

Cloudflare WAF Scanner



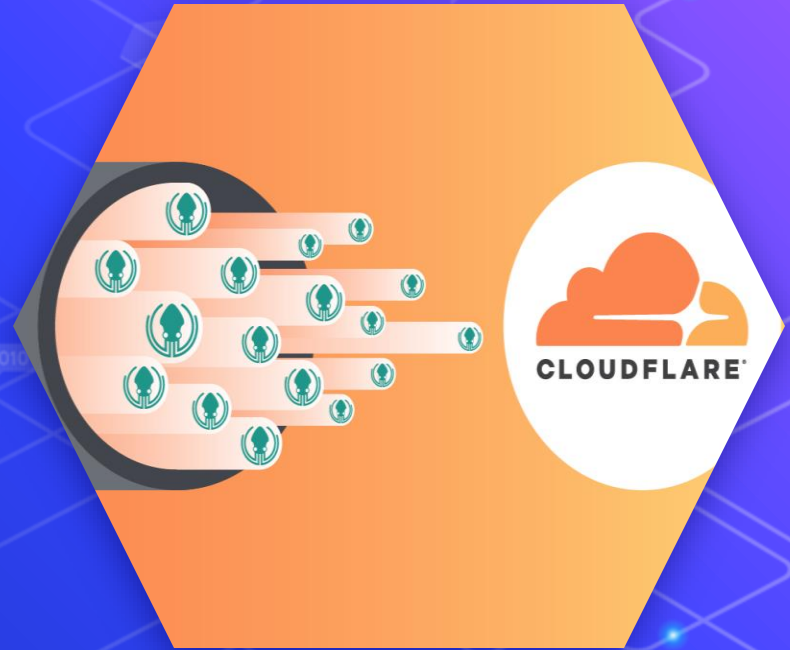
Hello!

We are sd-may21-16

Team Website URL: <http://sdmay21-16.sd.ece.iastate.edu/>

Advisor: Berk Gulmezoglu

Client: Andrew Dakin (Cylosoft)

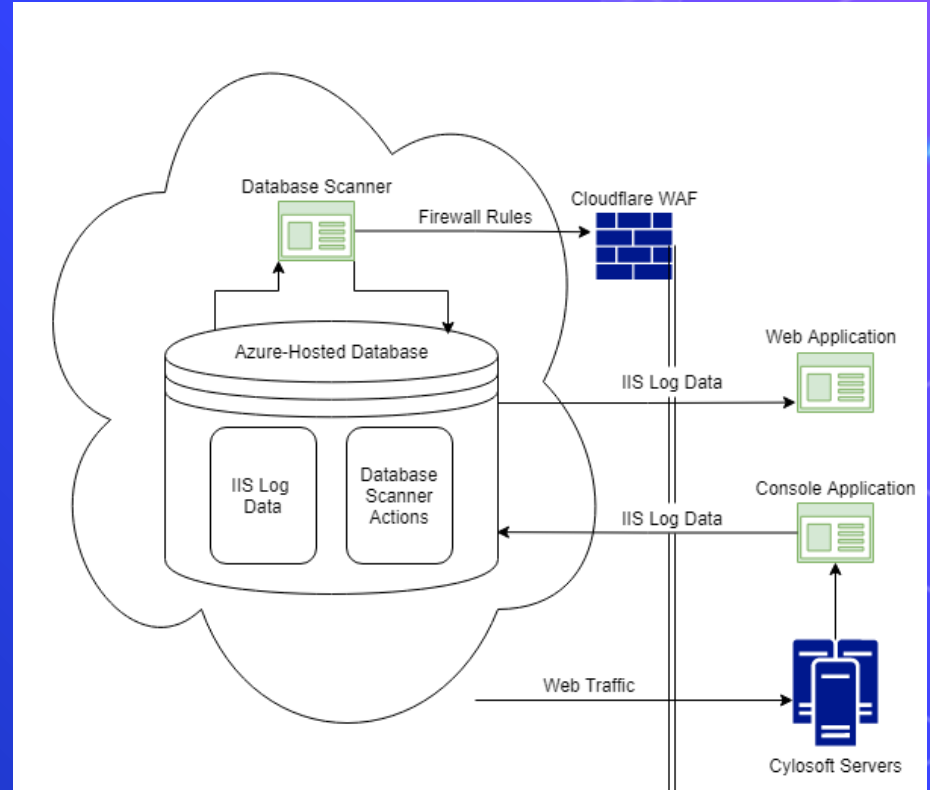


Presenting: Ryan Burgett







Project Introduction








- Console Application
- Database Scanner
- Web Application



Microsoft IIS

- Cylosoft servers run IIS
- Multiple sites on server
- New log file per site per day

