| 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:

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

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

| Screenshots of website at the bottom |
| --- |

## Day 1 Questions

### General Questions

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

| I selected an Azure free domain |
| --- |

1. What is your domain name?

| Aliscybersafehub |
| --- |

### Networking Questions

1. What is the IP address of your webpage?

| 20.211.64.16 |
| --- |

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

|  |
| --- |

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?

| When selecting a runtime stack I selected PHP 8.2 PHP is a server-side language, so it is a backend. It is responsible for processing server-side logic, interacting with databases, and generating dynamic content that is sent to the client's browser for display on the front end. |
| --- |

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

| Css and images |
| --- |

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

| The /var/www/html/assets directory contains resources for a web application. Specifically, the directory includes CSS (Cascading Style Sheets) files. It also contains images used in the graphical user interface. These assets are associated with the front-end development of the web application. |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

| A cloud tenant is someone or a group that utilizes cloud services from a provider. In a tenant cloud setup several tenants use the same infrastructure and resources but their data and applications are kept separate, for security and privacy purposes. |
| --- |

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

| The importance of Access policies in a key vault are crucial for controlling who can perform specific operations for example individuals or applications (like reading, writing, and managing) for keys, secrets, and certificates stored in the key vault. These policies help maintain the principle of least privilege, ensuring that only authorized individuals or applications have access to their sensitive cryptographic materials. |
| --- |

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

| * Differences in Key Vault:      * + Keys:     - Used for cryptographic operations.     - Examples include encryption and decryption keys.     - Managed by Azure Key Vault. * Secrets:      * Sensitive information like passwords or connection strings. * Can be text or binary data. * Managed by Azure Key Vault.      * Certificates:      * Digital certificates used for secure communication. * Typically include a public key and information about the entity. * Managed by Azure Key Vault. |
| --- |

### Cryptography Questions

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

| * Self-Signed Certificate Advantages:   + Quick setup for testing and internal use.   + No cost associated with acquiring from a Certificate Authority.   + Provides full control over certificate creation and management. |
| --- |

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

| * Self-Signed Certificate Disadvantages:   + Not Trusted: Browsers and devices don't automatically trust self-signed certificates.   + No Validation: Unsuitable for public-facing websites.   + Limited Use: Inappropriate for e-commerce or scenarios requiring broad trust. |
| --- |

1. What is a wildcard certificate?

| * Wildcard Certificate:   + Is a type of SSL/TLS certificate covering main domain and subdomains.   + Denoted by asterisk (\*) in the subdomain part.   + Allows flexibility and cost savings in securing multiple 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.

| SSL 3.0 has known vulnerabilities, such as POODLE (Padding Oracle On Downgraded Legacy Encryption). Due to these security flaws, it's deprecated and considered insecure. Azure focuses on providing more secure TLS versions (1.0, 1.1, and 1.2) to ensure a higher level of encryption and data protection. |
| --- |

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, no warning message |
| --- |

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

| It expires on 07/03/2025 |
| --- |

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

| Microsoft Azure RSa TLS Issuing CA 07 |
| --- |

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

| 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.

| GTS CA 1C3 |
| --- |

## Day 3 Questions

### Cloud Security Questions

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

| * Azure Web Application Gateway and Azure Front Door Overview   + Similarities:     - Both services route traffic to backend services.     - Both offer load balancing for better performance and availability.     - Both support SSL offloading, terminating SSL connections at the gateway or front door. * Differences: * WAG focuses on application-level routing, load balancing, and web application firewall. * AFD provides content delivery network (CDN) capabilities, global load balancing, caching, and acceleration. * WAG is suitable for regional applications. * Azure Front Door includes CDN capabilities for improved performance. |
| --- |

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

| * ⁤SSL offloading: ⁤ * SSL offloading is a process where a device or service handles SSL/TLS encryption and decryption tasks before traffic reaches backend servers, offering benefits such as faster response times and reduced costs. ⁤⁤some SSL benefits include ⁤ * Reduces Server Load: By offloading SSL processing from backend servers reduces their load, which allows them to focus on other tasks. ⁤ * Improved Performance: SSL offloading can improve overall application performance by freeing up server resources and reducing latency related with SSL/TLS handshake and encryption.   ⁤   * Centralized Management: SSL/TLS certificates and configurations can be managed centrally at the offloading device, simplifying certificate management and updates. ⁤ |
| --- |

1. What OSI layer does a WAF work on?

| Web Application Firewall Overview:   * Operates at Layer 7 of OSI model. * Analyzes and filters HTTP traffic. * Protects web applications from attacks and vulnerabilities. |
| --- |

