



# Cybersecurity

## Project 1 Technical Brief

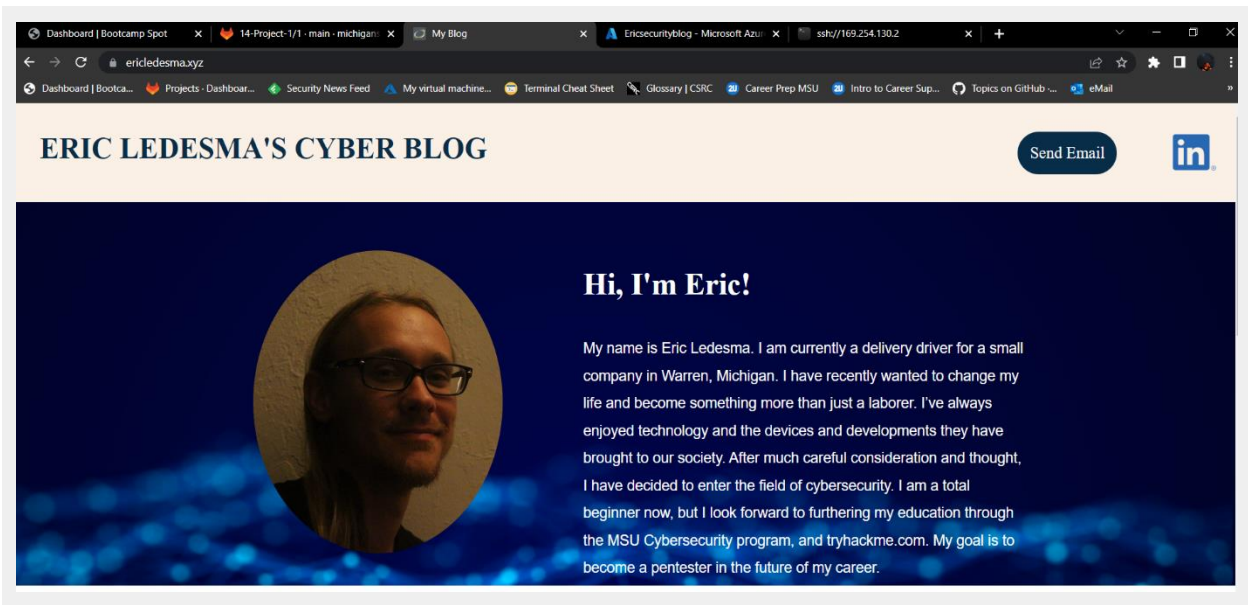
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

### Your Web Application

Enter the URL for the web application that you created:

ericsecurityblog.azurewebsites.net

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



## Blog Posts



### U.S. Offering \$10 Million Reward for Info on North Korean Hackers

bounty, reward, North Korea, hacker, government

The U.S. State Department has doubled their \$5 million bounty only since March of 2022. They are asking for any information to help disrupt North Korea's cryptocurrency theft, cyber-espionage, and other illicit state-backed activities. The most known North Korean hacker group, Lazarus Group is known to have stolen over \$400 million from mainly cryptocurrency scams. Of course, these are only reported numbers, so millions of more illicit dollars may be in their hands. They tend to target bigger institutions with more money, but they will exploit anyone they can. Small businesses all over the world have been targeted. The government-backed group employs tactics such as ransomware, cryptojacking, and extortion operations. Most likely the North Korean government then uses the stolen financials to fund government priorities, such as nuclear and missile programs.



### Cryptocurrency Scams

FTC, scam, crypto

The Federal Trade Commission has filed reports of major increases of cryptocurrency scams since 2018. With just \$12 million scammed from unwilling participants in 2018, to a whopping \$680 million reported scammed in 2021. Currently, the number for 2022 is already \$329M, just for the first quarter of the year. Graphed from January 2021 to March 2022 the FTC has listed some top frauds that are reported. They are Investment Related Fraud at \$575M, Romance Scams at \$185M, Business Imposters at \$93M and Government Imposters at \$40M. With numbers like these it's hard to ignore. Surprisingly, but at the same time, not, the younger generation of people ages 20 to 49 were more than *three times* likely as older age groups to have reported losing their cryptocurrency to a scammer.

