Cybersecurity

Project 1 Technical Brief

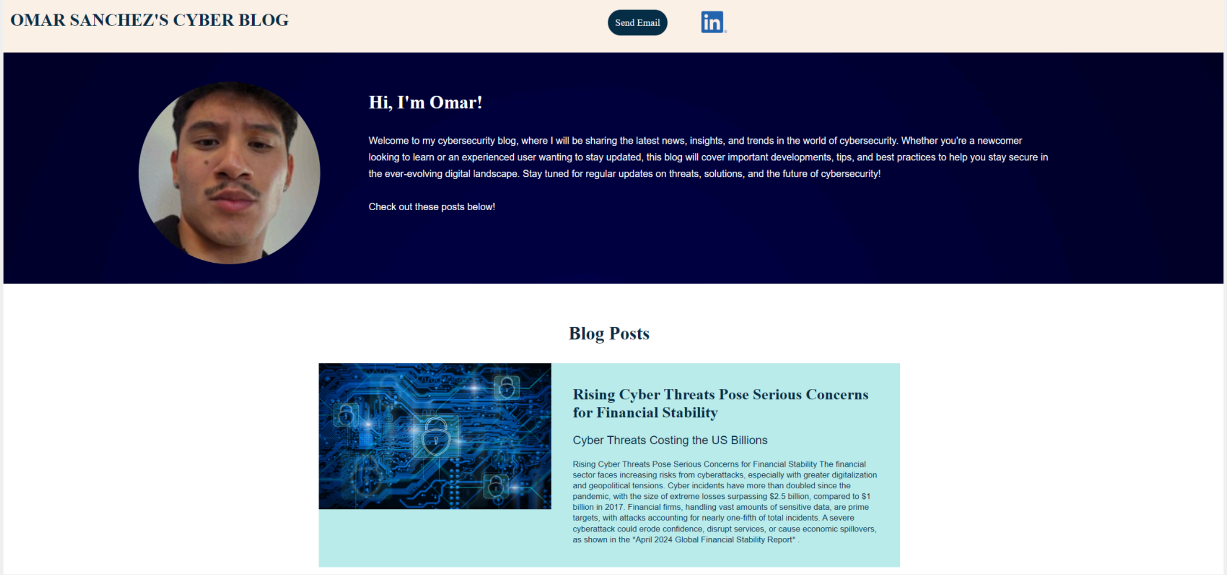
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
omarproject1-endefwbufncdd4c2.brazilsouth-01.azurewebsites.net
```

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



Hi, I'm Omar!

Welcome to my cybersecurity blog, where I will be sharing the latest news, insights, and trends in the world of cybersecurity. Whether you're a newcomer looking to learn or an experienced user wanting to stay updated, this blog will cover important developments, tips, and best practices to help you stay secure in the ever-evolving digital landscape. Stay tuned for regular updates on threats, solutions, and the future of cybersecurity!

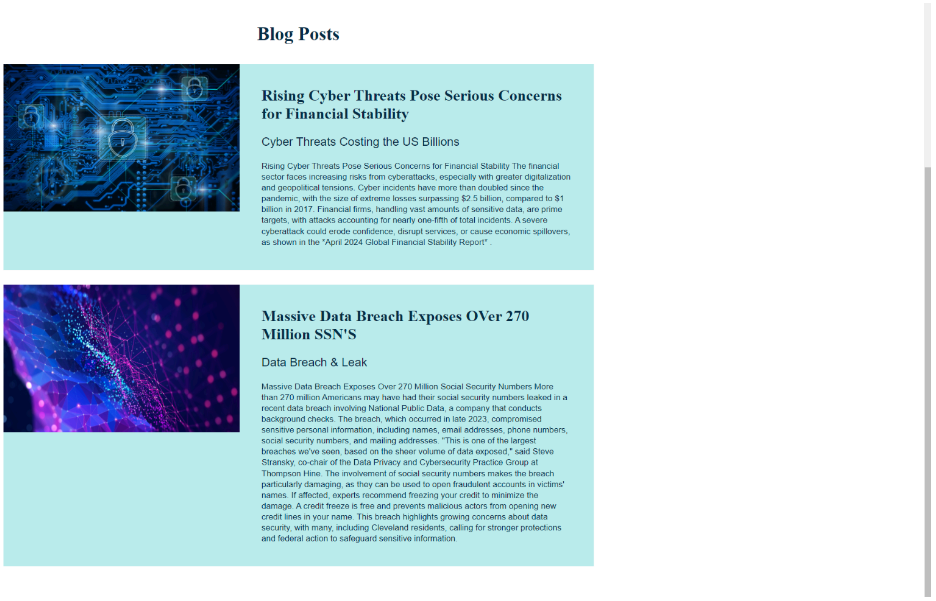
Check out these posts below!

Blog Posts

Rising Cyber Threats Pose Serious Concerns for Financial Stability

Cyber Threats Costing the US Billions

Rising Cyber Threats Pose Serious Concerns for Financial Stability The financial sector faces increasing risks from cyberattacks, especially with greater digitalization and geopolitical tensions. Cyber incidents have more than doubled since the pandemic, with the size of extreme losses surpassing $2.5 billion, compared to $1 billion in 2017. Financial firms, handling vast amounts of sensitive data, are prime targets, with attacks accounting for nearly one-fifth of total incidents. A severe cyberattack could erode confidence, disrupt services, or cause economic spillovers, as shown in the *April 2024 Global Financial Stability Report* .



Blog Posts

Rising Cyber Threats Pose Serious Concerns for Financial Stability

Cyber Threats Costing the US Billions

Rising Cyber Threats Pose Serious Concerns for Financial Stability The financial sector faces increasing risks from cyberattacks, especially with greater digitalization and geopolitical tensions. Cyber incidents have more than doubled since the pandemic, with the size of extreme losses surpassing $2.5 billion, compared to $1 billion in 2017. Financial firms, handling vast amounts of sensitive data, are prime targets, with attacks accounting for nearly one-fifth of total incidents. A severe cyberattack could erode confidence, disrupt services, or cause economic spillovers, as shown in the *April 2024 Global Financial Stability Report* .

Massive Data Breach Exposes OVer 270 Million SSN'S

Data Breach & Leak

Massive Data Breach Exposes Over 270 Million Social Security Numbers More than 270 million Americans may have had their social security numbers leaked in a recent data breach involving National Public Data, a company that conducts background checks. The breach, which occurred in late 2023, compromised sensitive personal information, including names, email addresses, phone numbers, social security numbers, and mailing addresses. "This is one of the largest breaches we've seen, based on the sheer volume of data exposed," said Steve Stransky, co-chair of the Data Privacy and Cybersecurity Practice Group at Thompson Hine. The involvement of social security numbers makes the breach particularly damaging, as they can be used to open fraudulent accounts in victims' names. If affected, experts recommend freezing your credit to minimize the damage. A credit freeze is free and prevents malicious actors from opening new credit lines in your name. This breach highlights growing concerns about data security, with many, including Cleveland residents, calling for stronger protections and federal action to safeguard sensitive information.

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?

