Cybersecurity

Project 1 Technical Brief

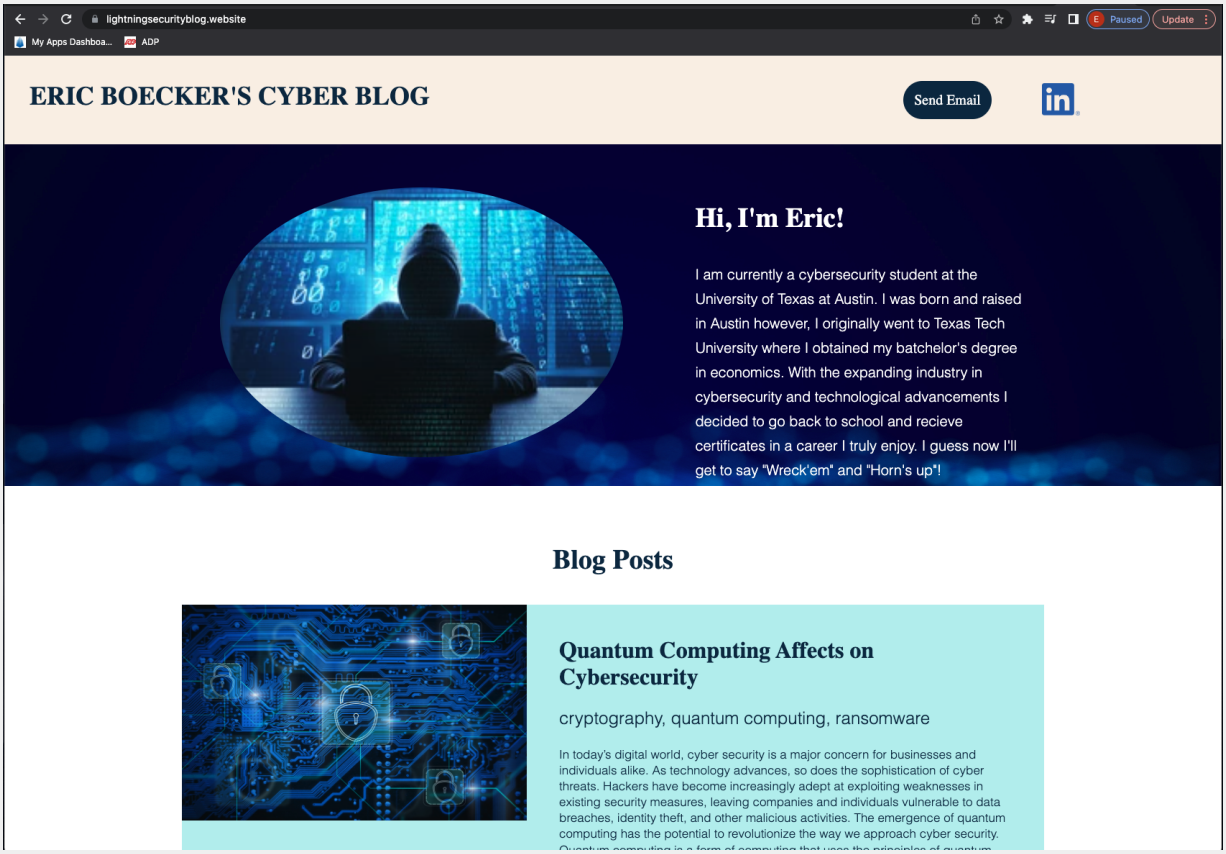
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

