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:

```
jettjanssen.info
```

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

My Blog

Not secure | https://jettjanssen.info

JETT JANSSEN'S CYBER BLOG

Send Email

Hi, I'm Jett!

This is my personal cybersecurity blog! I will cover a broad variety of topics in my posts. If you have any question feel free to email me or check out my LinkedIn.

Blog Posts

Are Humans The Weakest Link in Security?

Security, Cyber, Phishing, Social Enginnering

Are Humans Really The Weakest Security Link? With the exponential growth of cybersecurity as a field there have been many changes. Changes to security policy, architecture, and design allow us to make our policies more secure, but there is always the weakest link, Humans. Humans are deeply ingrained in the cybersecurity culture as the weakest links in the chain. Phishing attacks are targeted directly towards us and the phishing scams themselves become more complex and believable as time passes. Social engineering attacks also play a big part in major cyber security breaches. With employees leaving bigger digital footprints on the web, it becomes easier to engineer data around what they have already left behind. What can we do to make the human link stronger? We can promote the teaching and addition of useful cybersecurity frameworks, rules, and culture. We can also add automation to reduce the possibility for human error. For example, instead of just trusting that no one will click a phishing link, look into a service that will automatically flag and remove the suspicious emails before they are delivered. Additionally, training can be and should be an important part of onboarding any new employee. Not only should training be done initially, but it should be continued further as the employee remains in the company.

Quantum Computing V.S. Cybersecurity

Quantum Computing, Cyber, Security, Encryption, Decryption

How Could Quantum Computing Affect Cybersecurity? While quantum computing (Q-C) still is not a commercially available service its potential threats to cybersecurity are very real now. While potential threat actors wait for access to Q-C capabilities they can be scraping and storing data now to be decrypted later. If we do not implement measures to counteract the use of Q-C to crack our current encryption protocols now, it will be too late in the future for us to protect our data. Although still a way off, the rapid development of quantum computers that are large enough to brute force crack a 2048-bit encryption should not be discounted. The greater risk at hand though is not your personal security, but the security of national level. Encrypted data that needs to stay encrypted at a high level for a long period of time needs to be protected now rather than later. How can we address the threat to cybersecurity? Many groups of researchers have been working at developing new levels of quantum safe encryption. The U.S. National Institute of Standards and Technology (NIST) has already started to evaluate nearly 70 potential new methods for quantum cryptography.

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?

```
jettjanssen.info
```

Networking Questions

1. What is the IP address of your webpage?

```
52.231.38.95
```

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

```
Country: Korea (Republic of)
State/Region: Seoul-teukbyeolsi
City: Seoul
```

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

```
jettm@DESKTOP-2CQSDE9 MINGW64 ~
$ nslookup -type=ns jettjanssen.info
Server:  2603-8080-2800-9756-0000-0000-0000-0001.res6.spectrum.com
Address:  2603:8080:2800:9756::1

Non-authoritative answer:
jettjanssen.info        nameserver = ns44.domaincontrol.com
jettjanssen.info        nameserver = ns43.domaincontrol.com

ns43.domaincontrol.com  internet address = 97.74.101.22
ns43.domaincontrol.com  AAAA IPv6 address = 2603:5:2152::16
ns44.domaincontrol.com  internet address = 173.201.69.22
(root)  ??? unknown type 41 ???
```

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 8.1, and it works on the back end.
```

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

```
It contained all the images, assets, and other files for the website.
```

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

```
This works with the back end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
Someone who is purchasing cloud resources.
```

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

```
So that only the correct users can access or change the keys in the vault
```

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

```
A secret is anything that's sensitive that's not an asymmetric key.
A Certificate contains a public key binding it to a name
Keys are public and private  and bound to the certificate.
```

Cryptography Questions

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

```
They are fast to create and have zero-dependency on a third party for
insurance of the certificate.
```

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

```
They do not get signed by a Certificate Authority so they will not be
immediately trusted by operating systems and browsers.
```

3. What is a wildcard certificate?

