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.

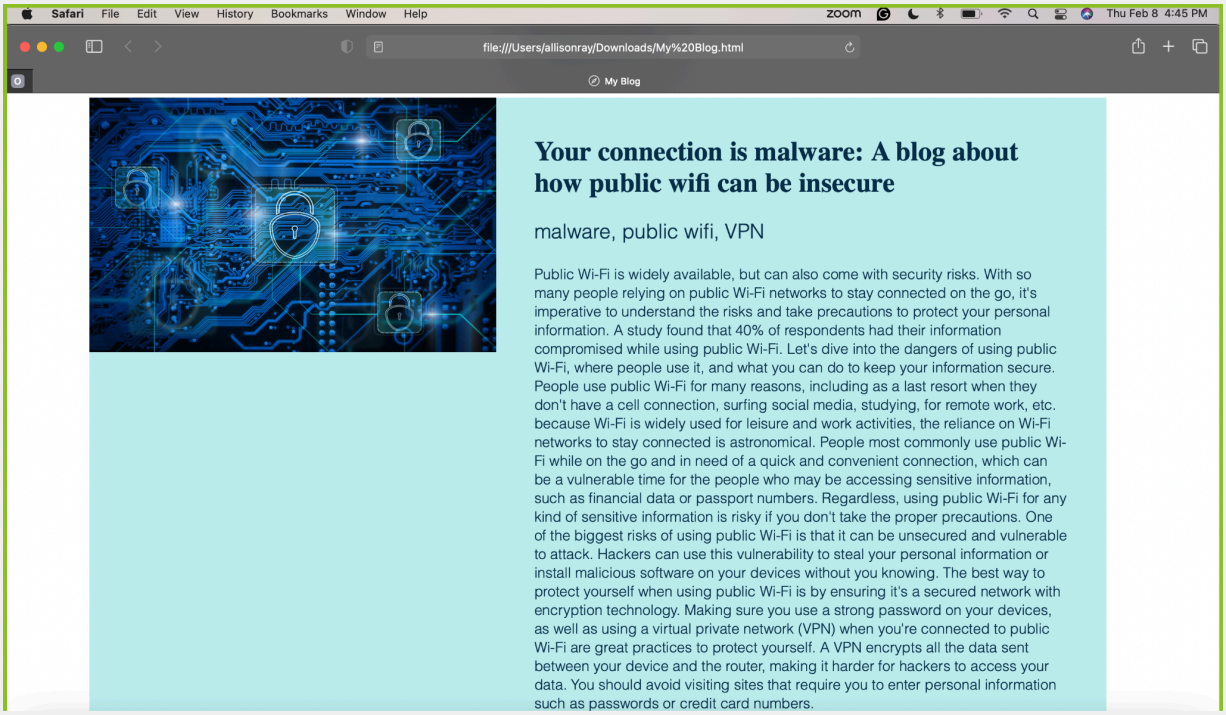
Your Web Application

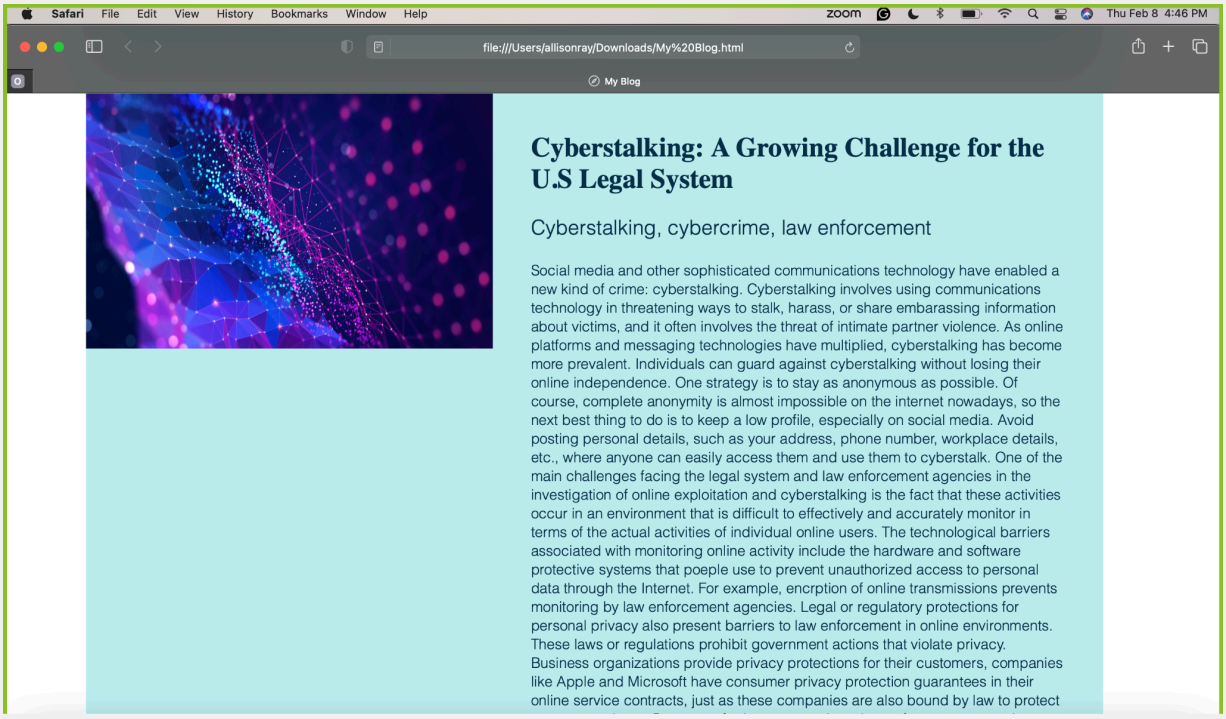
