| 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://dmytrogsecurityblog.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?

| 20.211.64.11 |
| --- |

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

| Cydney, NSW, Australia |
| --- |

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

| No NS 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?

| Runtime stack is a collection of components that are used to run web application. It usually includes frameworks, language and database. In our case we use the PHP8.0 environment and MySQL database. It refers to both the front end and back end. |
| --- |

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

| There are 2 directories there - css and images. In images there are images used for the website and in css there is style.css file (together with it’s backup copy) which contains formatting details for the page |
| --- |

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?

| It means a person or organization that uses cloud service provided by a service provider. |
| --- |

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

| As key vault keeps major secrets and important assets like certificates the proper access policy is crucial for secrecy and integrity of of web application |
| --- |

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

| The keys are symmetric and asymmetric keys used for encrypting and decrypting and signing documents of connection. Secrets usually are passwords, API keys or any other information which is confidential. Certificates are the files containing information about the entity along with a digital signature, used for others to prove that you are you. |
| --- |

### Cryptography Questions

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

| They are easy to setup and free |
| --- |

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

| They are not validated and not verified by trusted third parties. This makes such certificates untrusted. All web browsers issue warnings not to trust to such websites. |
| --- |

1. What is a wildcard certificate?

| Wildcard certificates used to secure multiple subdomains of a domain with 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 had significant security issues and was discarded. Today's best practice recommends using TLS 1.2 and higher |
| --- |

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, as my website is automatically covered by Microsoft certificate. |
| --- |

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

| One year |
| --- |

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

| Yes, Microsoft Azure TLS Issuing CA 02 |
| --- |

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

| Yes, Microsoft RSA Root Certificate Authority 2017 |
| --- |

* 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.

| AmAzon Root CA1 |
| --- |

## Day 3 Questions

### Cloud Security Questions

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

| Both of these services provide load balancing and SSL Offloading, but they differ in the following: AWAG focuses on application-level load balancing while AFD provides a wider set of features for global routing, content delivery and traffic management. AFD supports more protocols and also has built in DDoS protection. |
| --- |

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 handling SSL/TLS encryption and decryption at a point before reaching the backend servers or applications. Instead of the backend servers performing the resource-intensive task of SSL encryption/decryption, it is offloaded to a specialized service. This means improved performance, scalability, reduced resource consumption, simplified certificate management, traffic balancing. |
| --- |

1. What OSI layer does a WAF work on?

| WAF usually operates on layer 7 |
| --- |

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

| “SQL Injection attack:common injection testing detected” - this rule defines behavior if certain activity is noticed. This rule is enabled, and if such activity is registered it should be blocked on anomaly. |
| --- |

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?

| This rule refers to database vulnerability. As my blog does not have any database attached, this rule will not help me at all. |
| --- |

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?

| It means that all IP addresses registered in Canada will be blocked, but residents of Canada still can access the website via proxies or VPN as long as proxies and VPN points do not reside in Canada. |
| --- |

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.*
* ***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.