# Cybersecurity

## Project 1 Technical Brief

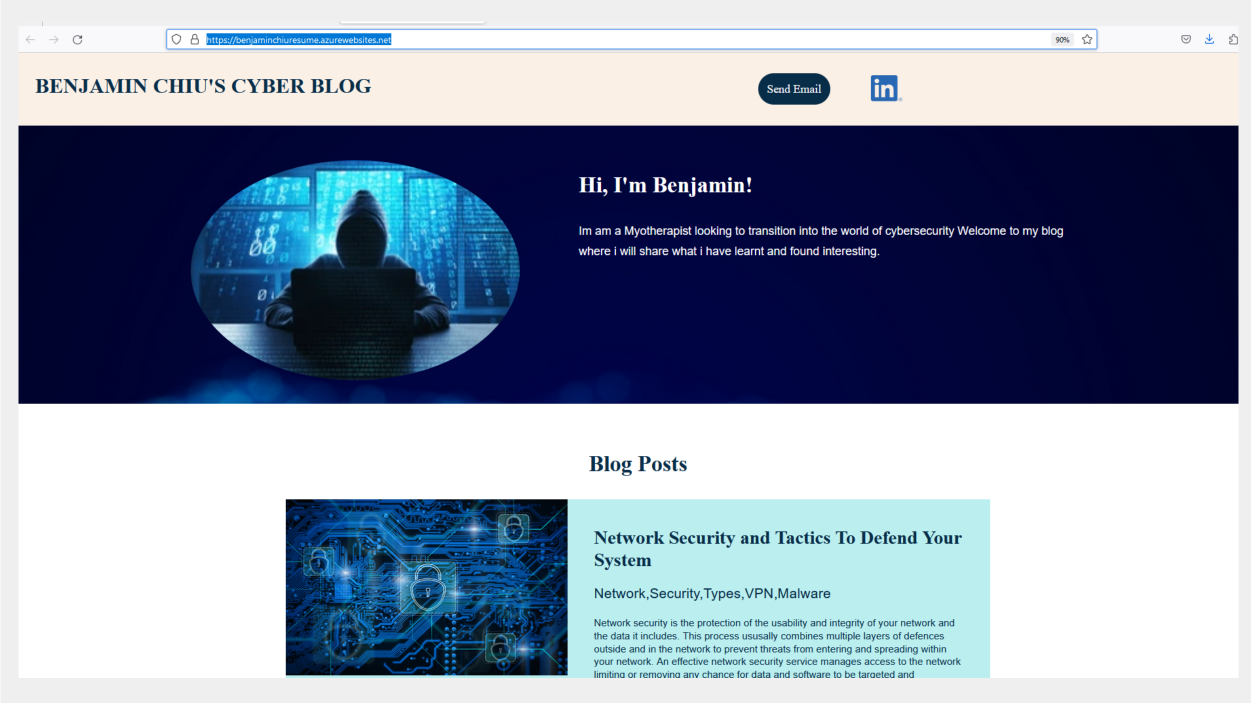
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

## Your Web Application

Enter the URL for the web application that you created:

```
https://benjaminchiuresume.azurewebsites.net/
```

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



BENJAMIN CHIU'S CYBER BLOG

Hi, I'm Benjamin!

Im am a Myotherapist looking to transition into the world of cybersecurity Welcome to my blog where i will share what i have learnt and found interesting.

Blog Posts

Network Security and Tactics To Defend Your System

Network,Security,Types,VPN,Malware

Network security is the protection of the usability and integrity of your network and the data it includes. This process ususally combines multiple layers of defences outside and in the network to prevent threats from entering and spreading within your network. An effective network security service manages access to the network limiting or removing any chance for data and software to be targeted and

# Blog Posts

## Network Security and Tactics To Defend Your System

### Network,Security,Types,VPN,Malware

Network security is the protection of the usability and integrity of your network and the data it includes. This process ususally combines multiple layers of defences outside and in the network to prevent threats from entering and spreading within your network. An effective network security service manages access to the network limiting or removing any chance for data and software to be targeted and compromised.

There are different types of network security that build up a protective layer. These include but not limited to :

Firewall : A firewall puts up a protective barrier/layer between your trusted internal network and any external networks filtering traffic. This can be applied to both or individually to software or hardware

Email Security : Emails are a common way that networks can be breached. A breach via email generally occured when an email has been compromised or tactics such as phishing scams decieve the target and causes them to download malware that compromises the system.

Anti-Virus - Antiviruses are software that scan and potenially remove malicious software from a system.

VPN - Virtual Private Networks are tools that help secure information that is being sent over a networks (Ususally the internet). This provides a further layer of protection by encrypting data between your network and your target

Network segmentation : By splitting softwares and devices into different network classification, this helps split information and data based on role,location and other factors. By splitting the data into different classifications it allows security policies to be enforced to restrict access to data based on the identity and clearance of the user accessing the information

## Cryptography and You

### Cryptography,Password,Protection,Data,Security

Securing and encrypting information is important in the digital world to prevent the data from reaching unintended recipients. This is generally achieved through cryptography which converts messages and information into a code that can only be encrypted by the appropriate recipients. Although it is still possible for third parties to capture and encrypt the said data, it would be a long and hard process that can take ages to achieve the results they want. Although the protection of data is an important advantage of encrypting information, there are many other uses and advantages which makes the use of cryptography important. Such uses include: Limiting Access, Securing communications and assisting with companies to comply with legal requirements.

