Cybersecurity

Project 1 Technical Brief

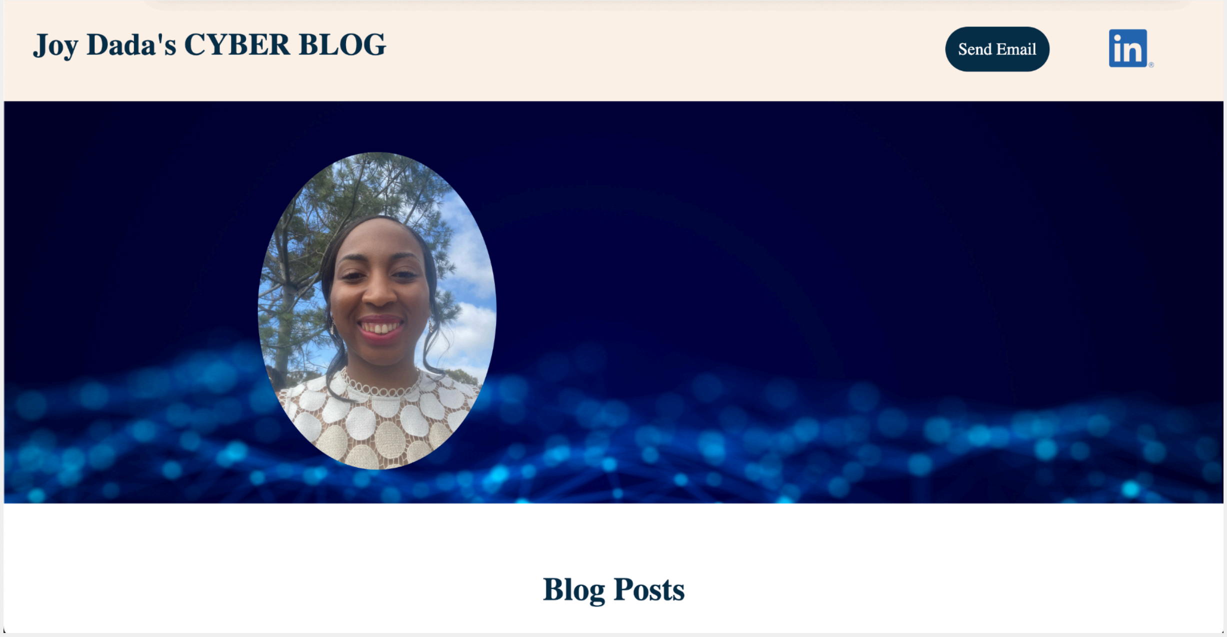
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

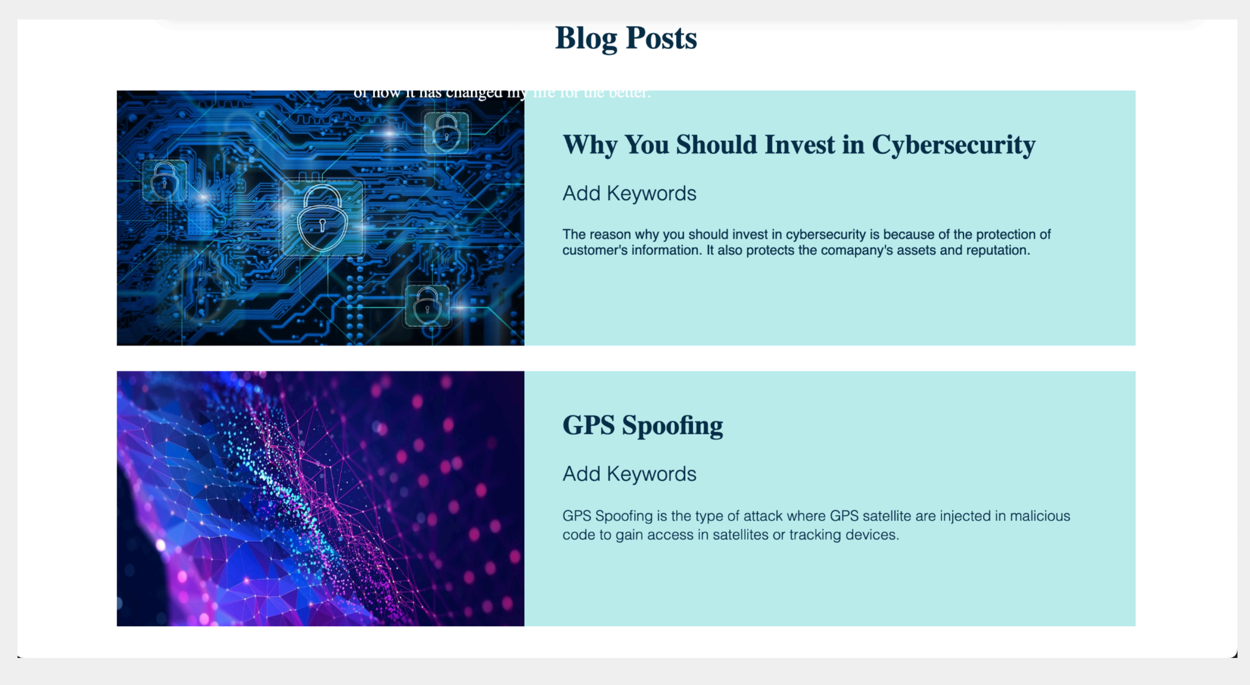
```
blackcyberspace.azurewebsites.net
```

