| 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:

| rishabhsecurityresume.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 |
| --- |

1. What is your domain name?

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

### Networking Questions

1. What is the IP address of your webpage?

| 52.231.38.95 |
| --- |

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

| City: Seoul  State: Seoul Special City  Country: South Korea |
| --- |

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

|  |
| --- |

### 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?

| Runtime: PHP 8.0  Yes it works on the Back end |
| --- |

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

| Layout of the website(CSS) and Visuals of the website (Images) |
| --- |

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

| Back end |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

| CLOUD TENANT: It refers to an individual or organization that utilizes cloud services provided by a cloud provider. It represents its own isolated environment within the cloud infrastructure, where it can deploy and manage applications, data, and services. Cloud tenants have control over their resources and can scale them according to their needs while relying on the cloud provider for underlying infrastructure management. Tenancy is divided two parts single-tenant SAAS and multi-tenant SAAS |
| --- |

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

| Access policy is important to the key vault it allows different users, applications, or user groups to have proper security and control over sensitive cryptography and secrets stored within it. Some of the reasons why access policy is important as: -   1. Access policy helps in providing authorization control in a key vault by creating, deleting, or updating the key and secrets. Access policies help to enforce authorization control by only allowing selective individuals and groups to access the vault. 2. Helps in segregating the duties by assigning a specific role to individuals to reduce conflict and confusion. 3. Helps in compliance and auditing by assigning permission to a specific user or group can be used as an effective way to track and log all activities in the vault. |
| --- |
|  |

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

| Keys: used to encrypt information without releasing the private key to the consumer. It acts like a black box encryption and decrypts content using RSA algorithm.  Secrets: Helps in providing a secure store of secrets and information like application settings, tokens, passwords, and database connection strings  Certificates: Build o top of keys and secrets and add a automated renewal feature/auto rollover |
| --- |

### Cryptography Questions

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

| 1. SSl helps in data security: Provides secure encryption of data transmitted between a web server and a client's browser. This encryption ensures that the information exchanged remains confidential and protected from unauthorized access. SSL certificates use cryptographic algorithms to encrypt sensitive data, making it virtually impossible for attackers to intercept and decipher. 2. Authentication: SSL certificate verifies the identity of a website or server, assuring users that they are communicating with the intended organization and not an imposter or malicious entity. The Certificate is issued by certified authorities after a rigorous validation process, which includes verifying the domain ownership and organization details. 3. Compliance: In recent times many industry regulations and standards require the use of SSL certificates to ensure data privacy and security 4. Prevents different attacks: SSL certificates help to prevent different types of attacks such as: - A) Man-in-the-middle attack: Attacks: SSL encryption prevents attackers from intercepting and altering data exchanged between a client and server. It ensures that the communication remains confidential and tamper-proof, making the attack extremely difficult  B) Phishing: SSL certificates will help in combatting phishing attacks by displaying visual indicators, such as the padlock icon or a green address bar, indicating a secure connection. This makes it easier for users to identify legitimate websites and avoid falling victim to phishing scams   c) Data interception: SSL encryption prevents eavesdropping and data interception by encrypting all communication between the client and server. Even if someone manages to intercept the data, they won't be able to understand or use it without the decryption key. |
| --- |

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

| Some of the most common disadvantages of self-signed certificates are-   1. Slows down the connections due to encryption and decryption of data before it can used. 2. Highly expensive because of the maintenance and verification process, depending upon the type of certificate cost may vary. 3. SLL certificate needs to renew occasionally as it expires. If the customer doesn’t renew the certificate on time they might lose some important data as the site might not be secure anymore |
| --- |

1. What is a wildcard certificate?

| A wildcard certificate often called as SSL/TLS uses a wildcard character (\*) in the domain name field to secure multiple subdomains under a base domain. For instance, a wildcard certificate for \*.example.com can protect subdomains like blog.example.com, app.example.com, and support.example.com. Clients employ a matching procedure to determine if a subdomain matches the wildcard certificate. |
| --- |

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.

| Microsoft Azure aims to create a highly secure environment for its users. They took action to address a significant vulnerability found in SSL 3.0, which affected not just a few machines but all websites and virtual machines. As a result, Microsoft made the decision to disable 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?

| My browser is not returning an error for my ssl certificate as my certificate is valid and connection is secured. |
| --- |

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

| Thurday March 9, 2023 to Sunday March3 ,2024 |
| --- |

A screenshot of a computer

Description automatically generated with medium confidence

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

A screenshot of a computer program

Description automatically generated with low confidence

|  |
| --- |

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

| Yes , It’s called as DigiCert Global Root G2 |
| --- |

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

| No |
| --- |

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

| No |
| --- |

A screenshot of a computer

Description automatically generated

## 

## Day 3 Questions

### Cloud Security Questions

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

| Differences: Azure front door filters at the edge location before the data center whereas Azure Web Application filters when it enters VNET via gateway. Moreover, Front door is a global service whereas Azure web application gateway is regional.  Similarities: Both Front Door and Azure web application gateway are in layer 7 (HTTP/HTTPS). Adding more to it front Door and Application Gateway offer session affinity capabilities. With Front Door, subsequent traffic from a user session can be directed to the same cluster or backend within a specific region. On the other hand, Application Gateway can direct traffic to the same server within a cluster, ensuring affinity for the session |
| --- |

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

| When using the SSL secure protocol, the web server is responsible for encrypting and decrypting web traffic, which can put a significant strain on its performance. To alleviate this burden, many networks utilize SSL offloading, a technique where SSL encryption is handled by a separate device before the traffic reaches the web server. By offloading the SSL process, the web server's performance remains unaffected.  Some of the benefits of SSL offloading are:-  a) Increase page load speed time  b) better web server performance  c) used as a load balancer for serving web traffic using different servers |
| --- |

1. What OSI layer does a WAF work on?

| WAF works on layer 7 |
| --- |

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

SQL Injection: Often called as SQLi it can be defined as a malicious SQL code injected into an application that allows an attacker to gain unauthorized access to view and modify a database

| [Enter answer here] |
| --- |

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, my website will be impacted if the front door wasn’t enabled as it allows any individual or user group to make changes to my website content. |
| --- |

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?

| No blocking people who reside in Canada won’t be a viable option as a user can access the website using VPN , using ip instead of URL using free PING tools or web browsers like tor to access the website. These techniques are used to mask the user’s identity in order to have access for a website |
| --- |

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

| [Paste screenshot here] |
| --- |

A screenshot of a computer

Description automatically generated with medium confidence

* 1. A WAF custom rule

|  |
| --- |
|  |
|  |

A screenshot of a computer

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

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