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:

yazminsecurityblog.azurewebsites.net

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

Blog Posts

Open-source vs Closed source. Which is more secure?

Zero-Day vulnerability,Open-Source,Closed-Source

Some examples of open-source software's are Mozilla Firefox, Linux, WordPress, etc. The main advantage of open-source software is that the source code is available for anyone to inspect it.It can be checked for any vulnerabilities from the large and active communities of users. This allows any suggested fixes or identified vulnerabilities to be fixed quickly. The contributions of the community are what makes open-source software to have the potential to become more secure. Now let's talk about closed source software. The code is not available for review to identify vulnerabilities. This means vulnerabilities may exist for many years before they are found which are also known as a zero-day vulnerability.People checking the code are employed by the company and are likely to have an in-depth knowledge of the product. Both open and close source software's come with vulnerabilities, the difference is not as significant and mostly comes down to various factors. How are organizations staying informed about security practices and what are they doing to protect user ^'^ys data.

Is 2 Factor Authentication enough?

Cryptography,Man in the Middle,VPN

Cryptocurrency is a digital currency that is secured by cryptography. You might be thinking this is a good way to protect currency, but attackers will still find a way to exploit that. In January 2022 Crypto.com was targeted and a small number of user had unauthorized crypto withdrawals on their accounts. The transactions were being approved without the 2fa authentication and this triggered a response from teams to assess the situation. Since cookies contain users' data and their activity i being tracked, hijacking them allows attackers to bypass 2FA easily. In Man in the Middle attacks, an attacker intercepts the communication between two systems. This method uses malware to extract user's sessions cookies and many more sensitive information. These attacks mostly occur on public Wi-Fi because the connection is less secure than a home or office network. Some ways to protect yourself from using public Wi-Fi is using your mobile data instead or using a VPN which masks your IP address by bouncing it though a private server. This doesn't fully protect you, but it will make it harder for an attacker to intercept and steal sensitive information. Always ensure you protect your data as much as you can an be sure to read the rest of my blogs to be aware of new techniques attackers will use and how to protect from them.