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



Joy Dada's CYBER BLOG

Blog Posts



Blog Posts

of how it has changed my life for the better.

Why You Should Invest in Cybersecurity

Add Keywords

The reason why you should invest in cybersecurity is because of the protection of customer's information. It also protects the comapany's assets and reputation.

GPS Spoofing

Add Keywords

GPS Spoofing is the type of attack where GPS satellite are injected in malicious code to gain access in satellites or tracking devices.

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?

```
blackcyberspace.azurewebsites.net
```

Networking Questions

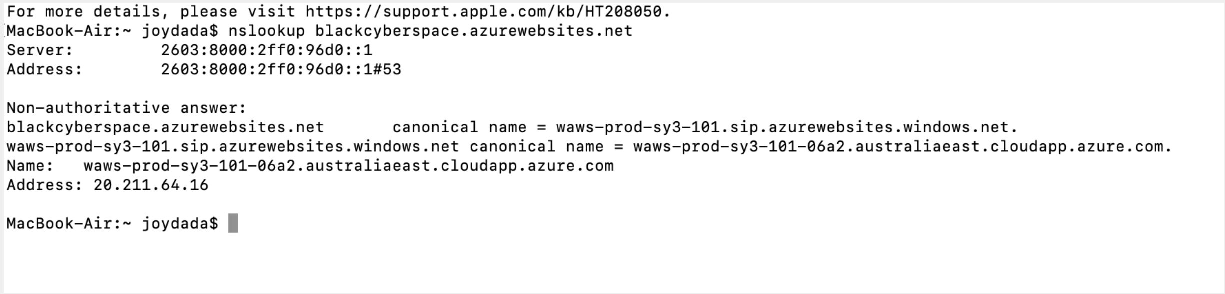
1. What is the IP address of your webpage?

```
20.211.64.16
```

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

```
Corona, CA, United States
```

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



```
For more details, please visit https://support.apple.com/kb/HT208050.
MacBook-Air:~ joydada$ nslookup blackcyberspace.azurewebsites.net
Server:         2603:8000:2ff0:96d0::1
Address:        2603:8000:2ff0:96d0::1#53

Non-authoritative answer:
blackcyberspace.azurewebsites.net       canonical name = waws-prod-sy3-101.sip.azurewebsites.windows.net.
waws-prod-sy3-101.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-101-06a2.australiaeast.cloudapp.azure.com.
Name:   waws-prod-sy3-101-06a2.australiaeast.cloudapp.azure.com
Address: 20.211.64.16

MacBook-Air:~ joydada$ 
```

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.

Assets are static files which will be deployed in the same directory as the generated documentation. Assets are usually used to add CSS, JavaScript or Images to the final documentation but they are not limited to those kind of files: any file type can be added as an asset to a template.

Answer from:

https://www.helpndoc.com/documentation/html/Assets.html#:~:text=Assets%20are%20static%20files%20which,an%20asset%20to%20a%20template.

