Cybersecurity

Project 1 Technical Brief

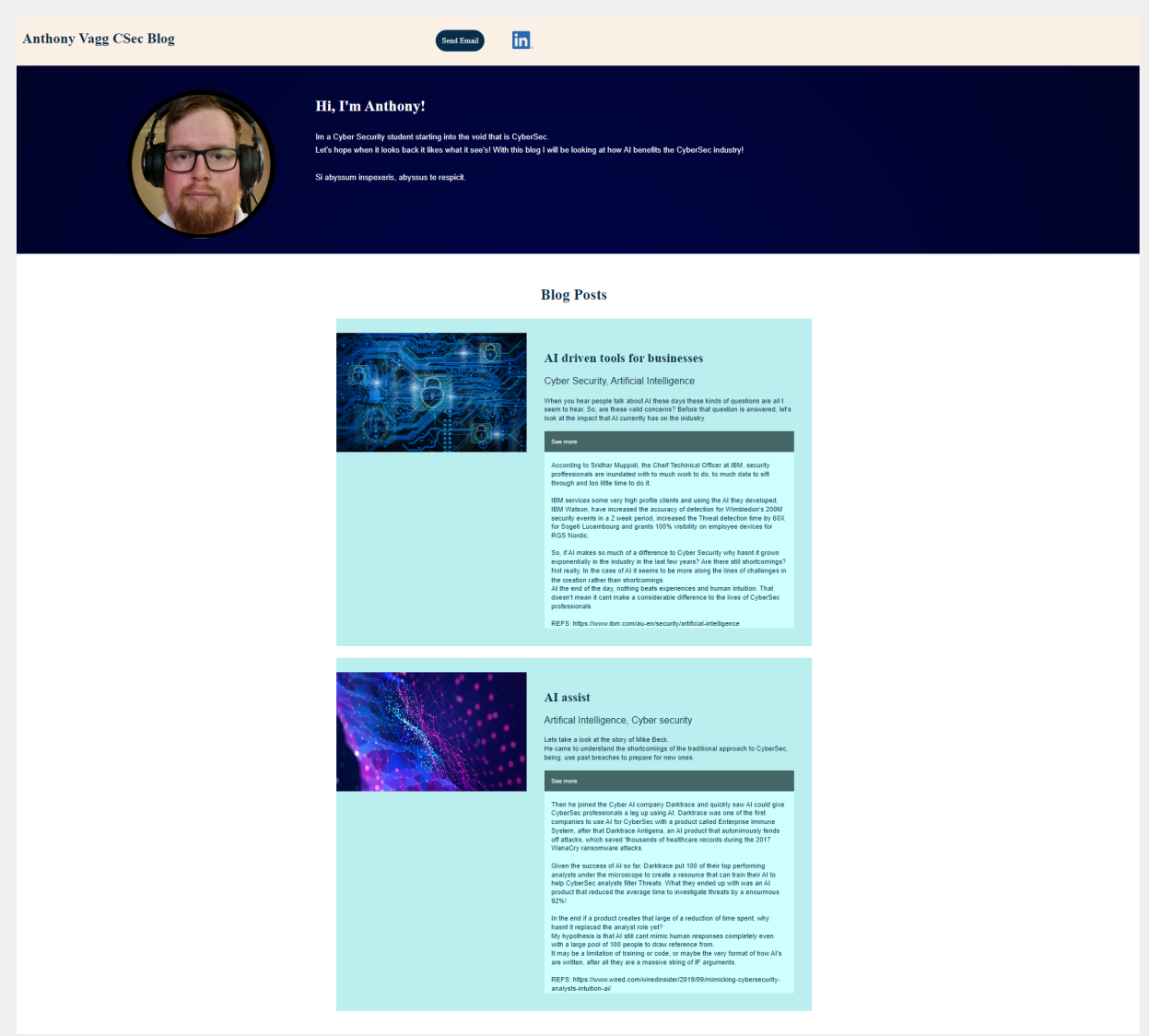
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://csecblog.azurewebsites.net/
```

Paste screenshots of your website created (Be sure to include your blog posts):



Day 1 Questions

General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

```
Azure free domain
```

2. What is your domain name?

```
CSecBlog.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.13
```

2. What is the location (city, state, country) of your IP address?

```
Sydney, NSW, Australia
```

3. Run a DNS lookup on your website. What does the NS record show?

