|  |
| --- |
| 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):

|  |
| --- |
| Graphical user interface, text, application  Description automatically generatedText  Description automatically generated |

## Day 1 Questions

### General Questions

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

|  |
| --- |
| GoDaddy |

1. What is your domain name?

|  |
| --- |
| Ericledesma.xyz |

### Networking Questions

1. What is the IP address of your webpage?

|  |
| --- |
| 20.49.104.52 |

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

|  |
| --- |
| Tappahannock, Virginia, United States |

1. 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. |

1. 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. |

1. 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. |

1. 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. |

1. 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 dependance on others for certificate issuance. |

1. 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. |

1. What is a wildcard certificate?

|  |
| --- |
| A digital certificate that is applied to a domain and all its subdomains. |

1. 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. |

1. After completing the Day 2 activities, view your SSL certificate and answer the following questions:
   1. 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. |

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

|  |
| --- |
| 8/1/2022 – 2/2/2023 |

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

|  |
| --- |
| Yes. |

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

|  |
| --- |
| Yes. |

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

|  |
| --- |
| No. It only appears in the Intermediate CA. |

* 1. 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. |

1. 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. |

1. What OSI layer does a WAF work on?

|  |
| --- |
| Layer 7 – Application Layer |

1. 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. |

1. 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. |

1. 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. |

1. Include screenshots below to demonstrate that your web app has the following:
   1. Azure Front Door enabled

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

* 1. A WAF custom rule

|  |
| --- |
| Graphical user interface  Description automatically generated with medium confidence |

## 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*](https://docs.google.com/document/d/1ZzC4oTJFdlkkeWuzuJAyVSqtDFbuAWilmwXg8PZgzMs/edit) *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**