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.

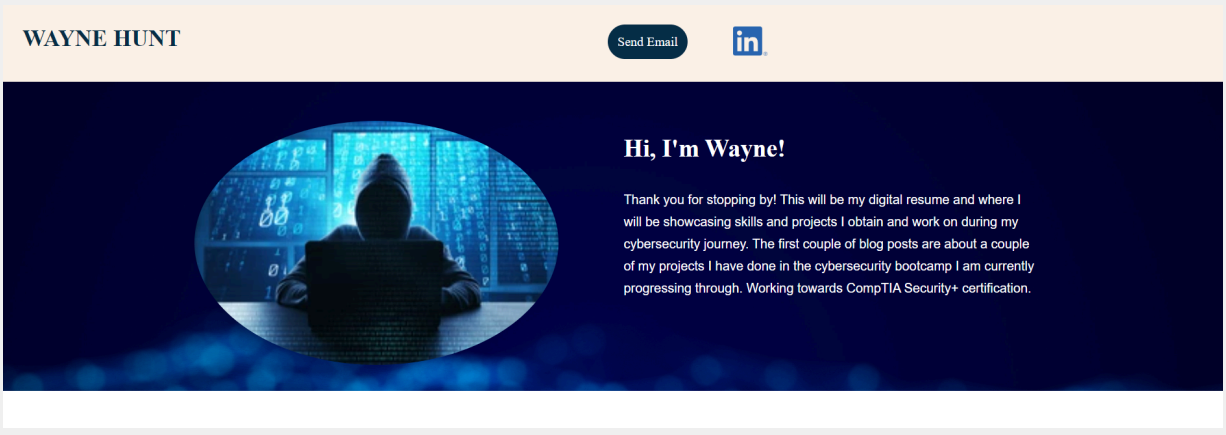
Your Web Application

Enter the URL for the web application that you created:

```
waynehunt.azurewebsites.net
```

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

```
These are screenshots from my web page.
```



Blog Posts

A Day in the Life of a Windows Sysadmin

sysadmin, windows, active directory group

This is a post for the Module 7 challenge in the UWA Cybersecurity Bootcamp we did. We needed to be a Windows System Administrator where we needed to set and create Group Policy Objects (GPO's) and create a script to enumerate Access Control Lists (ACL's) too! We used a virtual machine through Azure to work on a Windows 10 terminal and server. We used powershell logs to set policies and user permissions.

Lucky Duck Casino

security analyst, database management, evidence gathering

This is a project we did in Module 3 of the UWA Cybersecurity Bootcamp. We played the role of a security analyst, contracted to a casino, The Lucky Duck Casino. Our objective was to investigate large losses on some of the games on different dates and times. We needed to gather evidence of any dealers and players collaborating together to steal thousands of dollars from the casino. We analyzed lots of data provided by the casino. Such data as dealer rosters, player profiles, loss amounts with days and times. By running different scripts and analysis techniques, we were able to find out that there was a rogue dealer colluding with a player at the times the large losses occurred. We were able to identify that these two persons of interest had stolen over $100,000 in just a few days. All the evidence was handed over to the casino where they could take further action against the persons.

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?

```
WayneHunt
```

Networking Questions

1. What is the IP address of your webpage?

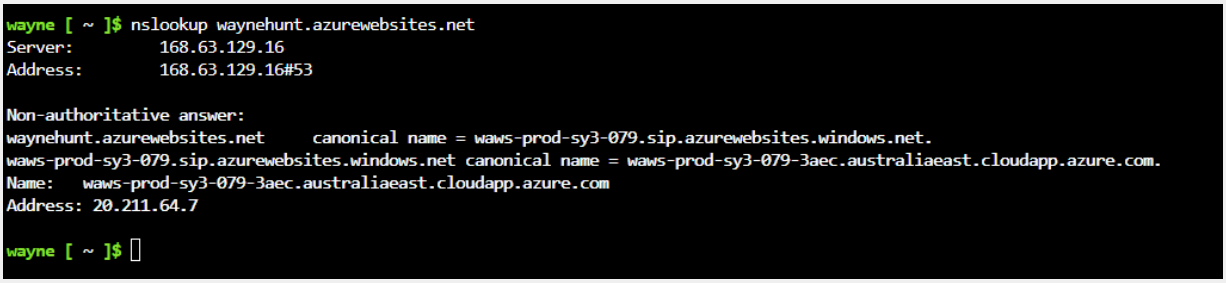
```
20.211.64.7
```

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

```
Redmond, Washington, United States
```