In general there are three types of cryptography:

Systemetric Key - This is where a single key is used to encrypt and decrypt information and used by both the sender and reciever. This is a fast and simple way of achieving encrpyiton but has a major flaw where the key has to be exchanged in a secure manner.

Hash Function - Commonly used to encrypt passwords on a system. Hash Function generations a hash value with a fixed length where it is impossible for contents to be recovered. No key is used for this method.

Asymmetric Key Cryptography - This method requires two sets of keys, one private and one public. In this case the users public key is used for encryption while the reciever private key is used to decrypt the information. This is a secure method as even if the public key gets intercepted or aquired by a third party, they do not have the required private key to decrpyt the information prevening easy access to the data

# 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?

```
benchiuresume.azurewebsites.net
```

## Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.15
```

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

```
Sydney NSW Australia
```

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

```
No NS record found
```

## 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    - Back end
```

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

```
Contains the format/template of the website including its layout and images
involved.
```

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?

```
Sharing of computer resources in an isolated enviroment
```

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

```
To restrict unwanted access to keys from both internal and external threats
```

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

```
Key - Public Key + Private Key - Both Interact to Authenticate data and
allow the access and transfer of encrypted data

Certificate - A File that Authenticates the authenticity of the website and
allows the transfer of data

Secret - An information that wants to be encrypted and stored
```

## Cryptography Questions

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

```
  -  Unlimited Certificate generation
  -  Free
  -  Quick set up
```

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

```
  -  Personal data can be set at risk
  -  Permanent “unknown publisher” Warning
  -  Data security isn't guaranteed
  -  Can possibly transfer errors
```

3. What is a wildcard certificate?

```
A Single certificate that can authenticate the user to multiple subdomains
related to the base 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 has flaws that allow external attackers to potentially attack and
steal information and cookies
```

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. The Domain/Website is certified by microsoft
```

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