Day 1 Questions

General Questions

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

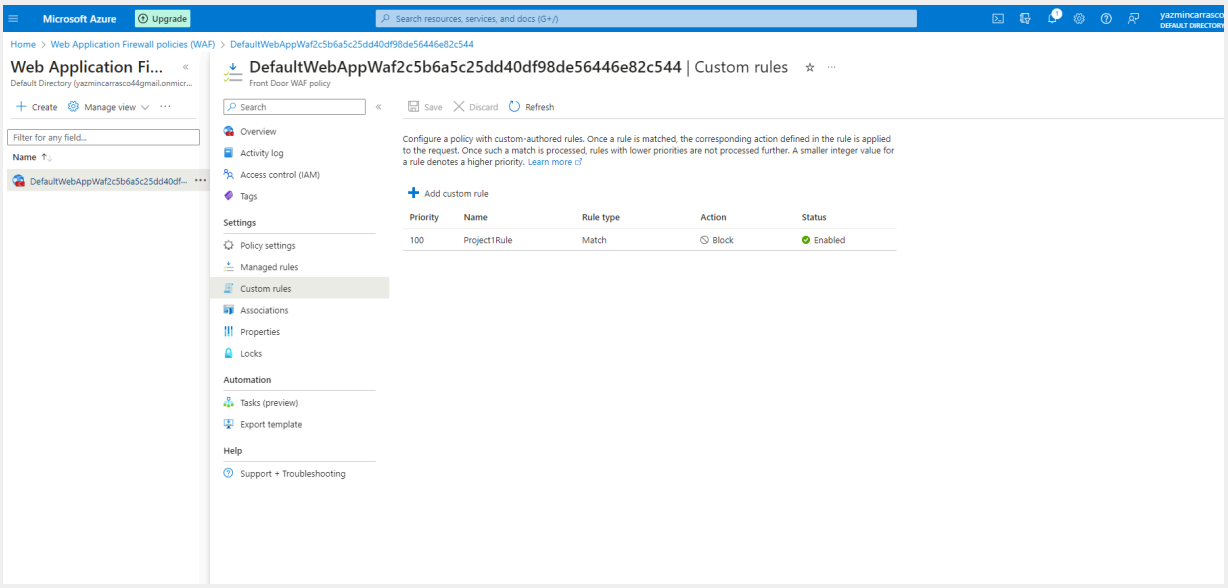
```
Azure free domain
```

2. What is your domain name?

```
yazminsecurityblog
```

Networking Questions

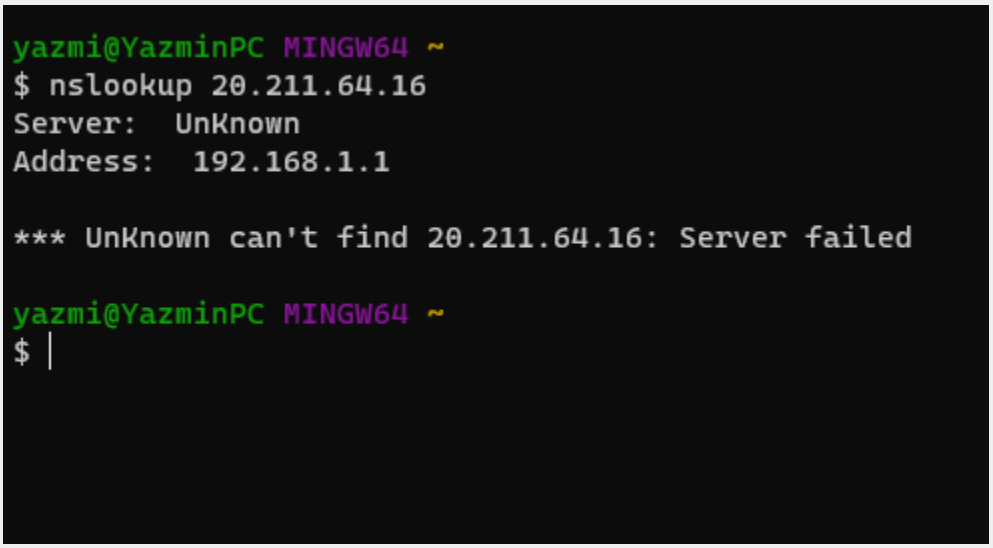
1. What is the IP address of your webpage?



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

```
City: Sydney
State/Region: New South Wales
Country: Australia
```

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



When I do a DNS lookup this is what the ns records show.I didn't run it before setting up the firewall so I don't know if that has anything to do with it.
I ran a DNS lookup for the parent domain azurewebsites.com instead

NS records

Name server	Revalidate in
ns1-224.azure-dns.com.	5m
ns2-224.azure-dns.net.	5m
ns3-224.azure-dns.org.	5m
ns4-224.azure-dns.info.	5m

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

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

There are css and images files in there. If we wanted to change an image of the linkedin I can change it there.

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?

```
Cloud service providers offer a range of services such as IaaS, PaaS, SaaS. A tenant refers to an individual or organization that uses the services provided by a cloud computing provider without having to invest or maintain their own physical infrastructure. A tenant rents or subscribes to the services offered by the cloud service provider.
```

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

```
It is important because an access policy allows you to control who can perform various operations within the key vault. Since the vault has passwords and sensitive information we want to make sure only administrators and people you trust have access to that key vault.
```

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

- Keys are used for encryption and decryption. There is two types, Symmetric encryption involves using a single key to encrypt and decrypt data, while asymmetric encryption uses two keys - one public and one private - to encrypt and decrypt data
- Secrets are sensitive pieces of information you want to tightly control access to such as API keys, passwords or certificates.Secrets are used to authenticate and access various services such as databases.
- Certificates are built on top of keys and secrets . Certificates contain a public key and information about its owner. They are used for authentication and to

establish a secure connection through SSL .

Cryptography Questions

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

```
Some advantages are:
Having a quick and easy set up
Developers can test secure communication without needed a commercial
certificate
Self signed certificates are free so this helps if someone is on a budget.
It still provides encryption for communication
```

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

```
Some disadvantages are:
They are not automatically trusted by web browser or operating systems,and
can encounter browser warnings which leads to lack of trust
Are more susceptible to man in the middle attacks.
```

3. What is a wildcard certificate?

```
A wildcard certificate is designed to secure a domain and its subdomain with
a single certificate. In the domain field there is an asterisk that serves
as a placeholder for any subdomain.This is useful when there are multiple
subdomains that need to be secure
```

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 is an outdated and insecure version of the SSL protocols and is
known to have security vulnerabilities. One is the POODLE vulnerability that
allows attackers to decrypt data encrypted with SSL 3.0.
```

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, when I go to our project website there is no error because I
successfully added a certificate to my website.
```

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

```
Issued On
Tuesday, October 31, 2023 at 5:15:02 PM
Expires On
Thursday, June 27, 2024 at 5:59:59 PM
```