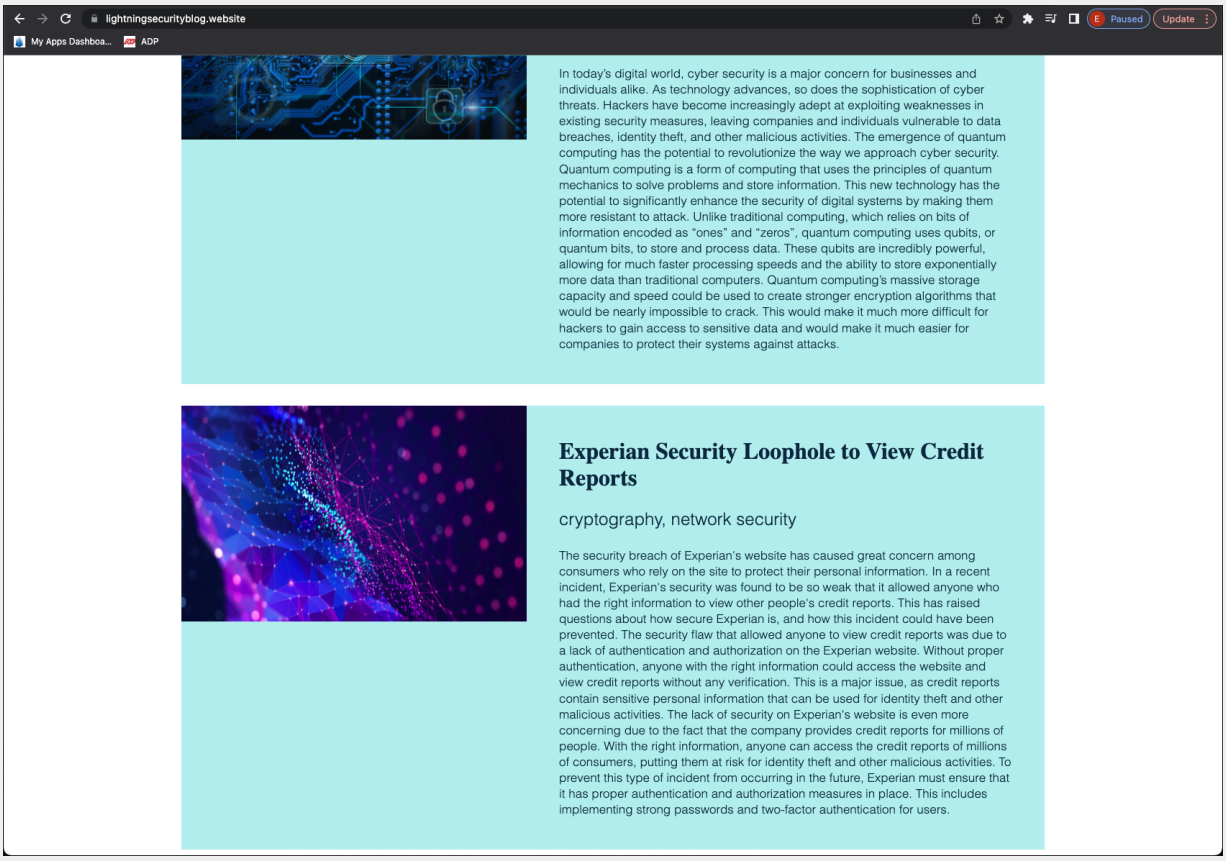
Your Web Application

Enter the URL for the web application that you created:

```
http://lightningsecurityblog.website
```

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


lightningsecurityblog.website
My Apps Dashboa...
ADP
Paused
Update
ERIC BOECKER'S CYBER BLOG
Send Email
Hi, I'm Eric!
I am currently a cybersecurity student at the University of Texas at Austin. I was born and raised in Austin however, I originally went to Texas Tech University where I obtained my batchelor's degree in economics. With the expanding industry in cybersecurity and technological advancements I decided to go back to school and recieve certificates in a career I truly enjoy. I guess now I'll get to say "Wreck'em" and "Horn's up"!
Blog Posts
Quantum Computing Affects on Cybersecurity
cryptography, quantum computing, ransomware
In today's digital world, cyber security is a major concern for businesses and individuals alike. As technology advances, so does the sophistication of cyber threats. Hackers have become increasingly adept at exploiting weaknesses in existing security measures, leaving companies and individuals vulnerable to data breaches, identity theft, and other malicious activities. The emergence of quantum computing has the potential to revolutionize the way we approach cyber security.