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

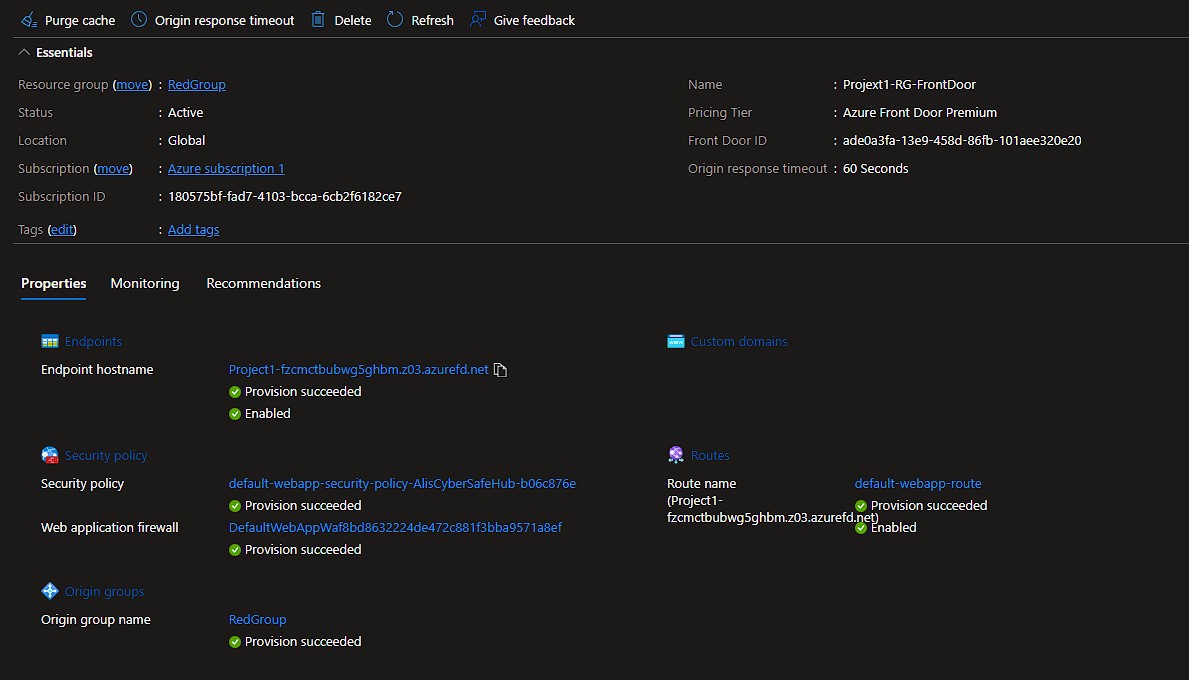
| Selected Managed Rule: SQL Injection  Definition:  SQL Injection is a type of web security vulnerability where an attacker can change the SQL queries in an application's database by using malicious SQL code into input fields, such as forms or URL parameters. This can lead to unwanted access to sensitive data, change to database contents, and can even take control of the whole application. |
| --- |

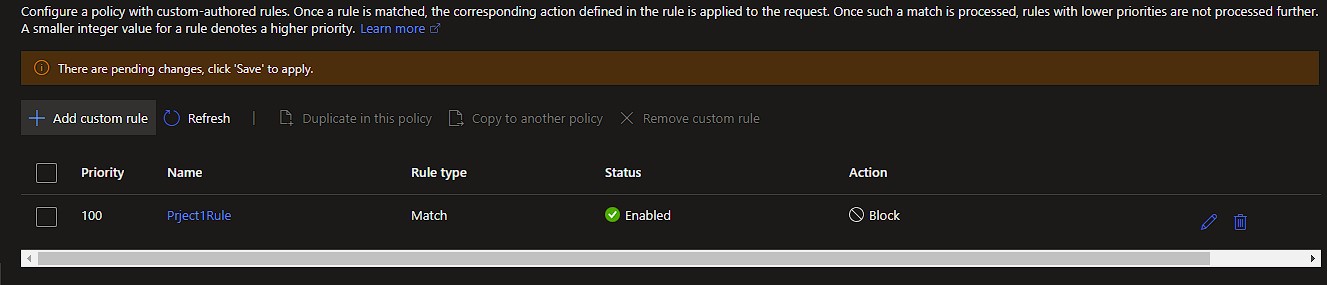
1. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn’t enabled? Why or why not?

| Impact Without Front Door:  The website could be vulnerable to a SQL Injection vulnerability if Front Door was disabled. The website is open to incoming traffic without Front Door meaning that it will receive harmful requests with SQL injection payloads. SQL Injection attacks could be used on the website's databases if appropriate security measures, like a Web Application Firewall (WAF) or input validation methods, aren't in place. |
| --- |

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?

| Custom WAF Rule Blocking Traffic from Canada:  Creating a custom WAF rule to block all traffic from Canada would not ensure that anyone from Canada wouldn't be able to access the website. While the rule would block requests coming from Canadian IP addresses, it doesn't necessarily guarantee that all requests from Canada would be blocked. Users could still access the website by utilizing tools to disguise their actual location like VPNs.  IP-based blocking can sometimes lead to false positives, where actual users are incorrectly blocked due to shared IP addresses or other factors. Therefore, while the custom WAF rule may reduce the amount of incoming traffic from Canada, it may not completely block Canadian users, and it may also block non-Canadian users. |
| --- |

1. Include screenshots below to demonstrate that your web app has the following:
   1. Azure Front Door enabled
   2. 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.*
* ***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.

