Cybersecurity

Project 1 Technical Brief

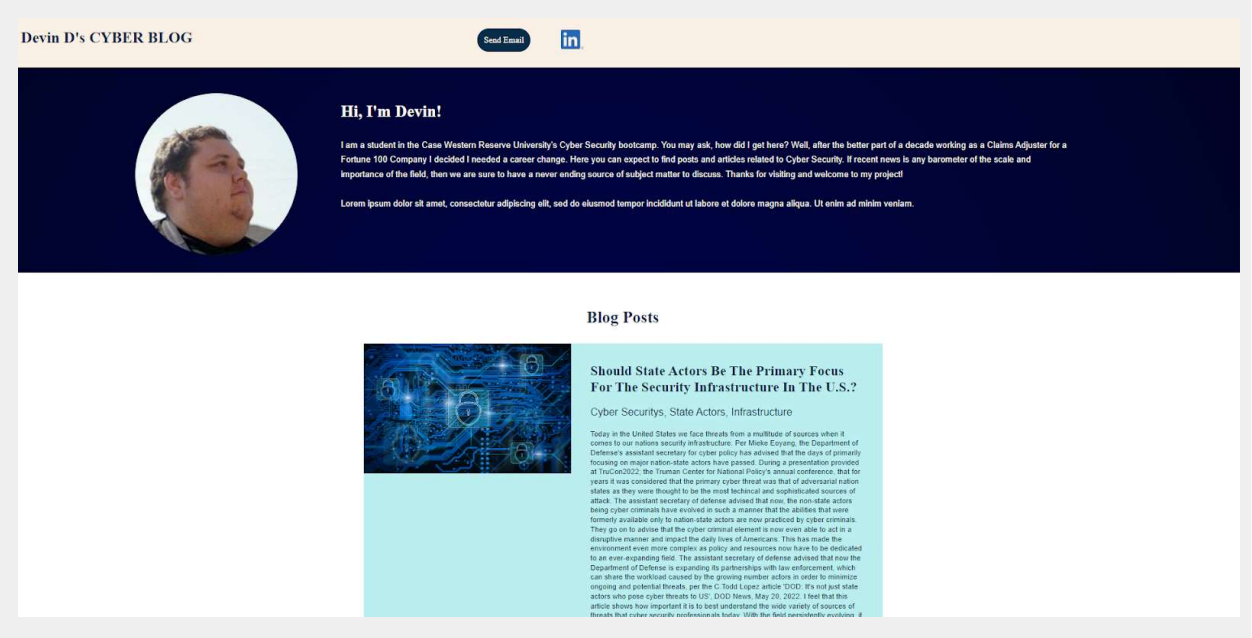
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

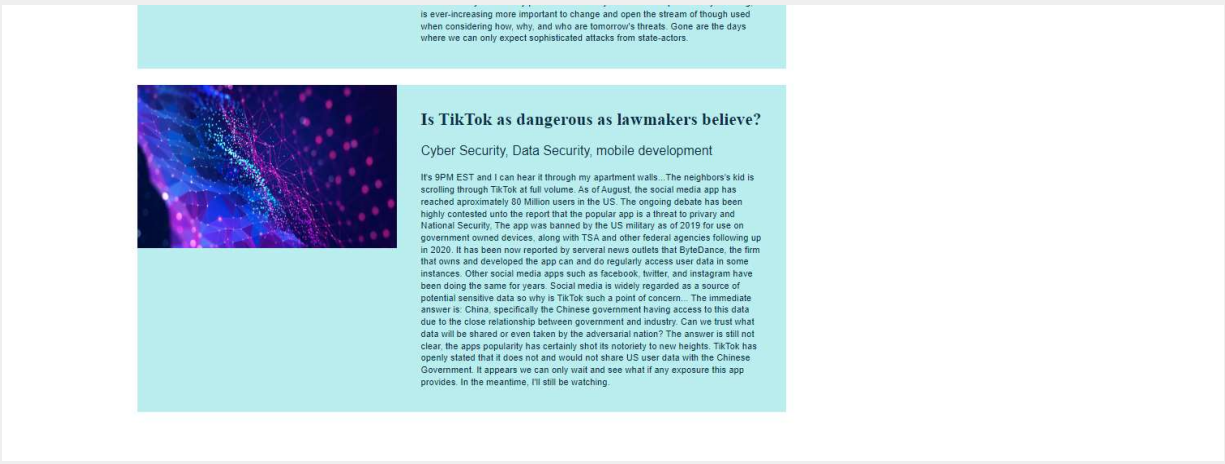
Your Web Application

Enter the URL for the web application that you created:

```
devydoessecurity.com
```

