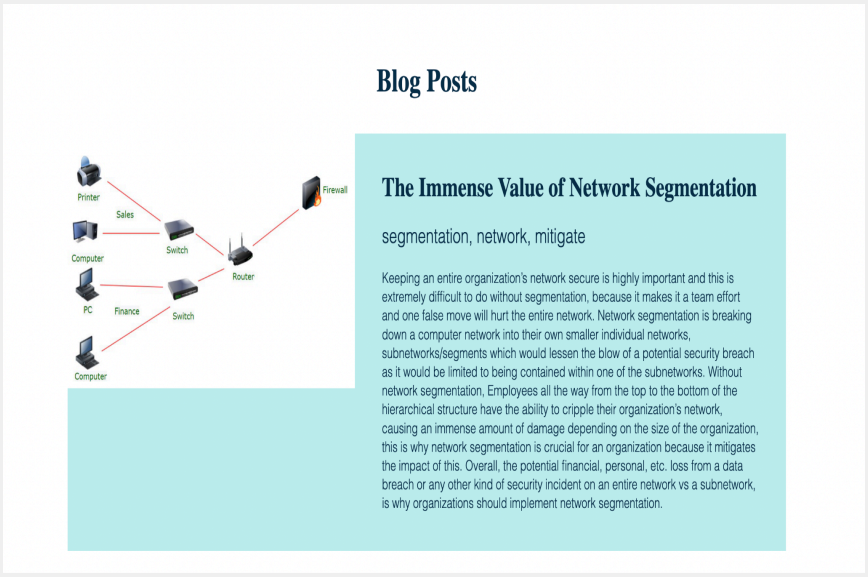
My Azure Web Application

the URL for my web application that you created:

```
https://dagimendalecybersecurityresume.azurewebsites.net
```

screenshots of the website created:



The Lazarus Group: North Korea's Illicit Lifeline

crypto, malware, data, phishing

North Korea's state sponsored hacker group, known as Lazarus Group, are responsible for some of the most notorious cyber incidents of the past decade. These attacks are usually financially motivated and it is fair to say that this hacker group is a HUGE source of funding for the isolated North Korea. They have committed countless notable heists dating from 2014 to current day including, the hacking of Sony in 2014, nearly getting their hands on $1 billion dollars from the Central Bank of Bangladesh in 2016, over $500 million crypto stolen in 2022, and stealing over $250 million in crypto based assets in 2023 alone. The hacking of Sony in 2014 was simply them gaining access to sony's network through malware phishing messages to their employees, which led to them stealing terabytes worth of confidential data and deleting the original copies of the confidential data from Sony's systems. Funnily enough, the attack seemingly had to do with the release of the movie "The Interview", as one of the attackers primary demands were to stop the release of that movie, with them referring to the movie as an act of "terrorism". In the end Sony partially caved in to that demand pulling "The Interview" from major theaters, although they were still victimized with countless sensitive data in the form of unreleased movies, contracts, emails, etc. still being released to the public, causing the company millions in damages. The "Billion dollar" Bangladesh heist was an extremely well-plotted and meticulous scheme that started out in 2015 with a simple phishing email, which one of the employees opened and gave these hackers access to the bank's systems and they sat on this access for a year while they made their grand scheme. They created countless fake bank accounts in the Philippines and made their first move over a year later in 2016, which was to hack the software of the bank's printer and render it useless, to get rid of the immediate paper trail that would alert the bank. After they successfully did that, they initiated 35 transfers totalling nearly $1 billion dollars, unfortunately for the bank these transfers were irreversible and on their way to the Philippines by the time they caught on to the situation. At this point it looked like the Lazarus Group just got away with one of the biggest heists in history, but unluckily for them the address of the Philippines bank they used contained the flagged word "jupiter", so this caused most of their transfers to be placed in review and most of them were caught, with them netting $81 million dollars from this heist. The 2022 number of over $500 million in crypto comes from two heists, the second largest crypto theft of all time $540 million from the Ronin Network Hack and the Harmony Horizon Bridge Hack which totalled $99.6 million in crypto. Their 2023 crypto crimes have put them in the limelight in terms of financial crimes, with them stealing $100 million in crypto from Atomic Wallet users, $37.3 million in crypto from CoinsPaid, $60 million in crypto from Alphapo, $41 million in crypto from Stake.com, and $54 million from CoinEx, all of these attacks being done within 105 days of each other. Overall, these attacks don't paint the full picture of the chaos these North Korean hackers have caused, but hopefully it illustrates how this pariah of a country is powered by illicit funds obtained by hackers and the need to strengthen crypto wallets to protect from these kinds of attacks.