<input type="checkbox"/> Name	Date modified	Type
 W3SVC1	2/12/2021 4:07 PM	File folder
 W3SVC2	1/20/2021 4:27 PM	File folder
 W3SVC3	2/23/2021 3:40 PM	File folder
 README.txt	1/22/2021 3:13 PM	Text Document

<input type="checkbox"/> Name	Date modified	Type	Size
 u_ex210108.log	1/8/2021 4:30 PM	Text Document	2 KB
 u_ex210111.log	1/11/2021 4:24 PM	Text Document	13 KB
 u_ex210113.log	1/13/2021 3:33 PM	Text Document	6 KB
 u_ex210118.log	1/18/2021 3:35 PM	Text Document	3 KB
 u_ex210202.log	2/2/2021 1:33 AM	Text Document	1 KB
 u_ex210203.log	2/2/2021 11:50 PM	Text Document	1 KB
 u_ex210212.log	2/12/2021 4:08 PM	Text Document	1 KB



Console Application

⬡ ≈ 500 lines

⬡ Config file

⬡ 4 database tables (Azure)

⬡ Languages

- Python
- C#
- .NET



Database structure

4 database tables

- Main log table
- (Test log table)
- Server list table
- Server values table
- Error log table

	date-time	universal-site-id	c-ip	cs-username	s-sitename	s-computername	s-ip	s-port	cs-method	cs-uri-stem	cs-uri-query	sc-status
1	2021-02-12 22:07:43.000	23	10.16.16.51	-	NULL	NULL	10.16.16.44	80	GET	/	-	200
2	2021-02-12 22:07:45.000	23	10.16.16.51	-	NULL	NULL	10.16.16.44	80	GET	/HNAP1/	-	404
3	2021-01-13 19:54:22.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	200
4	2021-01-13 19:54:22.000	24	:::1	-	NULL	NULL	:::1	80	GET	/iisstart.png	-	200
5	2021-01-13 19:54:23.000	24	:::1	-	NULL	NULL	:::1	80	GET	/favicon.ico	-	404
6	2021-01-13 19:54:25.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
7	2021-01-13 19:54:30.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
8	2021-01-13 19:54:32.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
9	2021-01-13 19:54:34.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
10	2021-01-13 19:54:36.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
11	2021-01-13 19:54:38.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
12	2021-01-13 19:54:39.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
13	2021-01-13 19:54:41.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
14	2021-01-13 19:54:42.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
15	2021-01-13 19:54:44.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
16	2021-01-13 19:54:45.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304
17	2021-01-13 19:54:46.000	24	:::1	-	NULL	NULL	:::1	80	GET	/	-	304

server-id	site-id	site-name	site-url	universal-site-id	folder-path	count
0	1	NULL	NULL	17	C:\Users\brfed\Desktop\LogFolder\W3SVC1	305
0	2	NULL	NULL	18	C:\Users\brfed\Desktop\LogFolder\W3SVC2	159
4	10	NULL	NULL	14		136
4	1	NULL	NULL	1		289
4	2	NULL	NULL	2		28
4	3	DrakeNation	https://www.drakenation.com/	3		25876
4	4	NULL	NULL	4		482
4	5	NULL	NULL	5		226
4	7	NULL	NULL	6		160
4	8	NULL	NULL	7		522
4	9	NULL	NULL	8		622



Console Application Testing

- Individual Component/Unit Testing
- Local Testing- Server simulators
 - Local IIS system
 - Python scripts
- Acceptance Testing- Client test server