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)?

```
Godaddy,com
```

2. What is your domain name?

```
devydoessecurity.com
```

Networking Questions

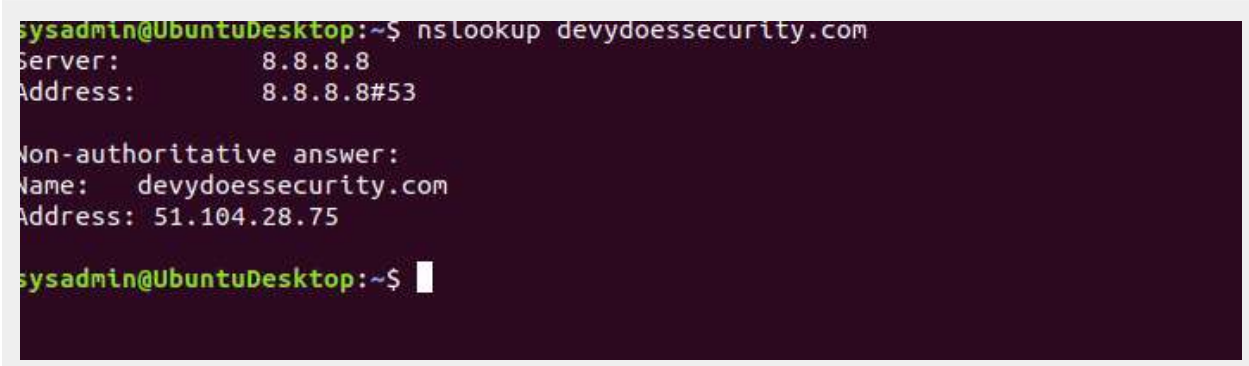
1. What is the IP address of your webpage?

```
51.104.28.75
```

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

```
London, England, GB
```

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



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?

```
The runtime stack is the technology stack used to develop the app, this
works on the backend of the app.
```

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

```
This directory contains the css, used for the website styling and the photos
used for the site.
```

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?

```
A cloud tenant is a person or group that rents the use of a cloud server.
```

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

```
Restricting access is important to a key vault as the keys are used to write the ssl certificates needed to verify the domain, if there was not an access policy, a 3rd party could use their access to the keys, use their own SSL certs for nefarious reasons.
```

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

```
Keys are used to create SSL certs that create unique SSL Certs, certificates are the data files used to verify the identity of the site owner/operator.

When azure creates the certificate, it creates a secret that stores the password as a secret and the key is stored as an azure key.
```

Cryptography Questions

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

```
They are free, suitable for internal network websites and development/testing environments.
```

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

```
Browsers and Operating systems do not trust self-signed since there is not a trusted third party certificate authority confirming the validity of the site.
```

3. What is a wildcard certificate?

```
A wildcard cert uses a wildcard character in the domain name that way you can use it for multiple subdomains on a site
```

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 no longer secure as a major vulnerability was found, known as the POODLE vulnerability.
```

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 azure has now provided a managed SSL certificate that is a third party which is verifying the sites authenticity
```

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

```
Through 04/03/2023
```

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

```
Yes,GeoTrust TLS RSA4096 SHA2560 2022 CA1
```

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

```
Yes,Digicert Global Root CA
```

    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.

```
Microsoft Root Authority
```

Day 3 Questions

Cloud Security Questions

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

```
Both are layer 7 load balancers whereas the front door is a non-regional
service while the application gateway is regional. Front Door can load
balance between different scale units across regions, gateway will load
balance between VM/Containers within the unit.
```

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 the process of removing the SSL based encryption from
incoming traffic that a web server receives to relieve it from description
of data. It allows the transfer of data to be less compute intensive.
```

3. What OSI layer does a WAF work on?

```
Layer 7, application layer
```

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