Enter the URL for the web application that you created:

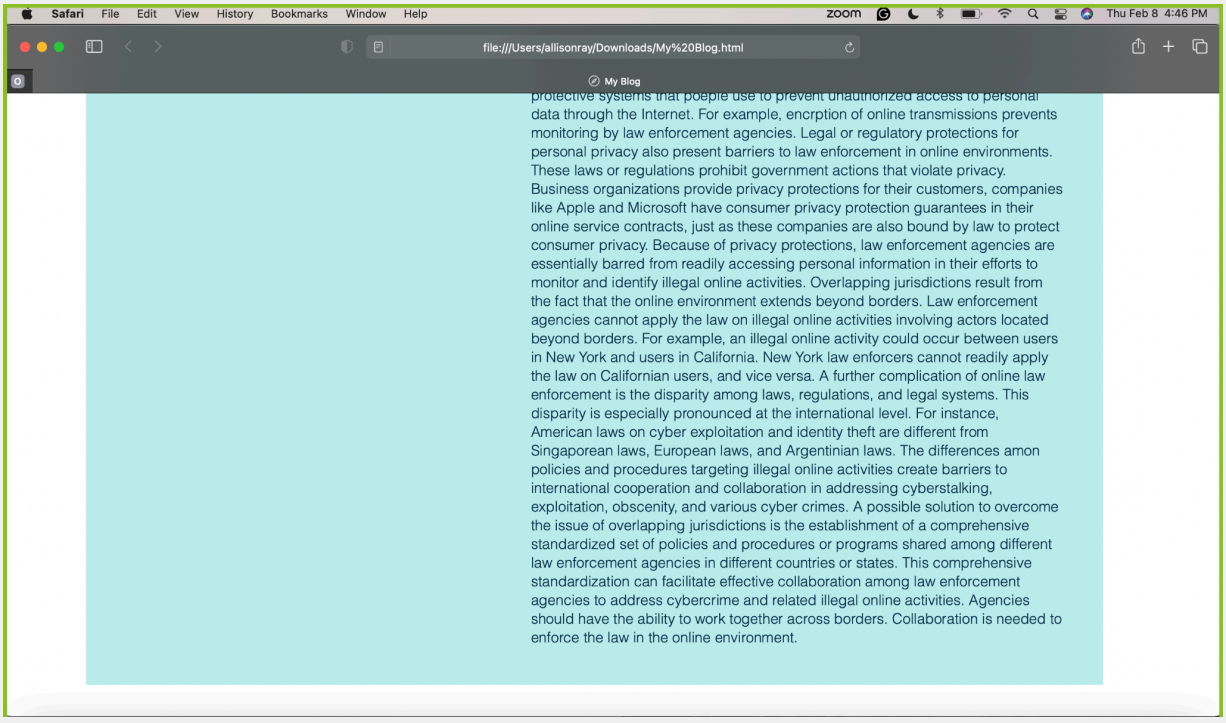
https://everythingcyber.azurewebsites.net/