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?

```
Tenancy in cloud computing refers to the sharing of computing resources in a
private or public environment that is isolated from other users and kept
secret.

Answer from:
https://www.loginradius.com/blog/identity/single-tenant-vs-multi-tenant/#:~:
text=Tenancy%20in%20cloud%20computing%20refers,other%20users%20and%20kept%20
secret.
```

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

```
A Key Vault access policy determines whether a given security principal,
namely a user, application or user group, can perform different operations
on Key Vault secrets, keys, and certificates. You can assign access policies
using the Azure portal, the Azure CLI, or Azure PowerShell.

Answer from:

https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-poli
cy?tabs=azure-portal
```

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

Keys: Supports multiple key types and algorithms, and enables the use of software-protected and HSM-protected keys.
Secrets: Provides secure storage of secrets, such as passwords and database connection strings.
Certificates: Supports certificates, which are built on top of keys and secrets and add an automated renewal feature. Keep in mind when a certificate is created, an

addressable key and secret are also created with the same name.
Answer from:
https://learn.microsoft.com/en-us/azure/key-vault/general/about-keys-secrets-certificates

Cryptography Questions

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

Cost effective: Self-signed certificates are free to generate and use. There are no fees associated with obtaining a certificate from a CA.
Easy to use: Self signed certificates can be generated and deployed rapidly, making them ideal for temporary or local environments.
Unlimited generation: Developers and application owners can create as many certificates as they need without limitation or dependence on other teams for certificate generation.
Internal use: Since self-signed certificates are not validated by third-party CAs, they are suitable for internal systems, private networks and test environments, where the focus is one encryption rather than trust validation.

Answer from:

https://venafi.com/blog/self-signed-certificates-cyber-criminals-can-quickly-turn-strength-vulnerability/

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

It can cost you more than you think. In the beginning, you can save some money using a free Self-Signed SSL Certificate. However, later on, the attackers can cause enormous damage to your website, compared to the price you would pay for buying an SSL Certificate.

It’s actually not free. When creating your own Self-Signed SSL Certificate, you will pay your developers to create it for you. Your developers’ work time doesn’t come for free, and it’s very expensive most of the time. If you are a developer yourself, you could probably earn more if you spend those hours working on your regular job, instead of trying to save some money by working on creating your own Self-Signed SSL Certificate. So, it takes both time and money to create a Self-Signed SSL Certificate. On top of that, you add the risk of attackers hacking you. The smallest mistakes in the Self-Signed SSL Certificate are backdoors for hackers to steal your customers’ personal information.

It is difficult to monitor. If you use Self-Signed SSL Certificates, the monitoring of your active and expiring certificates becomes difficult. At SSL Dragon we monitor your SSL Certificates and notify you when your SSL Certificates are about to expire.

It may be difficult to revoke. Self-Signed SSL Certificates are very difficult or impossible to revoke. At the same time, SSL Dragon can easily revoke an SSL Certificate, if you buy it from us.

Answer from:

https://www.ssldragon.com/blog/dangers-self-signed-certificates/

3. What is a wildcard certificate?

A wildcard certificate is a type of SSL/TLS certificate that can be used to secure multiple domains (hosts), indicated by a wildcard character (*) in the domain name field.

Answer from:

https://www.keyfactor.com/blog/what-is-a-wildcard-certificate/

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.

Microsoft switched to TLS as SSL had a lot vulnerabilities

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?

```
Yes because we are using a tls certificate
```

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

```
Issued On
Tuesday, October 31, 2023 at 4:15:02 PM
Expires On
Thursday, June 27, 2024 at 4:59:59 PM
```

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

```
Yes Microsoft azure TLS issuing CA 01
```

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

```
Yes.Digicert Global Root G2
```

    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 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.

Answer from:
https://learn.microsoft.com/en-us/answers/questions/301218/azure-waf-frontdoor-vs-azure-waf-application-gatew

Azure Front Door and Azure Application Gateway are both load balancers for HTTP/HTTPS traffic, but they have different scopes. Front Door is a global service that can distribute requests across regions, while Application Gateway is a regional service that can balance requests within a region.

