| Cybersecurity |
| --- |
| Project 1 Technical Brief |

## Your Web Application

Enter the URL for the web application that you created:

| dianakproject1-hnanevc8cnb6hrez.westeurope-01.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?

| DianaKProject1 |
| --- |

### Networking Questions

1. What is the IP address of your webpage?

| 13.69.68.62 |
| --- |

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

| West Europe |
| --- |

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?

| I selected PHP 8.2 runtime stack. 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.

| Inside the asset’s directory, is the originally configured web app material. It includes Robert Smith profile picture, LinkedIn logo image, background image, etc. I saw a CSS directory and observed HTML language in some documents. It seems like the directory is like a content management system. |
| --- |

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

| It works on the front end. |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

| A cloud tenant is a customer who uses a cloud service provider’s shared infrastructure, while maintaining secure and isolated access to their own resources. |
| --- |

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

| An access policy is important because it controls who can access and manage the keys, secrets, and certificates. |
| --- |

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

| Keys- Cryptographic keys used for encryption, decryption, signing, etc.  Secrets- Data such as passwords, connection strings, API keys, and other sensitive information.  Certificates-Digital certificates used for establishing secure connections. It also provides identity verification. |
| --- |

### Cryptography Questions

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

| Advantages include Complete control over a certificate, quick set-up, cost effective since it is free, and convenient for internal use. |
| --- |

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

| Disadvantages include Lack of trust leading to limited use cases, no identity verification since there is no third-party validation, and management complexity in large systems. |
| --- |

1. What is a wildcard certificate?

| It is a type of digital SSL/TLS certificate that secures a domain and all of its subdomains in a single 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.

| SSL 3.0 is not provided because it is outdated and considered insecure due to vulnerabilities. It is not best practice to use it. |
| --- |

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?

| Yes, it is saying that my “request is missing a bearer or PoP token.”. Full message below:  {"error":{"code":"Unauthorized","message":"AKV10000: Request is missing a Bearer or PoP token."}} |
| --- |

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

| 10/24/2024- 10/24/2025 (1 year) |
| --- |

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

| No, I do not have an intermediate certificate. |
| --- |

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

| Yes, I have a root certificate.  Subject:  C=NL, ST=West Europe, L=Shiphol, Noord-Holland, O=Student, CN=DianaKProject1Blog.com  Issuer:  C=NL, ST=West Europe, L=Shiphol, Noord-Holland, O=Student, CN=DianaKProject1Blog.com |
| --- |

* 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.

| Certum CA (Find image below) |
| --- |

## Day 3 Questions

### Cloud Security Questions

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

| Both services are made to manage and optimize web traffic.  Similarities:  They both offer Traffic management, Load balancing, Routing capabilities, Security features (I.e. WAF), Autoscaling, SSL termination support, and Integration w/ Azure Services. They both operate at Layer 7.  Differences:  Azure Web App Gateway- Best for single regional traffic, best for regional latency, Supports URL path-based routing, and custom routing rules, Does not have built-in caching, and Works with internal load balancers  Azure Front Door- Best for global load balancing, best for multi-region applications, provides global traffic routing, uses anycast and latency based routing, made for global latency, includes caching, integrates with Azure DNS for custom domains, and allows CDN-like global DNS Load balancing.  Depending on purpose of the services, prices may also differ between the two. |
| --- |

1. What is SSL offloading? What are its benefits?

| SSL offloading is the process where encrypting and decrypting SSL/TLS traffic is handled by a dedicated device or service. Benefits include better web server performance, reduced server load, simplified SSL management, scalability, and enhanced security in the server. |
| --- |

1. What OSI layer does a WAF work on?

| Layer 7- Application Layer. Functions of this layer include traffic monitoring, content inspection, and HTTP request filtering. |
| --- |

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

| SQL injection: A web security vulnerability that allows an attacker to interfere with the queries than an application makes to its database. Malicious SQL codes are injected into an input field (i.e. login forms, search bars, URLs, etc.). |
| --- |

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, enabling the front door alone isn’t enough to prevent SQL injection. Azure front door adds security layers such as WAF capabilities that help mitigate SQL injection attacks, but secure coding practices are essential in the long run. That is the primary defense against SQL injection. |
| --- |

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, ideally, users who physically reside in Canada, or who’s IP is from Canada will not be able to access my website. |
| --- |

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