



# Cybersecurity

## Project 1 Technical Brief

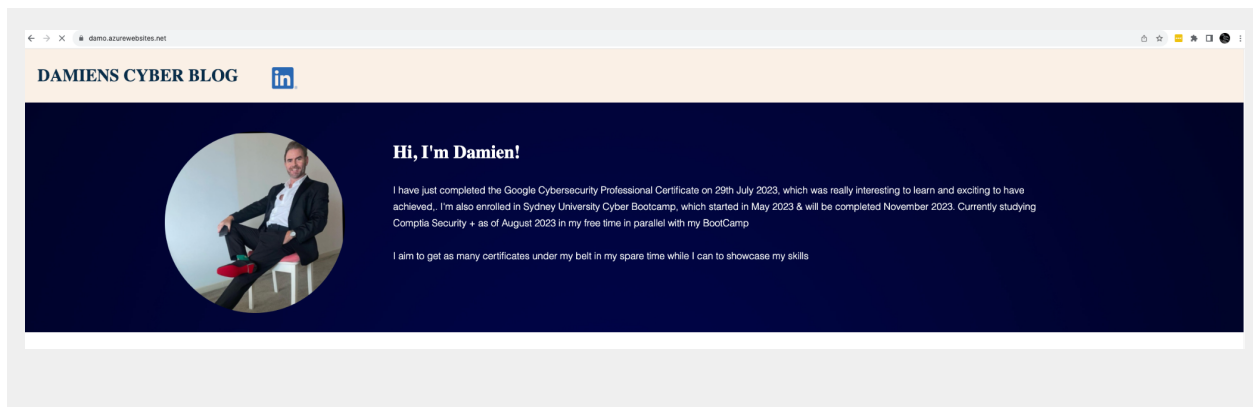
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

### Your Web Application

Enter the URL for the web application that you created:

`https://damo.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?

https://damo.azurewebsites.net/

## Networking Questions

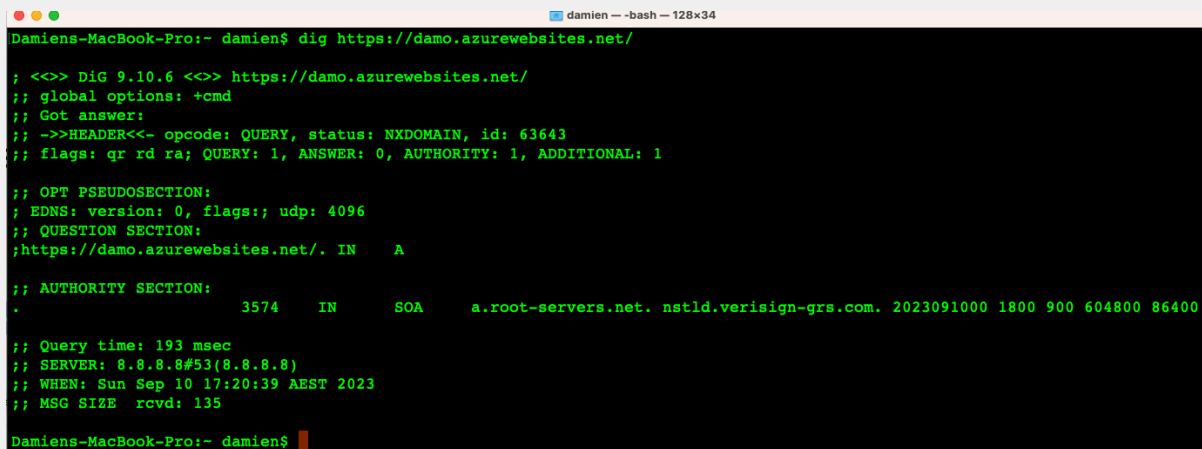
1. What is the IP address of your webpage?

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?

A terminal window titled 'damien -- -bash -- 128x34' shows the output of a 'dig' command. The command is 'dig https://damo.azurewebsites.net/'. The output shows a query for the domain 'https://damo.azurewebsites.net/' with a status of 'NXDOMAIN', indicating the domain does not exist. The output also shows the question section, authority section, and query time.

```
Damiens-MacBook-Pro:~ damien$ dig https://damo.azurewebsites.net/

; <<>> DiG 9.10.6 <<>> https://damo.azurewebsites.net/
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 63643
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;https://damo.azurewebsites.net/. IN      A

;; AUTHORITY SECTION:
.                3574      IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2023091000 1800 900 604800 86400

;; Query time: 193 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Sep 10 17:20:39 AEST 2023
;; MSG SIZE  rcvd: 135

Damiens-MacBook-Pro:~ damien$
```

## 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?

8.2

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

Yes assets, used for loading the image files and static files

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

Front end to load image files

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

A cloud tenant is a customer of the application.

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

An access policy is important on a key vault because it determines whether a user group or user can perform certain operations on KV secrets, certificates and keys

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

The differences between keys, secrets, and certificates are that certificates are used in communication to establish trust between parties, secrets are sensitive pieces of information that need to be stored securely, keys can be used to encrypt and decrypt data

### Cryptography Questions

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

The advantages of a self-signed certificate are cost, easy to create, and self-signed certificates give the user complete control of a certificate.