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


Safari File Edit View History Bookmarks Window Help
Thu Feb 8 4:45 PM
file:///Users/allisonray/Downloads/My%20Blog.html
My Blog
ALLISON RAY'S CYBER BLOG
Send Email
Hi, I'm Allison!
Hey there, welcome to my blog! I talk about all things cyber, striving to keep you up to date on cyber threats, news, and ways to protect yourself. It's something that I'm passionate about and I think it's important to share my thoughts and opinions with others.
So, grab a cup of coffee or tea, sit back, and let's dive into this topic together!
Blog Posts


Safari File Edit View History Bookmarks Window Help
Thu Feb 8 4:45 PM
file:///Users/allisonray/Downloads/My%20Blog.html
My Blog
Your connection is malware: A blog about how public wifi can be insecure
malware, public wifi, VPN
Public Wi-Fi is widely available, but can also come with security risks. With so many people relying on public Wi-Fi networks to stay connected on the go, it's imperative to understand the risks and take precautions to protect your personal information. A study found that 40% of respondents had their information compromised while using public Wi-Fi. Let's dive into the dangers of using public Wi-Fi, where people use it, and what you can do to keep your information secure. People use public Wi-Fi for many reasons, including as a last resort when they don't have a cell connection, surfing social media, studying, for remote work, etc. because Wi-Fi is widely used for leisure and work activities, the reliance on Wi-Fi networks to stay connected is astronomical. People most commonly use public Wi-Fi while on the go and in need of a quick and convenient connection, which can be a vulnerable time for the people who may be accessing sensitive information, such as financial data or passport numbers. Regardless, using public Wi-Fi for any kind of sensitive information is risky if you don't take the proper precautions. One of the biggest risks of using public Wi-Fi is that it can be unsecured and vulnerable to attack. Hackers can use this vulnerability to steal your personal information or install malicious software on your devices without you knowing. The best way to protect yourself when using public Wi-Fi is by ensuring it's a secured network with encryption technology. Making sure you use a strong password on your devices, as well as using a virtual private network (VPN) when you're connected to public Wi-Fi are great practices to protect yourself. A VPN encrypts all the data sent between your device and the router, making it harder for hackers to access your data. You should avoid visiting sites that require you to enter personal information such as passwords or credit card numbers.





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?

```
everythingcyber.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.119.8.42
```

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

```
Washington, Virginia, United States
```

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

```
Server:         192.168.12.1
Address: 192.168.12.1#53
Non-authoritative answer:
everythingcyber.azurewebsites.net canonical name = waws-prod-blu-479.sip.azurewebsites.windows.net.
waws-prod-blu-479.sip.azurewebsites.windows.net    canonical name =
waws-prod-blu-479-85bd.eastus.cloudapp.azure.com.
Name:    waws-prod-blu-479-85bd.eastus.cloudapp.azure.com
Address: 20.119.8.42
```

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-8.2.
```

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

```
The assets directory holds files that contain images with font colors, etc. that make up the design of your webapp.
```

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 cloud tenant is a cloud computing architecture that allows customers to share computing resources in a public or private cloud. Each tenant's data is isolated and remains invisible to other tenants.
```

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

```
A key Vault access policy is important because it determines whether a given security principle, a user, application, or user group, can perform different operations on Key Vault secrets, keys, and certificates.
```

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

```
Keys: keys are cryptographic keys that offer support and are used for encrypting and decrypting data.

Secrets: secrets are any sensitive information that needs to be stored securely, such as passwords, connection strings, or API keys. Secrets act as a key to unlocking protected resources or sensitive data.
```

Certificates: certificates support the certificates that are built on top of the keys and secrets with an automated renewal feature.

Cryptography Questions

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

~Self-signed certificates are fast, free, and easy to issue.
~Self-signed certificates are appropriate for development/testing environments and internal network websites.
~Self-signed certificates are simple to modify or customize; for instance, they can carry more metadata or have greater key sizes.
~There are zero dependencies on others for the issuance of certificates, which saves time for testing purposes.