```
From:  Fri, 10 Mar 2023 03:05:55 GMT
To :   Mon, 04 Mar 2024 03:05:55 GMT
```

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

Yes - *.azurewebsite.net

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

Yes - Microsoft Azure TLS Issuing CA 02

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.

Go Daddy Class 2 CA

# Day 3 Questions

## Cloud Security Questions

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

Both Azure Web Application Gateway and Azure Front Door are load balances, helping reduce the strain on the server

Differences

| Azure Web Application Gateway | Azure Front Door |
|---|---|
| Non-Regional Service | Regional Service |
| Load Balance Between different scale units across regions | Load Balance between VM/COntains within the Same scale |

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 where encryption/decryption occurs on a separate device.

This reduces the load on the web server increasing its overall performance

3. What OSI layer does a WAF work on?

Layer 7

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

SQL Injection Attack : Common Injection Testing Detected

- Detects and automatically blocks common methods of SQL Injection attacks.

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?

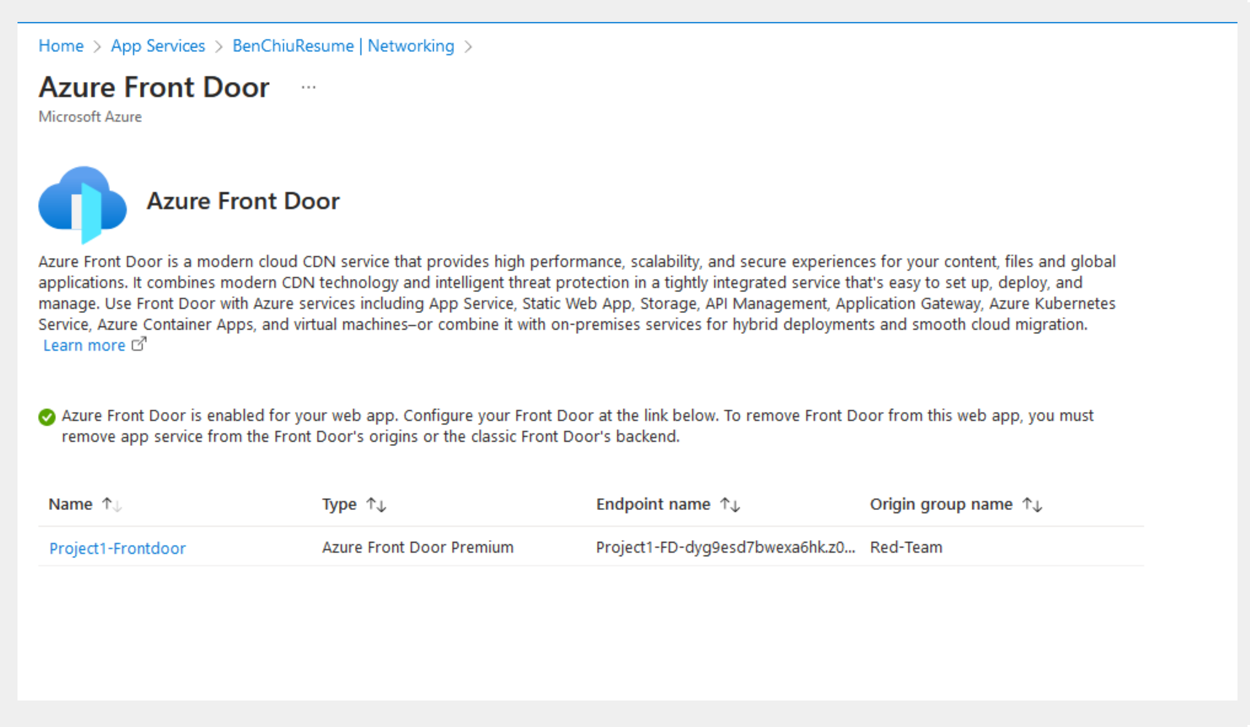
The website could be impacted by an SQL attack as the attacker could access the databases and potentially steal or modify data inside for their use.

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?

Anyone with a Canadian IP would not be able to access the website. However this can be bypassed via a VPN as that can mask their location to be from a different country.

7. Include screenshots below to demonstrate that your web app has the following:

a. Azure Front Door enabled



## Azure Front Door

Microsoft Azure

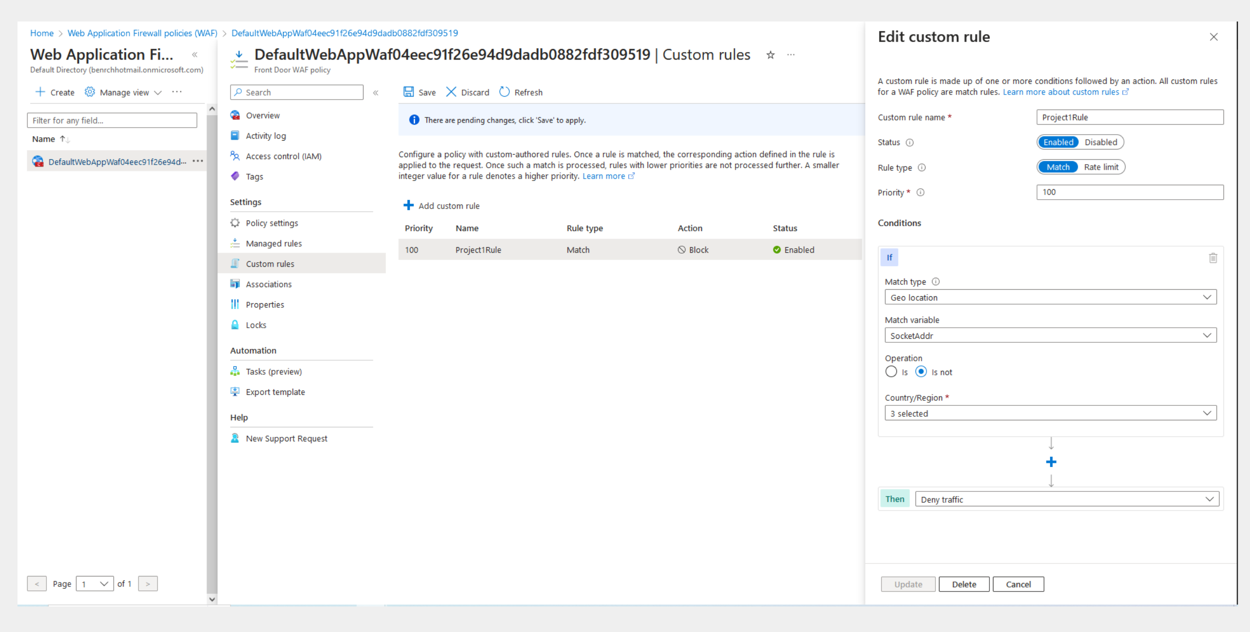
### Azure Front Door

Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. Use Front Door with Azure services including App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines–or combine it with on-premises services for hybrid deployments and smooth cloud migration. Learn more

✓ Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove app service from the Front Door's origins or the classic Front Door's backend.

| Name ↑↓ | Type ↑↓ | Endpoint name ↑↓ | Origin group name ↑↓ |
|---|---|---|---|
| Project1-Frontdoor | Azure Front Door Premium | Project1-FD-dyg9esd7bwexa6hk.z0... | Red-Team |

b. A WAF custom rule



There are pending changes, click 'Save' to apply.

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. Learn more

| Priority | Name | Rule type | Action | Status |
|---|---|---|---|---|
| 100 | Project1Rule | Match | Block | ✓ Enabled |

**Edit custom rule**

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. Learn more about custom rules

Custom rule name * Project1Rule

Status [✓ Enabled] Disabled

Rule type [✓ Match] Rate limit

Priority * 100

Conditions

If

Match type: Geo location

Match variable: SocketAddr

Operation: ○ Is ● Is not

Country/Region *: 3 selected

Then: Deny traffic

# 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***