Cybersecurity

Project 1 Technical Brief

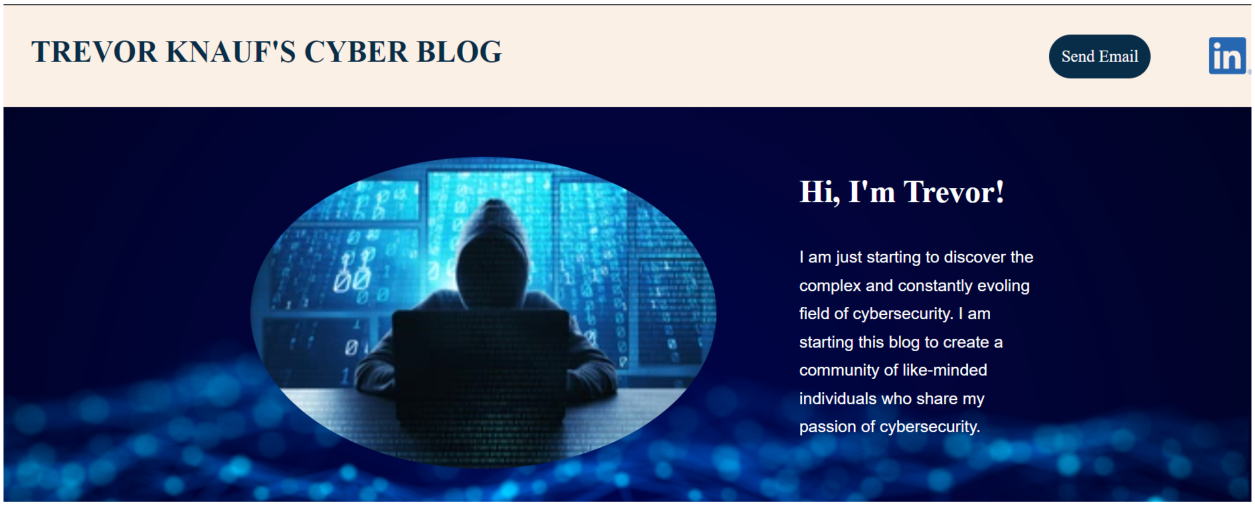
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
trevorsecurityresume.azurewebsites.net
```

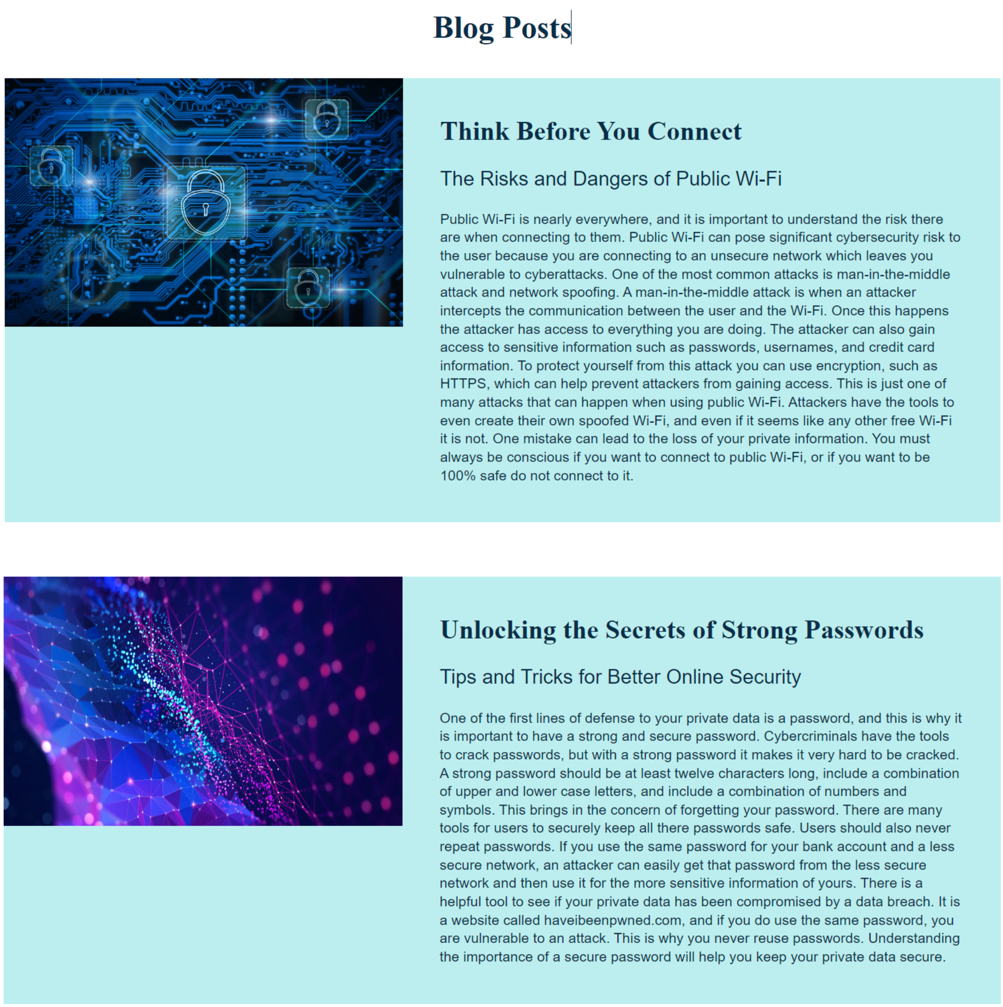
Paste screenshots of your website created (Be sure to include your blog posts):



TREVOR KNAUF'S CYBER BLOG

Hi, I'm Trevor!

I am just starting to discover the complex and constantly evoling field of cybersecurity. I am starting this blog to create a community of like-minded individuals who share my passion of cybersecurity.



Blog Posts

Think Before You Connect

The Risks and Dangers of Public Wi-Fi

Public Wi-Fi is nearly everywhere, and it is important to understand the risk there are when connecting to them. Public Wi-Fi can pose significant cybersecurity risk to the user because you are connecting to an unsecure network which leaves you vulnerable to cyberattacks. One of the most common attacks is man-in-the-middle attack and network spoofing. A man-in-the-middle attack is when an attacker intercepts the communication between the user and the Wi-Fi. Once this happens the attacker has access to everything you are doing. The attacker can also gain access to sensitive information such as passwords, usernames, and credit card information. To protect yourself from this attack you can use encryption, such as HTTPS, which can help prevent attackers from gaining access. This is just one of many attacks that can happen when using public Wi-Fi. Attackers have the tools to even create their own spoofed Wi-Fi, and even if it seems like any other free Wi-Fi it is not. One mistake can lead to the loss of your private information. You must always be conscious if you want to connect to public Wi-Fi, or if you want to be 100% safe do not connect to it.

Unlocking the Secrets of Strong Passwords

Tips and Tricks for Better Online Security

One of the first lines of defense to your private data is a password, and this is why it is important to have a strong and secure password. Cybercriminals have the tools to crack passwords, but with a strong password it makes it very hard to be cracked. A strong password should be at least twelve characters long, include a combination of upper and lower case letters, and include a combination of numbers and symbols. This brings in the concern of forgetting your password. There are many tools for users to securely keep all there passwords safe. Users should also never repeat passwords. If you use the same password for your bank account and a less secure network, an attacker can easily get that password from the less secure network and then use it for the more sensitive information of yours. There is a helpful tool to see if your private data has been compromised by a data breach. It is a website called haveibeenpwned.com, and if you do use the same password, you are vulnerable to an attack. This is why you never reuse passwords. Understanding the importance of a secure password will help you keep your private data secure.

Day 1 Questions

General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

