



Cybersecurity

Project 1 Technical Brief

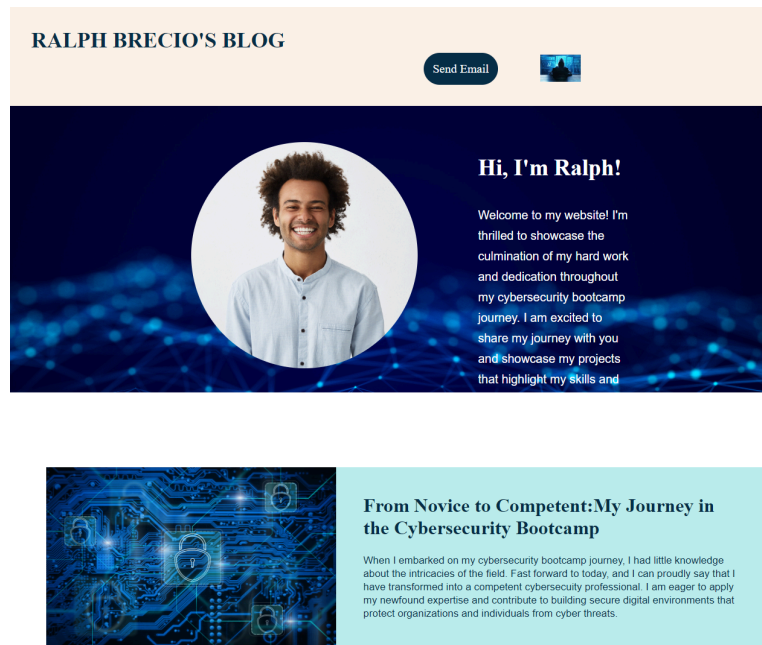
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

ralphssecurityresume.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?

Ralphssecurityresume

Networking Questions

1. What is the IP address of your webpage?

20.119.136.8

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

City: Boydton

State: VA

Country: US

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

```
C:\Users\ralph>nslookup ralphssecurityresume.azurewebsites.net
Server:  G3100.mynetworksettings.com
Address:  2600:4040:25e2:e000::1
```

Non-authoritative answer:

Name: waws-prod-bn1-191-1ef5.eastus2.cloudapp.azure.com

Address: 20.119.136.8

Aliases: ralphssecurityresume.azurewebsites.net
waws-prod-bn1-191.sip.azurewebsites.windows.net

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. Front end

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

Contains 2 directories: `css` and `images`

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?

A logical or virtual environment created within a cloud service provider's infrastructure to isolate and manage resources for a specific organization or user group.

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

You can ensure that only authorized individuals or applications have the necessary permissions to read, write or manage the stored secrets. Access policies help protect confidentiality and integrity of sensitive information stored in the Key Vault by providing controlled access to authorized entities.

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

Keys are used for encryption, decryption, signing or verifying signatures. Usually used in scenarios where you need to protect data with encryption or ensure data integrity with digital signatures. Secrets are sensitive information, such as passwords, connection strings, API keys, or any other application-specific configuration values and are typically used to store credentials or sensitive data that applications require for their functionality. Secrets can be stored as strings of text. Certificates are digital documents that contain an entity's public key and are used for authentication, encryption, or secure communication.

Cryptography Questions

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

- free to create and used
- have full control over the self-signed certificates
- suitable for internal use or for development and testing purposes
- secure communication

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

- not trusted by default web browsers
- do not provide any external validation
- very limited external use

3. What is a wildcard certificate?

A type of SSL/TLS certificate that is used to secure multiple subdomains under a single domain with a single 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.

It is due to security concerns and vulnerabilities associated with the protocol. SSL 3.0 has been deprecated and considered insecure due to several vulnerabilities, including the POODLE attack which exploited the weakness in SSL 3.0 that allowed an attacker to decrypt secure information by downgrading the connection to use SSL 3.0.

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. This is due to the fact that the certificate was not created by a trusted CA and was created by me.

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

1 year

- 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?

No

- 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?

Similarities:

- both services can route incoming requests to different backend resources based on various criteria such as URL path, host headers, or request headers
- they offer load balancing functionality
- both services can handle SSL/TLS termination
- both services provide web application security

Differences:

- Web Application Gateway operates at layer 7 of the OSI model while Azure front door operates at the layer 4
- Azure front door is designed to be a global service with a distributed network of points of presence while Web Application Gateway operates within a specific region
- Azure front door offers more advanced routing capabilities

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

SSL offloading helps optimize performance, simplifies SSL management, enhances security controls, and provides flexibility in SSL configuration, making it a valuable feature for handling SSL/TLS traffic in a scalable and secure manner.

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:

It is a type of attack where an attacker maliciously injects SQL code into a web application’s input fields, typically in forms of URL parameters, with the intention of manipulating the application’s database backend.

