Cybersecurity

Project 1 Technical Brief

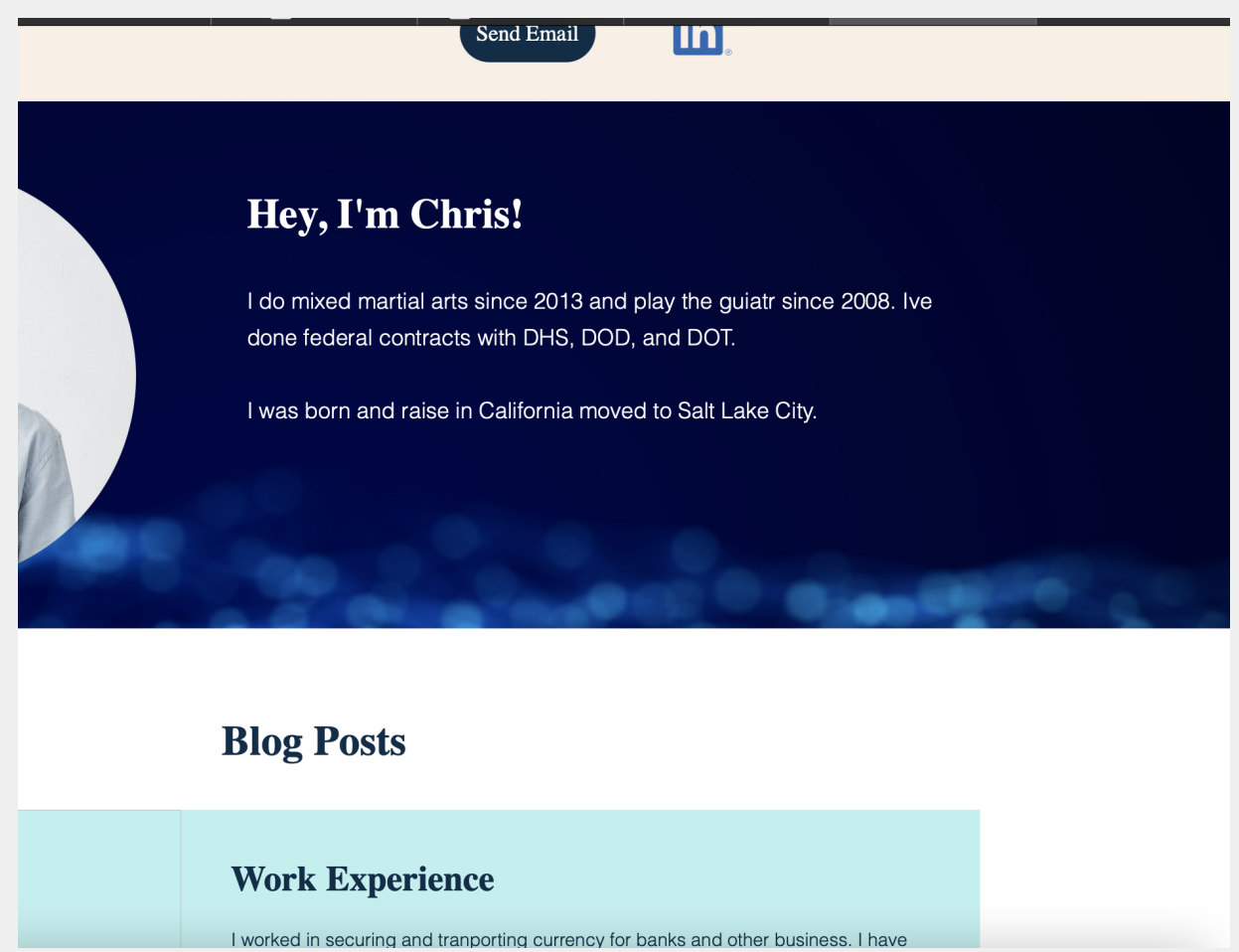
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://crs444.azurewebsites.net
```

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)?

Azure free domain

2. What is your domain name?

crs444.azurewebsites.net

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?

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

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

```
Test Result Status Ok HTTP Connect  Status Ok HTTP Filter  Status Ok HTTP
Delay Check Success - response in 879 ms Status Ok HTTPS Certificate Check
Status Ok HTTPS Certificate Expiration

Common Name: *.azurewebsites.net Issuer: Microsoft Azure TLS Issuing CA 02
Expires: 5 months Valid From: 3/9/2023 Valid To: 3/3/2024 Serial:
3300990E6F5FE8E7D385902BDA000000990E6F Algorithm: sha384RSA Organization:
Microsoft Corporation Location: Redmond,WA,US
```

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?