## Day 1 Questions

### General Questions

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

GoDaddy

2. What is your domain name?

Ericledesma.xyz

## Networking Questions

1. What is the IP address of your webpage?

20.49.104.52

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

Tappahannock, Virginia, United States

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

```
ericledesma.xyz nameserver = ns34.domaincontrol.com
ericledesma.xyz nameserver = ns33.domaincontrol.com

ns33.domaincontrol.com internet address = 97.74.106.17
ns34.domaincontrol.com internet address = 173.201.74.17
ns33.domaincontrol.com AAAA IPv6 address = 2603:5:21a1::11
ns34.domaincontrol.com AAAA IPv6 address = 2603:5:22a1::11
```

## 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 7.4.  
PHP is a scripting language used for web development.  
It runs on the back end.

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

The assets folder contains all the pictures and styling options for the

website.

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

Front end. Because the front end works with visual elements of a website or app.

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

Cloud computing software that allows customers to share computing resources in a public/private cloud.

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

An access policy determines whether a given security principal, namely a user, application or user group, can perform different operations on Key Vault secrets, keys, and certificates.

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

**Keys:** 'Cryptographic keys' used to encrypt information without releasing the private key to the users.

**Secrets:** Provides secure storage of secrets, such as passwords and database connection strings.

**Certificates:** Supports certificates, which are built on top of keys and secrets and add an automated renewal feature.

### Cryptography Questions

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

They are free.  
Fast and easy to use.  
They are flexible and customizable.  
No dependence on others for certificate issuance.

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

They are not vetted by a trusted process.  
If compromised, they pose a serious risk.  
They cannot be revoked by a CA.  
Security teams lack visibility and control over certificates and trust stores.

## 3. What is a wildcard certificate?

A digital certificate that is applied to a domain and all 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.

There is currently a security vulnerability with 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?

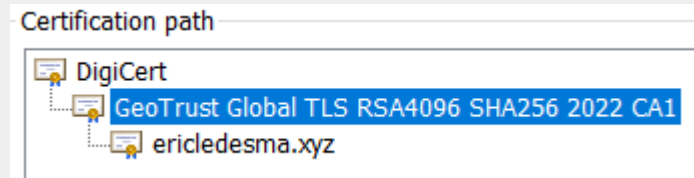
No. I configured it properly. It has a valid Certificate issued by DigiCert.

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

8/1/2022 - 2/2/2023

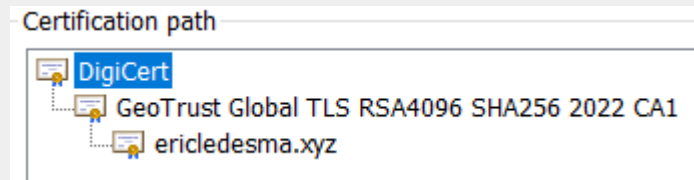
- c. Do you have an intermediate certificate? If so, what is it?

Yes.



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

Yes.



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

No. It only appears in the Intermediate CA.

Intermediate Certification Authorities			Trusted Root Certification Authorities			Trusted P...		
Issued To			Issued By			Expiratio...		
DigiCert Assured ID Ro...			DigiCert Assured ID Root CA			11/9/2031		
DigiCert Assured ID Ro...			DigiCert Assured ID Root CA			11/9/2031		
DigiCert Global Root CA			DigiCert Global Root CA			11/9/2031		
DigiCert Global Root G2			DigiCert Global Root G2			1/15/2038		
DigiCert Global Root G3			DigiCert Global Root G3			1/15/2038		
DigiCert High Assuranc...			DigiCert High Assurance EV Root CA			11/9/2031		
DigiCert High Assuranc...			DigiCert High Assurance EV Root CA			11/9/2031		
DigiCert Trusted Root G4			DigiCert Trusted Root G4			1/15/2038		
DST Root CA X3			DST Root CA X3			9/30/2021		

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

Certum CA

## Day 3 Questions

## Cloud Security Questions

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

Both are Layer 7 HTTP/S Load Balancers.