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

~**Lack of Trust:** Self-signed certificates are not issued by a recognized and trusted certificate authority. This means that users visiting a website secured with a self-signed certificate will likely see a security warning in their browser, leading to a lack of trust.
~**Vulberability to Man-in-the-Middle Attacks:** Since there is no external authority verifying the identity of the certificate holder, self-signed certificates are more susceptible to man-in-the-middle attacks. Attackers can intercept communication between the user and the server, presenting their self-signed certificate and potentially compromising the security of the connection.
~**Not Suitable for Public-facing Websites:** Self-signed certificates are generally not recommended for public-facing websites or applications because users are less likely to trust them. For websites that handle sensitive information, it's crucial to use a certificate signed by a well-known CA to ensure the security and trustworthiness of the communication.
~**Limited Browser and Application Support:** Some browsers and applications may restrict or limit support for self-signed certificates, making it more difficult for users to access services secured with these certificates. Users might need to take extra steps to add exceptions or trust self-signed certificates in certain applications.

3. What is a wildcard certificate?

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

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 has a flaw that could allow an attacker to decrypt information, such as authentication cookies. SSL is provided to protect customers from the 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, because Azure set up a secure SSL certificate.
```

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

```
Monday, December 18, 2023 at 2:20:21AM - Thursday, June 27, 2024 at 7:59:59PM.
```

    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?

```
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.

```
ec-acc.
```

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

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 protocool, making SSL traffic common. The processing is
offloaded to a separate server designed specifically to perform SSL
acceleration or SSL termination.
```

3. What OSI layer does a WAF work on?

```
A WAF is a protocol layer 7 defense, and is not designed to defend against
all types of attacks.
```

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

```
An SQL injection is a type of vulnerability in which an attacker uses a
piece of SQL code to manipulate a database and gain access to potentially
```

