**CEG 4430/6430 Cyber Network Security**

**Project 3**

**(20 Points)**

Through this project, students will learn **unrestricted file uploading vulnerability**, launching attacks against this vulnerability, and perform mitigation (graduate students).

**Submission**

1. Undergraduate:
   1. A report of your answers.
   2. Each team submits one report.
   3. Each team member needs to submit a list of all team members.

**Questions**

Assume that you are an attacker and you have access to the source code of the PHP file (you do not have access to the server).

1. What is the directory (or the path) in the server that stores the uploaded image? (1 points) and Justify your answer by analyzing the source code. (2 points)
2. Suppose the uploaded image has a name called “myphoto.jpg”. How can you directly access this image in your browser? Show the path. (3 points)
3. Can you upload files that are not images to the server and directly get access to uploaded files? Justify your answer using both testing (2 points) and code analysis. (2 points)
4. Create a PHP file and upload it to the server. This PHP file will allow the attacker to remotely execute arbitrary commands in the server. (hint: see “system()” API in PHP). (5 points)
5. Mitigation (5 points)
   1. **Undergraduates**: Briefly but precisely explain how you can expand the sanitization function in the PHP script to mitigate this vulnerability.
   2. **Graduates**: Expand the sanitization function in the PHP script to mitigate this vulnerability. You need to submit the patched “profile\_image.php”.

**References**

It may be helpful for the project to read the following articles.

1. <https://cwe.mitre.org/data/definitions/434.html>
2. PHP $\_FILES: <http://php.net/manual/en/reserved.variables.files.php>