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:

```
drewnewton.co
```

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

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?

```
drewnewton.co
```

Networking Questions

1. What is the IP address of your webpage?

```
20.119.8.26
```

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?

```
The NS record shows that there are two nameservers associated with my domain
at ns43.domaincontrol.com and ns44.domaincontrol.com.
```

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 chose PHP 8.1 as my runtime stack. This is the interpreter that deciphers
and runs the web applications code. This is done on the back end.
```

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

```
That directory contains different styling options for html such as fonts and
```

```
images that the webpage can access.
```

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

```
This works on the front end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is the name for an organization or individual who utilizes
and manages cloud services.
```

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

```
The key vault is configured so that certain assets are non-readable or
inaccessible for those that should not have access to those assets so it is
imperative that only those that need access to the key vault are granted
access to avoid privilege escalation.
```

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

```
Keys in Azure's key vault are tools for encrypting and decrypting data that
you intend to keep secret. Keys use an asymmetric algorithm to ensure that a
public and private key are required to encrypt and decrypt content. Secrets
are assets (such as passwords or database connection strings) that the Key
Vault encrypts as a series of octets. Secrets can be retrieved at any time
considering you are authorized to do so. Certificates in the key vault are
x.509 certificates that can encrypt traffic over the internet or validate
the identity of your web applications. Certificates create a key and secret
that can be used to manage your certificate. Certificates are unique in that
they can be renewed or not depending on the needs of the certificate owner.
```

Cryptography Questions

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

```
Self-signed certificates are easy to make, independent, quick and free. Since they do not require validation from a third party, self-signed certificates can be created and deleted quickly.
```

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

```
Since there is no approval process for a self-signed certificate browsers do not trust them. There is no way to verify that a self-signed certificate has not been created by an attacker which leaves you vulnerable to man-in-the-middle attacks.
```

3. What is a wildcard certificate?

```
A wildcard certificate uses a * as a wildcard character that allows a single certificate to cover all of the subdomains of the primary domain.
```

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 no longer supported on Azure as a result of a widely known vulnerability. It has been found that SSL 3.0 is susceptible to what is called POODLE attacks which allows malicious actors to decrypt sensitive information.
```

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, the app service managed certificate that we created is from Azure, which is a trusted CA.
```

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

```
Six months, mine expires on July 6th, 2023.
```

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

```
Yes, the intermediate certificate is GeoTrust Global TLS
```

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

```
Yes, mine is 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.

```
Entrust Root Certification Authority - EC1
```

Day 3 Questions

Cloud Security Questions

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

```
Azure Web Application Gateway and Azure Front Door both act as layer 7 load balancers but Front Door works as a non-regional service whereas the Web Application Gateway load balances regionally.
```

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

```
SSL Offloading refers to the practice of utilizing a dedicated server for encrypting and decrypting SSL traffic so that it doesn't take resources away from the host CPU.
```

3. What OSI layer does a WAF work on?

```
Application layer
```

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

```
A path traversal attack is when files or directories are exposed and can be
accessed using ../[directory] or absolute paths in the url. This WAF rule
detects and blocks these kinds of attacks.
```

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?

