Cybersecurity

Project 1 Technical Brief

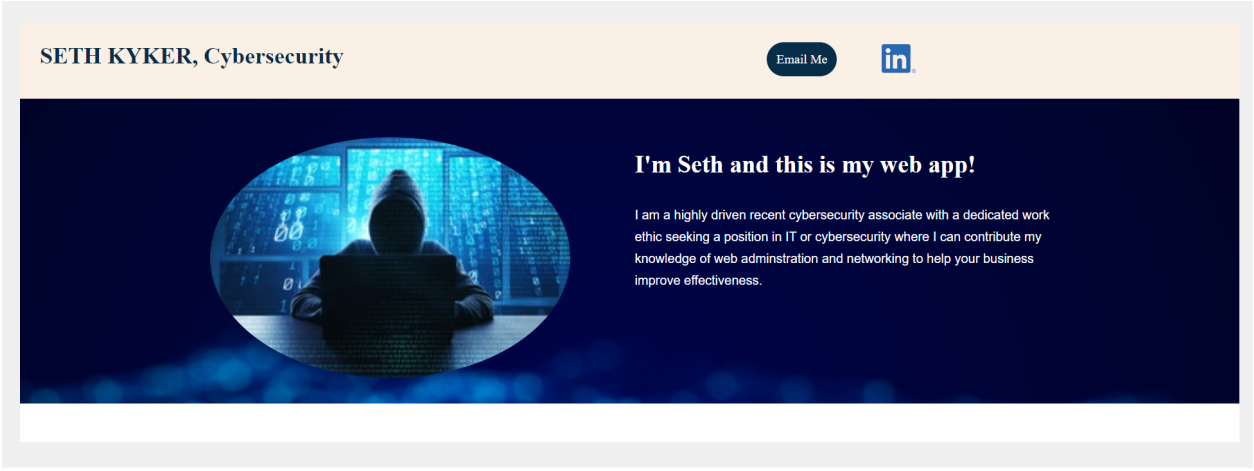
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://sethkykersecurityresume.azurewebsites.net/
```

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



My Blogs

Phish Out of Water

How the best defense against phishing is afk

Ever since the pandemic began, the necessities and benefits of remote online work have only increased exponentially which lead to the increase in cyber attacks such as phishing. The source of many people's people's livelihoods are online and for many it is a new frontier to navigate. Phishers seek to take advantage of this by deploying fake messages in the hopes of tricking them into yielding personal data. This is nothing new. Many online applications have phishing prevention protocols built in to help identify malicious links. However the easiest and most cost effective way to navigate and prevent these attacks is knowledge and education. If online workers can safely spot the signs of a phishing attack and avoid them, it would be simplier and less expensive than launching automations meant to spot these attempts. The proper departments could help manage any reports and promote a strong security culture within the workspace. Of course, this system isn't 100% effective as human error can and will persist. However, education on the matter at hand will go a long way and open eyes to any other dangers posed in a cyber workspace.

Should I Pay Or Should I Go?

When and why organizations shouldn't pay a ransomware attacker

A study at Forbes in May, 2018 showed that there are 2.5 quintillion bytes of data created online every day with an accelerating pace. In a PC Mag article posted in November, 2020, the most valuable data is owned US men of middle eastern descent, living in the Northeast between the ages of 18 and 24, who all total an annual networth of $66 million. Personal data is one of the most valuable comodities in the current world and it is no surprise that there are criminals out there that will look to ransom it for hundreds of thousands if not millions of dollars. But should a company find themselves on the receiving end of a ransomware attack, should the ransom be paid? Well, it is rarely ever so cut and dry, however more often than not it is more advantageous not to give in to the demands. From a business perspective, it tells these cybercriminals (as well as potentially others) that it is easy to extort money from you and they may not even hand over the decryption key. It may even encourage another ransomware attack that is bigger than the last. There are reasons to pay, but there are solutions to recover from the attack without paying. If the company's IT department had good preventative measures in place, the attack should be reported to the authorities and backups should be restored. Just because you can afford to pay the ransom, doesn't mean you should.

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?