Day 1 Questions

General Questions

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

```
GoDaddy domain
```

2. What is your domain name?

```
lightningsecurityblog.website
```

Networking Questions

1. What is the IP address of your webpage?

```
20.49.104.9
```

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

```
Washington, Virginia, USA
```

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

```
Server:           2600:1700:2f02:7010::1
Address:    2600:1700:2f02:7010::1#53

Non-authoritative answer:
Name: lightningsecurityblog.website
Address: 20.49.104.9
```

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 8.1 , and 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.

```
All front end assets that are located on the website
```

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?

```
An individual user, group of users, or a company who purchases cloud
computing resources.
```

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

```
By mitigating what users have access, you can centralize the storage of
application secrets. A policy like this helps reduce the chance of sensitive
information being leaked, and only allows authorized users access.
```

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

```
Keys - Cryptographic keys used to encrypt information

Secrets - Any sensitive information that is not an asymmetric key or
certificate

Certificates - Built on top of keys and secrets white adding an automated
renewal feature allowing trusted access to a specific domain
```

Cryptography Questions

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

```
Self-signed certificates are fast, free, and easy to use. Plus they are
great for development/testing environments due to the increased speed and
easy use.
```

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

```
The disadvantages of self-signed certificates are that they do not provide
```

```
any trust value and no validation from a third-party authority. This can create security issues for the website while showing the website may not be trusted.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a single certificate that has a wildcard character in the domain field which secures multiple subdomains within the primary 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.

```
Due to an issue that SSL 3.0 has with the protocol and there not being any solution at this time, disabling SSL 3.0 would be best practice. This vulnerability is due to the way data is encrypted under a specific type of encryption algorithm within the SSL protocol.
```

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 the certificate is a trusted CA from Azure.
```

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

```
Expires on July 6, 2023. Therefore, six months.
```

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

```
Yes, GeoTrust Global TLS RSA4096 SHA256 2022CA1
```

    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, and it expires on 10-11-2031
```

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

```
CN=DigiCert Assured ID Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US
```

Day 3 Questions

Cloud Security Questions

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

```
Front Door is a global service and can load balance across regions while
Application Gateway is a regional service that allows you to load balance
within the specific region.

Both Front Door and Application Gateway are layer 7 (HTTP/HTTPS)
applications.
```

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

```
SSL offloading uses a dedicated server to process incoming SSL encrypted
traffic, therefore allowing relief to the main web server. This allows your
main web servers to be freed up instead of being forced to deal with
constant encryption and decryption of data.
```

3. What OSI layer does a WAF work on?

```
A WAF works on layer 7.
```

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. This prevents an attacker from inserting SQL queries through the SQL database underlying the system.
```

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?

