|  |
| --- |
| 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:

|  |
| --- |
| https://webappproj.azurewebsites.net/ |

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)?

|  |
| --- |
| Azure free domain |

1. What is your domain name?

|  |
| --- |
| azurewebsites.net |

### Networking Questions

1. What is the IP address of your webpage?

|  |
| --- |
| 20.40.202.15 |

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

|  |
| --- |
| Des Moines, Iowa, United States |

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

|  |
| --- |
| No record found |

### 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, back-end |

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

|  |
| --- |
| css and images directories. These directories create additional styling rules to the previously created HTML structure. |

1. 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?

|  |
| --- |
| Cloud tenant is a customer who purchases cloud computing resources such as Azure Microsoft cloud services. The user of cloud infrastructure is not the owner but a tenant who pays for access to it. |

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

|  |
| --- |
| A key vault is a cloud service for securely storing and accessing secrets such as API keys, passwords, certificates, or cryptographic keys. Due to the sensitivity of data stored within a key vault, a key vault access policy is used to determine whether a given security principal such as user, application or user group is able to perform different operations on Key Vault secret, keys, and certificates. |

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

|  |
| --- |
| Within key vault, secrets are stored such as passwords, database connection strings, or keys of a storage account. The key vault accepts the data, encrypts it, stores it and returns a secret identifier. This secret identifier can be used to retrieve the secret a later time.  Within key vault, keys are used and stored to support multiple key types and algorithms and enables the use of Hardware Security Module (HSM) for high value keys.  Within key vault, certificates are built on top of keys and secrets and add an automated renewal feature. It provides support for management of X.509 certificates. It allows certificate owners to create a certificate through a key vault creation process or through importing of existing certificate.  Key vault key allows key operations, key vault secret allows retrieval of certificate value as a secret and key vault certificate contains public X.509 certificate metadata. |

### Cryptography Questions

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

|  |
| --- |
| Self-signed certificates are free; suitable for internal network websites and development/testing environments; and encryption and decryption of data is done with the same ciphers used by paid SSL certificates. |

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

|  |
| --- |
| Browsers and Operating systems do not trust self-signed certificates; attackers can generate self-signed certificates, which can be used for man-in-the-middle attacks- this leaves users vulnerable to data theft and other forms of cyber-attacks; and security team lacks visibility and control over the certificates. |

1. What is a wildcard certificate?

|  |
| --- |
| Wildcard certificate allows to secure main domain and unlimited number of subdomains under the main domain with just one certificate. It offers full encryption for the subdomains, making it an affordable and effective solution for most websites. |

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.

|  |
| --- |
| SSL 3.0 isn’t provided because of an industry-wide vulnerability called POODLE. |

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 because Azure domain provides a trusted certificate for my domain. |

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

|  |
| --- |
| March 14, 2022 – March 9, 2023 |

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

|  |
| --- |
| Yes, Microsoft Azure TLS Issuing CA 01 |

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

|  |
| --- |
| Yes, DigiCert Global Root G2 |

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

|  |
| --- |
| Yes |

* 1. List one other root CA in your browser’s root store.

|  |
| --- |
| Digitalsign Global Root RSA CA |

## Day 3 Questions

### Cloud Security Questions

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

|  |
| --- |
| Both Front Door and Web Application Gateway are layer 7 load balancers, the protocols handled are HTTP and HTTPS. The differences are: the Front Door is a non-regional service while Web Application Gateway is regional service; Front Door is a global, scalable entry-point used to create fast, secure and widely scalable web applications while Web Application Gateway is a web traffic load balancer enabling users to manage traffic on their web applications; and Front Door can load balance between different scale units/clusters/stamp units across regions while Web Application Gateway allows to load balance between VMs/Containers etc that is within the scale unit. |

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 the process of removing SSL based encryption from incoming traffic that a web server receives to relieve it from decryption of data. SSL encrypts communications between client and server sending messages safely across networks. Encryption of sensitive information protects against potential hackers and man-in-the-middle attacks. Since SSL offloading moves the processing to a dedicated server, this frees up the web server to handle other application delivery demands. Some benefits of SSL Offloading are: boost page load speed time; faster response from the Web Server; better web server performance; enhanced website stability; autoscaling of web servers during peak traffic hours; and using a load balancer for serving web traffic using different servers. |

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 attack consists of insertion or injection of SQL query via input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, recover content of a given file present on the DBMS file system and some cases issue commands to the operating system. The SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands. |

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?

|  |
| --- |
| Yes, it will be impacted because if Front Door is not enabled. Front Door Azure-managed Default Rule Set includes SQL injection protection and if disabled, will be vulnerable to this attack. |

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 this will block traffic from anyone residing Canada to access the website because Block rule requests sends WAF response to the client without forwarding the request to the back-end. |

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

|  |
| --- |
|  |

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

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.