```
C:\Users\Kalic>nslookup -type=ns csecblog.azurewebsites.net
Server:  resolv.on.ii.net
Address:  2001:44b8:1::1

Non-authoritative answer:
csecblog.azurewebsites.net      canonical name = waws-prod-sy3-091.sip.azurewebsites.windows.net
waws-prod-sy3-091.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-091-a15c.australiaeast.cloudapp.azure.com


australiaeast.cloudapp.azure.com
        primary name server = ns1-06.azure-dns.com
        responsible mail addr = msnhst.microsoft.com
        serial  = 10001
        refresh = 900 (15 mins)
        retry   = 300 (5 mins)
        expire  = 604800 (7 days)
        default TTL = 60 (1 min)
```

Web Development Questions

1. When creating your web app, you selected a runtime stack. What was it? Does it work on the front end or the back end?

```
As PHP 8.2 was the selected option it would be back end as PHP is a server
-side scripting language.
```

2. Inside the `/var/www/html` directory, there was another directory called assets. Explain what was inside that directory.

```
The assets dir contains all of the images and style settings (style.css) for the default html.
It can vary depending on build so may include javascript and different CSS as well.
```

3. Consider your response to the above question. Does this work with the front end or back end?

```
These files work on the front end as they are client-side assets required by the web application.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is an isolated virtual environment within cloud infrastructure to which resources are allocated on an as needed basis.
Being completely isolated from other “tenants” it is good for security and is scalable.
```

2. Why would an access policy be important on a key vault?

```
Access policy allows you to set duty specific access and role assignments, fulfilling need to access requirements for good security practices as well as limiting points of failure due to limiting who has access to the key vault, thus mitigating risk.
Furthermore it can give you a trial to audit in the event of a breach and there may be a compliance requirement depending on what data is being stored.
```

3. Within the key vault, what are the differences between keys, secrets, and certificates?

```
Keys are required for encryption and decryption.
Secrets is a broad classification for, well, secrets. Could be API keys, passwords, cryptographic keys, etc.
```

```
Certificates are the digital documents that are used to establish trust and verify the users identity or the application or device.
Or in a web sense if a website is a legitimate website and not one made to look like your bank, hoping you won't notice and enter your login information. Before that event takes place the browser should alert you that the page is suspicious and may be lying about what it is.
```

Cryptography Questions

1. What are the advantages of a self-signed certificate?

```
Self signed Certificates are an easy, cost effective method of certification internally in an organization, used for encryption or testing purposes, or both.
It can be used outside of an organization but… see question 2 below.
```

2. What are the disadvantages of a self-signed certificate?

```
The certificate will not have the same effectiveness as a certificate signed by a trusted CA as some browsers may not accept a self-signed certificate, causing an alert via the browser trying to redirect you away from the site or users AV blocking the site.
While it can be used privately/internally it would be difficult to use a self-signed certificate if you were wanting to host a website open to the public.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a cert that allows you to certify the main domain and any sub domains using the same name. E.g Example.com, mail.example.com and blog.example.com or say csecblog.azurewebsites.net
```

4. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn't provided.

```
TLS 1.* is the successor to SSL as SSL 3.0 had a fatal vulnerability that was not fixable. By not providing it they are protecting their customers from known vulnerabilities and ensuring their websites stay secure with up to date encryption protocols.
```

5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

    a. Is your browser returning an error for your SSL certificate? Why or why not?

```
No as it already has a signed certificate as I am using the azure free
domain.
```

    b. What is the validity of your certificate (date range)?