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

```
I ran the command line prompt: nslookup waynehunt.azurewebsites.net
Which displayed the below result.
The NS record tells the internet where to go to find out a domain's IP
address.
```



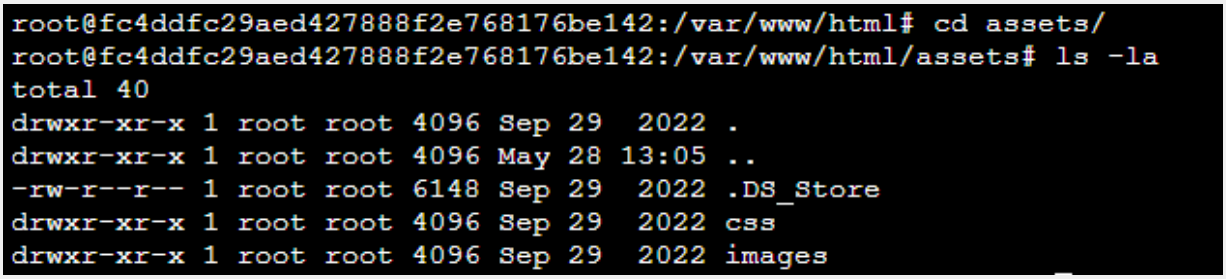
Web Development Questions

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?

```
PHP 8.2
Runs on the backend
```

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

```
Inside the assets directory, there is a css folder and an images folder.
This directory contains images and links for the website. The css folder
contains the style settings for the web page.
```



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

```
Front end
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
This is a customer account within a cloud environment
```

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

```
The access policy controls the keys, secrets and certificates
```

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

```
Keys: used for encryption
Secrets: store sensitive data
```

```
Certificates: verify identity to enable a secure connection and
communication.
```

Cryptography Questions

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

```
- No payment required for the signature
- Quick initiation.
- Unlimited certificate generation.
```

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

```
- Permanent “unknown publisher” warning could lead to lack of user
  trust.
- Data security not guaranteed
- Fail to display correctly if configured incorrectly.
```

3. What is a wildcard certificate?

```
A single certificate that contains the wildcard character * in the domain
name field. This allows for multiple sub domain names.
```

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.

```
SSL 3.0 isn’t provided because of how vulnerable it is. Attackers may
calculate the plaintext of encrypted connections, which is a huge flaw in
the design of the protocol. Google security researchers discovered this and
dubbed it the POODLE vulnerability. Therefore, TLS versions are more secure
and preferred by most organizations.
```

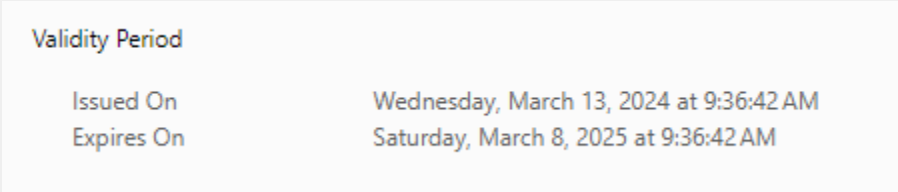
5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

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

No, because it is secured by an app service managed certificate from Azure.

