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

Report 6

03/30/2021 – 04/12/2021 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

Summary

This week we got an environment where we are able to run all parts of our application. This meant that we were able to do work on connecting IIS and the database to our application. We also began work on our PIRM presentation as well as some of the other projects/presentations we need to do for the end of the semester.

Past Week Accomplishments

- IIS Settings Jamie
 - Tested functions that called IIS APIs to ensure they communicated correctly with IIS. Ran into some issues with duplicate entries causing the app to crash, but resolved them.
 - Defaulted values so that users don't have to provide all fields along with creating a document listing details on what features Smartblock was compatible with.
 - Ensured multiple sites each with different JSON settings were initialized correctly on app start-up.

 Internet Information Services (IIS) Manager

← → Ø → DESKTOP-FKAGAS4 → Sites → Default Web Site →						
File View Help						
Connections Connec						
✓ iii Sites	🕒 File Name Exter	nsions 🥳 Rules	•::• Hidden Segment	nts 😇 URL 🥖 HTTP Verbs 👜 Headers 🕜 Query Strings		
> 🏀 Default Web Site	Name	Scan	Applies To	Deny Strings		
	testFilter	Query string, Url		wordpress, dino		

Salaria Internet Information S	ervices (IIS)	Manager
--------------------------------	---------------	---------

←→ € DESKTOP-FKAG	GAS4 + Sites + Default Web	Site 🕨					
File View Help							
Connections	Use this feature to configure filtering rules.						
✓ Sites	🕒 File Name Extensions	🛃 Rules	Hidden Segments	🔤 URL		👜 Headers	Query Strings
> 🏠 Default Web Site	Url CVS/Entries phpinfo.php WS_FTP.log database.inc admin.conf iisadmin Googlebot hello world cgi-bin trace.axd wp-admin phpliteadmin.php	Action Deny Deny Deny Deny Deny Deny Deny Den					
Internet Information Services (IIS)	5						
	AS4 ▶ Sites ▶ Default Web	Site 🕨					
File View Help							
Connections DeskTOP-FKAGAS4 (DESKTOF Application Pools	Use this feature to restrict of priority.		emain Restrictio		lresses or doma	in names. Set t	he restrictions in order of
 Sites Sites Oefault Web Site 	Group by: No Grouping	-					
> 🦳 App_Data	Mode Requestor		Entry Type				

• Remote Desktop - Jamie

Deny

104.223.94.210

> 📔 aspnet_client

• Requested the CS department to create a remote desktop space for our team so that we could all access a shared environment where we could connect to the database, IIS, and our application.

Inherited

- All the joys of setting up a new environment to run all parts installing and Googling how to resolve unique issues in setup.
- File Watcher Paul
 - Created automated subdirectory functionality for file watcher
 - Created a backup method for the small chance FileWatcher can't access the files in read mode while the file is being written to in read write mode.
 - Changed the functionality where the file watcher only parses recent log entries to work with subdirectories.
- Parsing sc-substatus field Andrew
 - Added parsing of sc-substatus field, which returns a particular HTTP code.
 - If it returns 501/502, then the entry's IP is already blocked. We want to use this information for our website component.
- Final Report Andrew
 - Began outline for final report, started brainstorming for various components.

- Used past years projects as an example on how to structure it.
- Database Emily
 - We're finally connecting to the database consistently
 - All query testing is completed
 - Complete overhaul of Insert() (lots of syntax errors and it was easier to scrap and start over)
 - Website is now able to utilize these methods to display real data
- Website Megan
 - Downloaded applications necessary to run website on remote server
 - Figured out bugs around running website in new environment
 - Connected website to database using knex
 - Wrote SQL queries to query for data to display on website
 - Wrote js code to parse results of sql queries into expected data
 - Adapted existing UI to use information from database
 - Adapted UI to handle a wider range of values (future-proofing)

Data						
4 3- 2 1 09/03/2020		osoftwebsite.cor osoftwebsite2.co		20		
sIP	cIP	Cloudfla	csHost	csUriStem	Date and Time	
10.10.2.1	162.158.15	77.88.5.67	www.cylosoftwebsite.com	/BVModules/Themes/Foundation4+Responsive/ProductTemplates/B	2020-09-03T01:40:34.000Z	
10.10.2.1	300.132.15	77.88.5.67	www.cylosoftwebsite2.com	/BVModules/Themes/Foundation4+Responsive/ProductTemplates/B	2020-09-03T01:40:34.000Z	
10.10.2.1	300.132.15	77.88.5.67	www.cylosoftwebsite2.com	/BVModules/Themes/Foundation4+Responsive/ProductTemplates/B	2020-09-03T12:40:34.000Z	
10.10.2.1	300.132.15	77.88.5.67	www.cylosoftwebsite2.com	/BVModules/Themes/Foundation4+Responsive/ProductTemplates/B	2020-09-06T01:40:34.000Z	
10.10.2.1	300.132.15	77.88.5.67	www.cylosoftwebsite2.com	/BVModules/Themes/Foundation4+Responsive/ProductTemplates/B	2020-09-05T01:40:34.000Z	
					1-5 of 6	< :

Pending Issues

- Figuring out a useful similar to what we would be given way of mimicking IP requests to our website as a testing environment. Jamie
- Related to the testing environment, getting actual data populating our database instead of the mock data we are using now. Megan

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Megan Hill	Wrote SQL queries for the data we would need on the website. Connected website to database. Updated UI to reflect the wider variety of data that is possible.	10	32
Jamie Sampson	Ensured that site settings were set correctly within IIS. Fixed duplicates causing crashes. Added documentation. Setup a remote desktop to run the app.	9	30.5
Emily Young	Overhaul Insert() to work smoothly. Completed all testing to query methods	6	26.5
Andrew Marek	Added more features to log parser basically. Unit tested those as well. Started on final report.	3	17
Paul Degnan	Created automated subdirectory functionality for file watcher. Created a backup method for FileWatcher in case it can't access the files in read mode while the file is being written to. Extended subdirectory functionality where the file watcher only parses recent log entries instead of all.	3	22

Plans for Coming Week

- Give a demo / walkthrough of what our application does to our client to receive feedback. - All
- Establish a complete trip or "demo" of our application. All
- Attempt to set up making requests to our website to mimic some kind of traffic not necessarily the same type of requests in real implementation. Jamie
- Make significant progress on final report
- Add Search (by IP) functionality to website Megan
- Clean up UI on website Megan
- Aid in database transaction coding Emily