```
sethkykersecurityresume.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.40.202.21
```

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

```
Central, US
```

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

```
C:\Windows\system32> nslookup sethkykersecurityresume.azurewebsites.net
Server:   cdns01.comcast.net
Address:   2001:558:feed::1

Non-authoritative answer:
Name:   wawa-prod-dm1-219-70c3.centralus.cloudapp.azure.com
Address:   20.40.202.21
Aliases:   sethkykersecurityresume.azurewebsites.net
           wawa-prod-dm1-219.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 HTML which works on the front end
```

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

```
It contains two directories named css and images
```

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

```
The front end
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
In a software as a service cloud environment, a tenant is the customer. A
single tenant architecture supports a database for one cloud tenant whereas
a multi tenant architecture supports databases for multiple cloud tenants.
```

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

```
Access policies provide an addditional layer of restrictions for signatures.
```

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

```
Keys are asymmetric algorithms, yielding a public and a private key that are
independant of one another. A certificate binds an identification to the
```

```
public key. A secret is a catch all for sensitive objects not categorized as a key or a certificate.
```

Cryptography Questions

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

```
They are easy, free and unlimited in regards to certificate generation.
```

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

```
Data security isn’t guaranteed, personal data set isn’t entirely protected, and there is involvement of unknown publisher warnings.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a digital certificate that applies to the domain and its 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.

```
SSL 3.0 is a vulnerability observed by Microsoft Azure
```

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?

```
The SSL certificate did not return an error
```

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

```
Monday, March 14, 2022, 2:39:55 PM to Thursday, March 9, 2023, 2:39:55 PM
```

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

```
I do not
```

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

```
I do not
```

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

```
I do not
```

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

```
DST Root CA X3
```

Day 3 Questions

Cloud Security Questions

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

```
Both serve as load balancers. The front door places the WAF at edge
locations within the network and the gateway places the WAF near the
entrance of the datacenter
```