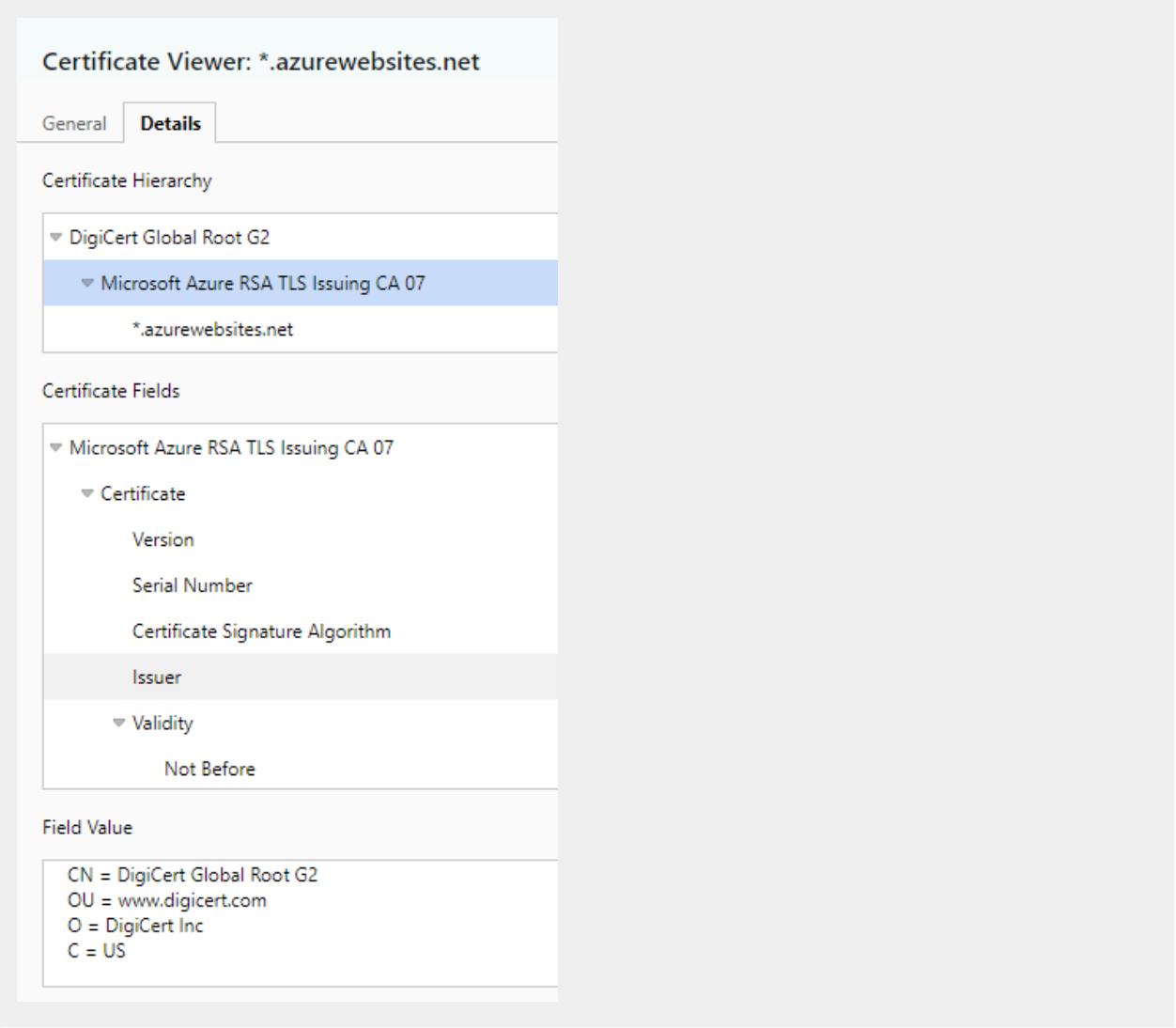
b. What is the validity of your certificate (date range)?

Issued on Wednesday March 13th 2024 at 09:36:42
Expires on Saturday March 8th 2025 at 09:36:42
So this makes the validity 360 days.



