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://timothysecurityresume.azurewebsites.net
```

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

Blog Content:

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?

```
timothysecurityresume.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?

```
Country: Australia
City: Sydney
Region: New South Wales
Region: Australia East
```

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

```
Timothy pang@TKHP-Desktop MINGW64 ~
$ nslookup timothysecurityresume.azurewebsites.net
Non-authoritative answer:
Server:  UnKnown
Address:  192.168.86.1

Name:    waws-prod-sy3-091-a15c.australiaeast.cloudapp.azure.com
Address:  20.211.64.13
Aliases:  timothysecurityresume.azurewebsites.net
          waws-prod-sy3-091.sip.azurewebsites.windows.net


Timothy pang@TKHP-Desktop MINGW64 ~
$
```

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?

```
Runtime stack that was selected was: PHP 8.1 and it works on the backend
```

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

```
Within this directory, is the css and link to the image files, so they are
files that affect what the styles are for the web page ie: what it looks
like, how it transforms depending on screen size, font, and color. As well
as the image files used within the site.
```

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

```
Frontend
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
Cloud tenants are different environments within a cloud service provider
```

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

```
You would need an access policy because within the key vault contains
secrets such as, API keys, passwords, certificates and cryptographic keys
that attackers will want in order to access more information stored within
the database or web server. With those keys, they can access anything that
you have connected to your computer, or any websites created.
```

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

```
Keys: It's a piece of data that is used to encrypt or decrypt data. In a key
vault, keys are typically used to secure sensitive information, such as
passwords, credit card numbers, and other types of data

Secrets: It's a piece of sensitive information that is stored securely in a
key vault. This can include things like passwords, connection strings, and
API keys.

Certificates: It's a digitally signed document that is used to establish the
identity of a person, device, or organization. Within the key vault,
certificates can be stored and managed securely, and can be used for things
like secure communication, authentication, and digital signing.
```

Cryptography Questions

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

```
Advantages:
   -  One of the advantages of a self-signed certificate is that it is free
```

```
   -  Useful for test environments
   -  Flexible and customizable
```

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

```
Disadvantages:
   -  One disadvantage is that it is not secure, the information inputted or
      shown is not safe, and can be exploited and taken by attackers.
   -  Another is that they cannot be revoked by the CA
   -  Not considered trusted.
```

3. What is a wildcard certificate?

```
It is a certificate that means that any domain name no matter what it is
called, as long as it is followed by what is after the wildcard, all those
domains would have the certificate. Ie: *.google.com , anything related to
google.com is covered by the trusted certificate
```

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 not provided because it has vulnerabilities within that people
could exploit. It is not secure or trusted.
```

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, it is not because it is a certificate given by azure, which is issued by
a verified CA to azure, so it is considered secure and trusted. When the app
service is created, the domain is given the certificate generated by azure.
```

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

```
March 14 2022 - March 9 2023
```

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

```
Microsoft Azure TLS Issuing CA 01
```

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.

```
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?

```
Similarities:
   -  They both work on Application layer 7
   -  Resides in the front on web application
   -  Can incorporate a WAF to protect against web attacks

Differences:
   -  The front door is more global and better for when there are different
      regions in a cloud environment
   -  The gateway is more regional, and can protect web application in a
      single 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 is removing the SSL encryption on incoming web traffic so
that when a web server receives the traffic it does not need the extra
processing to decrypt the data.

The benefits:
   -  Because the web server does not directly decrypt the data and consumes
      more processing power, the web server's performance won't be affected
      or slowed.
```

3. What OSI layer does a WAF work on?

```
Application Layer 7
```

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