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 removing SSL encryption outside of the chain of incoming
traffic.
```

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 the process of pushing malicious SQL queries into web
requests to do things such as extracting 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?

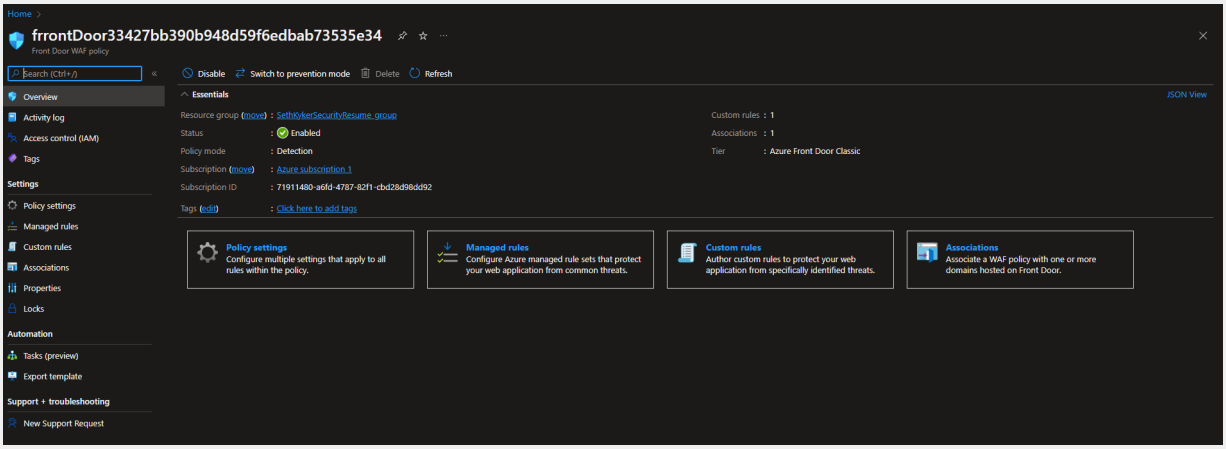
```
A SQL Injection could take place on my web application without the enabling
of Front Door because it blocks all non https traffic.
```

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?

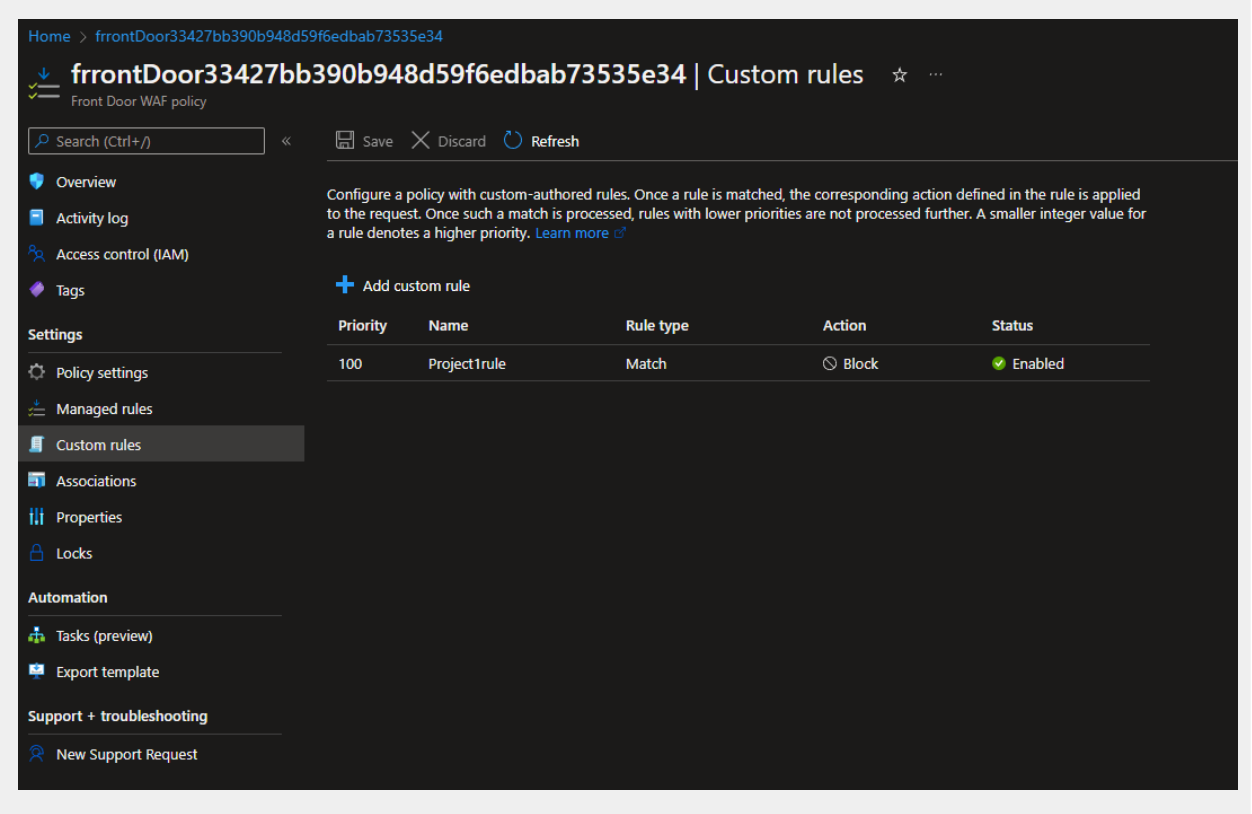
```
This does not mean people who reside in Canada can't access my site because
any Canadian user could use a VPN
```

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.*