CYBR 615: Cybersecurity Vulnerability Assessment
Spring 2022

Lab Assignment #4

- Name only: ____
- Release date: Feb 22, 2022 (Tuesday) 6:20pm
- Due date: Mar 01, 2022 (Tuesday) 4:00pm
- It should be done INDIVIDUALLY; Show ALL your work
- Total: 10 pts

1. Go to https://owasp.org/www-project-vulnerable-web-applications-directory/, OWASP Vulnerable Web Applications Directory Project, choose one **On-Line Web Application**, and perform the following testing activities.

   - Testing for Bypassing Authorization Schema [1 pt]
   - Testing for Privilege Escalation [1 pt]
   - Testing for Insecure Direct Object References [2 pts]

Before performing any testing activity, please give a brief introduction of chosen web application.

(Currently, OWASP is migrating to a new web platform. The previous url, https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project, is not available. Please visit the following urls, https://owasp.org/www-project-vulnerable-web-applications-directory/ or https://github.com/OWASP/OWASP-VWAD, for The OWASP Vulnerable Web Applications Directory Project. You will be able to find archived previous wiki pages.)

For each testing, please take screenshots and provide brief explanation to show the complete testing process.

2. Go to https://github.com/WebGoat/WebGoat/releases, download webgoat-server-8.1.0.jar and webwolf-8.1.0.jar, and run webgoat and webwolf application (https://github.com/WebGoat/WebGoat), and complete the following challenge in (A3) Sensitive Data Exposure and (A5) Broken Access Control.

   - (A3): Insecure Login [2 pts]
   - (A5): Insecure Direct Object References [2 pts]
   - (A5): Missing Function Level Access Control [2 pts]

For each testing, please take screenshots and provide brief explanation to show the complete testing process.

Before you perform some testing activities, you might have to install the right tool and set it up correctly on your machine. You can either install individual tool, or install **Virtual Machine** (i.e., VMware) and **Kali Linux**.

Notes:

- The OWASP Vulnerable Web Applications Directory (VWAD) Project is a comprehensive and well-maintained registry of all known vulnerable web applications currently available. These vulnerable web applications can be used by web developers, security auditors and penetration testers to put in practice their knowledge and skills during training sessions (and especially afterwards), as well as to test at any time the multiple hacking tools and offensive techniques available, in preparation for their next real-world engagement.
- Except for vulnerable web applications maintained by OWASP VWAD, it is illegal to perform any type of penetration test on any other web application without permission and authorization.

- In a nutshell, though, if you access any computer without its owner's permission, and obtain any information from it or cause any damage (even accidentally), you've broken the law. See 18 U.S.C. § 1030, https://www.law.cornell.edu/uscode/text/18/1030