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:

[My Blog (dstrubeblog.azurewebsites.net)](dstrubeblog.azurewebsites.net)

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

Hi, I'm Dylan!

I am an aspiring cybersecurity professional and enjoy sharing happenenings in the field that seem important.

Please feel free to contribute!

Blog Posts

US Navy's New Cyber Warfare Job

CWT

After 19 years, the US Navy has made the decision to remove the Cryptographic Technician- Networks (CTN)rating with the Cyber Warfare Technician (CWT) rating. This change took place to allow a rate that is more specialized within the cyber warfare field. To be able to enlist into the rating you must enlist for a minimum 72 month service obligation. The rating will allow Sailors to serve in both shore and afloat commands, as well as limited opportunities in Naval Special Warfare. Training will consist of 33 weeks of learning networking, hardware maintenance and operation, and offensive/defensive measures. The job responsibilities of a CWT will include monitoring, identifying, collecting, and analyzing information to provide mission critical support. Also, CWTs will react or attack to threat actors. Current CTNs will transition to the CWT rating, while the CWT rating is now open for those interested. All new accessions to the rate will also be required to take the Cyber Test.

US Army Prepares for Space Operations

Army Cyber

In wars of the future, while the Army will continue to fight ground wars. But with the development of technology, the Army must also be prepared to engage the enemy in space. Satellite surveillance, high-altitude balloons, and aircraft are used to recieve and disrupt enemy communications. Currently, leaders in the Army Cyber, Signal, and Space and Missile Commands are planning methods on how to inform leaders on the capabilities of Cyber Soldiers. US Cyber Command is also working with European space agencies to develop new training methods for allied nations in cyber warfare and missile defense. With continued developments in weapons development, there is also increases in defense methods. Army Cyber Command trains Soldiers to use equipment to detect and destroy threats using advanced methods. Currently, a large struggle for Army leadership is not knowing the uses and capabilities of Cyber Soldiers, hence the need for planning on informing all levels of leadership. Leaders understanding the capabilities will ensure Soldiers have the proper resources. While the cyber branches of the military are new, they continue to grow and expand their capabilities, resources, and knowledge.

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?

```
dstrubeblog.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.19
```

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?

```
Server:  209-018-047-062.inf.spectrum.com
Address:  209.18.47.62

*** 209-018-047-062.inf.spectrum.com can't find
https://dstrubeblog.azurewebsites.net/: Non-existent domain
```

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 8.2., backend
```

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

```
The assets directory is a css folder and images folder, which contains
images and links for the web app
```

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

```
Front end
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
An individual or organization that uses cloud services
```

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

```
Because a key vault is crucial for managing and controlling access to
sensitive information, such as cryptographic keys, secrets, and certificates
stored within the key vault
```

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

```
Key vaults, keys, secrets, and certificates are distinct types of sensitive
information that can be stored and managed
```

Cryptography Questions

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

> Self-signed certificates are free and easy to create which means they can be
> created and used in a short timeframe and the user has complete control of
> it

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

> Lack of trust: are not inherently trusted by web browsers, operating
> systems, or other applications, can be vulnerable to attacks if not
> maintained properly

3. What is a wildcard certificate?

> It allows a certificate to secure a domain and all the subdomains that fall
> under it with a single certificate

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 has many well-known security vulnerabilities

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, there is a secure SSL certificate

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

> 1/10/2024-1/9/2025

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

> No

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

```
DigiCert
```

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.

```
AAA Certificate Services
```

Day 3 Questions

Cloud Security Questions

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

```
A similarity is that both have load balancing abilities and offer SSL
termination. A difference is that Azure Front Door offers global services
while Azure Application Gateway offers regional services
```

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 a process where a server receives SSL-based encryption and
is removed from incoming traffic to relieve it from decryption of data. A
benefit of SSL Offloading is a faster loading of the website.
```

3. What OSI layer does a WAF work on?

```
Layer 7: Defense
```

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

```
SQL injection-when a threat actor can input malicious SQL into a query input
```
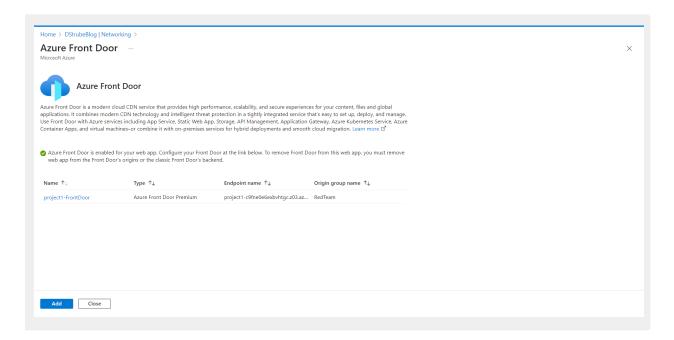
5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn't enabled? Why or why not?

```
No, because the managed rules will investigate and block all malicious SQL
code and queries
```
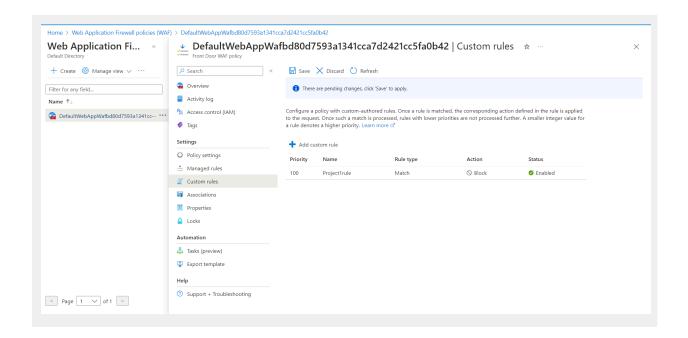
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

```
No, because that WAF rule would block any IP addresses originating in Canada
from accessing the website
```

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.*

Sí