```
Back end
```

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

```
It contains two directories css and images. Images had the
following-Background.jpg  Image1.jpg  Image2.jpg  LinkedIn-logo.png
RobertSmith-profile.jpg  readme. css has style.css  style.css.bak.
```

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

```
Back end
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
It's a sharing of computing resources in a private or public environment
that is apart from other users and remains confidential. Tenancy in SaaS is
has two different categories: single-tenant SaaS and multi-tenant SaaS.
```

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

```
It ascertain a given security principal of a user, application or user
group. It is able to execute dissimilar operations on a Key Vault secrets,
keys, and certificates.
```

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

```
Secrets furnish secure storage of secrets like passwords and database
connection strings.
Supports certificates are made on top of keys and secrets and add an
automated renewal feature
source:https://learn.microsoft.com
```

Cryptography Questions

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

```
Its Cost-effective and self-signed certificates are free to generate and
user friendly and not hard to use: Self-signed certificates can be generated
and deployed quickly, which is ideal for temporary or local environments.
source https://venafi.com
```

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

```
Self-signed SSL Certificates are perilous because they have no validation or verification from a third-party authority, which is usually a Trusted SSL Certificate Company. Developers and businesses attempt to skimp money by operating or making a free Self-Signed SSL Certificate.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a public key certificate which is able to be utilized with multiple sub-domains of a domain.
```

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 encryption standard that's used to secure Web traffic using the HTTPS method. It has a flaw that could allow an attacker to decrypt information, such as authentication cookies, according to Microsoft.
source:www.coursehero.com
```

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?

```
There is no error for my SSL certificate because its valid.
```

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

```
March 3 2024
```

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

```
Yes it has digicert Global Root G2
```

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

```
Yes same answer for c.
```

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.

```
Issued by: Microsoft Azure TLS Issuing CA 02
```

Day 3 Questions

Cloud Security Questions

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

```
Azure Front Door WAF and Azure App Gateway WAF are very similar in
functionality, one of the main differences is where the WAF is applied.
Azure Front Door applies the WAF filters at edge locations, way before it
gets to the datacenter. App Gateway applies the filter when it enters your
VNET via the App Gateway
source:learnmicrosoft
```

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

```
SSL offloading takes care of the encryption/decryption process on a separate
device so that it doesn't affect the web server's performance. The idea
behind SSL offloading is to do encryption operations anywhere other than on
the web server.
source:https://www.appviewx.com
```

3. What OSI layer does a WAF work on?

```
protocol layer 7 defense
```

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

```
An SQL injection rule statement inspects for malicious SQL code. ... If you
specify more than one transformation, AWS WAF processes them in the order
listed.
source:https://docs.aws.amazon.com
```

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?

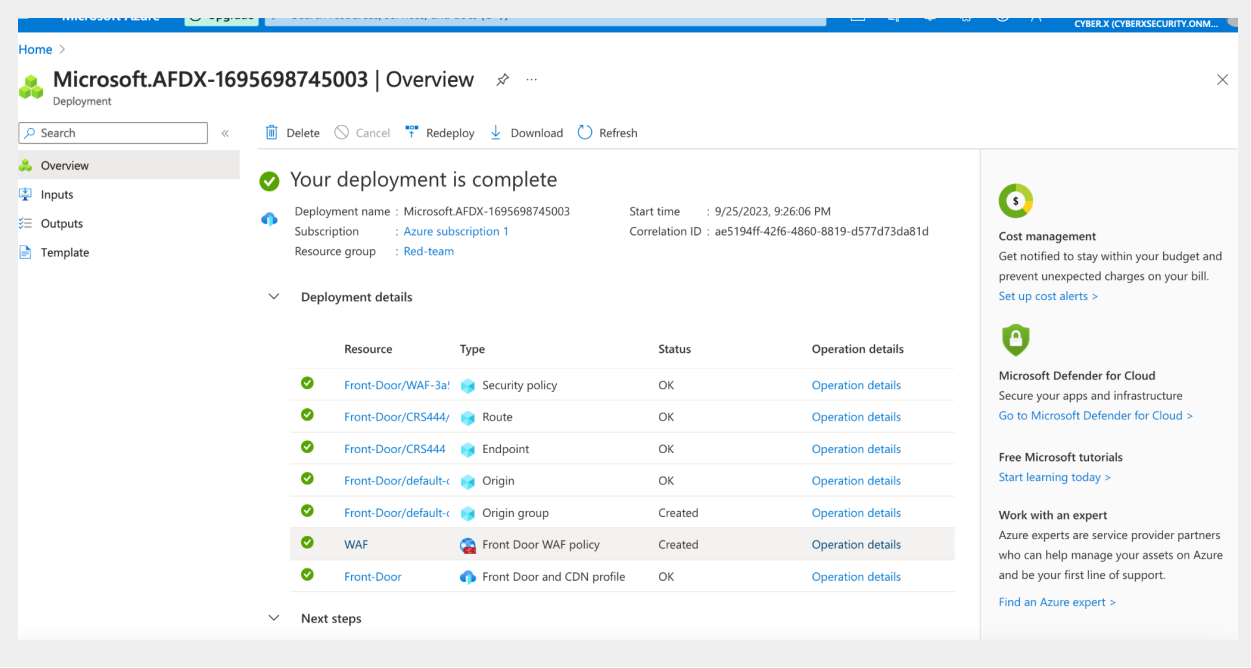
```
Yes my website can be affected by this susceptibility if the Front Door
wasn't enabled. This is because Front Door would not be able to block
traffic from the specific IP address that is responsible for the
vulnerability. My website without Front Door enabled would be susceptible to
attacks from the specific IP address.
source:https://www.coursehero.com
```