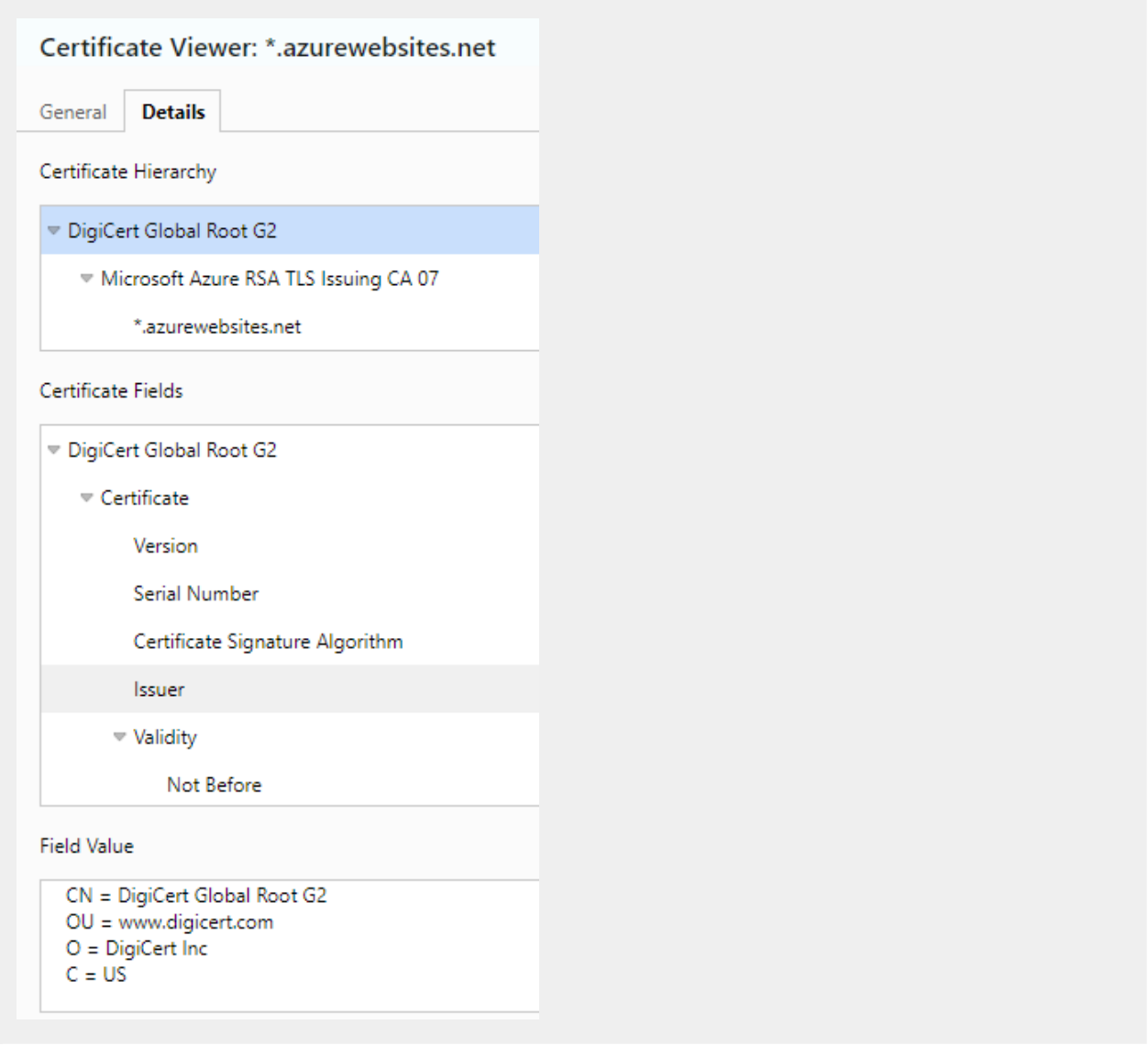
c. Do you have an intermediate certificate? If so, what is it?

Yes, there is an intermediate certificate. It is below the root certificate and named “Microsoft Azure RSA TLS issuing CA 07”. The Certificate Authorities (CA) issue an intermediate certificate with a private key which makes it trusted.