Console Application Demo

The image displays two side-by-side Jupyter Notebook windows. Both windows are titled 'ServerSimulator - Jupyter Note...' and show a Python script being executed. The left window, titled 'ServerSimulator', shows the script reading from 'sample_log.log' and writing to 'dynamic.log', outputting 'Added entry from simulated site #1'. The right window, titled 'ServerSimulator(2)', shows the script reading from 'sample_log2.log' and writing to 'dynamic.log', outputting 'Added entry from simulated site #2'. Both scripts include a sleep function to simulate a delay between entries.

```
In [*]: ##author brfed
#This is an application that I am writing to test the console application.
#A server's actions on a Log file by constantly adding lines to a sample Log
#test the console application's ability constantly read a dynamic log file at
#the Azure database.

import time

filepath = "C:/Users/brfed/Desktop/sample_log.log"
with open(filepath) as f:
    line = f.readline()
    while line:
        time.sleep(1)

        f2 = open("C:/Users/brfed/Desktop/LogFolder/W3SVC1/dynamic.log", "a")
        f2.write(line)
        print("Added entry from simulated site #1")
        f2.close()

    line = f.readline()
```

```
In [*]: ##author brfed
#This is an application that I am writing to test the console application.
#A server's actions on a Log file by constantly adding lines to a sample Log
#test the console application's ability constantly read a dynamic log file at
#the Azure database.

import time

filepath = "C:/Users/brfed/Desktop/sample_log2.log"
with open(filepath) as f:
    line = f.readline()
    while line:
        time.sleep(0.5)

        f2 = open("C:/Users/brfed/Desktop/LogFolder/W3SVC2/dynamic.log", "a")
        f2.write(line)
        print("Added entry from simulated site #2")
        f2.close()

    line = f.readline()
```



Web Application

- Consolidated data location
- Simple Visualization of data
- Easy to filter
- Easy to access

```
2021-01-15 21:02:43 10.9.0.4 GET / - 443 - 162.158.183.129 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:43 10.9.0.4 GET / - 443 - 162.158.183.129 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:43 10.9.0.4 GET / - 443 - 172.68.182.112 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:44 10.9.0.4 GET / - 443 - 162.158.183.171 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:44 10.9.0.4 GET /WebResource.axd d=pynGkmcFUV13He1Qd6_TZA0z0kmeEwjDQsqtYn1FY60uR85
2021-01-15 21:02:43 10.9.0.4 GET / - 443 - 172.68.182.112 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:44 10.9.0.4 GET /BVModules/Themes/RemedyNails2019/styles/css v=Y4BVW58F-Q61UqQZep4Ly
2021-01-15 21:02:44 10.9.0.4 GET /WebResource.axd d=pynGkmcFUV13He1Qd6_TZA0z0kmeEwjDQsqtYn1FY60uR85
2021-01-15 21:02:44 10.9.0.4 GET /WebResource.axd d=3aje5EVz5a65qlRd-GY67ml5G15QqTXDivCutK-eFlpemeb5M
2021-01-15 21:02:44 10.9.0.4 GET /BVModules/Themes/RemedyNails2019/styles/css v=Y4BVW58F-Q61UqQZep4Ly
2021-01-15 21:02:44 10.9.0.4 GET /BVModules/Themes/RemedyNails2019/styles/css v=Y4BVW58F-Q61UqQZep4Ly
2021-01-15 21:02:44 10.9.0.4 POST / - 443 - 162.158.183.171 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:45 10.9.0.4 GET /WebResource.axd d=pynGkmcFUV13He1Qd6_TZA0z0kmeEwjDQsqtYn1FY60uR85
2021-01-15 21:02:45 10.9.0.4 GET /WebResource.axd d=s2nkrMjGXkMELz33nwnakJfnTg8aTy80cdnNSbvF-kQasKBH
2021-01-15 21:02:45 10.9.0.4 GET /WebResource.axd d=3aje5EVz5a65qlRd-GY67ml5G15QqTXDivCutK-eFlpemeb5M
2021-01-15 21:02:45 10.9.0.4 GET /WebResource.axd d=3aje5EVz5a65qlRd-GY67ml5G15QqTXDivCutK-eFlpemeb5M
2021-01-15 21:02:45 10.9.0.4 GET / - 443 - 162.158.183.159 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:45 10.9.0.4 GET / - 443 - 162.158.183.159 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:45 10.9.0.4 GET / - 443 - 162.158.183.139 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:45 10.9.0.4 GET / - 443 - 172.68.182.112 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:45 10.9.0.4 GET /WebResource.axd d=x2nkrMjGXkMELz33nwnakJfnTg8aTy80cdnNSbvF-kQasKBH
2021-01-15 21:02:45 10.9.0.4 GET / - 443 - 172.68.182.112 Mozilla/5.0+(Windows;+U;+Windows+NT+5.2;+en-US;+rv:52.0) Gecko/20100801 Firefox/35.0
2021-01-15 21:02:45 10.9.0.4 GET /WebResource.axd d=3aje5EVz5a65qlRd-GY67ml5G15QqTXDivCutK-eFlpemeb5M
2021-01-15 21:02:45 10.9.0.4 GET /BVModules/Themes/RemedyNails2019/styles/css v=Y4BVW58F-Q61UqQZep4Ly
```