```
GoDaddy domain
```

2. What is your domain name?

```
trevorscyberblog.life
```

Networking Questions

1. What is the IP address of your webpage?

20.211.64.13

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

Sydney, New South Wales, Australia

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

When I ran nslookup -type ns trevorscyberblog.life the server was unknown but did return my IP address.

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?

Runtime stack that was selected was PHP 8.0. PHP is a scripting language which means it is a back end.

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

Inside that directory is the way the web page is designed. How the layout is and how it is displayed.

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

Front end because this is what the user will interact with.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant is where a user has access to the cloud resources like the servers. The main purpose is identity authentication and managing the resources.

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

The policy is very important because it controls who has access to the data and who doesn’t.

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

Keys are cryptographic to keep data protected and are managed HSM pools. Secrets include passwords, connection strings, and other types of credentials. Certificates are used to validate keys and secrets.

Cryptography Questions

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

One of the bigger advantages to a self-signed certificate is that it is free, and also iit allows the users to have control over the certificate. This includes the duration of validity.

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

One disadvantage is that the self-signed certificate is the lack of trust because you and only you created it, and users are more vulnerable to cyberattacks.

3. What is a wildcard certificate?

```
A wildcard certificate is designed to secure the domain and all of the
subdomains.
```

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 got rid of SSL 3.0 because of its known vulnerabilities in 2014.
```

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 I secured it with a trusted SSL certificate
```

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

```
03-14-2023 through 09-15-2023
```

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

```
GeoTrust Global TLS RSA4096 SHA256 2022 CA1
```

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

```
DigiCert Global Root CA
```

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