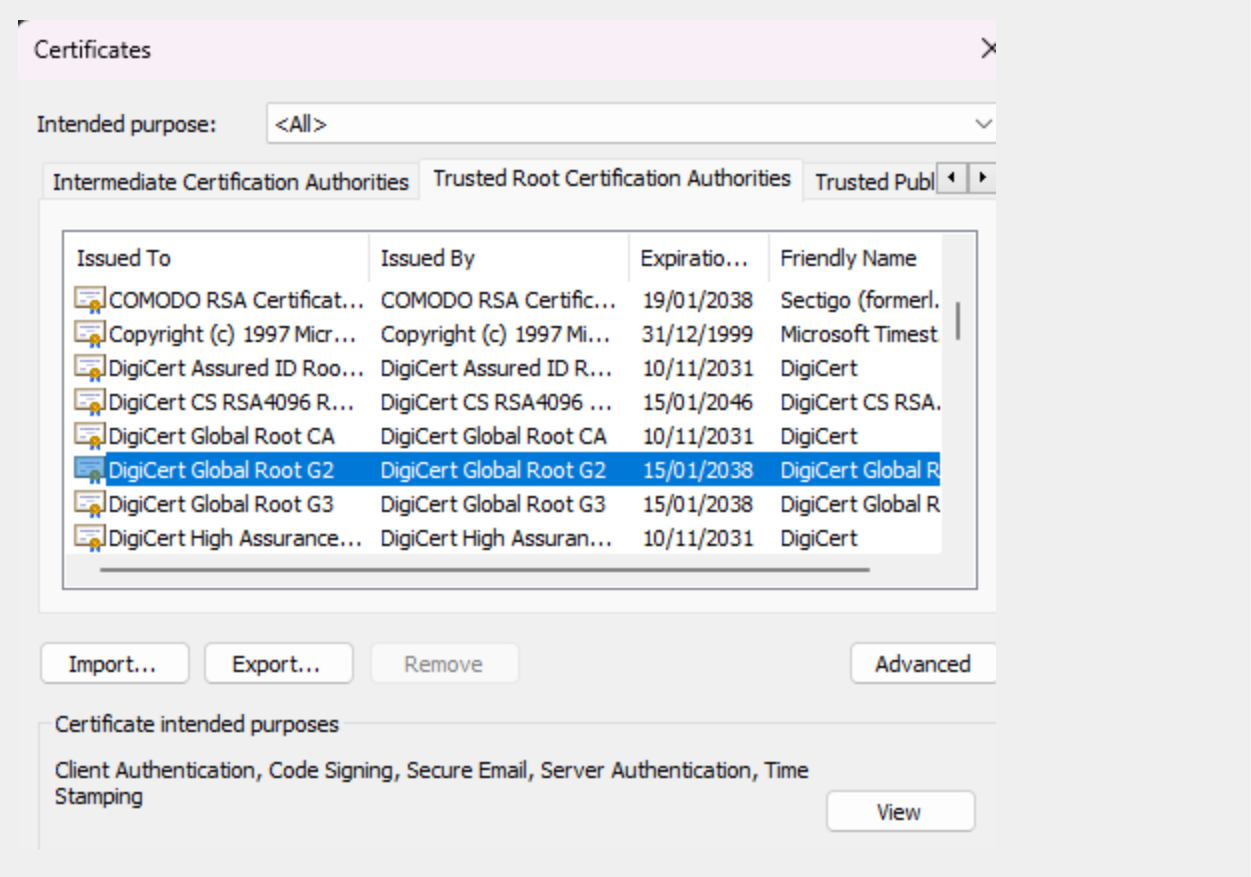
d. Do you have a root certificate? If so, what is it?

Yes, there is a root certificate. The root certificate is named “DigiCert Global Root G2”.
This is issued by a trusted Certificate Authority.



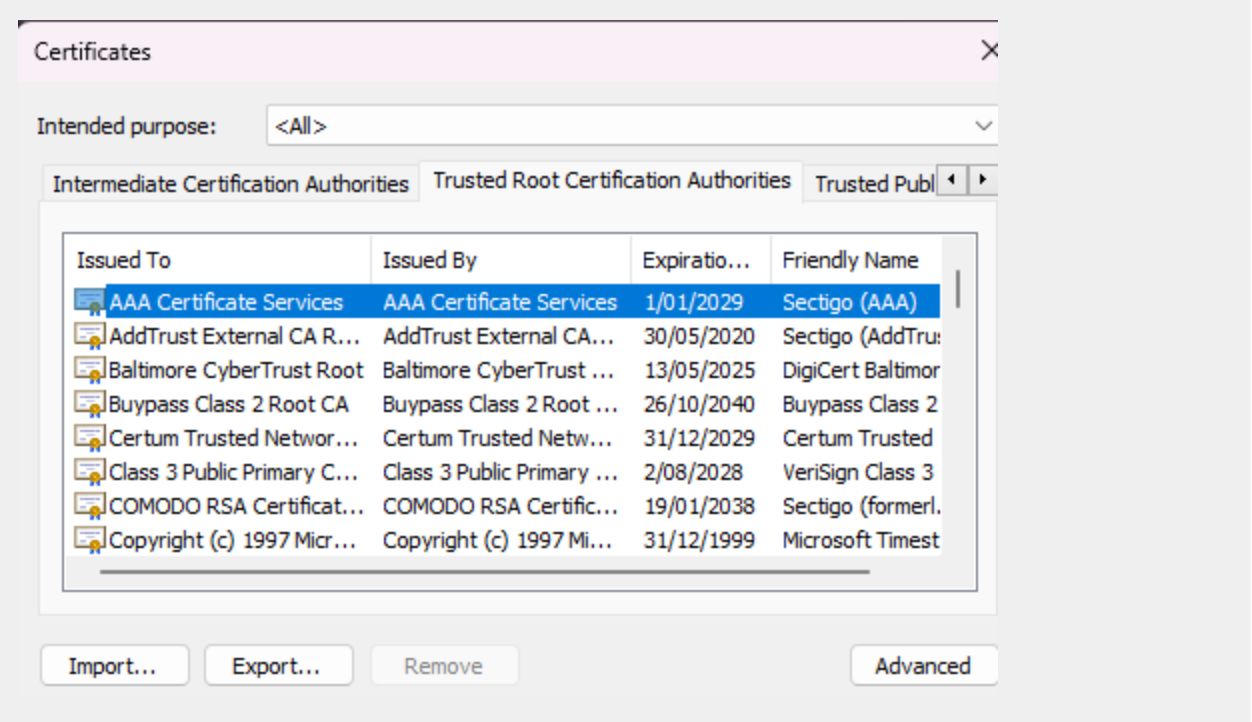
e. Does your browser have the root certificate in its root store?

```
Yes it does (DigiCert Global Root G2)
```



