|  |
| --- |
| A picture containing symbol, graphics, circle, font  Description automatically generated    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://melssecurityblog.azurewebsites.net/ |

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

|  |
| --- |
| A screenshot of a person's profile  Description automatically generated with medium confidence |

A picture containing text, screenshot

Description automatically generated

**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?

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

**Networking Questions**

1. What is the IP address of your webpage?

|  |
| --- |
| 20.48.202.167 |

A screenshot of a computer

Description automatically generated with medium confidence

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

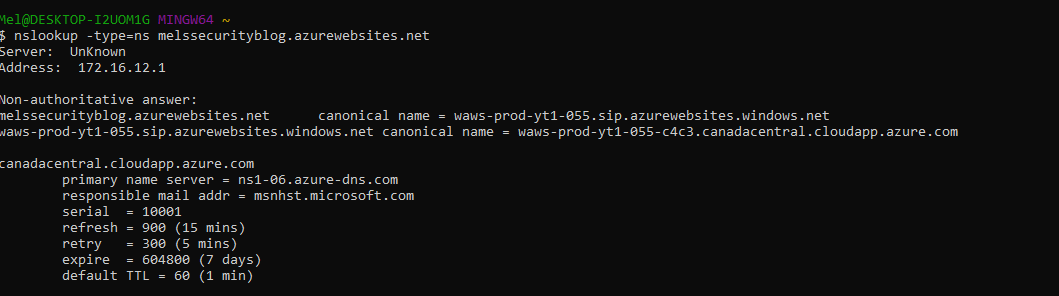
|  |
| --- |
| Toronto, Ontario, Canada |

A screenshot of a computer

Description automatically generated with medium confidence

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

|  |
| --- |
| Server unknown  Address 172.16.2.1  Then searched nslookup -type=ns melssecurityblog.azurewebsites.net  See below snip |



**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 PHP 80, runs on the back end it s the software stack responsible for installing your web service’s code and its dependencies and running service. |

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

|  |
| --- |
| CSS(Directory) is the website style example font. And the images from the website. |

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

|  |
| --- |
| This is the front end of the website as it is visual. |

**Day 2 Questions**

**Cloud Questions**

1. What is a cloud tenant?

|  |
| --- |
| A cloud tenant is a customer who purchases a cloud computing resource. |

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

|  |
| --- |
| An access policy is important on a key vault as it allows only certain people to have access to the key vault. |

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

|  |
| --- |
| **Keys**: supports multiple key types and algorithms and enables the use of software-protected and HSM-protected keys.  **Secrets**: Provides secure storage of secrets (passwords and database connection stings).  **Certificates**: supports certificates, which are built on top of keys and secrets. |

**Cryptography Questions**

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

|  |
| --- |
| * Opportunity for unlimited certificate generation * No payment required. * Quick initiation. |

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

|  |
| --- |
| * User personal data set at risk * Permanent “unknown publisher” warning * Data security is not guaranteed. * Lack of user trust resulted from the absence of a certification center signature. * Possible errors in the certificate may cause it to fail or not generated correctly. |

1. What is a wildcard certificate?

|  |
| --- |
| A wildcard certificate is used to secure multiple domains. If you have many domains this can save you money. |

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.

|  |
| --- |
| The SSL 3.0 vulnerability stems from the way blocks of data are encrypted under a specific type of encryption algorithm within the SSL protocol. The Poodle attack was letting attackers exploit this vulnerability to decrypt and extract information from inside an encrypted transaction. |

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?

|  |
| --- |
| I have used azures free website, but using <https://self-signed.badssl.com> this website returns an error for the site being not secure.  <https://melssecurityblog.azurewebsites.net/> - is a secured site, azure has its own certificate. |

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

|  |
| --- |
| <https://self-signed.badssl.com> - The Validity period is Sunday April 23, 2023 – Tuesday April 22, 2025 |
| <https://melssecurityblog.azurewebsites.net/> - is March 9, 2023 – March 3, 2024 |

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

|  |
| --- |
| <https://self-signed.badssl.com> – is not a certification authority.  <https://melssecurityblog.azurewebsites.net/> Maximum number of intermediate CAs: Unlimited. |

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

|  |
| --- |
| <https://self-signed.badssl.com> - has none  <https://melssecurityblog.azurewebsites.net/> - is DigiCert Global Root G2. |

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

|  |
| --- |
| Yes see snip |

A screenshot of a computer

Description automatically generated with medium confidence

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

|  |
| --- |
| AddTrust External CA Root see snip |

A screenshot of a computer

Description automatically generated with medium confidence

**Day 3 Questions**

**Cloud Security Questions**

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

|  |
| --- |
| Similarities:   * Both are in the front of the web application. * Both work on Layer 7 of OSI model (application layer) * Both primary solution is a load balancer. * Both can use WAD to protect against vulnerability attacks. * Both have additional features as URL path-based routing and SSL/TLS termination.   Differences:   * Web Application Gateway – best to protect a single region in your cloud. * Azure Front Door – global and better used with variety of regions in your cloud. |
|  |

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

|  |
| --- |
| SSL offloading removes the SSL based encryption from incoming traffic, relieves the web server of encrypting and decrypting traffic sent by SSL. |

1. What OSI layer does a WAF work on?

|  |
| --- |
| WAF protects the application layer (7). |

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

|  |
| --- |
| SQL Injection: A SQL injection is when an attacker can get into and interfere with queries that an app makes to its database. The attacker then can get information on users and in some cases get access to the server or other back-end infrastructure. |

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 can, but there is not much reason for the attacker to use my website as it is just a blog and I am not a known blogger. |

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, it is not possible to know if the user is accessing your website from Canada, they can use a VPN to mask their IP and bypass this custom WAF rule. |

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

1. Azure Front Door enabled

|  |
| --- |
| 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.*

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