Web Application Networking and Developing Questions

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.19
```

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

```
Sidney, New South Wales, Australia
```

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

```
It doesn't show an NS record when I run a DNS lookup.
```

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 8.0, I believe php 7.0 series reached its EOL and 8.0 will also reach
its EOL soon, it works on the back end.
```

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

```
Inside that directory was two subdirectories called css and images, css
works with the html document presentation and the images directory contains
the images within the document.
```

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

```
These are front end applications.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A user having their own isolated server.
```

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

```
It would make sure only authorized users would have access, very important
for security.
```

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

```
A key pair is used for encryption and decryption, secrets is secure storage
for sensitive data like passwords,etc., and certificates authenticate
```

```
identity & establish trust.
```

Cryptography Questions

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

```
A couple of advantages would be that the signature is free, easy to
initiate, and self-reliant.
```

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

```
Disadvantages could be the warning indication, data at risk, data security
not ensured, and potential user error.
```

3. What is a wildcard certificate?

```
A certificate that uses a wildcard (*), this type of certificate is used to
secure a domain with many sub-domains.
```

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 has a known exploit called POODLE and this vulnerability has
rendered SSL 3.0 unusable.
```

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 uses the Azure preset SSL certificate.
```

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

```
It was issued on Thursday,March 9, 2023 at 7:05:55 PM and expires on Sunday,
March 3, 2024 at 7:05:55 PM.
```

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

```
no
```

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

```
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.

```
The AAA certificate
```

Day 3 Questions

Cloud Security Questions

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

```
They are both load balancers, but Azure Web Application Gateway is a
regional service and Azure Front Door is not a regional service.
```

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 when a web server has the SSL encryption of its incoming
traffic decrypted. THis leads to faster processing times for the web server.
```

3. What OSI layer does a WAF work on?

```
It works on the defense layer, layer 7.
```

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

```
Directory traversal is an exploit that allows an attacker access to have
full control of unauthorized directories and files.
```

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?

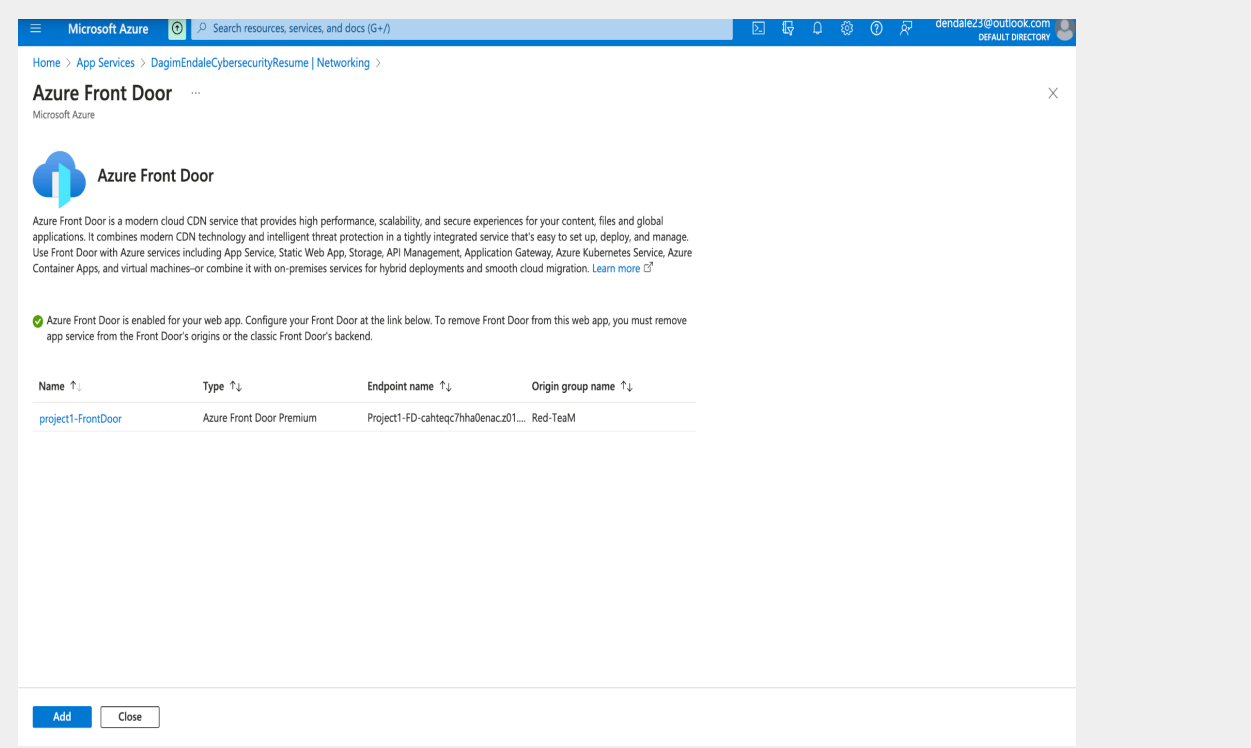
```
No, this vulnerability is dealt with by a Web Application Firewall rule.
```

