Garrett Reeve

Tests iteration 4

Thoughts going into test iteration

In this testing session for iteration 4 the main points of interest are the upload files which can be used maliciously, this includes the profile picture which can be updated on the edit profile page.

Trying to upload malicious files instead of images

* Because the front end team has added in the tag type="file" name="file" accept="image/\*" I am not able to easily just upload any file, this tag only allows, .jpg, .png, and .jpeg files to be uploaded.
* However this can be circumvented in some cases.
* Test 1
  + Trying with appropriate tag but adding second tag
    - Try with following file names
      * File.php.png – Allows the name, but getting file with php code uploaded makes issues
      * File.png.php – failed, does not recognize the .png
      * /file.jpg/index.php – does not allow / on web side
        + All special characters on files fails
* Test 2
  + Testing whether backend can be affected by executing code from file upload
    - It is possible to get php to run when submitting certain files. This php can be used to change entire columns such as passwords etc. Although passwords is hashed so it created a barrier
    - Pre hashed passwords can be injected
* Test 3
  + Try getting any php running code files to get through front end.
    - Basic .php or .php5 files cannot be uploaded.
    - .png file with underlying code was uploaded but was not able to get database to run as it is stored only. But created issue with this and combination of injection code to run underlying php code in uploaded files.
* Test 4
  + Tryin running simple xss and injections for any changes
    - All tests run in this section failed as they were fixed in previous iteration.
    - "<script>alert(1)</script>"@example.com
    - <a href='mailto:USER\_EMAIL'>email me</a>
    - foo'onclick='alert'foo='@example.com
  + Testing username/email entries with the following tags
    - 1' or '1' = '1
    - SELECT \* FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR '1' = '1'
    - SELECT \* FROM Users WHERE ((Username='$username') AND (Password=MD5('$password')))
    - 1' or '1' = '1'))/\*
    - Foo
  + All above tests failed as we have added filtering for email field and not allowed certain special characters

Conclusion

What needs to be addressed

* Hashing implemented causing more secure passwords on database
  + Helps prevent any commands that can display possible hashed values
* Things that I would like to test with proper equipment
  + There is a feature in Windows 8.3 that allows to use unconventional naming of certain files. This includes like
    - “web.config” can be replaced by “web~1.con” or “.htaccess” can be replaced by “HTACCE~1”
  + Scan using a appscan application would help to confirm that all tags are appropriately set and no further investigation into the simple setting on the html side would be needed

Front end team has done a lot of work filtering fields and also keeping all tags on the appropriate setting that will keep from exploits being run.

* These setting will have to be correctly configured if a full server is used and the database is moved into prod. For this project these have not been fully implemented so there are no real issues or concerns for this iteration.

Final thoughts

This team has worked with great efficiency and effort to complete this project. All team members have worked very well together to get the iterations done and we are very satisfied with the final product. There are things that could still be implemented, for instance an actual full server and web hosting as well as email service and other automated functions. But those are for more of production things that can be easily implemented.