```
Directory traversal is a web based exploit, occurs when an attacker accesses
files and directories from a web application outside a user's authorized
permissions
```

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?

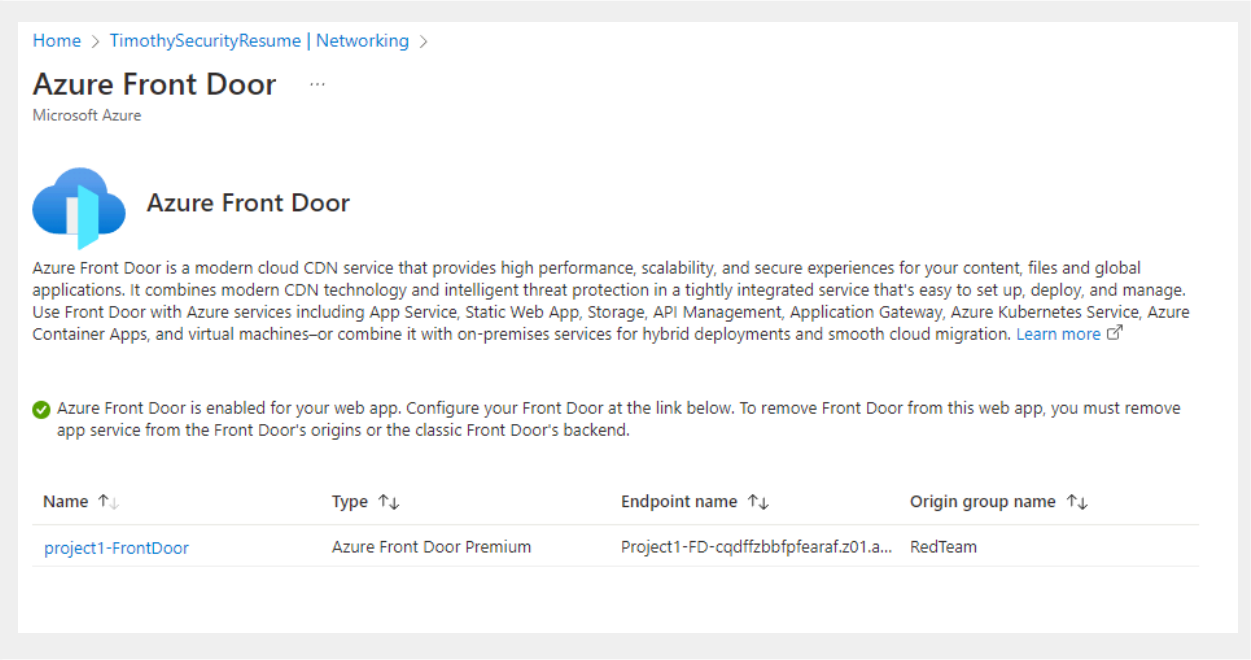
```
Yes, it would be impacted by this vulnerability because the website would
then not have the protection of the security measures in place. For the
reason that the directory traversal attack manipulates a website's file
system to gain access, if the website is not secured by some sort of
firewall or security measure, then the attacker can easily use the exploit
to access the files and directories.
```

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?

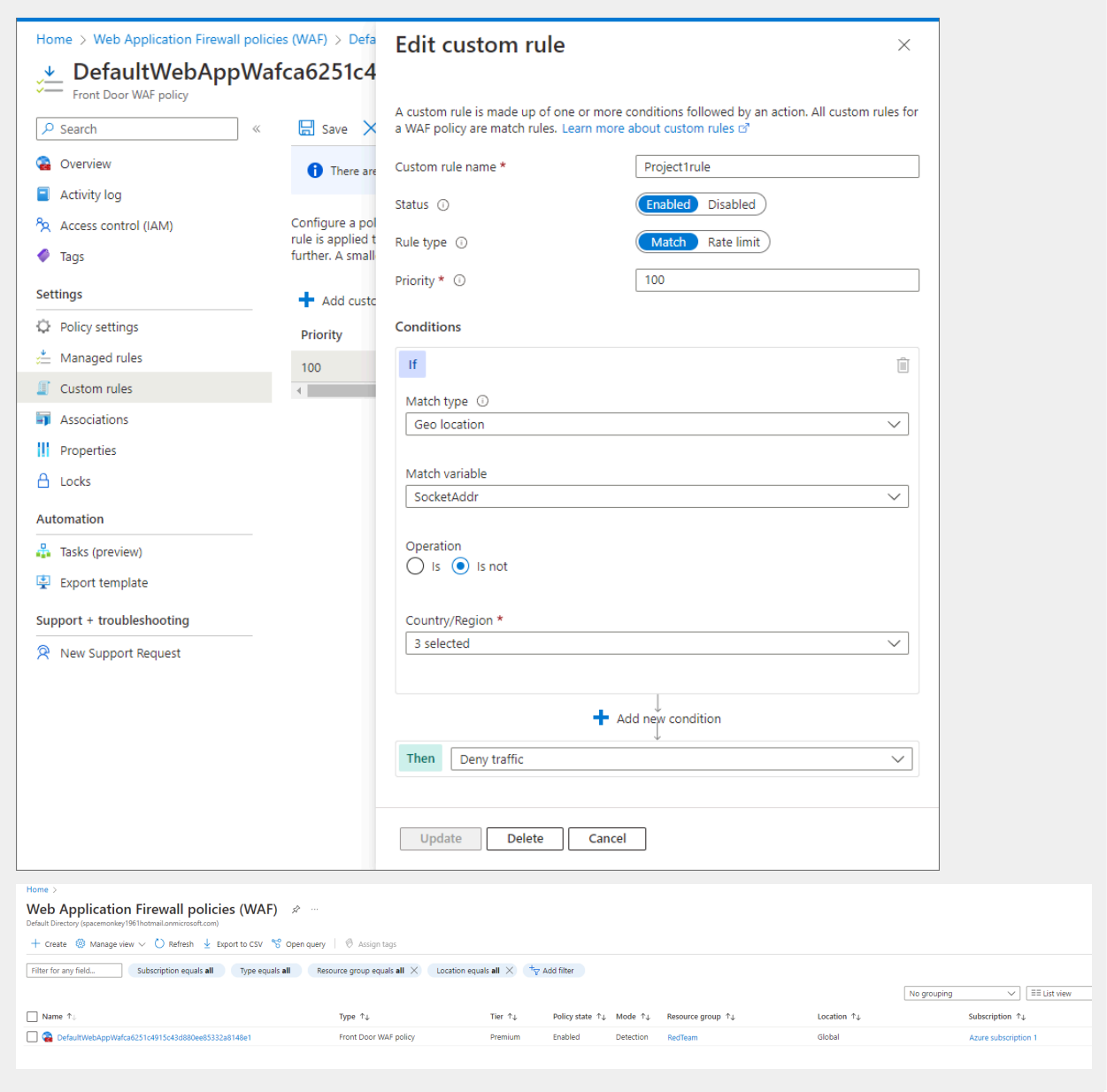
```
Yes, it means that anyone that resides in Canada would not be able to access
my website, because I am blocking a specific geolocation/country from being
able to view the website. However, because there are VPN's, an attacker
could use that within Canada and still be able to access the website.
```

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