



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:


`emilycybersecurityblog.azurewebsites.net`

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

EmilyCybersecurityBlog - Micro...My Drive - Google DriveCopy of [MAKE A COPY] Project1: Lesson Plans/14 Project 1/3/...Managing and Shipping Azure...My Blog

emilycybersecurityblog.azurewebsites.net


Send EmailLinkedIn logo



Hi, I'm Emily!

I am fascinated with the cyber world. All that entails in keeping up to date with whats new in the world and how to better protect societies data and information. I am currently enrolled in a cyber security bootcamp to help gain knowledge and land a career in the industry.

Blog Posts



Ransomware: Should organizations pay or not?

Ransomware


Type here to search

42°F Cloudy7:58 PM12/15/2022

EmilyCybersecurityBlog - Micro...My Drive - Google DriveCopy of [MAKE A COPY] Project1: Lesson Plans/14 Project 1/3/...Managing and Shipping Azure...My Blog

emilycybersecurityblog.azurewebsites.net


Blog Posts



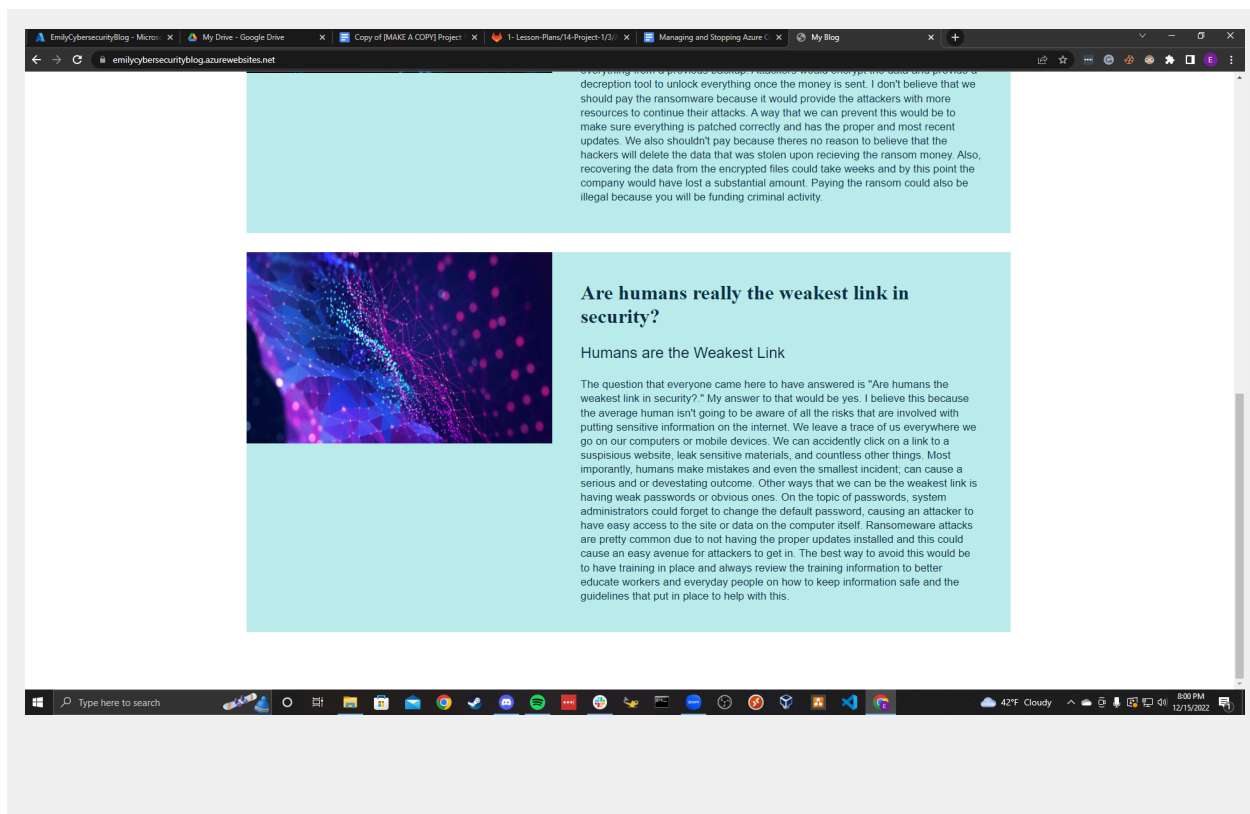
Ransomware: Should organizations pay or not?