```
DigiCert
```

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

```
DigiCert Global Root CA
```

Day 3 Questions

Cloud Security Questions

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

One similarity is that they are both on layer 7 the application of the OSI model, and they are both at the front end of the application analyzing traffic.They are different because Azure Front Door is global and Web Application is regional. Just as during this project we used Azure Front Door and I was able to use three different countries.

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

SSL offloading is the process of removing the encryption from incoming traffic. The offloaded ssl encryption is sent to a device designed to quickly decrypt the traffic, which allows a faster response from the web page.

3. What OSI layer does a WAF work on?

Layer 7 the application layer

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

SQL injection involves an attacker changing the intended purpose of the web application to an unintended purpose designed to gain access to the protected data.This can be avoided by adding **INPUT VALIDATION**.

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 my website is vulnerable to this attack because I do not have input

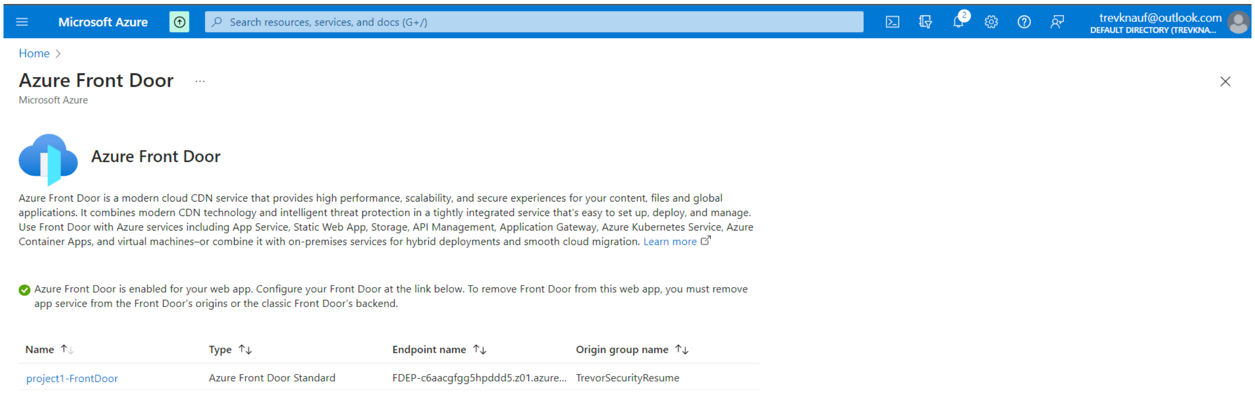
```
validation or filtering to see the attack.
```

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, anyone from Canada would not be able to access my web page unless they
use a VPN.
```

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

    a. Azure Front Door enabled


Microsoft Azure
Search resources, services, and docs (G+/)
trevknauf@outlook.com
DEFAULT DIRECTORY (TREVKNA...
Home

Azure Front Door

Microsoft Azure

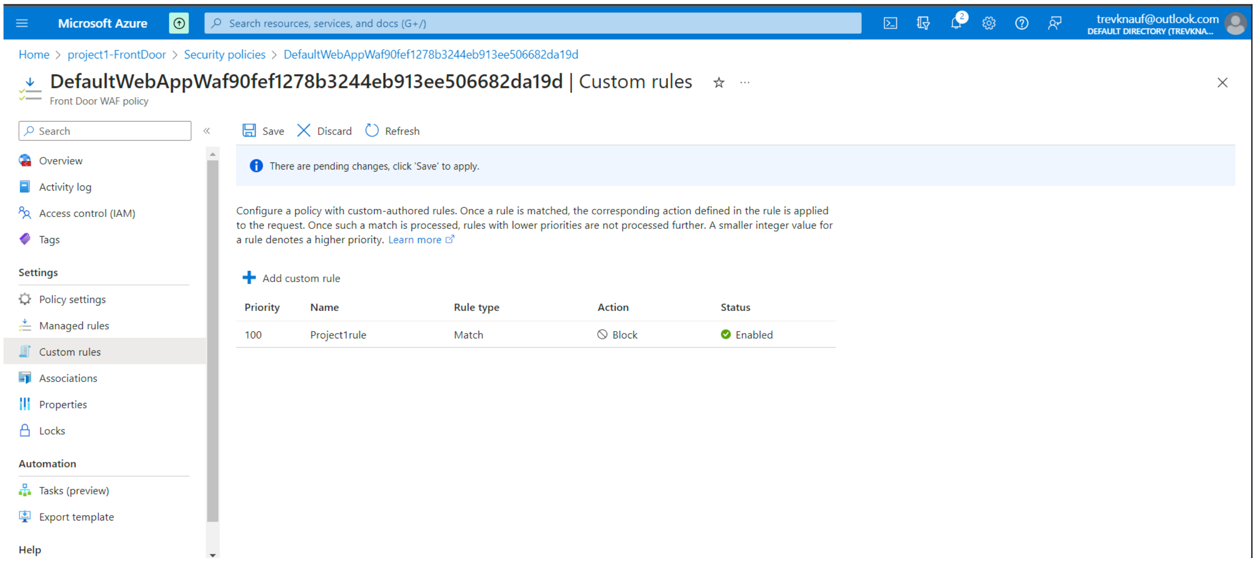
Azure Front Door

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 Standard	FDEP-c6aacgfgg5hpddd5.z01.azure...	TrevorSecurityResume

    b. A WAF custom rule


Microsoft Azure
Search resources, services, and docs (G+/)
trevknauf@outlook.com
DEFAULT DIRECTORY (TREVKNA...
Home > project1-FrontDoor > Security policies > DefaultWebAppWaf90fef1278b3244eb913ee506682da19d

DefaultWebAppWaf90fef1278b3244eb913ee506682da19d | Custom rules

Front Door WAF policy

There are pending changes, click 'Save' to apply.

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.*

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.*