```
360 days 28/12/22 - 23/12/23
```

    c. Do you have an intermediate certificate? If so, what is it?

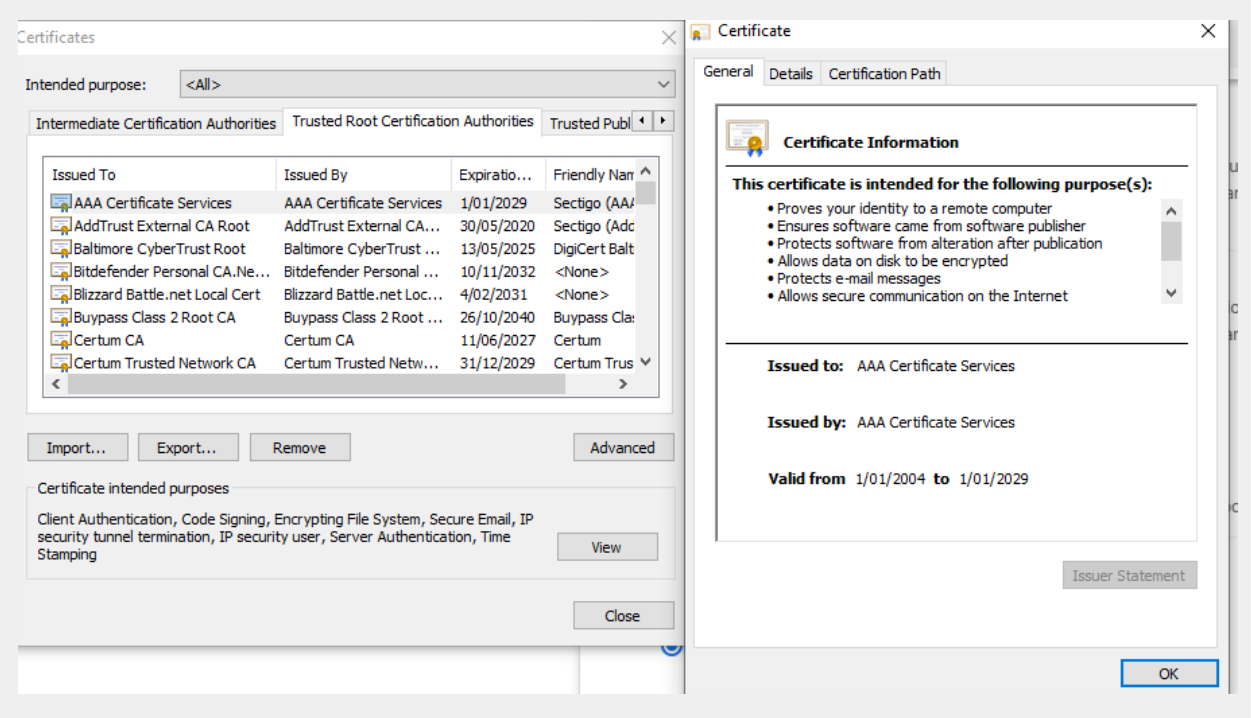
```
Yes, Microsoft Azure TLS Issuing CA 05 is the intermediate cert issued by
azure's own CA which is signed by the DigiCert Global Root cert.
This allows Azure to sign its own certificates for individual
servers/webapps streamlining their service.
```

    d. Do you have a root certificate? If so, what is it?

```
Yes. The root certificate is a DigiCert Global Root G2 and is self-signed
and in the trust store also known as a root store. A root store is a
collection of pre downloaded certificates and associated public keys that is
kept on the device itself. In my case it would be Bitdefender's root store
rewriting Microsoft's root store.
These root stores are generally made up of certificates signed directly by a
CA as it allows browsers to automatically trust websites using certificates
signed by certificates in the root store.
```

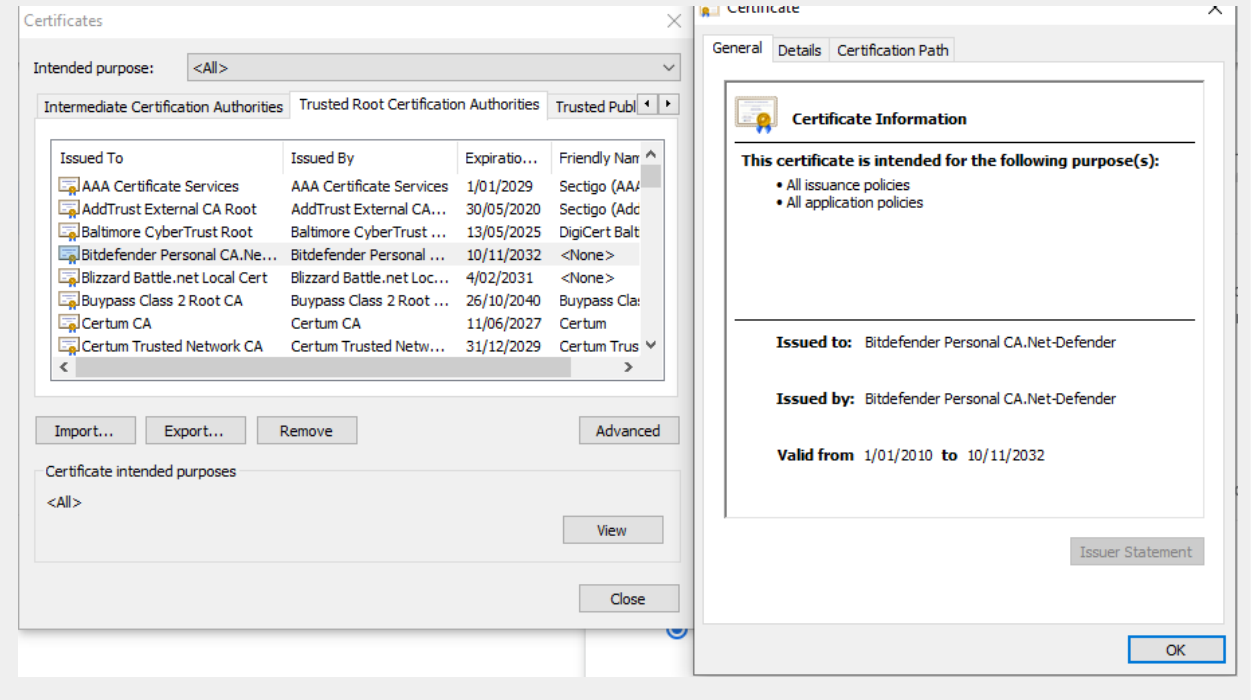
    e. Does your browser have the root certificate in its root store?

