CSC 234 Final Exam (Practical) – Fall 2020

The final practical exam is brand new for this semester and includes two applications that need to have their source code reviewed. Your target is to identify and explain the vulnerabilities you find; then, fix those problems and explain why your fix works. You do **not** need to demonstrate the vulnerabilities for this exam, but you may demonstrate them if you think it helps either your discovery or defense explanations.

You may use outside resources to include the Internet, previous assignments, and documentation for languages or technologies. You may not work with other people on this exam. Working with other people includes asking questions on any online forum (Chegg Study, CourseHero, etc.)

I believe I have listed all the vulnerabilities you will find. If I have missed one, please do include it or email me about it so I can let the class know.

vApp / VM Details

Exam vApp: <username>_CSC234_Zwach_Exam2
User: student
Password: Password1!
Exam VM: CSC234-Exam2

Personnel Files App

The Personnel Files app allows a logged in user to search the personnel database for files. It is written in PHP and runs inside of a docker container with a supporting mariadb database, also in a docker container.

Source Path: ~/course_files/_assignments/exam2/app/
URL: http://localhost:8007
Viewing PHP Logs: `docker-compose logs -f`
Vulnerabilities: XSS, SQLi, Information Leakage
User: jsmith@cookies.corp
Password: password

Cookie Order Program

The Cookie Order program is designed to manage orders and invoices of cookies from our company on the local system. It needs some work before we can use it in production. It is written in C.

Source Path: ~/course_files/_assignments/exam2/cookiecorp.c
Vulnerabilities: Buffer Overflow, User Controlled Format String, Race Condition, 2 Integer Overflows

Deliverables

Submit a single word or PDF document with the following for each vulnerability you discover:

- A screenshot of the vulnerable code
- An in-depth explanation of why it is vulnerable ("this is sqli" is not enough)
- A screenshot of your remediated code
- An in-depth explanation of why your fix works ("this code is no longer vulnerable to sqli" is not enough)

All screenshots must include your name. If your name is not in a screenshot either as a code comment or in the panel at the top of the VM, **you will receive a 0 on the exam.** You can put your name in the top panel with the `setname` command.

Scoring

10 points per vulnerability – 80 points total