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?

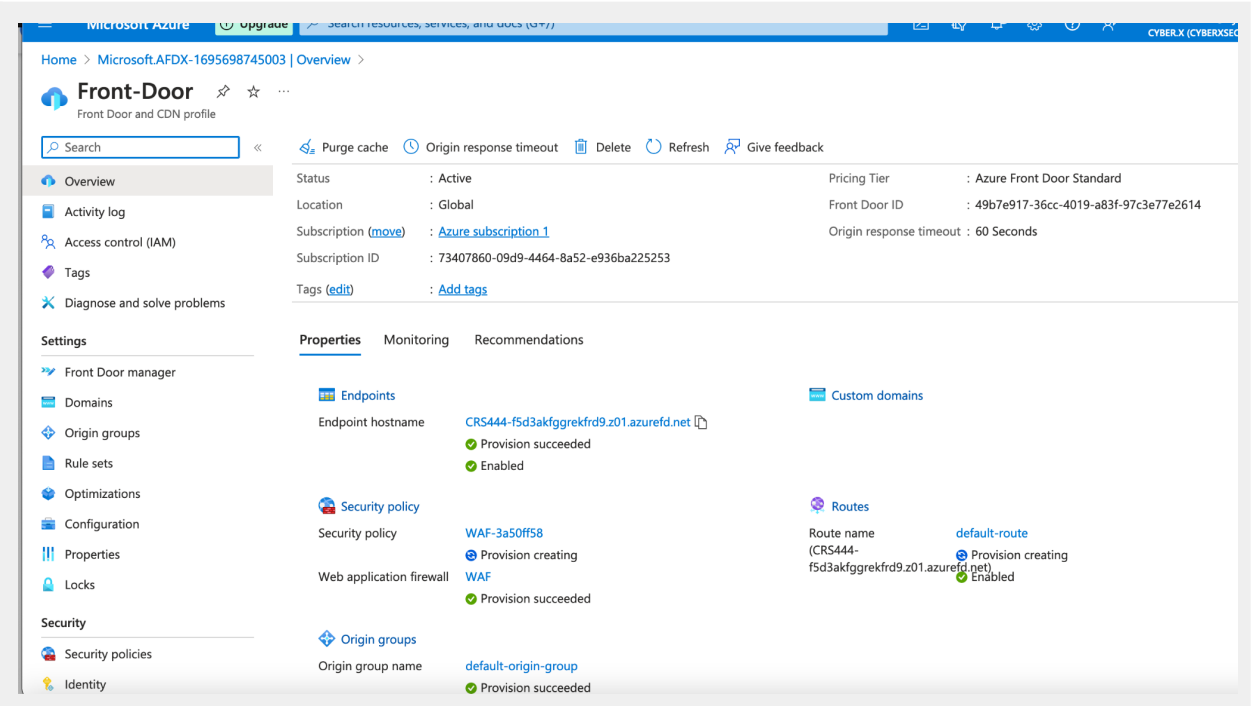
```
No. If I created a custom WAF rule to stop all traffic from Canada, that
doesn't inevitably mean that anyone who lives in Canada wouldn't be able to
access my website.
```

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:YES

- ***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.*