Damn Vulnerable Web Application Bug Bounty

Project Scope & Plan

By Justin S. Miller

ISM 3324-01Z

Professor Nicole Dyess

16 November 2022

**Project Scope:**

The overall goal is to assess the web application entitled “*Damn Vulnerable Web app*” to ensure that it is protecting the data of the company. I plan to run a series of tests that are considered standard for any web application and document my findings. The list of tests are located in the goals section of this document. In the next second, I will go over the authorization information followed by Goals and procedures. Since this is a web application these test will be conducted remotely and no sensitive data will be compromised during this assessment.

**Information that was Discussed prior to the assessment**

The development team of the web application “*Damn Vulnerable Web Application*” has asked & authorized me, Justin S. Miller, to conduct a security assessment on their application. Since this application is accessible over the Internet this is a remote assessment being conducted in my test environment. The team has been kind enough to provide me with the source code so that I can run it through my lab environment and locate any and all vulnerabilities. I will document each weakness and give a solution to patch each weakness in my final report. If I find any sensitive data it will not be tampered with, but it will be documented with a proper explanation on how to better secure it. Should a incident occur during my assessment I will immediately stop the assessment and report to the development team & assist them in solving the issue.

**Goals of the Assessment**

The main goal of this assessment is to locate and report bugs and/or vulnerabilities to the development team.

**Tests being conducted during assessment**

The tests listed below are the standard tests to run against any web application:

- Test resistance against SQL or command injections

- can a user run commands against the web server from the browser?

- Test resistance to unwanted file upload

-Can the user upload unwanted files to the web server

- Test File inclusion

Can the user browse to files on web server via URL address bar

- Test CAPTCHA

Can a user bypass CAPTCHA with a brute force attack

- Test session ID strength

can a users session be hijacked

These five tests help test the integrity, availability, and confidentiality. After I conduct each of these tests against the application. I will present a report with my findings and second report with a detailed guidelines on how to repair the bugs and vulnerabilities in the system.