```
Omarsanchezproject1
```

Networking Questions

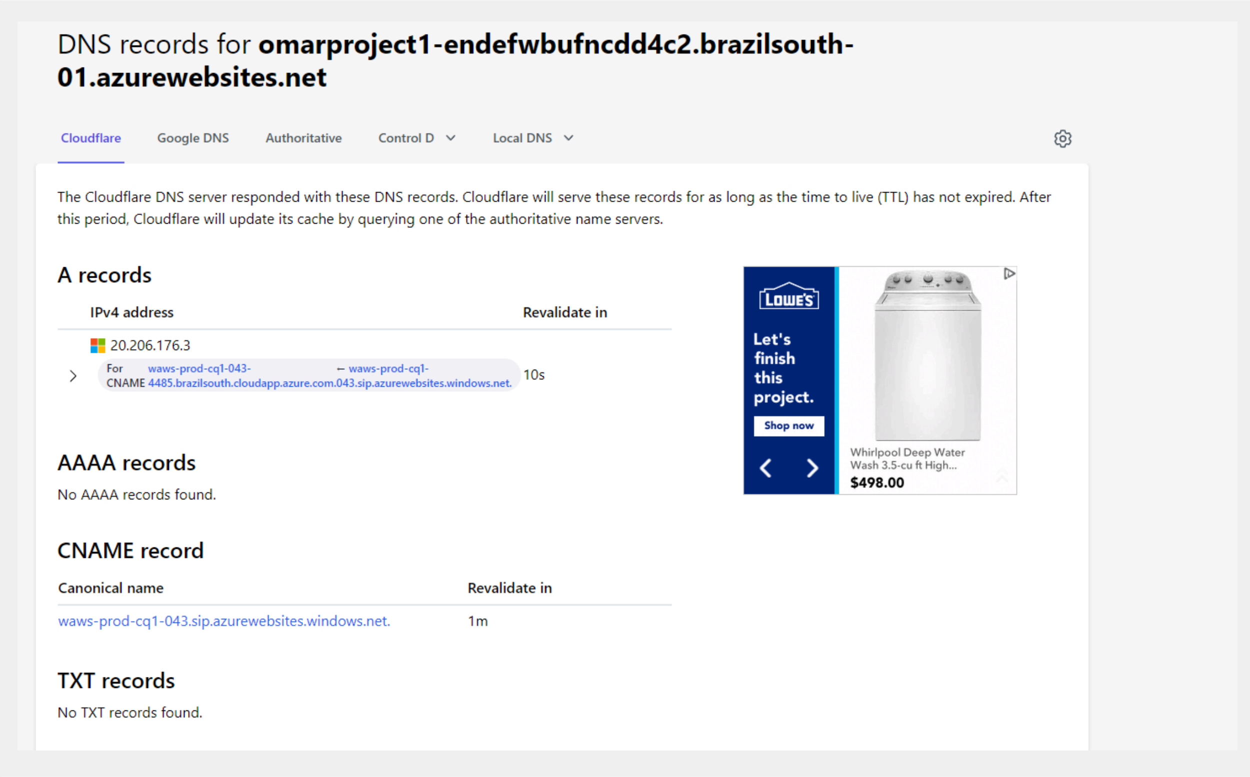
1. What is the IP address of your webpage?

20.206.176.3

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