Ransomware

Companies cannot 100% avoid a ransomware attack. Lets begin with the basics. A ransomware attack is a malicious software that threatens to block access to the data or computer system. This is an easy way for attackers to get money because the only way to gain access to the data would be to pay the ransom or restart everything from a previous backup. Attackers would encrypt the data and provide a decryption tool to unlock everything once the money is sent. I don't believe that we should pay the ransomware because it would provide the attackers with more resources to continue their attacks. A way that we can prevent this would be to make sure everything is patched correctly and has the proper and most recent updates. We also shouldn't pay because theres no reason to believe that the hackers will delete the data that was stolen upon receiving the ransom money. Also, recovering the data from the encrypted files could take weeks and by this point the company would have lost a substantial amount. Paying the ransom could also be illegal because you will be funding criminal activity.



Are humans really the weakest link in security?



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?

emilycybersecurityblog.azurewebsites.net

Networking Questions

1. What is the IP address of your webpage?

20.119.0.24

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?

Non-authoritative answer:

Name: waws-prod-blu-375-173d.eastus.cloudapp.azure.com

Address: 20.119.0.24

Aliases: emilycybersecurityblog.azurewebsites.net
waws-prod-blu-375.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?

I selected PHP 8.0. This works in the backend.

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

The important resources that are needed to keep the webserver running and the information that can be found on the website itself such as photos.

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

This works in the front end because it deals with the user interface.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant is a customer who purchases cloud computing resources.

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

The access policy would tell whether someone has permission to perform different operations in the key vault.

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

Keys are what is used to keep the certificate secure. Secrets is an area to keep passwords and other confidential information. Secrets is the place where the key for the certifications are kept. Certificates are the certifications that the user has created.

Cryptography Questions

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

The main advantage of a self-signed certificate is that it's free. Other advantages are encryption and decryption of the data is done with the same ciphers as the one you would pay for.

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

Disadvantages of a self-signed certificate are that they never expire and cannot be reversed. They also provide no trust because they are not signed by a certificate authority.

3. What is a wildcard certificate?

A wildcard certificate is a single certificate that can secure multiple domains

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 very outdated. It was created in 1996 and in 2014 Google discovered a way to defeat the protection provided by this(nystec.com)

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 it is a secure and valid certificate.

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

October 16, 2022 - October 11, 2023

- 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, *.azurewebsites.net

- e. Does your browser have the root certificate in its root store?

No, the root certification for the *.azurewebsite.net is not in the root store

- f. List one other root CA in your browser's root store.

Microsoft Root Certification. Expires on 06/23/2035.

Day 3 Questions

Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?

Similarities: both reside in front of your web application in order to protect it, work on layer 7 of the OSI model, primary solution is a load balancer, they can incorporate a web application firewall to protect against web vulnerability attacks

Differences: Web Application Gateway is more regional and Azure Front Door is more global

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

TLS Termination Policy: acts as a point between client and server models and is used to terminate or establish TLS tunnels. The benefits of this are it takes care of the encryption/decryption process on a separate device so it doesn't affect the server's performance.

3. What OSI layer does a WAF work on?

Application Layer 7

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

SQL injection is a web security vulnerability that allows the attacker to interfere with the queries that an application makes to its database

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?