```
Yes, for example AAA certificate services issued by themselves valid until
1/1/2029
```



f. List one other root CA in your browser's root store.

Bitdefender Personal CA.Net-Defender issued also by themselves valid until 11/10/2023



Day 3 Questions

Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?

```
Both are very similar in what they do and both run on layer 7 however Web
Application Gateways are regional where-as Front Door is global.
The WAF is deployed differently, Front door deploys at edge locations and
App Gateway is deployed as a filter when entering the VNET via App Gateway.
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq
https://learn.microsoft.com/en-us/answers/questions/301218/azure-waf-frontdo
or-vs-azure-waf-application-gatew
```

2. A feature of the Web Application Gateway and Front Door is “SSL Offloading.” What is SSL offloading? What are its benefits?

```
SSL offloading is where the decryption of traffic sent via SSL connections
is moved to a dedicated server for processing to reduce the strain on the
web servers and free up resources as the process is rather resource
intensive
```

3. What OSI layer does a WAF work on?

```
The WAF works on Layer 7 and according to cloudflare “is not designed to
defend against all types of attacks. This method of attack mitigation is
usually part of a suite of tools which together create a holistic defense
against a range of attack vectors.”
https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-w
af/
```

4. Select one of the WAF managed rules (e.g., directory traversal, SQL injection, etc.), and define it.