```
SOUTHERN BRAZIL
```

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



DNS records for **omarproject1-endefwbufncdd4c2.brazilsouth-01.azurewebsites.net**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
20.206.176.3 For CNAME waws-prod-cq1-043-4485.brazilsouth.cloudapp.azure.com. ← waws-prod-cq1-043.sip.azurewebsites.windows.net.	10s

AAAA records

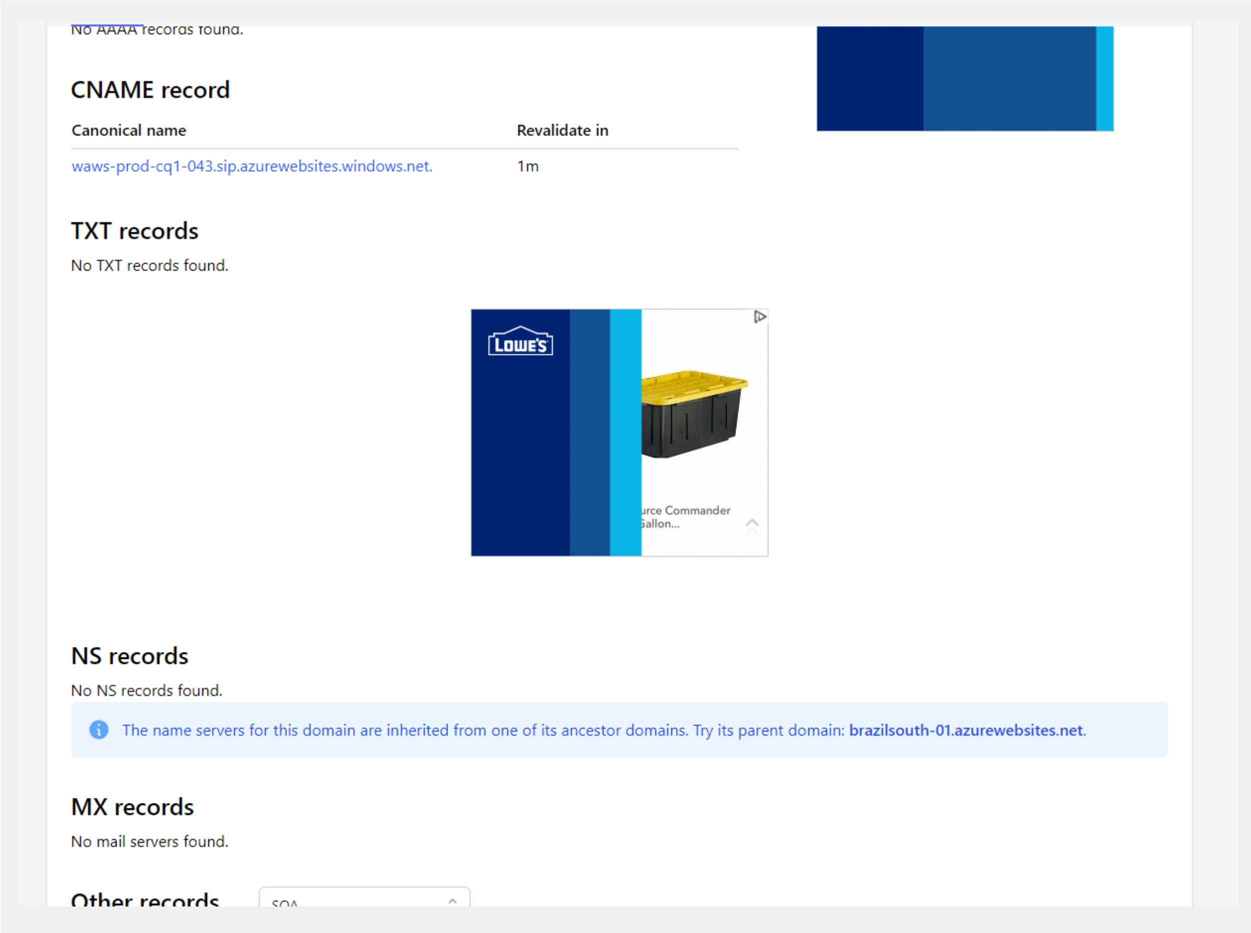
No AAAA records found.

CNAME record

Canonical name	Revalidate in
waws-prod-cq1-043.sip.azurewebsites.windows.net.	1m

TXT records

No TXT records found.



No AAAA records found.

CNAME record

Canonical name	Revalidate in
waws-prod-cq1-043.sip.azurewebsites.windows.net.	1m

TXT records

No TXT records found.

NS records

No NS records found.

The name servers for this domain are inherited from one of its ancestor domains. Try its parent domain: **brazilsouth-01.azurewebsites.net**.

MX records

No mail servers found.

Other records SOA

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?

Html So front end

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

Looks like data backups for my website

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