```
IE XSS FILTER ATTACK DETECTED, this means that a cross-site scripting attack
has been detected
```

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?

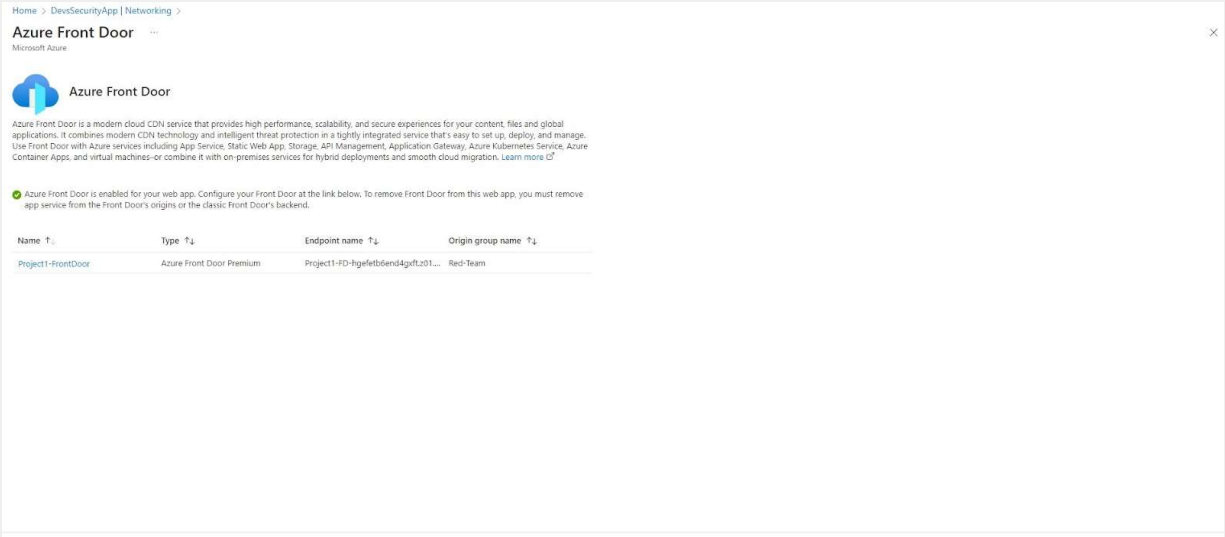
```
Yes, A hostile actor could use cross site scripting to inject a malicious
script into my web application that could affect the end user of the site
which could take sensitive data from accessing end user cookies, session
tokens, etc.
```

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?

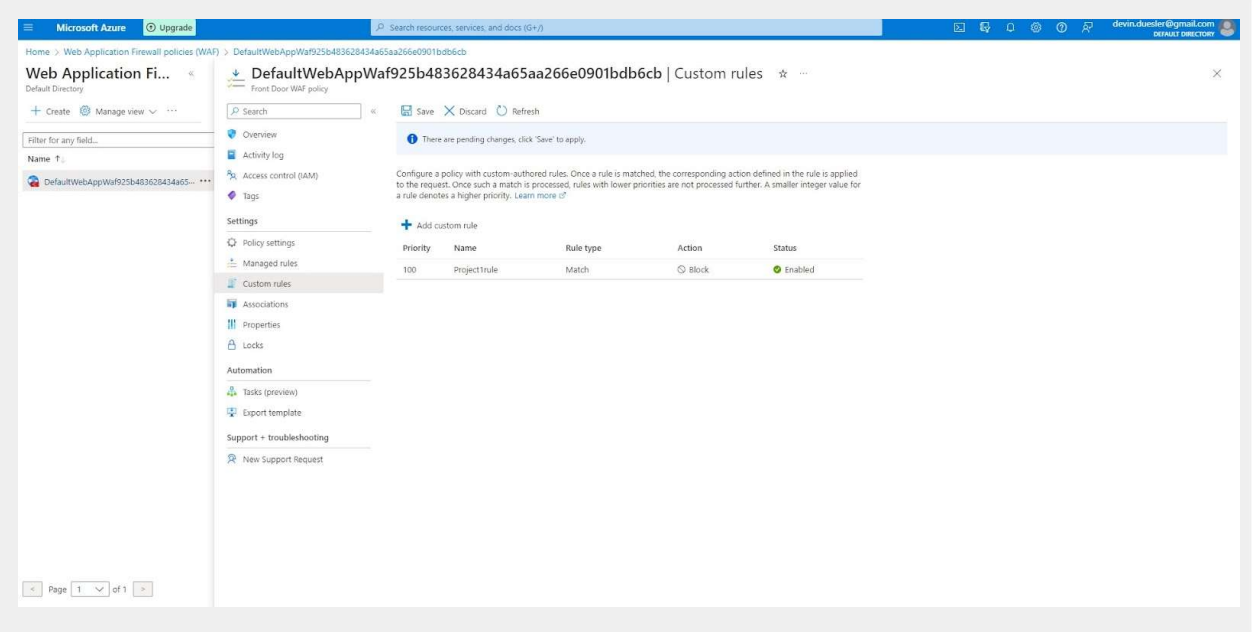
```
It would mean anyone with a Canadian IP address would not be able to access if that is the country of origin. Hypothetically if someone has a VPN that shows an IP address from outside of Canada could still access it.
```

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.*