Cybersecurity

Project 1 Technical Brief

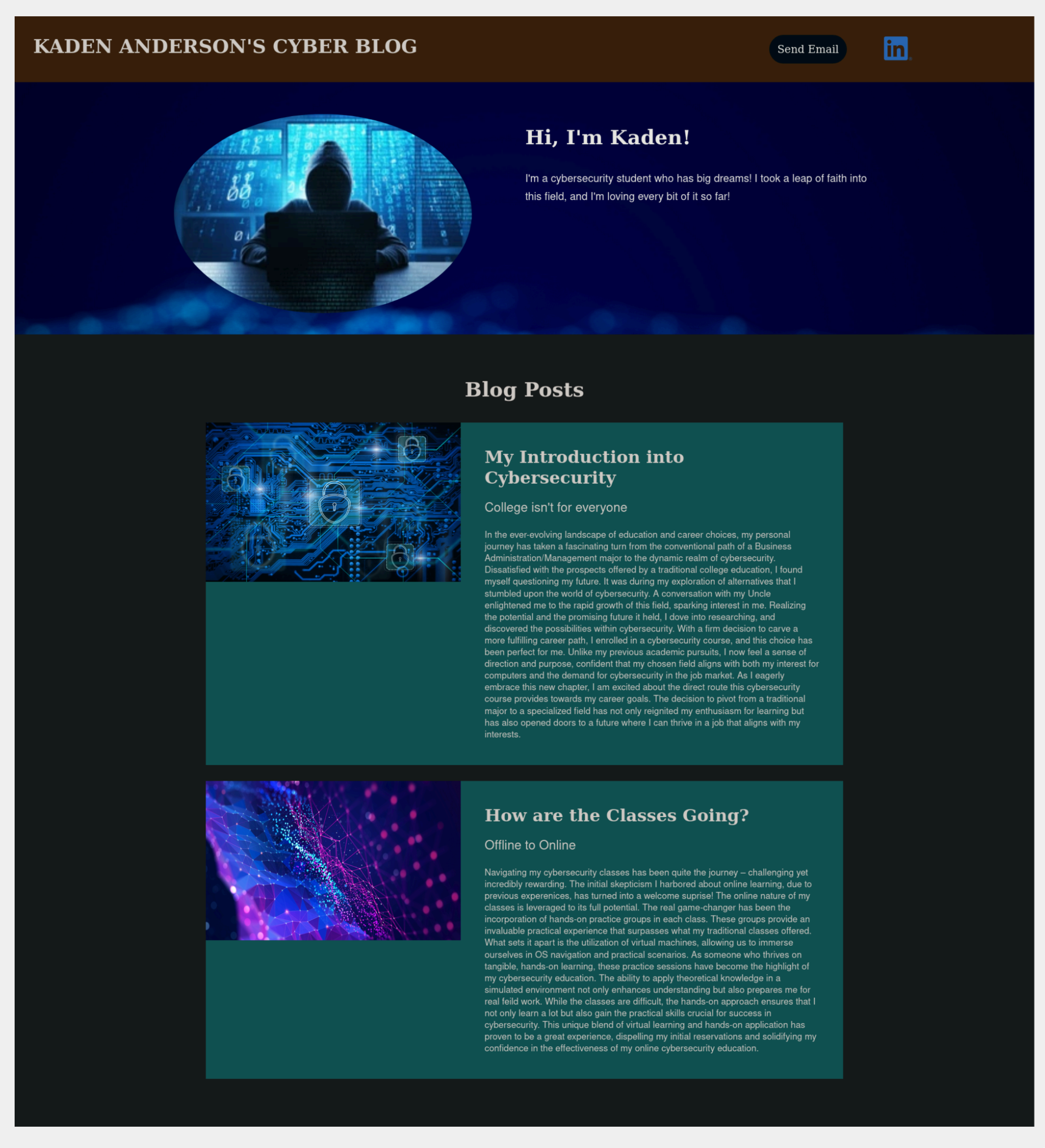
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://boss-security-resume.azurewebsites.net/
```

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



KADEN ANDERSON'S CYBER BLOG

Hi, I'm Kaden!

I'm a cybersecurity student who has big dreams! I took a leap of faith into this field, and I'm loving every bit of it so far!

Blog Posts

My Introduction into Cybersecurity

College isn't for everyone

In the ever-evolving landscape of education and career choices, my personal journey has taken a fascinating turn from the conventional path of a Business Administration/Management major to the dynamic realm of cybersecurity. Dissatisfied with the prospects offered by a traditional college education, I found myself questioning my future. It was during my exploration of alternatives that I stumbled upon the world of cybersecurity. A conversation with my Uncle enlightened me to the rapid growth of this field, sparking interest in me. Realizing the potential and the promising future it held, I dove into researching, and discovered the possibilities within cybersecurity. With a firm decision to carve a more fulfilling career path, I enrolled in a cybersecurity course, and this choice has been perfect for me. Unlike my previous academic pursuits, I now feel a sense of direction and purpose, confident that my chosen field aligns with both my interest for computers and the demand for cybersecurity in the job market. As I eagerly embrace this new chapter, I am excited about the direct route this cybersecurity course provides towards my career goals. The decision to pivot from a traditional major to a specialized field has not only reignited my enthusiasm for learning but has also opened doors to a future where I can thrive in a job that aligns with my interests.

How are the Classes Going?

Offline to Online

Navigating my cybersecurity classes has been quite the journey – challenging yet incredibly rewarding. The initial skepticism I harbored about online learning, due to previous experenices, has turned into a welcome suprise! The online nature of my classes is leveraged to its full potential. The real game-changer has been the incorporation of hands-on practice groups in each class. These groups provide an invaluable practical experience that surpasses what my traditional classes offered. What sets it apart is the utilization of virtual machines, allowing us to immerse ourselves in OS navigation and practical scenarios. As someone who thrives on tangible, hands-on learning, these practice sessions have become the highlight of my cybersecurity education. The ability to apply theoretical knowledge in a simulated environment not only enhances understanding but also prepares me for real feild work. While the classes are difficult, the hands-on approach ensures that I not only learn a lot but also gain the practical skills crucial for success in cybersecurity. This unique blend of virtual learning and hands-on application has proven to be a great experience, dispelling my initial reservations and solidifying my confidence in the effectiveness of my online cybersecurity education.

Day 1 Questions

General Questions

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