```
It's a front-end command that backs up my data for the front-end process of my website. So front end
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is a logical space within a cloud computing environment that provides isolation, resource sharing, scalability, and management capabilities for a specific user or organization
```

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

```
An access policy on a key vault is important and primarily related to the security, compliance, and effective management of sensitive data
```

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

```
Keys: Used for encryption/decryption.
Secrets: Store sensitive information like passwords and API keys.
Certificates: Bind a public key to an entity for identity verification and secure communication.
```

Cryptography Questions

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

```
Self-signed certificates are cost-effective, easy to create, and provide full control over the certificate properties. They are handy for development, testing, and internal applications where external trust is not a requirement. However, they are not recommended for public-facing services due to trust issues with users and browsers.
```

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

While self-signed certificates can be useful in specific scenarios, they lack trust from browsers, create user confusion, and require manual trust management. Their limitations make them unsuitable for production use in public-facing services, where security and trust are super important.

3. What is a wildcard certificate?

A wildcard certificate is an SSL/TLS certificate that secures multiple subdomains of a single domain under one certificate, providing cost savings, simplified management, and flexibility for organizations that need to secure multiple web services.

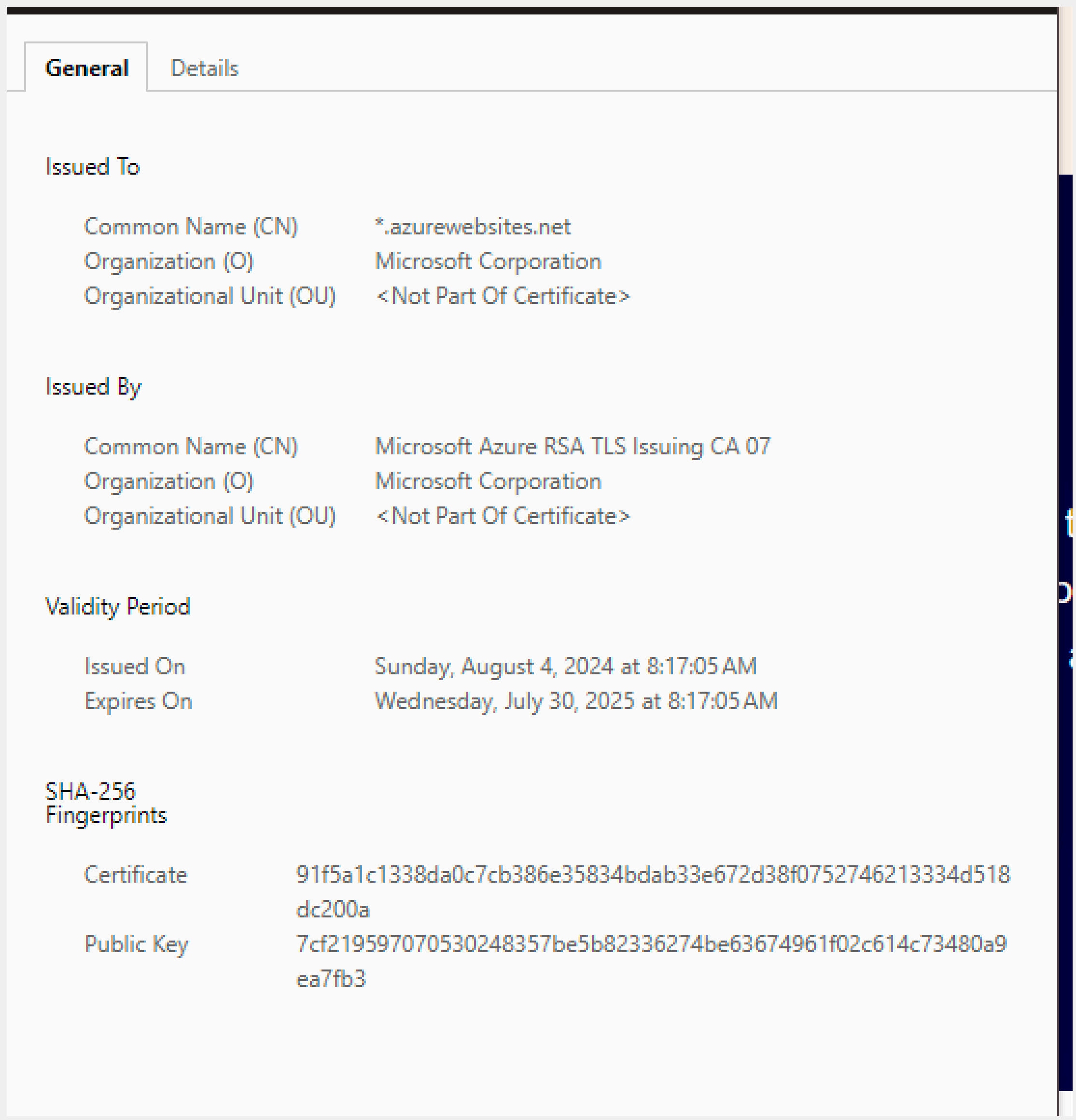
4. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn’t provided.

SSL 3.0 is not provided by Azure due to its significant security vulnerabilities, and outdated status. TLS proved to be stronger and more secure than its old counterpart.

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 error, My website is ecure.



Issued To

Common Name (CN)	*.azurewebsites.net
Organization (O)	Microsoft Corporation
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Microsoft Azure RSA TLS Issuing CA 07
Organization (O)	Microsoft Corporation
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Sunday, August 4, 2024 at 8:17:05 AM
Expires On	Wednesday, July 30, 2025 at 8:17:05 AM

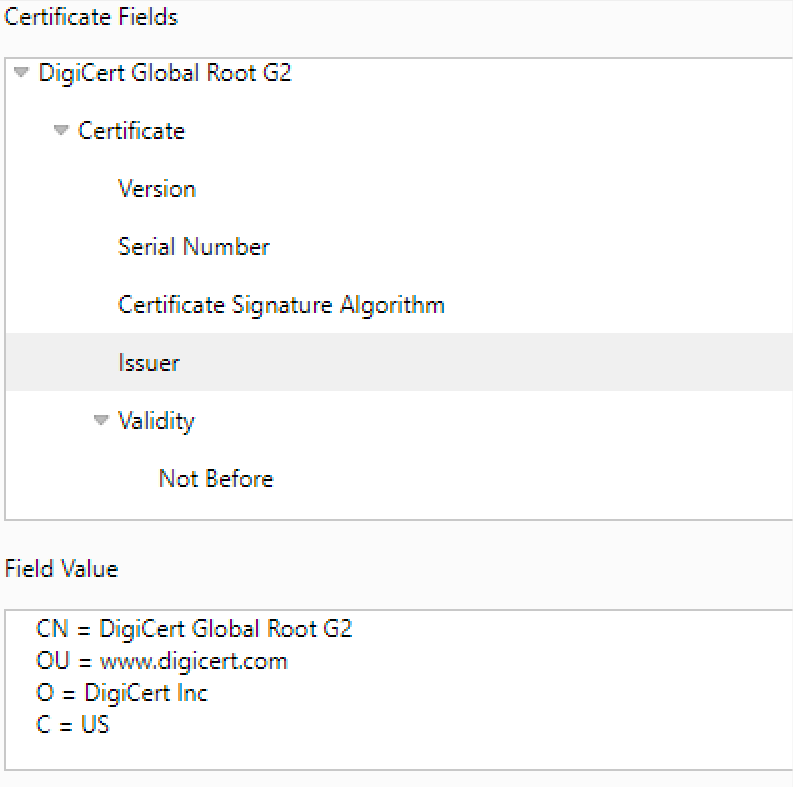
SHA-256 Fingerprints

Certificate	91f5a1c1338da0c7cb386e35834bdab33e672d38f0752746213334d518dc200a
Public Key	7cf219597070530248357be5b82336274be63674961f02c614c73480a9ea7fb3

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