```
A single certificate with 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.

```
Microsoft completely disabled SSL3.0 in Azure websites by default to protect
their customers from the vulnerability of the POODLE bug allowing hackers to
intercept traffic.
```

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?

```
It is not, the browser has verified the SSL certificate that I added to the website.
```

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

```
Issued On
Thursday, January 5, 2023 at 6:00:00 PM
Expires On
Thursday, July 6, 2023 at 6:59:59 PM
```

    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?

```
Yes
```

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

```
OU=certSIGN ROOT CA G2,O=CERTSIGN SA,C=RO
```

Day 3 Questions

Cloud Security Questions

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

```
Both Azure Web Application Gateway and Azure Front Door are layer 7 load balancers, but Front Door is a non-regional service while Application Gateway is a regional service.
```

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 taking incoming SSL-based encryption traffic and routing it to a different server to relieve the web server of having to process and decrypt/encrypt traffic. It can increase the number of connections that a cluster can handle.
```

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.

```
SQL Injection Attack, automatically blocks on anomaly detection by the WAF.
```

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?

```
I do not believe so, there is no area for text entry on the website so it in theory should not be vulnerable to an SQL injection.
```

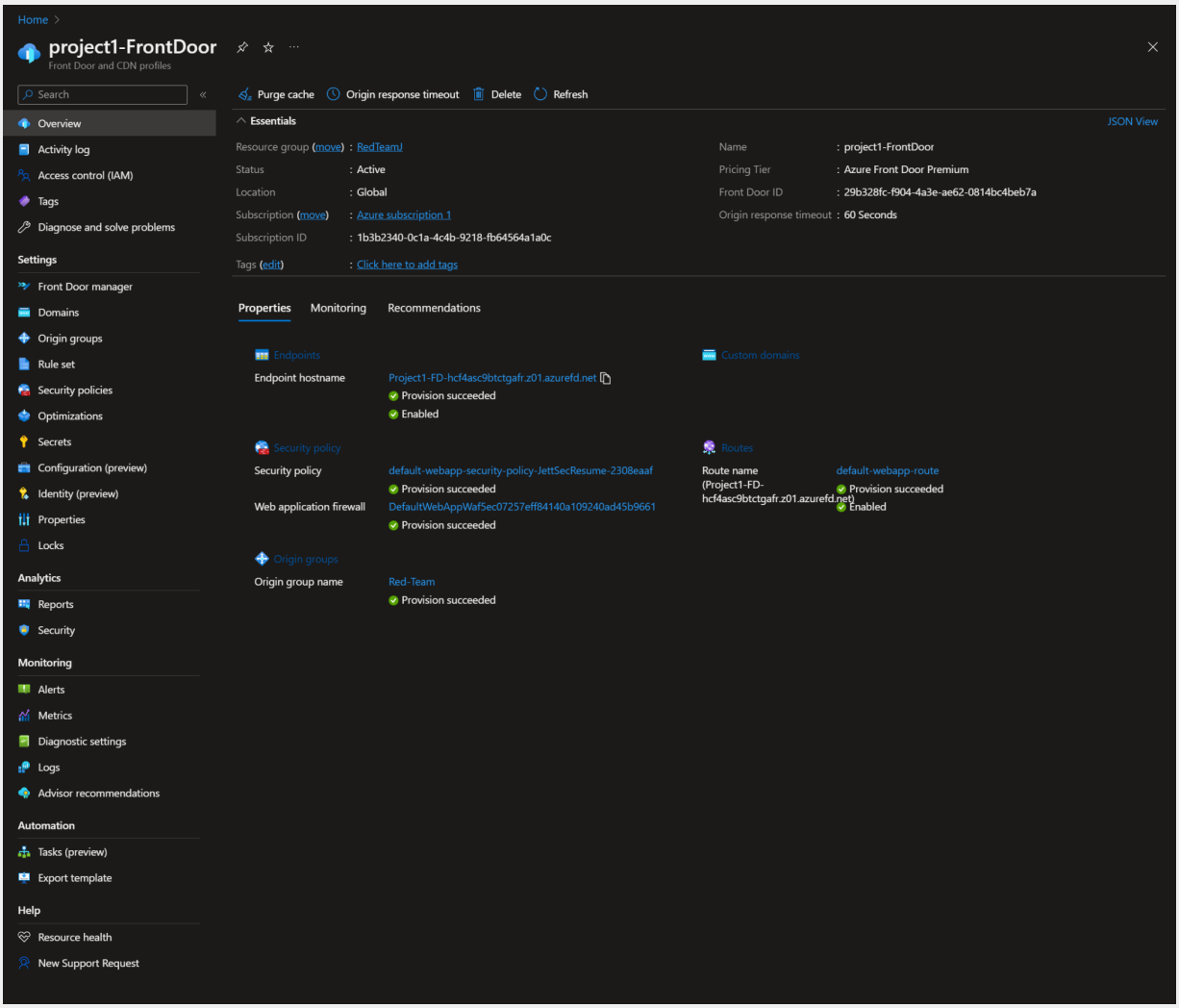
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