Drag a column header and drop it here to group by that column

date_time	site_name	site_url	connecting_ip	s_ip	url_stem
2/21/2021 11:59:55 PM	DrakeNation	https://www.drakenation.com/	2604.2d80.e083.4d00.20d5.d2c.1223.e141	10.9.1.4	/WebServices/Utilities.asmx?ParseF
2/21/2021 11:59:55 PM	DrakeNation	https://www.drakenation.com/	2601.200.4100.1eb0.c4e8.1c36.59b4.6371	10.9.1.4	/WebServices/WhosOn.asmx?js
2/21/2021 11:59:55 PM	DrakeNation	https://www.drakenation.com/	2601.200.4100.1eb0.c4e8.1c36.59b4.6371	10.9.1.4	/WebServices/Topics.asmx?js
2/21/2021 11:59:55 PM	DrakeNation	https://www.drakenation.com/	2601.200.4100.1eb0.c4e8.1c36.59b4.6371	10.9.1.4	/WebServices/Users.asmx?js
2/21/2021 11:59:55 PM	DrakeNation	https://www.drakenation.com/	75.162.182.162	10.9.1.4	/WebServices/Topics.asmx?js
2/21/2021 11:59:55 PM	DrakeNation	https://www.drakenation.com/	75.162.182.162	10.9.1.4	/WebServices/WhosOn.asmx?js
2/21/2021 11:59:55 PM	DrakeNation	https://www.drakenation.com/	75.162.182.162	10.9.1.4	/WebServices/Users.asmx?js
2/21/2021 11:59:57 PM	DrakeNation	https://www.drakenation.com/	2600.1014.b106.c78a.c935.3364.e7.d818	10.9.1.4	/WebServices/Users.asmx?js



Static Database Scanning

- .Net Core Program That Periodically Scans
- Looks for Attacks
- Scans for Flooding, SQL Injection, OS, and Authentication attacks



Database Scanner Testing

- ⬡ Isolation
- ⬡ Interface
- ⬡ Acceptance



Database Scanner Demo

The screenshot displays Microsoft SQL Server Management Studio (SSMS) with a query window open. The query is a T-SQL script for a SelectTopNRows command, which scans a table for various system properties. The results pane shows a list of 16 rows, each representing a scan of a specific date-time value across various system properties.

```
SELECT TOP (1000) [date-time]
, [universal-site-id]
, [c-ip]
, [s-sitename]
, [s-computername]
, [s-ip]
, [s-port]
, [cs-method]
, [cs-uri-stem]
, [cs-uri-query]
, [sc-status]
, [sc-substatus]
, [sc-win32-status]
, [sc-bytes]
, [cs-bytes]
, [time-taken]
, [cs-version]
, [cs(User-Agent)]
```

date-time	universal-site-id	c-ip	s-sitename	s-computername	s-ip	s-port	cs-method	cs-uri-stem	cs-uri-query	sc-status	sc-substatus	sc-win32-status	sc-bytes	cs-bytes	time-taken	cs-version	cs(User-Agent)
2021-04-24 02:51:48.000	3	162.158.74.218	NULL	NULL	10.9.1.4	443	GET	/ShowMessage	-	404	0	2	NULL	0	0	0	
2021-04-24 02:51:48.000	3	172.68.34.145	NULL	NULL	10.9.1.4	443	POST	/WebServices/Topics.aspx/SelectTopicsPag	-	200	0	0	NULL	0	0	0	
2021-04-24 02:51:47.000	3	172.69.63.16	NULL	NULL	10.9.1.4	443	POST	/WebServices/Topics.aspx/SelectTopicsPag	-	200	0	0	NULL	0	0	0	
2021-04-24 02:51:46.000	3	172.68.34.145	NULL	NULL	10.9.1.4	443	GET	/WebServices/Users.aspx	-	304	0	0	NULL	0	0	0	
2021-04-24 02:51:46.000	3	172.68.34.145	NULL	NULL	10.9.1.4	443	GET	/WebServices/Topics.aspx	TopicID=136461&PageIndex=11	304	0	0	NULL	0	0	0	
2021-04-24 02:51:46.000	3	172.68.34.145	NULL	NULL	10.9.1.4	443	GET	/WebServices/WhoOn.aspx	-	304	0	0	NULL	0	0	0	
2021-04-24 02:51:46.000	3	172.69.63.16	NULL	NULL	10.9.1.4	443	GET	/WebServices/Topics.aspx	-	304	0	0	NULL	0	0	0	
2021-04-24 02:51:46.000	3	172.69.63.16	NULL	NULL	10.9.1.4	443	GET	/WebServices/WhoOn.aspx	-	304	0	0	NULL	0	0	0	
2021-04-24 02:51:46.000	3	172.69.63.16	NULL	NULL	10.9.1.4	443	GET	/WebServices/Users.aspx	-	304	0	0	NULL	0	0	0	
2021-04-24 02:51:43.000	3	172.69.63.16	NULL	NULL	10.9.1.4	443	GET	/ShowMessage.aspx	TopicID=152522&PageIndex=2	200	0	0	NULL	0	0	0	
2021-04-24 02:51:43.000	3	172.68.34.215	NULL	NULL	10.9.1.4	443	POST	/WebServices/Topics.aspx/SelectTopicPag	-	200	0	0	NULL	0	0	0	
2021-04-24 02:51:43.000	3	172.68.34.215	NULL	NULL	10.9.1.4	443	POST	/WebServices/Topics.aspx/SelectTopicPag	-	200	0	0	NULL	0	0	0	
2021-04-24 02:51:43.000	3	172.68.34.215	NULL	NULL	10.9.1.4	443	GET	/WebServices/WhoOn.aspx	-	304	0	0	NULL	0	0	0	
2021-04-24 02:51:43.000	3	172.68.34.215	NULL	NULL	10.9.1.4	443	GET	/WebServices/WhoOn.aspx	-	304	0	0	NULL	0	0	0	
2021-04-24 02:51:43.000	3	172.68.34.215	NULL	NULL	10.9.1.4	443	GET	/WebServices/Users.aspx	-	304	0	0	NULL	0	0	0	