```
Not before 8/4/24, 8:17:05 AM PDT, Not After 7/30/25, 8:17:05 AM PDT
```

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



Certificate Fields

- DigiCert Global Root G2
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

```
CN = DigiCert Global Root G2
OU = www.digicert.com
O = DigiCert Inc
C = US
```

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

```
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.

```
Let's Encrypt
```

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 designed to optimize application delivery and provide security features such as Web Application Firewall.

they both offer load-balancing capabilities to distribute traffic across multiple instances of applications.

Azure Front Door is focused on global load balancing and routing, optimizing traffic across multiple regions, while Azure Web Application Gateway is designed for regional load balancing and operates at the application layer.

Front Door supports SSL offloading at the edge, reducing latency for global users, whereas Web Application Gateway provides SSL termination closer to the backend services.

Front Door is suitable for multi-region applications with global reach, while Web Application Gateway is ideal for single-region applications requiring more fine-grained control over traffic management within a region.

2. What is SSL offloading? What are its benefits?

SSL offloading is the process of removing the SSL-based encryption from incoming requests at a dedicated device, such as a load balancer or application gateway, instead of having the web server handle it. This approach offers several benefits, including improved performance by reducing the load on web servers, allowing them to focus on content delivery and improving response times. SSL offloading enhances scalability, enabling better handling of higher traffic volumes. It also simplifies SSL certificate management by centralizing it on the offloading device, making updates and renewals more efficient. Furthermore, SSL offloading allows for the implementation of advanced security features, such as Web Application Firewalls, without negatively impacting server 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 is a type of web application vulnerability that occurs when an attacker is able to manipulate an application's SQL queries by injecting malicious SQL code into input fields. This can lead to unauthorized access to the database, allowing attackers to retrieve, modify, or delete data.

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?

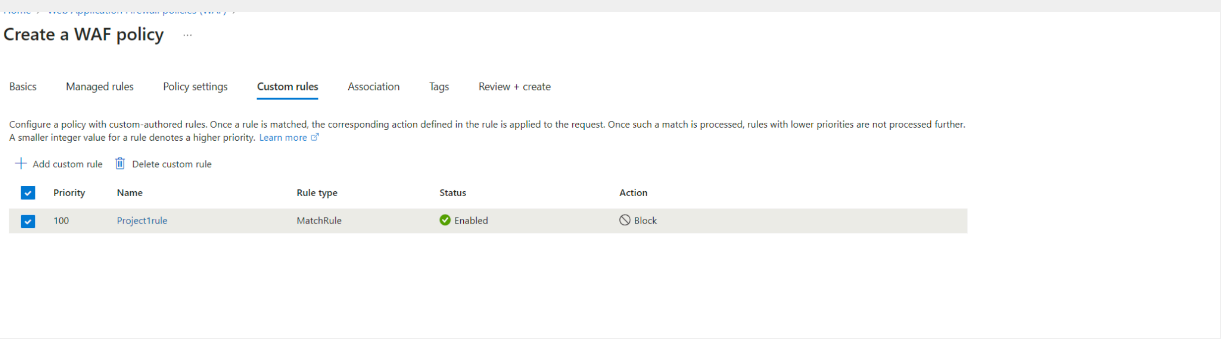
I think yes, Just cause there is always a chance that an attack could happen and someone could get the root access to my website and i only flagged USA AUSTRALIA AND CANADA

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, if you create a custom WAF rule to block all traffic from Canada, it would mean that anyone physically located in Canada would not be able to access your website, but those users could use private VPNS to use a different IP and still access my website

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

   a. A WAF custom rule



Home > Web Application Firewall policies (WAF) >

Create a 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	Status	Action
☑	100	Project1rule	MatchRule	✓ Enabled	⃠ Block

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*