Differences: Front Door is a non-regional service and Application Gateway is 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 a process of removing SSL based encryption from incoming traffic that a web server receives to relieve it from decryption of data.

3. What OSI layer does a WAF work on?

Layer 7 - Application Layer

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

SQL Injection - an attacker gains unauthorized access to a web application database by adding a string of malicious code to a database query.

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?

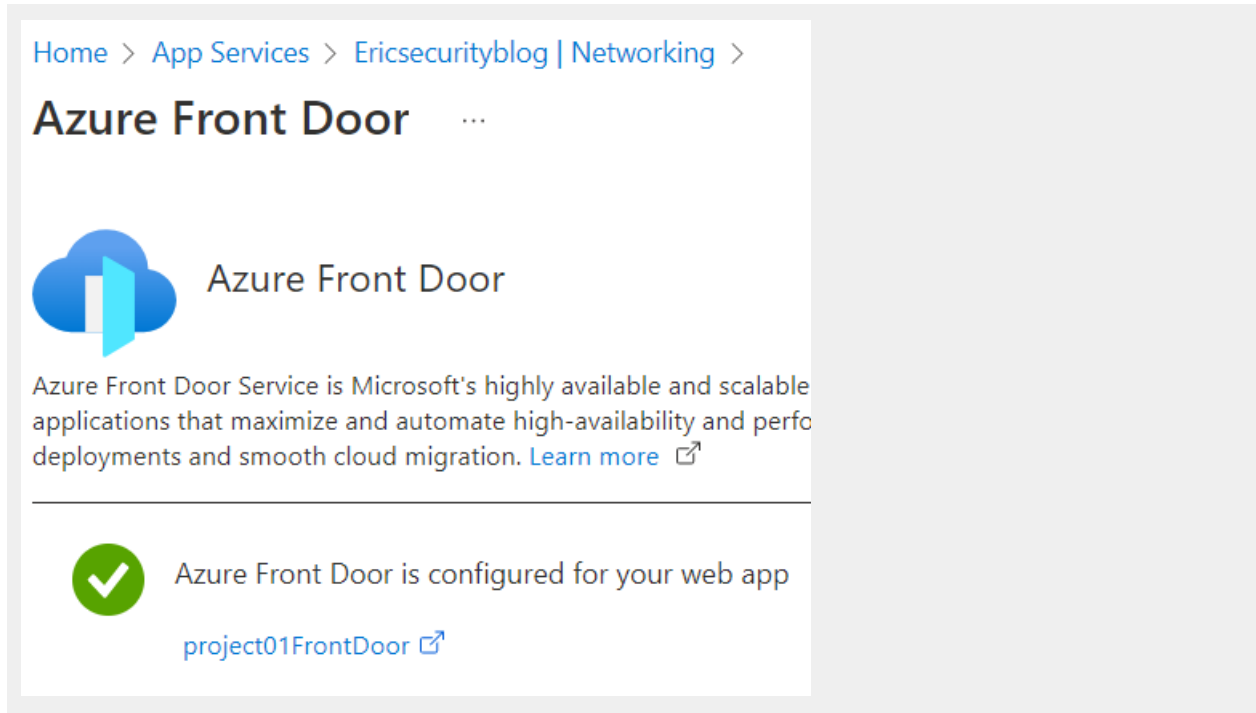
No, this attack would not affect my website because it doesn't use an application database, such as MySQL.

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?




Yes, and no. They would only be able to access the website if they used a VPN to 'change' their geo location.

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

a. Azure Front Door enabled



b. A WAF custom rule

 Add custom rule				
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**