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

```
AAA Certificate Services
```



Day 3 Questions

Cloud Security Questions

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

```
The Azure Web Application Gateway is a regional service that balances
requests within a region.
The Azure Front Door is a global service that can distribute requests across
regions.
```

2. What is SSL offloading? What are its benefits?

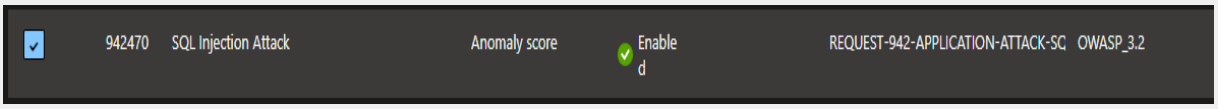
```
SSL offloading relieves the web server of data decryption. This results in
smooth website loading and faster processing of requests at the end of the
web application.
SSL offloading increases the performance and efficiency of the web server,
by offloading the data decryption from my application server to a separate
device.
```

3. What OSI layer does a WAF work on?

```
Layer 7 - Application
```

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

```
A SQL injection attack is a security exploit where an attacker inserts or
manipulates SQL queries in order to execute malicious SQL code. This allows
the attacker to bypass authentication, gain admin access, or
read/modify/delete data.
The Azure WAF managed rule detects and blocks common attempts by looking for
suspicious input patterns and query manipulations.
Below is screenshot of selected managed rule for SQL injection attacks.
```



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?

```
Yes, my website could be impacted by an SQL injection attack if Front Door
wasn't enabled. Without the WAF protective measures enabled, my website
would need to solely rely on its internal security measures to defend
against SQL injection attacks.
Without WAF my website is directly exposed to potential attackers who
exploit existing vulnerabilities.
```

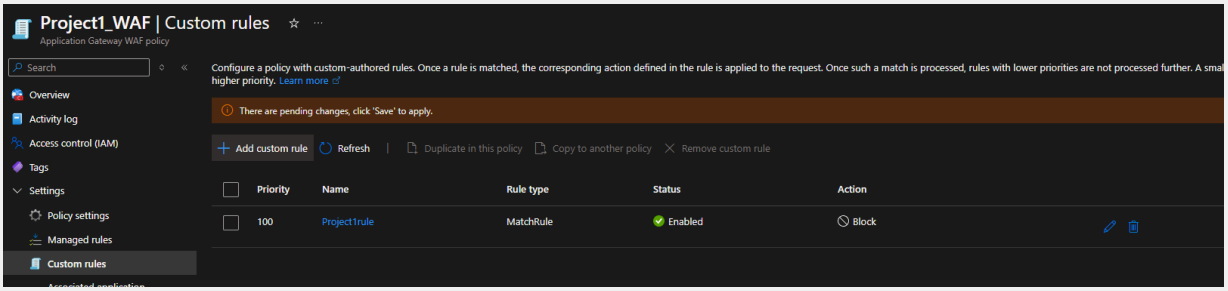
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

```
Creating a custom WAF rule to block all traffic from Canada, would mean that
anyone that resides in Canada would not be able to access my website. They
would be presented with an error message or a blocked access notification.
Basically, any IP address originating from Canada would be prevented from
accessing my website, due to the custom WAF rule geolocation setting.
Even if someone used a VPN, there is a good chance that the WAF would detect
```

```
and block traffic from known VPN and proxy ranges.
```

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

    a. 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.*

- ***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**