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?

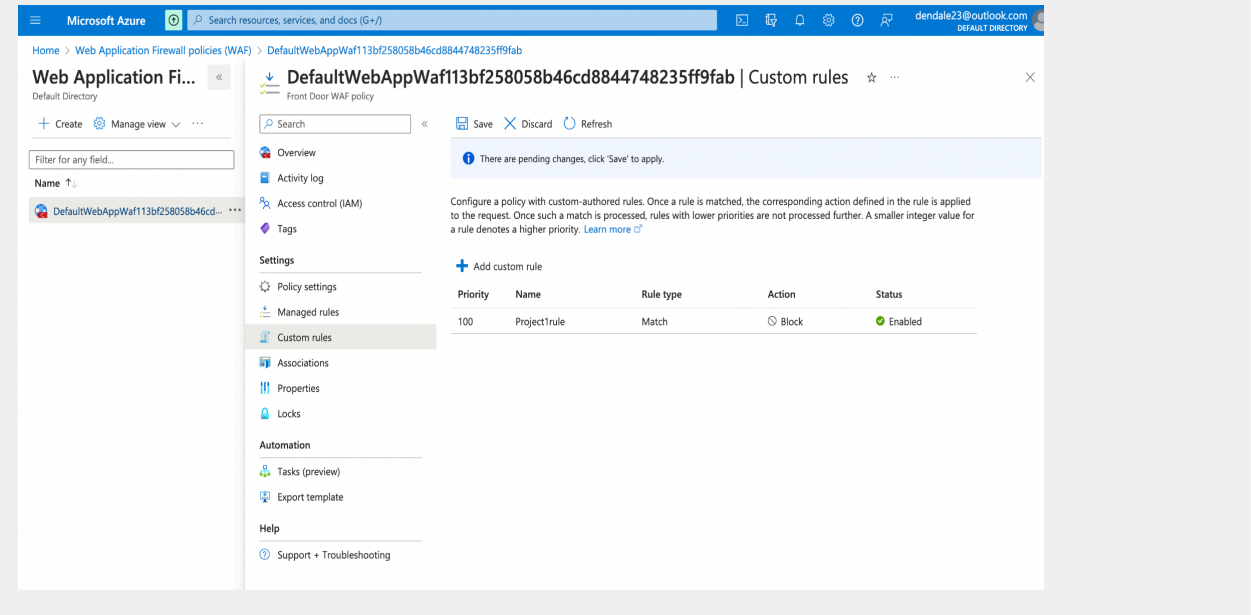
```
Yes, any Canadian IP would be unable to access the website unless they use a
VPN.
```

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.*