|  |
| --- |
| Cybersecurity |
| Securing Cloud Apps Technical Brief |

## Your Web Application

|  |
| --- |
| mbscybersec.azurewebsites.net |

|  |
| --- |
|  |

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

|  |
| --- |
| Azure free domain |

1. What is your domain name?

|  |
| --- |
| mbscybersec.azurewebsites.net |

1. What is the IP address of your webpage?

|  |
| --- |
| 20.211.64.24 |

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

|  |
| --- |
| Sydney, New South Wales, Australia |

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

|  |
| --- |
| The NS record shows me the IP address & the alias for my website.  Non-authoritative answer:  Name: waws-prod-sy3-111-c793.australiaeast.cloudapp.azure.com  Address: 20.211.64.24  Aliases: mbscybersec.azurewebsites.net  waws-prod-sy3-111.sip.azurewebsites.windows.net |

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 the combination of language, tools and frameworks used to run the web app. It runs both on front end and back end depending upon what stack is used. |

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

|  |
| --- |
| It contains two folders, css and images.  Css folder contains the css files which are crucial for the front end designing and styling of the website and the html code refers to this file and displays the page accordingly.  The images folder as the title suggests contains the images needed to display on the webpage they can be referred to in the html code by using their path. |

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

|  |
| --- |
| Front end |

1. What is a cloud tenant?

|  |
| --- |
| A cloud tenant refers to someone who utilizes cloud resources and services provided by a cloud service provider such as Microsoft Azure. |

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

|  |
| --- |
| Implementing an access policy on a key vault is important for maintaining confidentiality, integrity and availability of the sensitive data stored within the vault. |

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

|  |
| --- |
| -Keys within a key vault are cryptographic keys used for encryption and decryption of data.  -Secrets within a key vault are sensitive information stored within the key vault such as passwords.  -Certificates in key vaults are digital certificates used for authentication or encryption. |

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

|  |
| --- |
| Self-signed certificates are cost efficient.  Easy and quick to set up.  They are suitable for temporary usage cases. |

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

|  |
| --- |
| Since self-signed certificates are not issued by third party certificate authorities they are not recognised by browsers which in turn leads to a bunch of security warnings.  Since they are not recognised by third party certificate authorities they coil leads to multiple security risks. |

1. What is a wildcard certificate?

|  |
| --- |
| A wildcard certificate is a type of digital certificate used to secure multiple subdomains with a single certificate. It is denoted by a \* on the leftmost of a Domain name. |

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 isn’t provided because it has many vulnerabilities and security weaknesses which makes it susceptible to many attacks. |

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?

|  |
| --- |
| It is not returning an error for the SSL certificate because I have a valid SSl assigned by a CA. |

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

|  |
| --- |
| Issued On Tuesday, March 12, 2024 at 9:36:42 PM  Expires On Friday, March 7, 2025 at 8:36:42 PM |

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

|  |
| --- |
| Yes, the certificate is Microsoft Azure RSA TLS Issuing CA 07. |

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

|  |
| --- |
| Yes, the certificate I have is DigiCert Global Root G2. |

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

|  |
| --- |
| Yes it does. |

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

|  |
| --- |
| AffirmTrust. |

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

|  |
| --- |
| Similarities  -Both Azure Web App and Azure Front Door provide load balancing capabilities.  -Both services operate on Layer 7 of the OSI model.  -Both services provide a web application firewall to protect against attacks.  Differences  -Azure front door is mainly global and more suitable if there are multiple regions in the cloud environment, whereas the Azure Web Application is more suited to protect a cloud environment in a single region. |

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 when the SSL encryption/decryption tasks are offloaded to/Handled by the Web Application gateway or Front Door to relieve the backend servers.  Benefits  -Better performance by relieving the backend servers.  -allows backend servers to handle more load. |

1. What OSI layer does a WAF work on?

|  |
| --- |
| Layer 7 |

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

|  |
| --- |
| ‘Restricted File Upload Attempt’  This WAF managed rule is a security measure implemented by WAF which detects and prevents malicious file uploads to the web app. |

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?

|  |
| --- |
| As my website is currently designed, it does not have an upload feature so even if the front door is not enabled since there is no upload feature, no malicious files could be uploaded, however if my website did have an upload feature then the website could be exposed to malicious file uploads if the front door is not enabled. |

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, It will block all traffic from Canada because the WAF rule will inspect all traffic and block the IPs originating from Canada, so anyone accessing the website from Canada will be blocked from visiting the website. |

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

|  |
| --- |
|  |

* 1. A WAF custom rule

|  |
| --- |
|  |