EE / CprE / SE 491 – sdmay 21-17
Webserver Attack Blocking AI
Report 5

03/15/2021 – 03/29/2021
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 ---------- Administrator / Software Engineer
Paul Degnan ---------- Automation Engineer

Past Week Accomplishments

- Database-Emily
    - I have made slight changes to the search method to fit more with the functionality of the website
    - I have been trying to work with our advisor for getting some help with our database connection issues, but our communication has been slow
    - I've mapped out a const file for the database values. I just have to fill in some blanks
- IIS Security - Jamie
    - Added capability to set security settings for individual websites by reading JSON files.
    - Converted IP Security work for blocking IP addresses to be dynamic to use JSON file settings.
- General Clean-Up - Jamie
    - Ran "cleanup code" in Rider (fixes spacing of functions, vars, and bracket to code text)
    - Created a "Constants" file and pulled constants from the rest of the code.
- File Watcher/IIS Log Directories - Paul
    - Received an example of an IIS log directory, went over it and analyzed the structure of the directory
    - Started working on making FileWatcher be able to watch subdirectories.
- Website Updates - Megan
    - I have added a chart to our website to display more information about blocked IPs
    - I have added the ability to display multiple lines on one graph so we can show more data at once
    - I have written some more backend infrastructure so that we have multiple endpoints that we can hit with different data types.
    - Researched ways to connect website to database

- General and PR Review - Andrew
    - Looked more into config file and how we can make the program more modular per the client's request.
    - Reviewed Git contributions from others.

Pending Issues

- Still pending actual functionality of IIS features (ie. to make sure they are activating / are being used correctly). - Jamie
- Still working on our ability to hit the client database. Currently the majority of us are not able to hit it, but a few people can. We have reached out to ETG to get an IP address range for ISU so we can add some more IP addresses and hit it over VDI/VPN.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Megan Hill	Add more data to chart on website. Added table to website, sent some communications to get more info about why we are unable to connect to database.	5	22
Jamie Sampson	Added classes/structure for IIS settings. Created logic to read json files, and update current code to use dynamic settings.	7	21.5
Emily Young	Map out const file for database, slight change to search method, work with advisor to move forward with connection solutions	3	20.5
Andrew Marek	Reviewed pull requests by other members, and looked into options for technology for configuration files.	2	14
Paul Degnan	Received and went over the IIS log directories and started working on changing FileWatcher so that it has the functionality to watch multiple subdirectories.	4	19

Plans for Coming Week

- Database-Emily
    - Continue to poke our advisor to move this solution along
    - Finale const file and merge with main branch

- IP Security - Jamie
    - Request client to review and create a sample json site security file.
    - Formally test security functionality / stand up workspace.
- File Watcher - Paul
    - Make sure the File Watcher has subdirectory functionality
    - Make sure the FileWatcher can access the files in read mode even if the file is being written to in read write mode.
    - Change the functionality where the file watcher only parses recent log entries to work with subdirectories.
- Website - Megan
    - Connect to Database
    - Reformat website as necessary to handle real data
    - Add error handling when unable to reach database
- General - Andrew
    - Aid others with various tasks as necessary
    - Review program flow
    - Begin presentation for PIRM 2
- Put all the moving parts together to make one continuous flow from start to end. - All