CYBR 615: Cybersecurity Vulnerability Assessment
Spring 2022

Lab Assignment #5

- Name only: _____
- Release date: Mar 08, 2022 (Tuesday) 6:20pm
- Due date: Mar 22, 2022 (Tuesday) 4:00pm
- It should be done INDIVIDUALLY; Show ALL your work
- Total: 10 pts

1. 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.
    - (A8: 2013): Cross-Site Request Forgeries [2.5 pts]
    - (A8: 2013): Server-Side Request Forgery [2.5 pts]

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

2. Go to http://www.dvwa.co.uk/, download and setup Damn Vulnerable Web Application (DVMA) on your machine, and complete the following challenge.
    - CSRF [2.5 pts]
    - Weak Session IDs [2.5 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