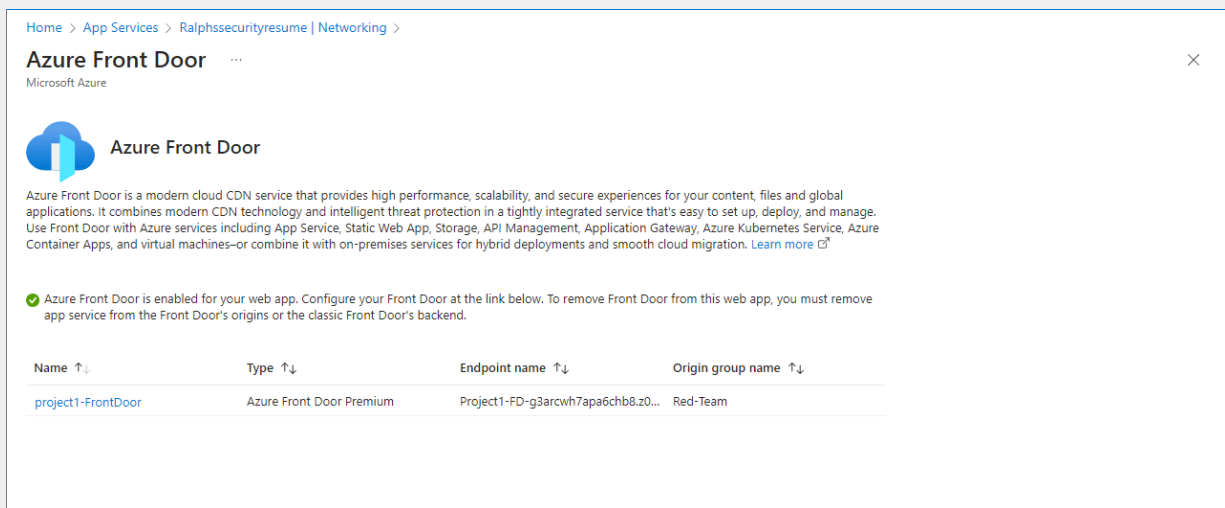
5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn’t enabled? Why or why not?

Yes. The absence of Front door wouldn't directly impact the existence of the vulnerability itself. The website needs more specific rules and configurations if the goal is to make it safe from SQL Injections

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. It would only prevent access from users with Canadian IP addresses and some users from Canada could use an IP address from a different country and still access the website.


7. Include screenshots below to demonstrate that your web app has the following:
- a. Azure Front Door enabled



Home > App Services > Ralphssecurityresume | Networking >

Azure Front Door

Microsoft Azure

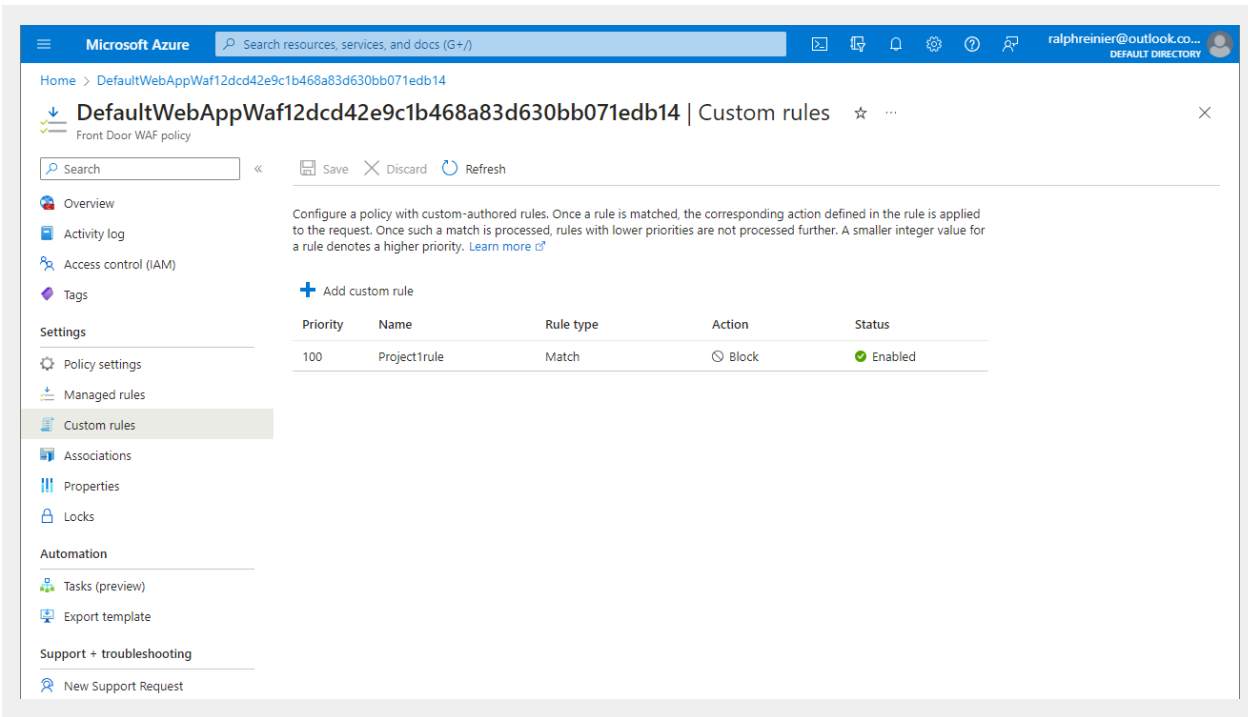
 **Azure Front Door**

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 ↑↓
project1-FrontDoor	Azure Front Door Premium	Project1-FD-g3arcwh7apa6chb8.z0...	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.*

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