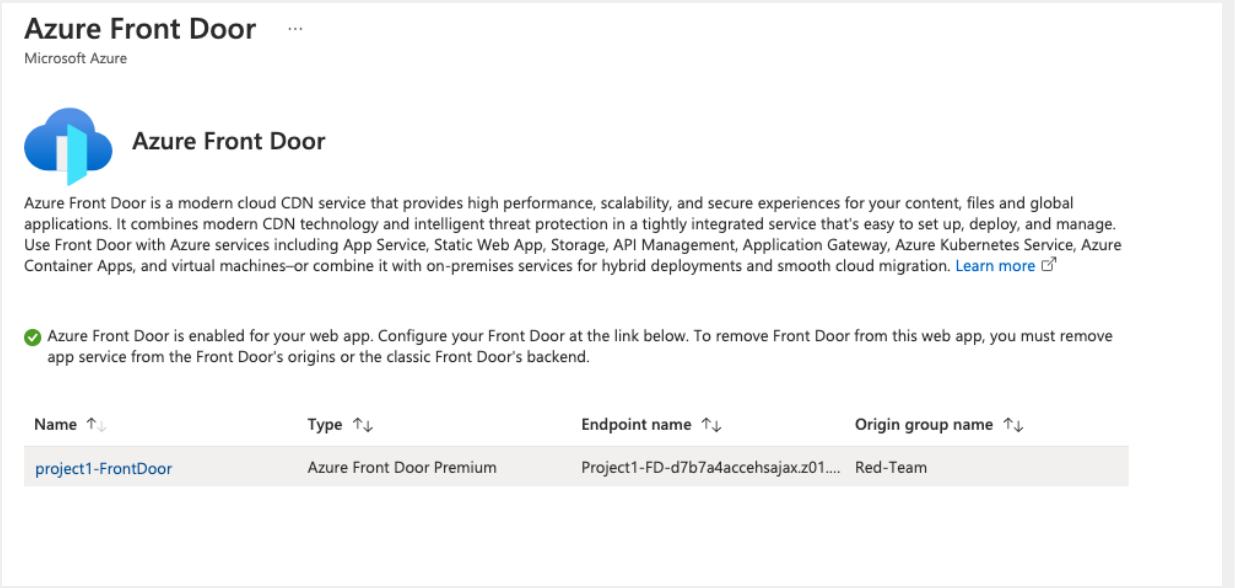
```
Yes, because with Front Door not enabled then all traffic will bypass and allow the web server be exposed to potential SQL injection attacks.
```

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?

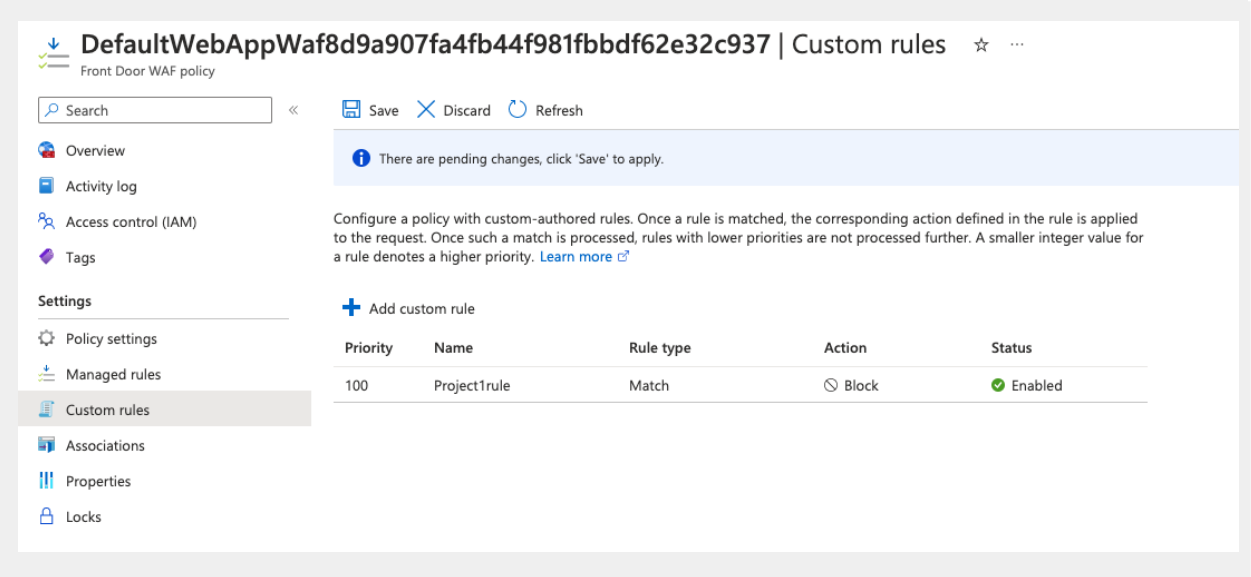
```
With a custom WAF rule you can block all traffic from Canada. However, a resident residing in Canada could still be able to access the website through the use of a VPN.
```

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.*
  YES

- ***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