Jordan Rhode

9/30/12

File Share Questions

1. How could you make the use of login and password more secure? List at least two suggestions.
   1. Build a one click registration form powered by Google. This allows you to use their security and code on your site instead of having to do all the work.
   2. Instead of using md5 for encryption enhance it with salt and hash encryption. Also it’s good practice not to use session variables to store sensitive data because they can be hacked in a variety of ways.
2. As a user of the application, what ways might I use to get around the requirement: “only be allowed to upload Web-safe images.”
   1. You could change the extension of an .exe or other file to .jpg or .jpeg and still be allowed to upload it to your server. Not good news.
3. What strategies might I use to prevent spam bots from being able to read my email address?
   1. Use the PHP function encode\_email() which replaces each character with its ASCII value.
4. As a user of the application, how might I try to get around the 8mb file limit?
   1. I found a hack where you can bypass image uploaders by uploading an exploit/shell here: <http://www.enigmagroup.org/articles/view/Web%20Hacking/83-Tricks-and-Tips:-Bypassing-Image-Uploaders.>
5. How might you improve upon the process for deleting images?
   1. Right now my script opens a blank php page, deletes the file, then redirects back to the homepage. I can instead just find a way to run the delete command on the same page I request it from then reload the page.