Answer from:
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq

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

SSL offloading relieves a web server of the processing burden of encrypting and decrypting traffic sent via SSL. Every web browser is compatible with SSL security protocol, making SSL traffic common. The processing is offloaded to a separate server designed specifically to perform SSL acceleration or SSL termination.

Answer from:
https://avinetworks.com/glossary/ssl-offload/#:~:text=SSL%20offloading%20relieves%20a%20web,SSL%20acceleration%20or%20SSL%20termination.

3. What OSI layer does a WAF work on?

Application

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

Directory traversal is a type of HTTP exploit in which a hacker uses the software on a web server to access data in a directory other than the server's root directory. If the attempt is successful, the threat actor can view restricted files or execute commands on the server.

Answer from:
https://www.techtarget.com/searchsecurity/definition/directory-traversal#:~:text=Directory%20traversal%20is%20a%20type,execute%20commands%20on%20the%20server.

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?

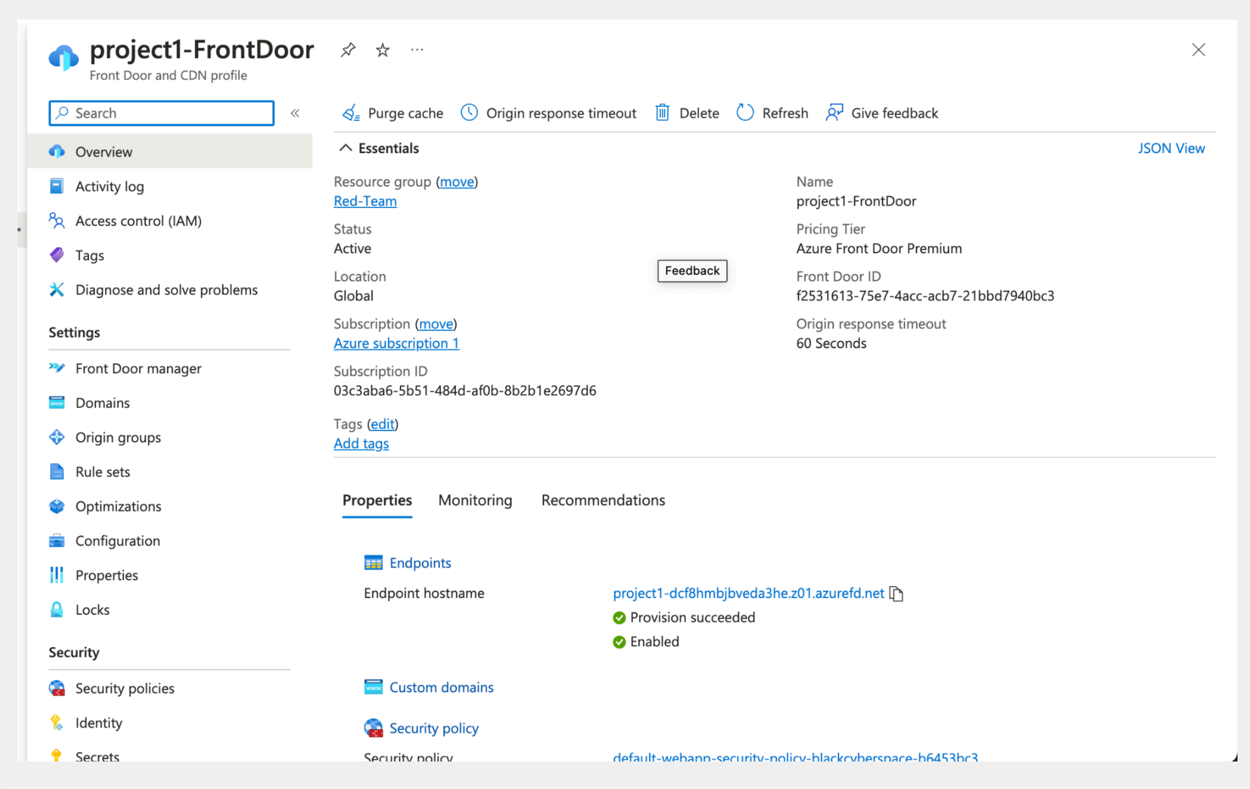
No, because my website is protected by SQL code and query strings.