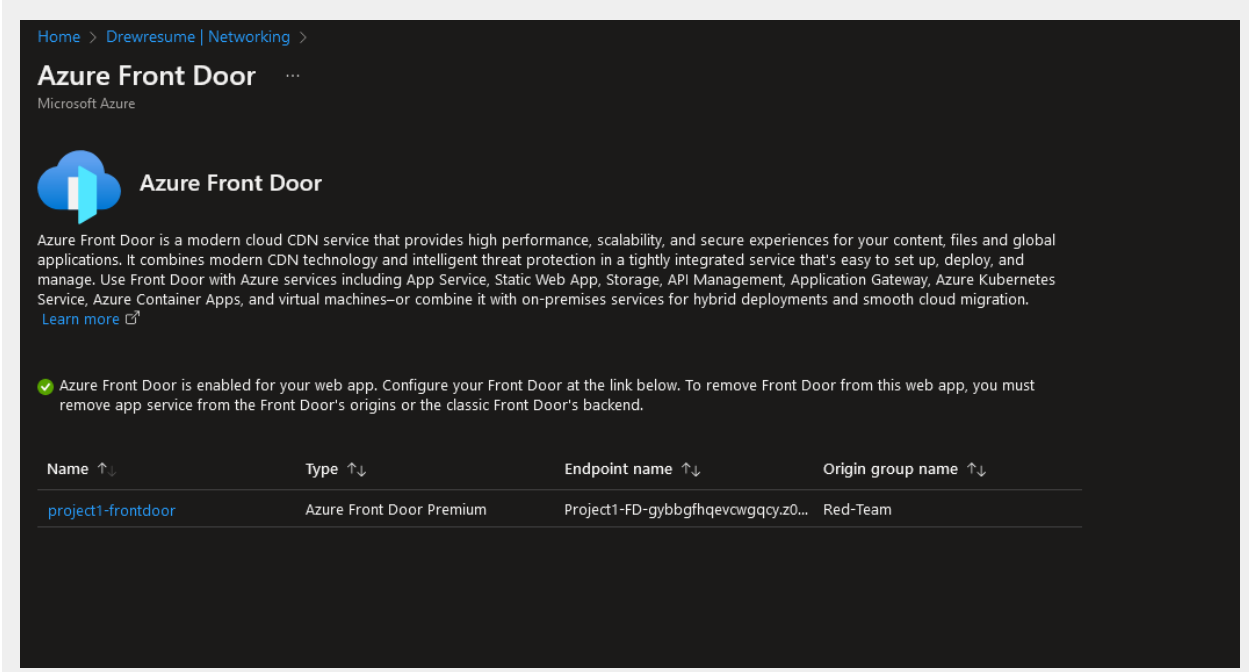
```
My website would not be vulnerable to this attack because I do not have any
vital files or directories on my website that could be exposed.
```

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?

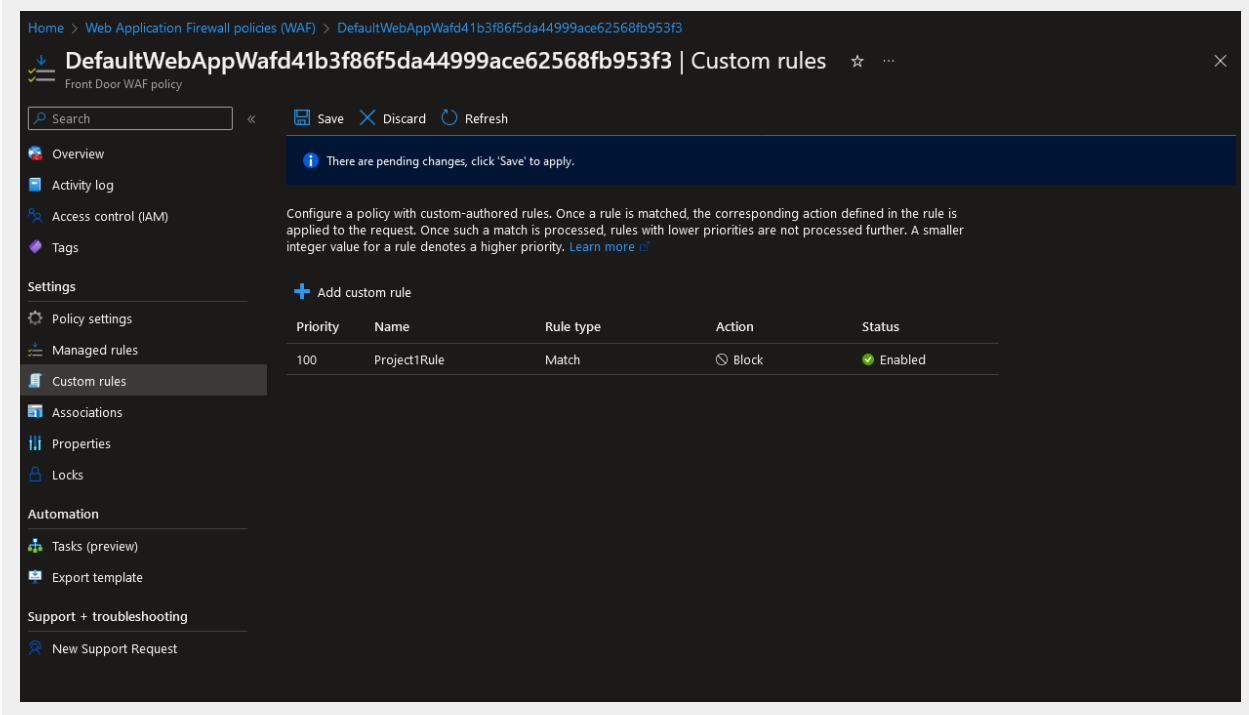
```
The WAF would block traffic from people who reside in Canada but that rule
is very easily gotten around by the use of VPNs.
```

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.*