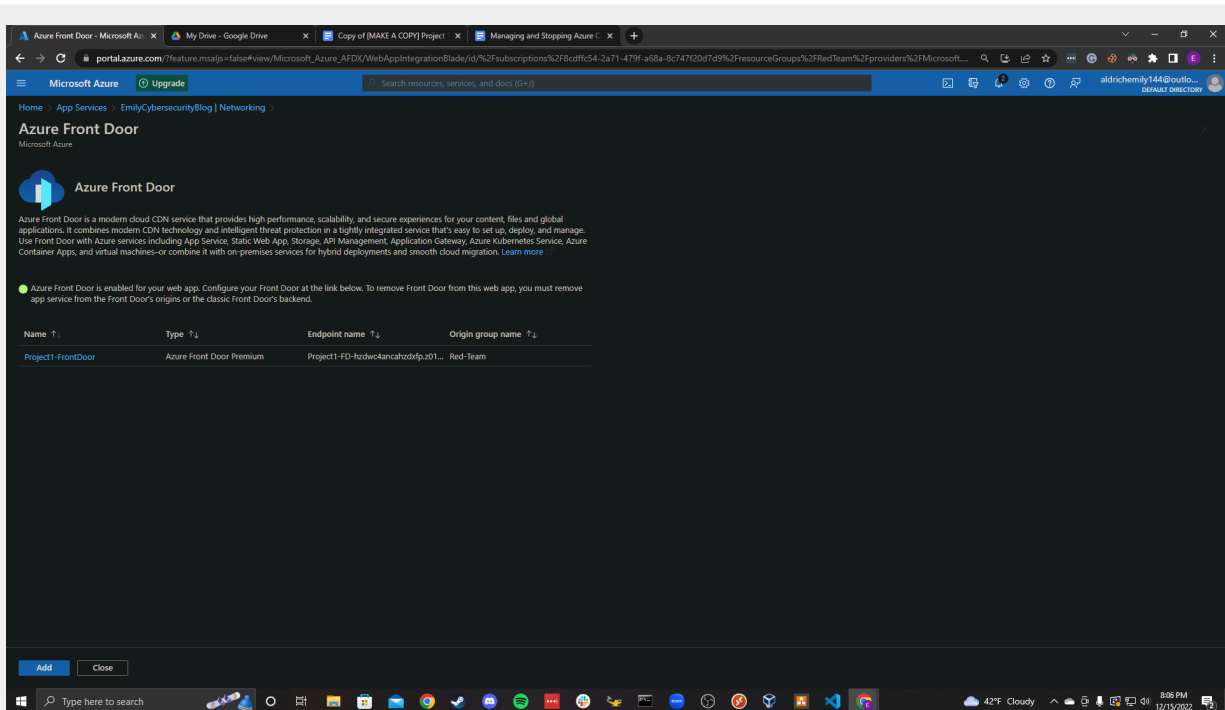
Yes, because the Front Door provides a secure connection between the user and the web content so if it was disabled then an attacker could gain access to the information in the application.

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?

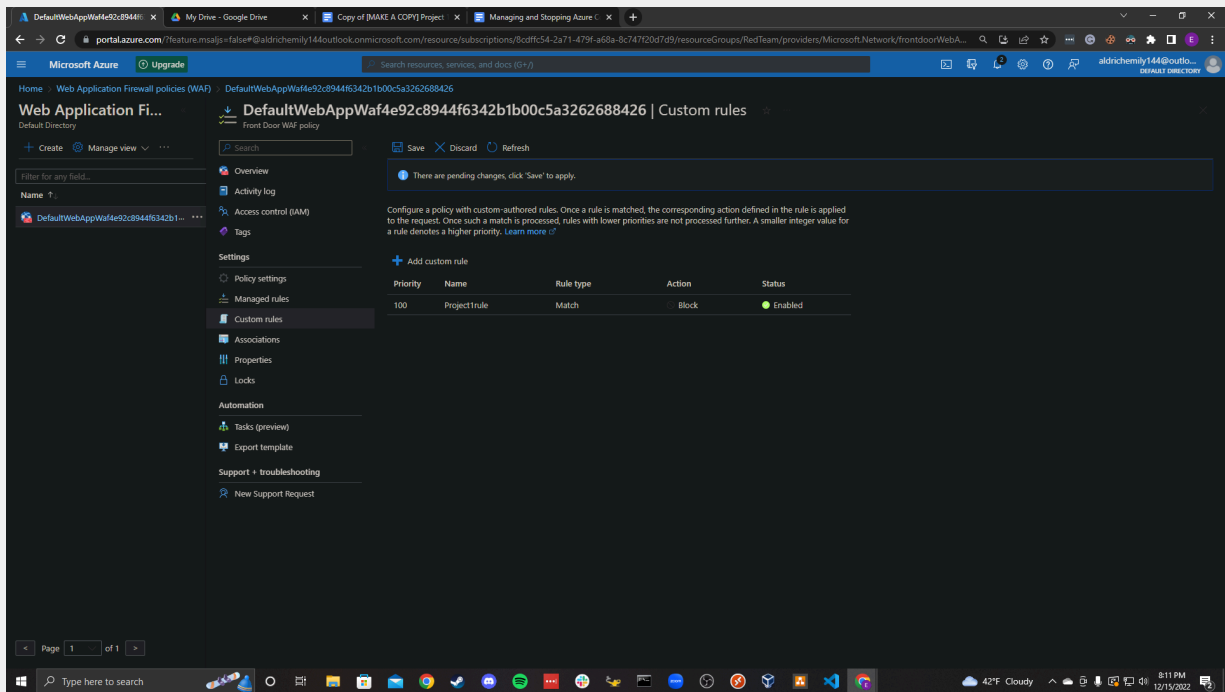
Yes and No. Yes, because it'll block all the traffic that comes from Canada but someone could get a virtual private network and say that they live in either Australia, USA, or anywhere else that the rule allows and then gain access that way.

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.
- ***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 screenshots and completed this document.

YES