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

The disadvantages of using self-signed certificates include lack of trust leading to warning messages when users attempt to access website and they can be more vulnerable to attacks if not properly managed

## 3. What is a wildcard certificate?

A wildcard certificate allows a single certificate to secure multiple domainhosts pertaining to the same 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.

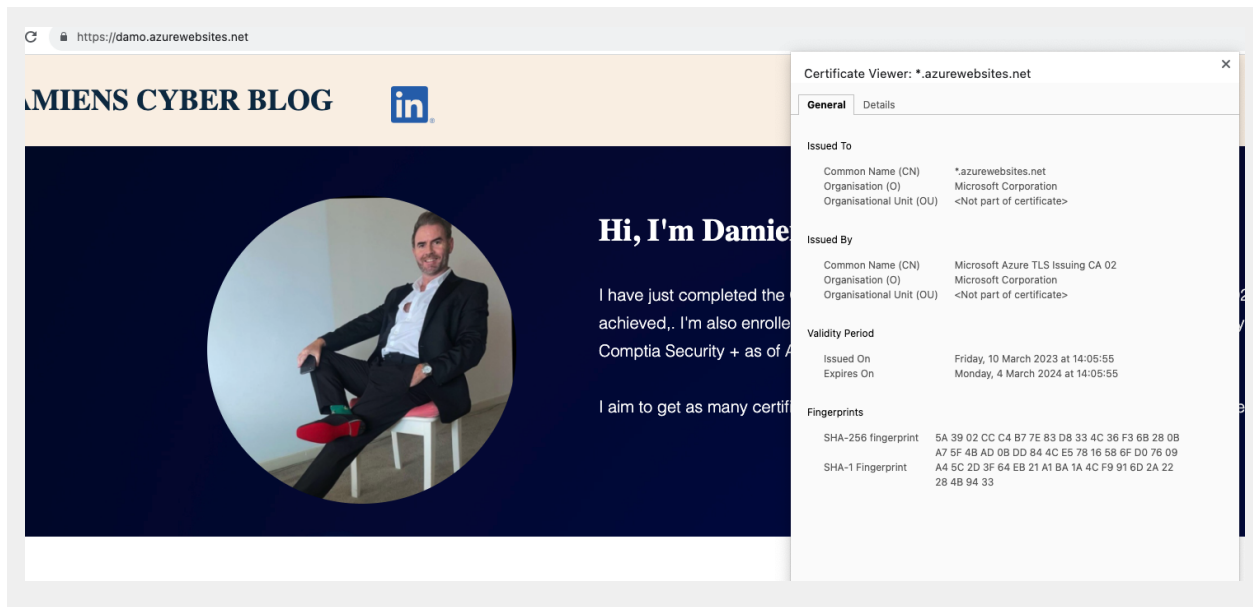
SSL 3.0 isn't provided because it is a known vulnerability.

## 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 azure is not setup for SSL cert

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



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

no

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



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?

Azure Web Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Front Door is a nonregional service whereas Application Gateway is a regional service

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

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.

A (WAF) is designed to protect against SQL injection attacks by monitoring network traffic at the application level. It inspects and blocks incoming requests for potentially malicious signatures, character sequences, or patterns indicative of an SQL injection attempt

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?

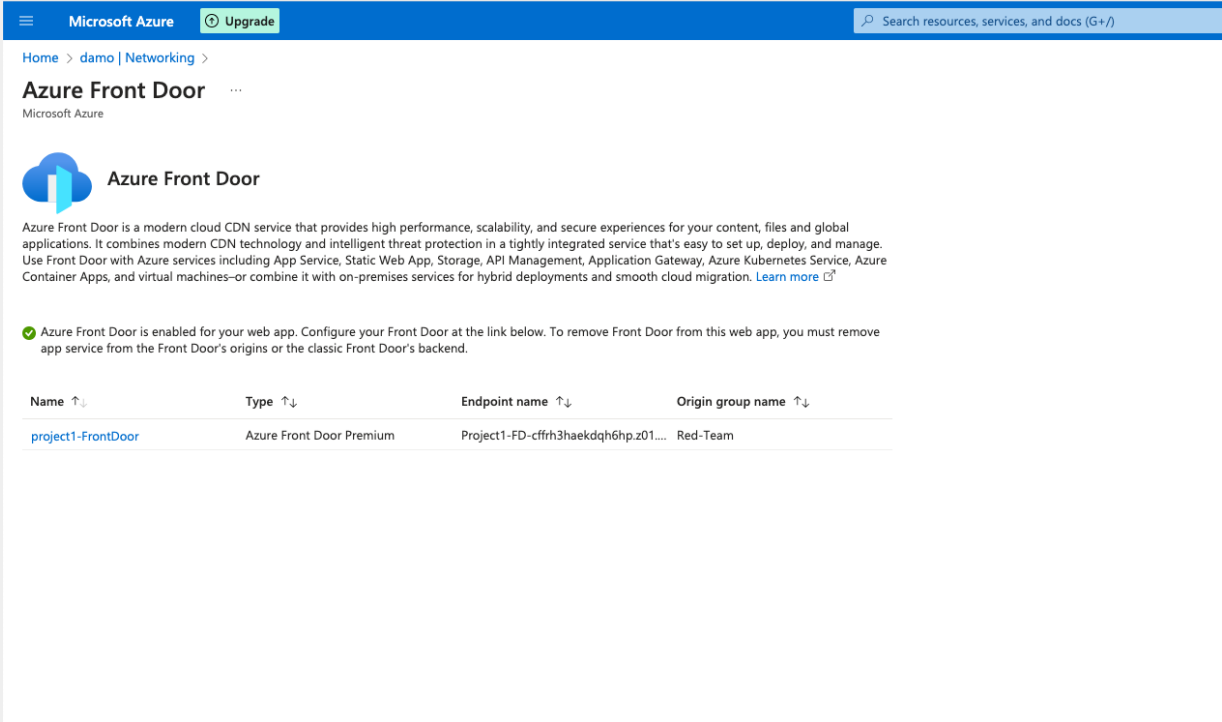
Not in particular for my site as I do not have a database linked running mysql so there is no potential risk for sql injection