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

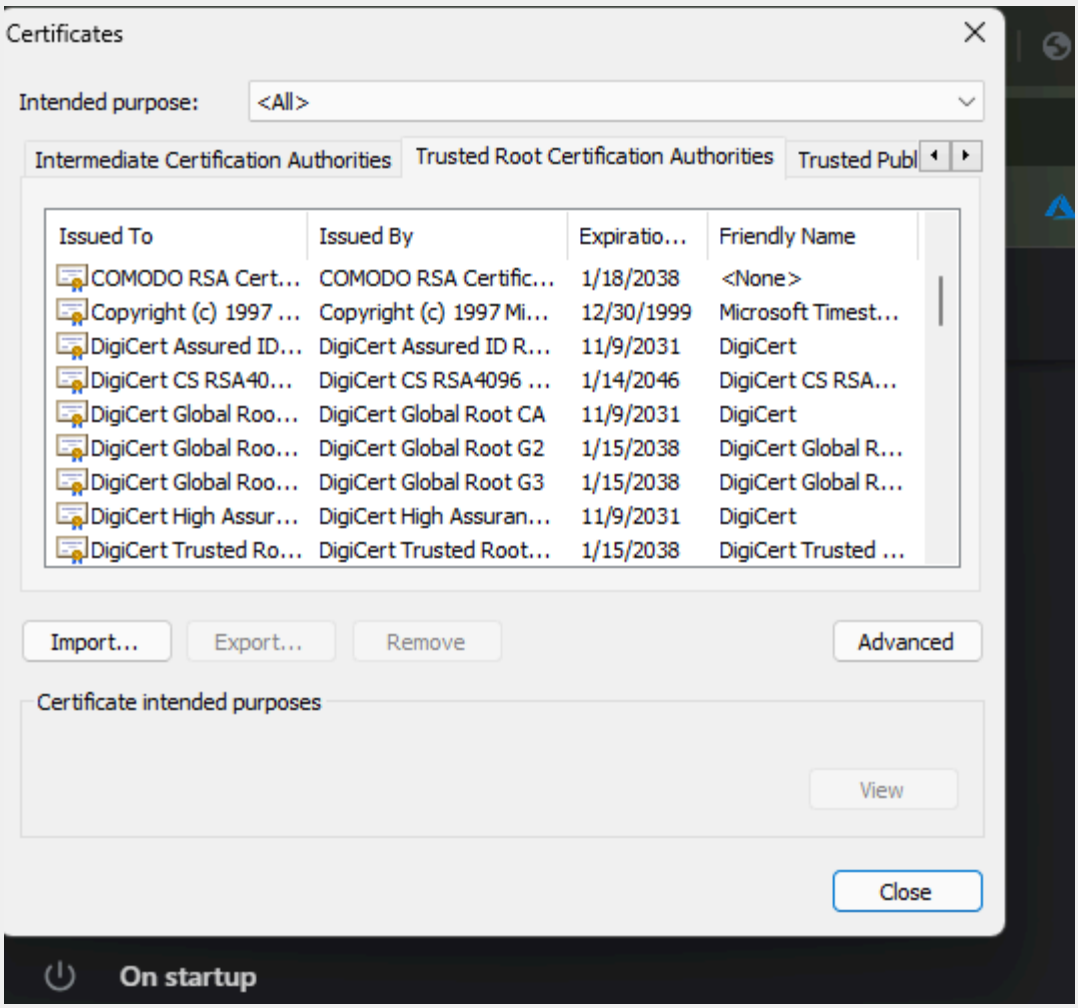
```
Yes, Azure is the intermediate certificate
```

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

```
Yes, DigiCert Global Root G2
```

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

Yes



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

```
COMODO RSA
```

Day 3 Questions

Cloud Security Questions

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

Azure Web Application Gateway and Azure Front Door are both load balancers for HTTP/HTTPS traffic. Front door is a global service that can distribute requests across regions . Application Gateway is a regional service that can balance request within a region

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

```
SSL offloading relieves a web server of the processing burden of encrypting and decrypting traffic sent SSL. This refers to the practice of having services handle SSL/TLS encryption and decryption on behalf of the backend servers.This improves the overall performance of the web application and backend web servers can focus on handling application logic. It also provides flexibility and control in configuring SSL/TLS settings and customized SSL/TLS parameters to align with security best practices.
```

3. What OSI layer does a WAF work on?

```
Layer7, application layer
It filters HTTP traffic between a web application and the internet.
```

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

```
SQL injection works against an application by sending requests to a SQL database through user input. This is when a website has some sort of search bar and someone is able to manipulate the backend database to access information that is not intended to be displayed. There is one SQL injection based on “=” is Always True, it will give you anything as long as it's True.
```

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?

