EE / CprE / SE 491 – sdmay 21-17
Webserver Attack Blocking AI
Report 4

3/2/2021 – 3/15/2021
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

- Project Maintenance - Jamie
    - Updated README to better describe our project's direction.
    - Updated all occurrences of "Console.Write" to use NLog.
- IP Security - Jamie
    - Looked into using "Request Filtering" and "DynamicIPSecurity" to handle rate limiting, flag url strings, and enabling an ISS feature where it logs what it would block if disabled.
- Database Methods - Emily
    - The database methods are currently being reviewed and merged from my branch
    - There is a suggestion in my PR that I am looking into making changes to help with future website use easier.
    - Cleaning up my code and documentation as well as continuing testing
- Database Connectivity - Emily
    - I have reached out to our advisor, client and ETG to begin working on a solution for our inconsistent connection issues
    - We've come up with a few different solutions
- File Watcher - Paul
    - Made sure the same IIS log lines are not being read over and over.
        - Moved the process of parsing lines only if they have not been parsed already from File Watcher to the new Log Parser code.
        - Added back only calling log parser if it was a change and not a deletion or addition.
        - Bug Fixes: Fixed header data bug. Fixed problem where new log parser created every change instead of file addition. Fixed problem where current line int not updated on new file change.
    - Automated the process of a new log file that needs to be watched being created.
        - Moved addition event handler that resets the lines already parsed from old code to refactored code.

```
2021-03-15 20:55:03.9190 SmartBlock.LogParser time
2021-03-15 20:55:03.9299 SmartBlock.LogParser s-ip
2021-03-15 20:55:03.9299 SmartBlock.LogParser cs-method
2021-03-15 20:55:03.9299 SmartBlock.LogParser cs-uri-stem
2021-03-15 20:55:03.9299 SmartBlock.LogParser cs-uri-query
2021-03-15 20:55:03.9505 SmartBlock.LogParser s-port
2021-03-15 20:55:03.9505 SmartBlock.LogParser cs-username
2021-03-15 20:55:03.9613 SmartBlock.LogParser c-ip
2021-03-15 20:55:03.9613 SmartBlock.LogParser cs(User-Agent)
2021-03-15 20:55:03.9613 SmartBlock.LogParser cs(Referer)
2021-03-15 20:55:03.9613 SmartBlock.LogParser sc-status
2021-03-15 20:55:03.9818 SmartBlock.LogParser sc-substatus
2021-03-15 20:55:03.9818 SmartBlock.LogParser sc-win32-status
2021-03-15 20:55:03.9818 SmartBlock.LogParser time-taken
2021-03-15 20:55:03.9959 SmartBlock.LogParser  2020-09-06 00:00:01 10.10.3.1 POST /
4.189.105.117 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_4)+AppleWebKit/537.36+(K
+Safari/537.36 http://www.hrclassroom.com/trainings/ThemeTraining.aspx 302 0 0 26
2021-03-15 20:55:03.9959 SmartBlock.LogParser  2020-09-06 00:00:01 10.10.3.1 POST /
4.189.105.117 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_4)+AppleWebKit/537.36+(K
+Safari/537.36 http://www.hrclassroom.com/trainings/ThemeTraining.aspx 302 0 0 26
2021-03-15 20:55:04.0076 SmartBlock.LogParser  2020-09-06 00:00:01 10.10.3.1 POST /
4.189.105.117 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_4)+AppleWebKit/537.36+(K
+Safari/537.36 http://www.hrclassroom.com/trainings/ThemeTraining.aspx 302 0 0 26
2021-03-15 20:55:04.0076 SmartBlock.LogParser  2020-09-06 00:00:01 10.10.3.1 POST /
4.189.105.117 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_4)+AppleWebKit/537.36+(K
+Safari/537.36 http://www.hrclassroom.com/trainings/ThemeTraining.aspx 302 0 0 26
2021-03-15 20:55:04.0076 SmartBlock.LogParser BLOCKED
2021-03-15 20:55:04.0228 SmartBlock.LogParser  2020-09-06 00:00:01 10.10.3.1 POST /
4.189.105.117 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_4)+AppleWebKit/537.36+(K
+Safari/537.36 http://www.hrclassroom.com/trainings/ThemeTraining.aspx 302 0 0 26
```

- Website Improvements Megan
  - Started working on connecting website to database
  - Made some general code/UI improvements
- Configurable Rules - Andrew
  - Started creating files for rules to be configurable
  - This will likely be in the form of a yaml file that is configured for the following:
    - Time between accesses to determine malicious.
    - Specific URL stems to watch out for.
    - Turn on and off certain features?

Pending Issues

- Currently banking on IIS to do what I'm telling it to, but I need to set up a more solid testing environment. - Jamie
- Current connection to database is inconsistent - Emily

Individual Contributions

Team Member	**Contribution**	**Weekly Hours**	**Total Hours**

Megan Hill	Worked on connecting website to database and made some other general website changes to conform to code standards or ui standards.	3	17
Jamie Sampson	Project repo maintenance. Investigation into ip/url filtering and ways to restrict access to web servers.	3.5	18.5
Emily Young	Merged my current work with the master branch. Making changes based on a review from a team member and continually testing. Begin stages of connection inconsistency solutions	4	17.5
Andrew Marek	Worked on making the project more configurable through the means of a configuration file as requested by the client earlier.	3	12
Paul Degnan	Made sure same lines were not being parsed every time there was a change. Only parses new lines now. Moved that process to newly refactored code. Also automated a new file process and added that to newly refactored code. Fixed header data bug. Fixed skip lines that shouldn't be skipped bug.	5	15

Plans for Coming Week

- Need to narrow down and work on what we want to focus on handling first for IP security as there are alot of options to consider. - Jamie
- Work with our client to understand needs and more specifics on what we are looking for. - Jamie
- Make a decision on a solution process and begin work on moving forward with it - Emily
- Make updates to database methods as needed - Emily
- Go back over the IIS log structure and create subdirectory functionality for file watcher if necessary. -Paul
- Finish connecting website to database - Megan
- Determine what data should be displayed on website - Megan
- Finish configuration file read in / iron out any other rules that need to be added. - Andrew
- Assess configurability and probe clients for more ideas on requirements for blocker. - Andrew

Advisor Meeting

- Here are a couple of notes from conversations about our database solutions
    - Set up a proxy? But SQL doesn't support
    - Set up vpn on campus
        - IP would be a fixed address

        - They can whitelist that address
    - Talk to ETG about availability of a VPN
        - Check whether it presents as a public address
        - ETG has been contacted and recommends a static IP
    - VM is a backup backup
    - Client doesn't have a VPN on his end for us to connect to