```
Free azure
```

2. What is your domain name?

```
boss-security-resume.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.119.0.49
```

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

```
Washington Virginia, USA.
```

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

```
There are no ns records for my site. I used nslookup and a third party site,
but both showed no records. Even for azurewebsites.net (my parent domain)
there are no records. I am not entirely sure why this is the case.
```

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. It works on the backend of my web app.
```

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

```
It holds the images, and the instructions for the website’s layout (CSS).
```

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

The frontend, because it tells the user’s browser how to style the webpage.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A person, or business, who uses cloud services provided by another entity.

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

To make sure that not just anyone could modify or change keys, secrets, etc…

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

Keys are used for encryption/decryption.

Secrets are bits of data, like passwords.

Certificates are used to verify connections. For example, they are used to verify a website’s integrity.

Cryptography Questions

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

They are cheap and easy to create

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

They are, mostly, distrusted and could pose a security risk.

3. What is a wildcard certificate?

```
A single certificate that is designed to verify many 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.

```
It was disabled by microsoft to protect websites from a vulnerability in 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?

```
No, it says that my certificate is “verified by Microsoft Corporation”
```

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

```
Not Before  Mon, 30 Oct 2023 22:48:44 GMT
Not After  Thu, 27 Jun 2024 23:59:59 GMT
```

   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. Microsoft RSA Root Certificate Authority 2017
```

   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.

