| 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://chuckssecurityspot.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?

| 20.119.16.35 |
| --- |

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

| Washington, Virginia, United States |
| --- |

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

| waws-prod-blu-435.sip.azurewebsites.windows.net (waws-prod-blu-435-246b.eastus.cloudapp.azure.com.) |
| --- |

### 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?

| The runtime stack was PHP 8.0. Runtime stacks run on the back end of development. |
| --- |

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

| Two directories: css and images that contain the css stylesheet and images that format the webpage. |
| --- |

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

| CSS works on the front end of development. |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

| A customer who has purchased cloud computing resources. |
| --- |

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

| A Key Vault access policy determines whether a given security principal, namely a user, application or user group, can perform different operations on Key Vault secrets, keys, and certificates. |
| --- |

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

| Cryptographic keys: Supports multiple key types and algorithms, and enables the use of software-protected and HSM-protected keys. Secrets: Provides secure storage of secrets, such as passwords and database connection strings. Certificates: Supports certificates, which are built on top of keys and secrets and add an automated renewal feature. |
| --- |

### Cryptography Questions

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

| Self-signed certificates are appropriate for development/testing environments and internal network websites. Self-signed Certificates are simple to modify or customize; for instance, they can carry more metadata or have greater key sizes. |
| --- |

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

| They do not provide any trust value, so are mostly useless in establishing identity assurance. Self-signed certificates cannot be revoked. It could be “invalidated” by removing it from a whitelist, but that requires trusting it in the first place. They are not managed by a public key infrastructure (PKI), so they are very likely to be “lost” (especially since they can’t be revoked), creating a significant gap in your security perimeter. |
| --- |

1. What is a wildcard certificate?

| a single certificate with a wildcard character (\*) in the domain name field. This allows the certificate to secure multiple sub domain names (hosts) pertaining to the same base domain. |
| --- |

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.

| Azure Websites has disabled SSL 3.0 for all sites by default to protect our customers from the vulnerability mentioned in Security Advisory 3009008. |
| --- |

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, I am using the azure free domain, which attaches the azure provided SSL certificate. |
| --- |

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

| March 9, 2023 - March 3, 2024 |
| --- |

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

| No, I have a root certificate |
| --- |

* 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 this certificate is in my browser root store |
| --- |

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

| Symantec Enterprise Mobile Root for Microsoft |
| --- |

## Day 3 Questions

### Cloud Security Questions

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

| While both Front Door and Application Gateway are load balancers, the primary difference is that Front Door is a non-regional service whereas Application Gateway is a regional service. |
| --- |

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

| SSL offloading relieves a web server of the processing burden of encrypting and decrypting traffic sent via SSL. The processing is offloaded to a separate server designed specifically to perform SSL acceleration or SSL termination. |
| --- |

1. What OSI layer does a WAF work on?

| WAF works on the 7th layer of OSI, the application layer |
| --- |

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

| 99005003 Web Shell Upload Attempt (POST) - CHOPPER PHP refers to a PHP web shell injection attack China Chopper. This web shell allows attackers to retain access to an infected system using a client-side application containing all the logic required to control the target |
| --- |

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 could be impacted by this type of attack. Without the front door WAF enabled, there is nothing in my current design that would prevent a PHP injection attack. |
| --- |

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, blocking all traffic from Canada does not necessarily mean that anyone who resides in Canada would not be able to access my website. This is because while a custom WAF rule can be used to block IP addresses originating from Canada, it is not possible to know whether the user accessing the website is located in Canada or not. For example, if someone is traveling to another country but accessing the website from a Canadian IP address, they would be blocked even though they are not located in Canada. Furthermore, a user located in Canada could use a VPN to mask their IP address and access the website from a different country, thus bypassing the custom WAF rule. Therefore, blocking all traffic from Canada does not guarantee that users from Canada will be blocked from accessing 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

|  |
| --- |

## 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 screenshots and completed this document. Yes*

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