EE / CprE / SE 491 – sdmay 21-17
Webserver Attack Blocking AI
Report 2

02/08/2021 – 02/22/2021
Client: Andrew Dakin (Cylosoft)
Faculty Advisor: Douglas W. Jacobson

Team Members:

Megan Hill ---------- Website Engineer
Jamie Sampson ---------- Security Engineer
Emily Young ---------- Database Engineer
Andrew Marek ---------- Fullstack Engineer / Administration
Paul Degnan ---------- Automation Engineer

Past Week Accomplishments

- IIS Module - Jamie
    - Researched possible IIS modules to use that would allow us to block IP addresses.
        - Decided to use the `<ipSecurity>` module that IIS has built in
        - Built out bar bones class using sample implementation
    - Looked into how IIS worked and gathered information on where the log files are saved from IIS
        - Installed IIS on Windows, along with the necessary modules enabled
        - Talked with our client about the future testing environment and the location of where log files are stored that come from their IIS setup
- Database Solutions - Emily
    - Created local Azure database but have used all of student credit
        - Researching different testing methods to keep from falling behind on writing Insert, Delete, Search query methods
        - In the process of renewing student license to regain access to database that was already established
    - Wrote Insert and Delete methods for database (untested at this time)
        - I took my skeleton code from last semester and made edits to personalize methods more to our project
        - Continued research and fine tune
- File Watcher - Paul
    - Fixed a known bug where for some reason temporary files were messing with file watcher
        - Temporary files created by visual studio shouldn't really be a problem
    - Worked on the automatic read through of a file when a file is changed in the directory being watched
        - Fixed a bug where the header was being read and therefore the program would have an out of bounds exception
        - ReadLine temporarily added to stop from the file being read that is changed again erroring the program out

- New rules and general changes - Andrew
    - Began refactoring and attempting to test for bugs within the program
        - Branch still in progress, mainly realized that we were looking for the wrong IIS field to make decisions.
    - Added a few more rules based on various items that came as a result of our adviser meeting
        - Research SQL injection detection. Not sure if implementing, as most sources say that IIS automatically handles this, and doing so with regex or anything else is very poor practice.
    - Brainstorming code structure /
- Website Infrastructure - Megan
    - Created basic Infrastructure for our Website
        - Using Next.JS and create-next-app to create infrastructure
    - Front-End
        - Created Styling for components including buttons using Styled Components
        - Added Global Styles for font-type
        - Added Theme for theme components shared between different pages
    - Backend
        - Created a custom server using Hapi
        - Created endpoints that serve (for now mock) data to the front end
        - Set up custom routing, so api paths are easily identified
    - Testing
        - Started creating basic testing using jest
        - Wrote some tests for custom server code

Pending Issues

- Not all of us have a Windows machine to run IIS - Everyone
- Still have many issues with database connection (local and client)-Emily/Everyone

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Megan Hill	Created Website Infrastructure, and some basic features.	6	9
Jamie Sampson	Investigated IIS modules we could use to block IPs	4	7
Emily Young	Researched database connectivity problems and wrote Insert and Delete methods	4	7.5
Andrew Marek	General refactor, fix using sIP instead of cIP, some new rules, research	4	6
Paul Degnan	Found and worked on fixing a problem where some	4	7

	programs create temporary files that mess with the file watcher. Made the file read every line except for the header of the IIS log.		

Plans for Coming Week

- IIS Module - Jamie
  - Setup IIS to run locally against a dummy website
  - Connect IpSecurity class to interact with the main body of our code
  - Dynamically handle unique file save locations along with IIS website target name
- Database Solutions - Emily
  - Locate a more secure testing environment
  - Make Insert and Delete methods fail-proof
  - Implement Search Method
- File Watcher - Paul
  - Make the File Watcher run successfully more than one time, currently can really only run once successfully and therefore have a ReadLine to stop it from erroring out.
  - Make sure the same IIS log lines are not being read over and over.
  - Automate this process: When a new log is created, watch it for changes
- Rule Implementation - Andrew
  - Brainstorm and implement new rules / investigate what more one could do to be more accurate
  - General refactor / look for structural issues
  - Potentially investigate testing / CICD
- Website Infrastructure - Megan
  - Add more tests so whole project is tested
  - Add linting rules to enforce code quality
  - Update styles to be more aesthetic

Client Meeting

- Planning adviser meeting for next week, but met with client (2/9)
- Talked about how we can begin connecting our product with their infrastructure.
  - Will likely end up on a VM in the Cloud on Azurer -- Windows Server 2019
- Discussed testing on their servers - necessary to setup IIS and able to test locally (although none of us have Windows computers, this will be a focus for next iteration).
- Discussed end goals - benchmarking is important, basic filter types, etc.
  - Focus on speed, false positives, faster than a human = ultimate goal.
- Discussed project timeline goals - none particular from their end (just something works at the end with the appropriate criteria).
- Decided we will have a UI in the form of a web application.