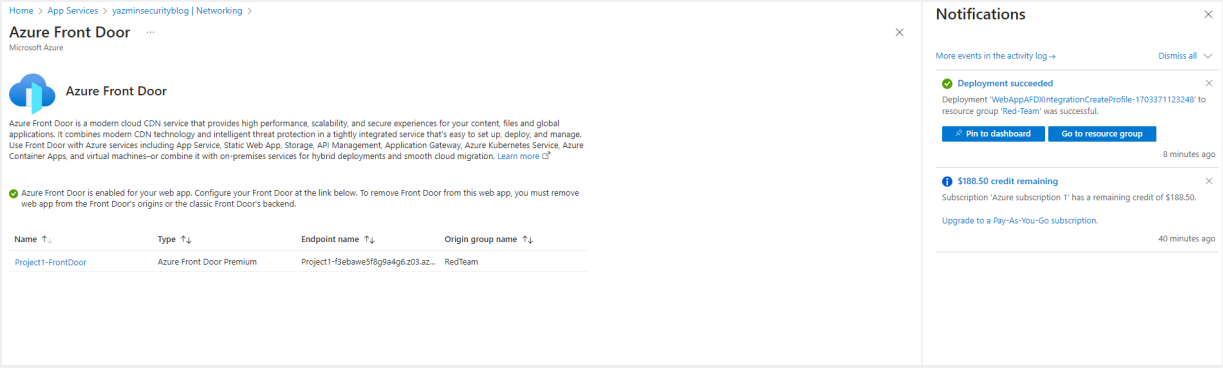
```
Yes because with SQL injection it depends more on the security practices implemented within the website's code, database and infrastructure. This can happen whether or not Azure Front Door is in use. Websites should implement proper input validation.
```

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?

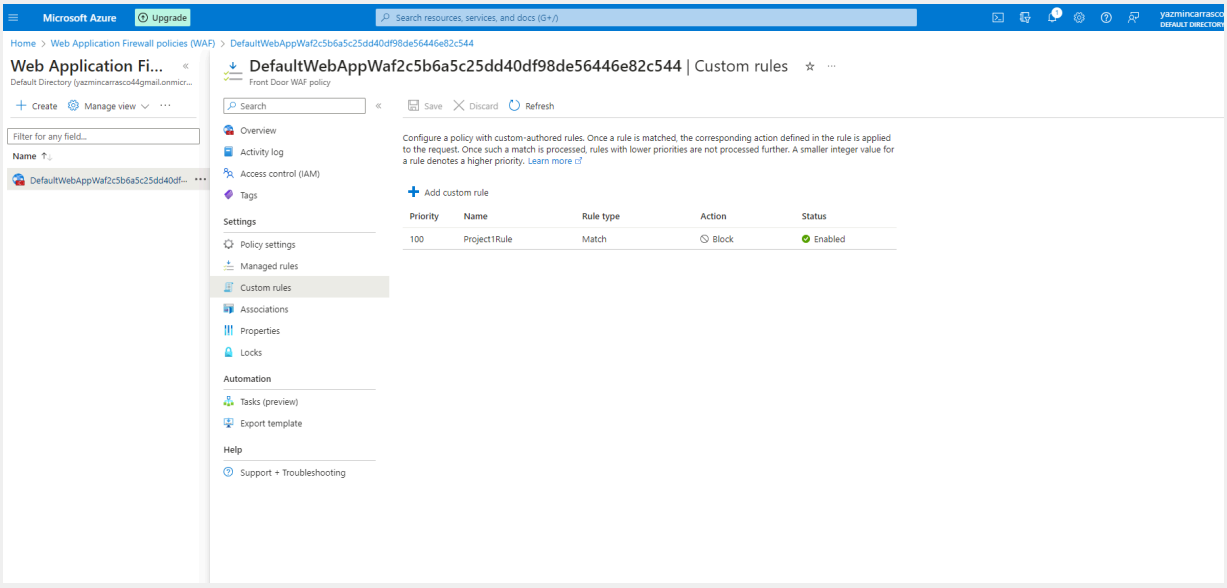
```
No because people can use a VPN or people who might be located in Canada but are not permanent residents
```

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.*

- ***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*