
* Remove unnecessary calls to iframes or external scripts.
* Remove hosting support for scripts or other services that do not need to be hosted on your webserver (Apache, Nginx, etc).
* Remove suspicious pages. For example, a suspicious page is a page that you were not provided the credentials for that does not use the default credentials.
* Add authentication for the pages on the website that need authentication.
* Make sure that the authentication with the active directory is using LDAPS.
* Set up HTTPS for the login page on the website.
* Set up HTTPS for the rest of the website if you can get it set up.
* Hook up the authentication for the website to the active directory.
* Make sure that the website does not provide version numbers or any revealing information about the website when an error is encountered. An error being going to a page that does not exist or something like that.
* Look for any additional pages that are not listed on the website header.
* Make sure that the ports for the boxes of services that the website is accessing are not publicly accessible outside of the internal network. You will have to work with the networking person(s) on this.
* Check the robots.txt file.
* Create new database user for each page of the website that needs to access the database to make sure that the users have as few permissions as possible while on the website.
* Make sure that debug mode is turned off if it is available on the website.
* Make sure any iframes are using TLS for communication when possible.

## Before Competition:

* Reset database contents back to the defaults.

NOTE: This checklist is only there to get you started.There may be other things wrong with the website.