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 they cannot get access to my website unless their IP address is added to the waf rule granting them access

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

    a. Azure Front Door enabled



project1-FrontDoor

Front Door and CDN profile

Essentials

Resource group (move)
Red-Team

Status
Active

Location
Global

Subscription (move)
Azure subscription 1

Subscription ID
03c3aba6-5b51-484d-af0b-8b2b1e2697d6

Tags (edit)
Add tags

Name
project1-FrontDoor

Pricing Tier
Azure Front Door Premium

Front Door ID
f2531613-75e7-4acc-acb7-21bbd7940bc3

Origin response timeout
60 Seconds

Endpoints

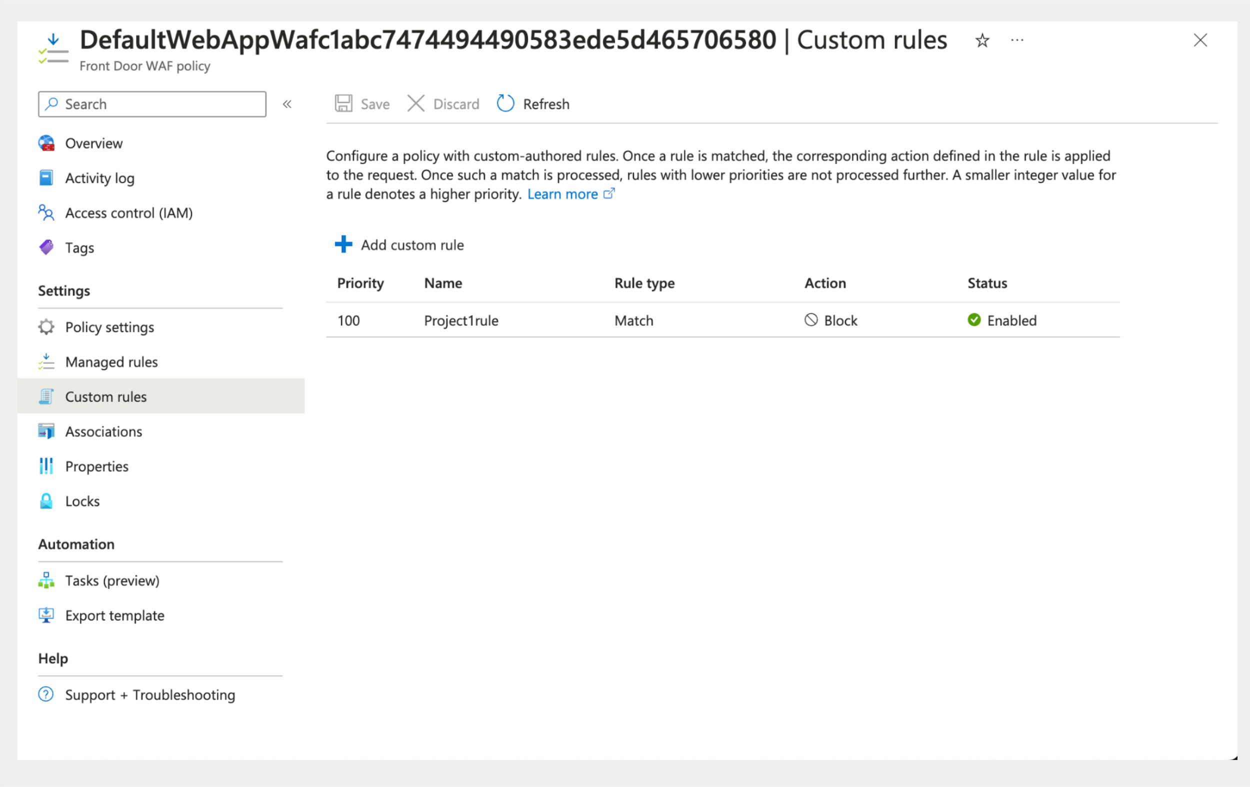
Endpoint hostname: project1-dcf8hmbjbveda3he.z01.azurefd.net
✓ Provision succeeded
✓ Enabled

Custom domains

Security policy

Security policy: default-webapp-security-policy-blackcyberspace-b6453bc3

b. A WAF custom rule



DefaultWebAppWafc1abc7474494490583ede5d465706580 | Custom rules

Front Door WAF policy

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

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.*