```
valuable information.
```

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?

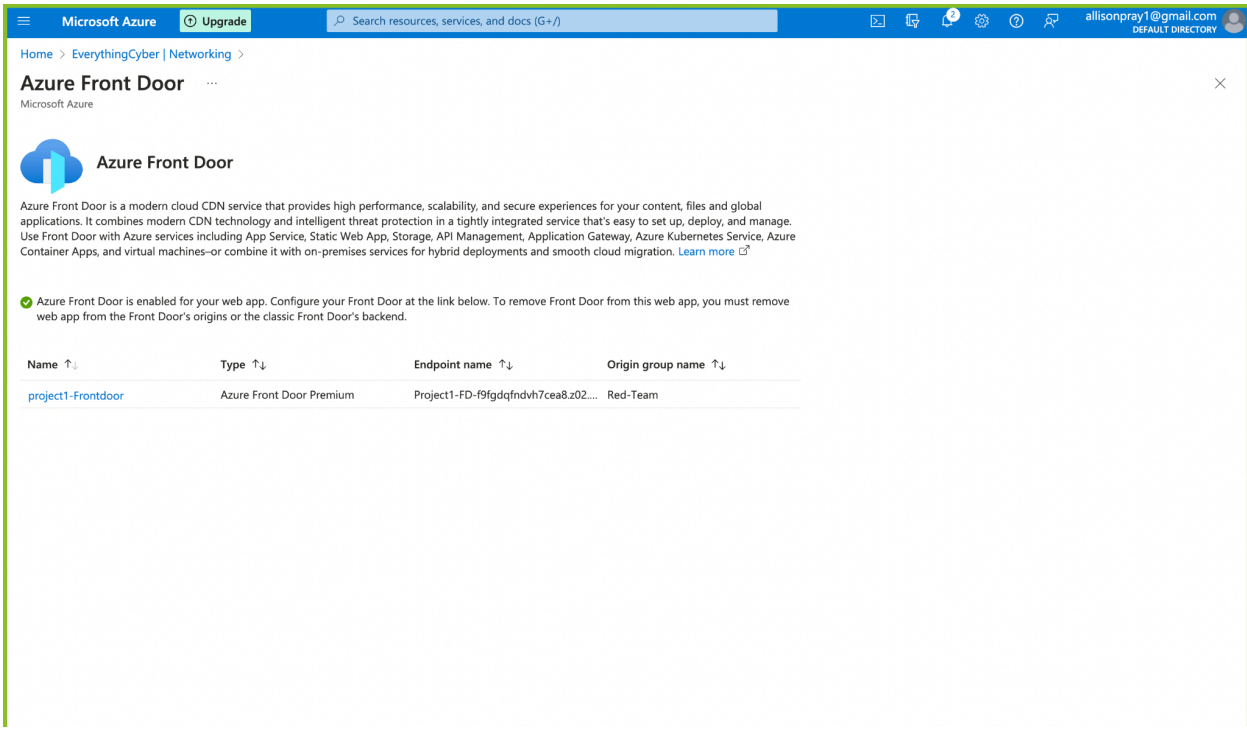
```
Yes, because with front door, it monitors network traffic at the application
level and inspects/blocks incoming requests for potentially malicious
signatures, character sequences, or patterns indicative of an SQL injection
attempt.
```

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?

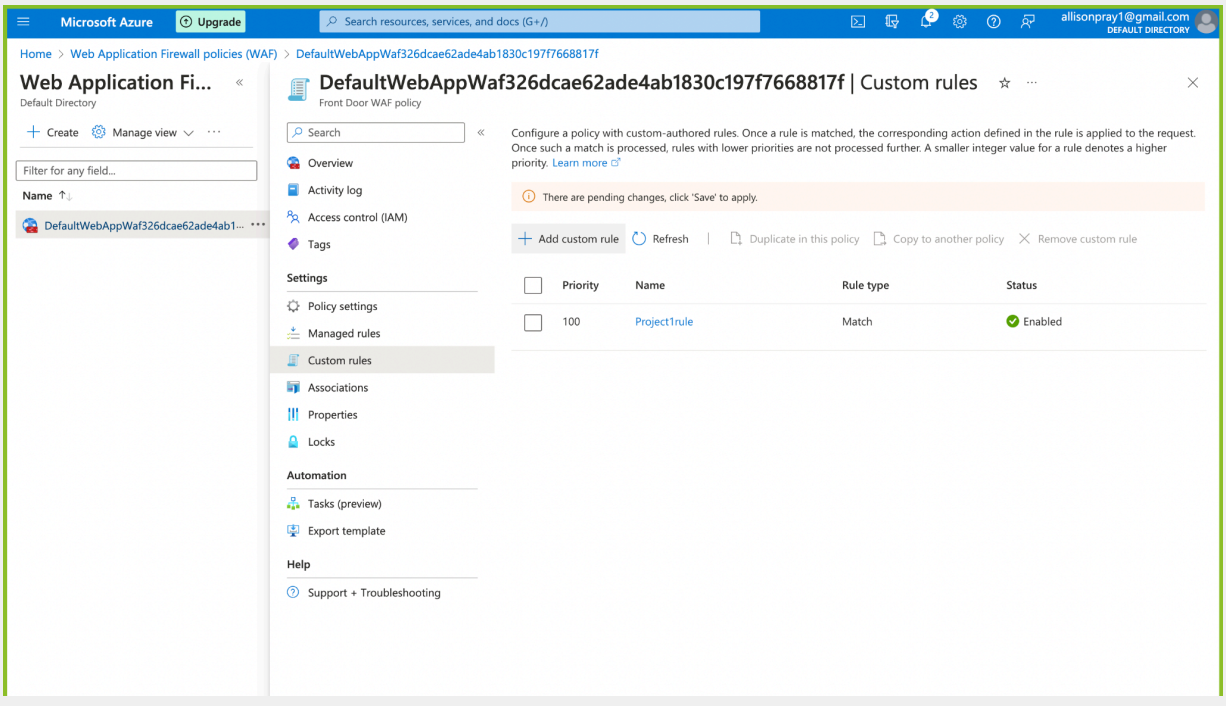
```
Technically, the custom WAF rule would block all canadian traffic, however
it is becoming easier for people with advanced skills to break this rule and
get in. So, it would most likely block most canadian traffic for your
average user, but given advanced features like VPN's, etc. it could still be
accessed.
```

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

a. Azure Front Door enabled



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.*