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, correct based on Geo Location and IP addressing anyone in Canada will not be able to access my site.

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

a. Azure Front Door enabled




The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, an 'Upgrade' button, and a search bar. Below the navigation bar, the breadcrumb trail reads 'Home > demo | Networking >'. The main heading is 'Azure Front Door' with a sub-heading 'Microsoft Azure'. To the left of the heading is the Azure logo. Below the heading, there's a paragraph describing Azure Front Door as a modern cloud CDN service. A green checkmark icon indicates that Azure Front Door is enabled for the web app. Below this, there's a table with four columns: 'Name', 'Type', 'Endpoint name', and 'Origin group name'. The table contains one row with the following data: 'project1-FrontDoor', 'Azure Front Door Premium', 'Project1-FD-cffrh3haekdqh6hp.z01....', and 'Red-Team'.

Home > demo | Networking >

## Azure Front Door

Microsoft Azure

 **Azure Front Door**

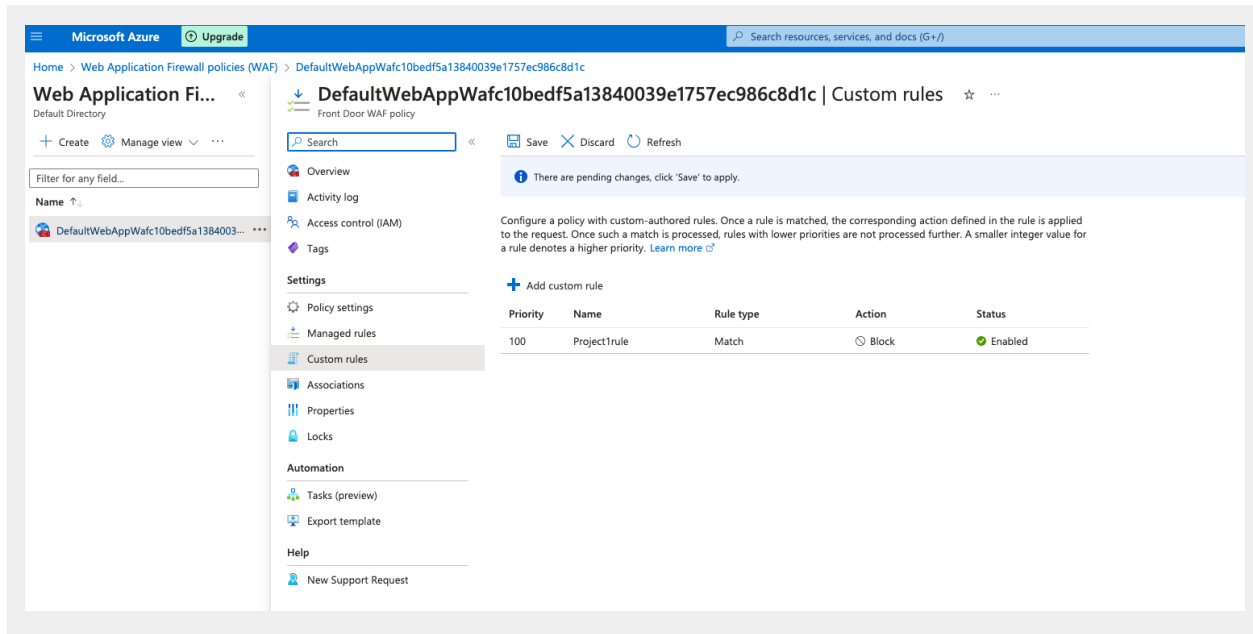
Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. 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 ↑↓
<a href="#">project1-FrontDoor</a>	Azure Front Door Premium	Project1-FD-cffrh3haekdqh6hp.z01....	Red-Team

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**