```
Rule 941101 XSS attack detected via Libinjection
CCS is a web vulnerability that allows an attacker to inject malicious
code/scripts into a webpage. The scripts can range from stealing sensitive
info, controlling the browser/hijacking user sessions.
```

The Libinjection is a library that is used to detect/prevent SQL injections and XSS attacks by analyzing input data and detecting patterns that could indicate an attack.
So this rule means that Libinjection has identified a malicious input that could be used to inject scripts into the webpage and can be indicative of an attack or attempt at exploiting a vulnerability.

5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn't enabled? Why or why not?

It's not good practice to say it's a 0% chance however from what I could find the impact would be minimal as the site is static and has no login credentials or potentially sensitive stored data.
In addition there is no where to input the initial script as there is no comment section or similar to actually submit data.

6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

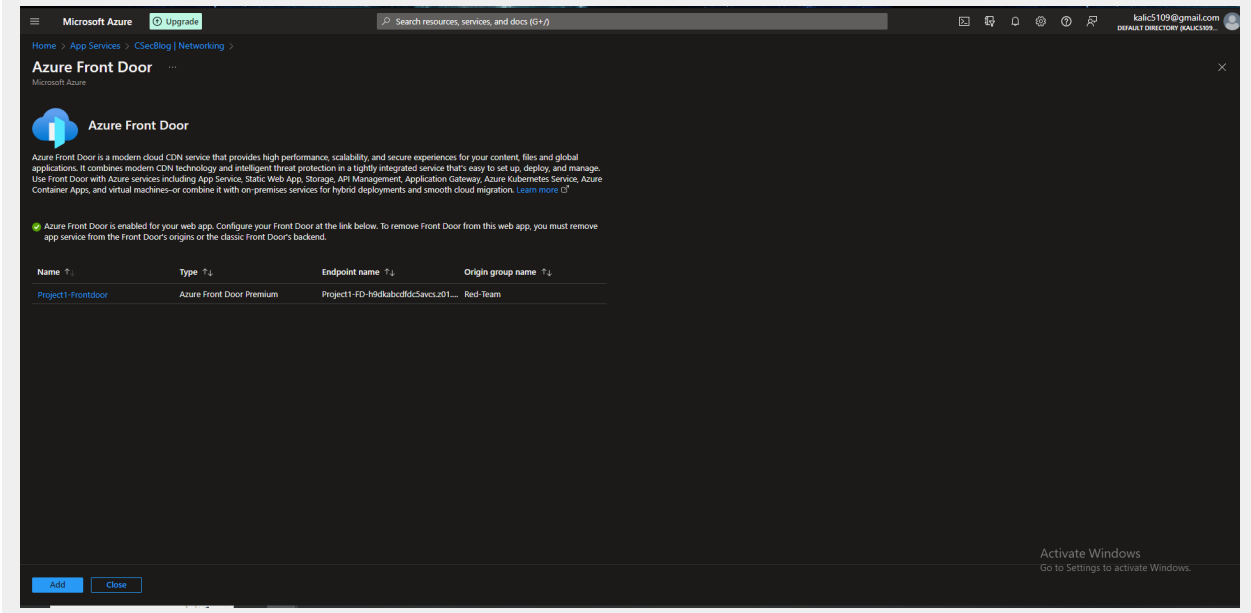
Yes it would block all traffic from Canada based IP's HOWEVER a VPN that is able to spoof the location (which is most if not all) would circumvent that rule as it would appear as if you were accessing from another country that is whitelisted.
This may also be fixed in Amazon Web Services by blocking anonymous IP addresses as per -

(https://aws.amazon.com/about-aws/whats-new/2020/03/aws-waf-adds-anonymous-ip-list-for-aws-managed-rules/)

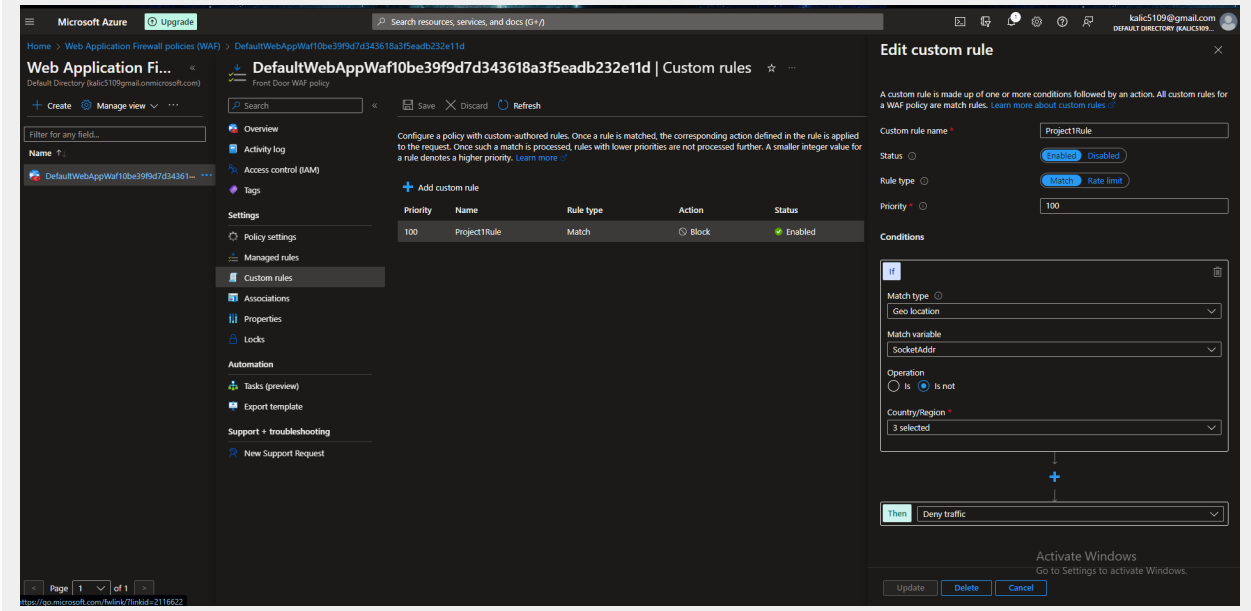
The geoblock may also be circumvented by attackers as they could have taken control of a machine that is outside the geoblocked location.

7. Include screenshots below to demonstrate that your web app has the following:

    a. Azure Front Door enabled



b. A WAF custom rule



Disclaimer on Future Charges

Please type “**YES**” after one of the following options:

- ***Maintaining website after project conclusion****: I am aware that I am responsible for any charges that I incur by maintaining my website. I have reviewed the guidance for minimizing costs and monitoring Azure charges.*

Yes

- ***Disabling website after project conclusion****: I am aware that I am responsible for deleting all of my project resources as soon as I have gathered all of my web application screen shots and completed this document.*

Yes

**No recommendations made by Microsoft Defender for Cloud made by the end of class so no security recommendations to change.

**Used code from w3schools.com in blog to create buttons
https://www.w3schools.com/howto/howto_js_collapsible.asp