```
NAVER Global Root Certification Authority
```

Day 3 Questions

Cloud Security Questions

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

- Similar
  - Both are used to protect web apps from vulnerabilities
- Different
  - Front door is easier to scale, on a global level.
  - AWAG is for more traditional web apps

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

Transferring SSL encryption to a separate device. It helps to improve server speed, and reduce the load on it as well.

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.

There are quite a few SQL injection rules. All of them seem to limit unexpected inputs, preventing anomalies from entering the database, which helps to secure the database’s 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?

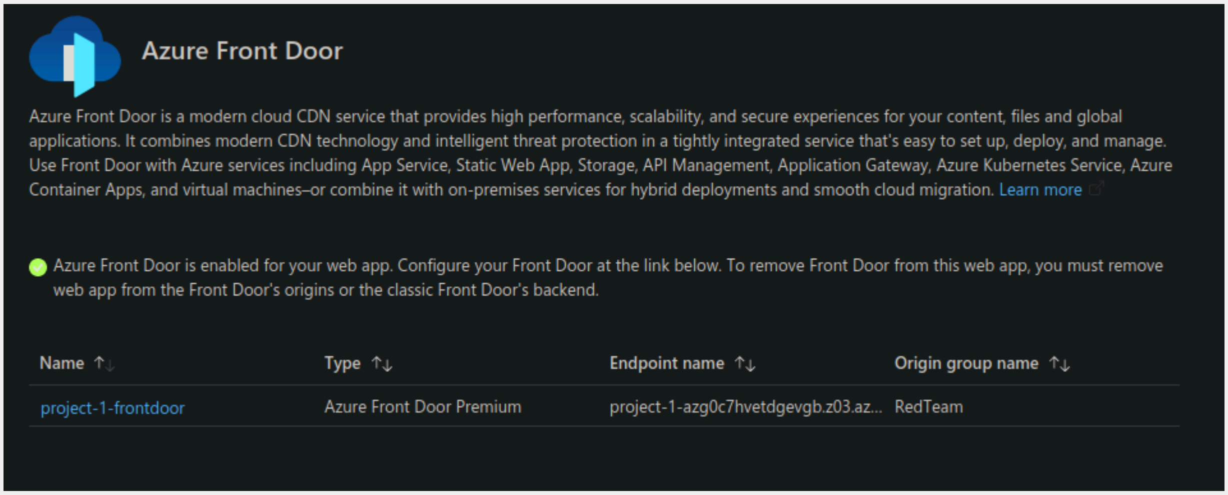
No. It would impact my website if it was pulling sensitive info from a much larger database. As it stands, my website functions as a glorified text and image document with no sensitive data.

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?

Unless a Canadian citizen was to use a bypass, like a VPN, IP addresses from Canada would not be able to access the website.

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

   a. Azure Front Door enabled



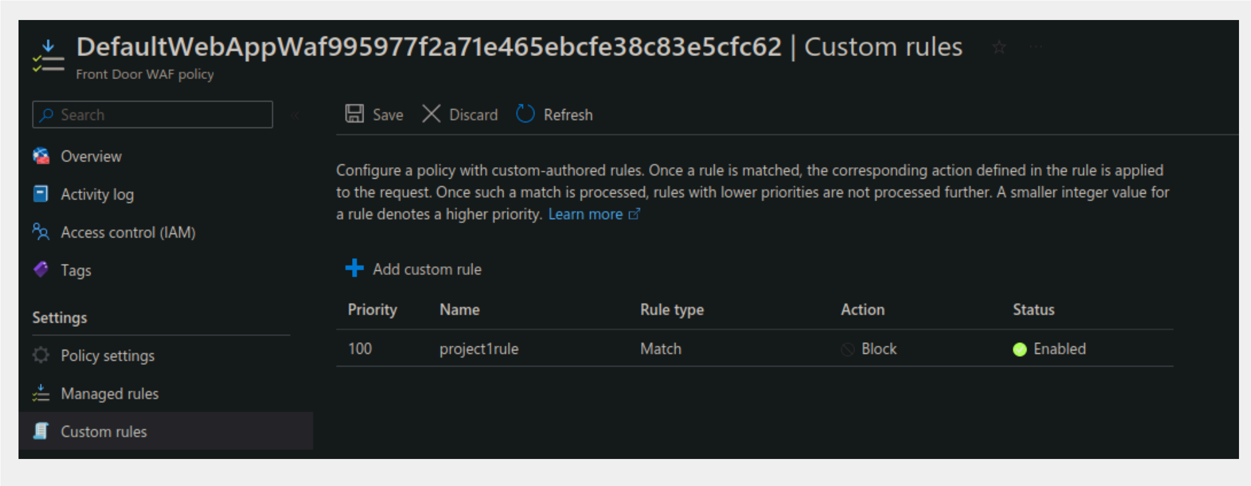
Azure Front Door

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 web app from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
project-1-frontdoor	Azure Front Door Premium	project-1-azg0c7hvetdgevgb.z03.az...	RedTeam

   b. A WAF custom rule



DefaultWebAppWaf995977f2a71e465ebcfe38c83e5cfc62 | Custom rules

Front Door 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	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.*

- ***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