```
No, someone could re-route their connection using a VPN to appear to be
```

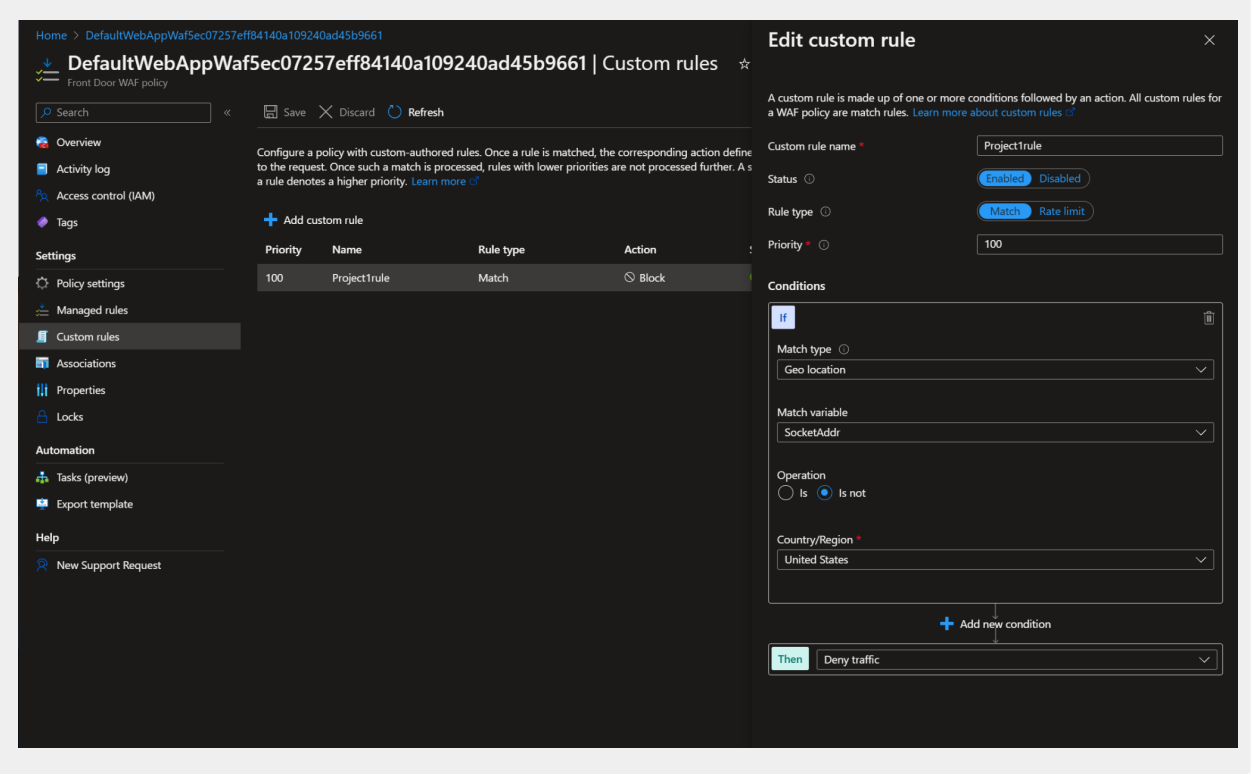
```
connecting from a different country.
```

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 screen shots and completed this document.*

YES