Query executed successfully. cyseniordesign.database.win... sdmaydev1 (62) sdmay21-16 00:00:00 1,000 rows



Technical Challenges



Presented by: Presiiian Iskrenov



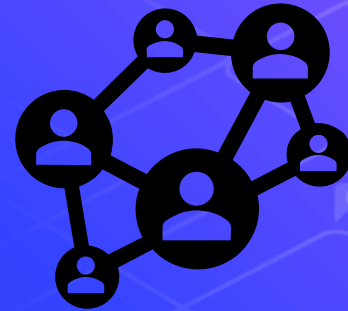
Console Application

- Originally written in Python
- Rewritten in C# using .NET
- Error log failed database connection
- Resume scanning after crash
- Truncating data silently
- Decoding special characters



Web Application

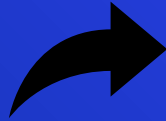
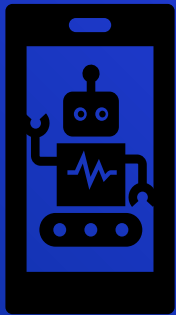
- Connecting to UIs
 - Telerik
 - Kendo ASP.NET MVC UI
- Auto-refresh
- Large data requests



Switch to Scanner

AI

- Had limited training data
- Inexperienced
- Solution



Engineering Requirements

- Functional
- Non-Functional



Presenting: Giovanni Mejia



Functional Requirements

- Microsoft ISS generating text-based log files per web request
- Console-based Application, created to find the log file for what site is being monitored
- Database scanning application, created to monitor the log files and identify any suspicious web activity with Cloud-Flare API



Non-Functional Requirements

- Scalability of the system
- Accommodation of high volumes of web traffic
- Restricted access to approved users and rightfully blocking suspicious traffic when identified.



Engineering Standards

- ⬡ IEEE 1028-1997 Standard for Software Unit Testing
 - Specific Unit Testing procedures/requirements
- ⬡ IEEE 12207-2017 Software Life Cycle Process
 - Process employed for controlling and improving software life
- ⬡ IEEE 16326-2009 Project Management
 - Specifications for project management in terms of preparation for project plans



Engineering Constraints

- ⬡ Covid
- ⬡ Team Size
- ⬡ Legal Obligations
- ⬡ Time Constraints
- ⬡ Acceptance Testing



Presenting: Jordan Heim



Team Members



Ryan Burgett
Software Engineering
Scanning Team



Presiiian Iskrenov
Software Engineering
Scanning Team



Giovanni Mejia
Computer Engineering
Scanning Team



Jordan Heim
Cyber Security Engineering
Scanning Team



Eric Reuss
Software Engineering
Scanning Team



Ben Feddersen
Software Engineering
Web App Team

Presenting: Jordan Heim



Thanks!

Any questions?

Email Us At:

sdmay21-16@iastate.edu



Credits

Special thanks to all the people who made and released these awesome resources for free:

- ⬡ Presentation template by [SlidesCarnival](#)
- ⬡ Photographs by [Unsplash](#)