| 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://wagnersecurityresume.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 |
| --- |

1. What is your domain name?

| wagnersecurityresume.azurewebsites.net |
| --- |

### Networking Questions

1. What is the IP address of your webpage?

| 20.90.134.16 |
| --- |

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

| UK, England, London |
| --- |

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

| There is nothing in the NS record for my subdomain, but there are four nameservers if one runs a NS record lookup on the parent azurewebsites.net domain. |
| --- |

### 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?

| PHP, a serverside language used primarily for web development, so it is back end. |
| --- |

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

| A CSS stylesheet (describes how a markup language such as HTML is presented on screen), a backup for this CSS file, and images used on the site. |
| --- |

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

| This is front end. HTML and CSS are directly involved with displaying the information to the user after it has been retrieved. |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

| A cloud tenant is the organization/individual and the cloud resources they are leasing. For example, my account with my resource group in this project makes me a single tenant. |
| --- |

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

| You only want administrators or other authorized stakeholders to manage the security credentials (keys, secrets, and certificates) that determine access to your cloud resources. |
| --- |

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

| Keys are the crypto (encryption) keys, secrets are strings (e.g. passwords), and certificates are the TLS certificates |
| --- |

### Cryptography Questions

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

| No cost, easily generated, generally good enough for internal testing/development |
| --- |

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

| Must be distributed to each user (incl. each time its changed), not as secure as a certificate from a CA, cannot be revoked (its good until the listed expiration date, no ‘root authority’ to shut it down before then), difficult to track ownership compared to trusted certificates. |
| --- |

1. What is a wildcard certificate?

| A certificate which can be used with multiple sub-domains of a given domain. E.g. the \*.azurewebsites.net certificate on my webapp provides security to any subdomain of azurewebsites.net. |
| --- |

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 was found to have a vulnerability to a man-in-the-middle attack called POODLE, so Microsoft disabled SSL 3.0 support in Azure 7 years ago. |
| --- |

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. It was issued by a trusted CA. |
| --- |

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

| March 14, 2022 thru March 9, 2023. |
| --- |

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

| Microsoft Azure TLS Issuing CA 01 |
| --- |

* 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 |
| --- |

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

| VeriSign Universal Root Certification Authority |
| --- |

## Day 3 Questions

### Cloud Security Questions

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

| Both reside in front of the application, use a load balancer as a primary solution, and can incorporate firewalls. However, Web Application Gateway a regional load balancer, while Front Door is a global one. |
| --- |

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 decrypting/encrypting SSL-encrypted traffic at a point other than the webserver (e.g. on a dedicated machine or device specifically for crunching encryption). This frees the webserver from the significant compute burden of decryption/encryption. This improves server performance (faster, more stable experience). |
| --- |

1. What OSI layer does a WAF work on?

| OSI layer 7 - Application. It is filtering & monitoring traffic at the application level, aimed at stopping application-level attacks (eg SQL injection). |
| --- |

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

| Bot100100 Malicious bots detected by threat intelligence  This rule blocks malicious bots by matching incoming activity against bot profiles provided by threat intelligence institutions (aka signature-based detection). Malicious bots are, in short, automated software that conducts harmful or fraudulent activities against victims, and can range from denial of service to theft to botnetting. |
| --- |

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. Bots are time/effort efficient method to probe and exploit many sites/machines. Other rules/nuances notwithstanding, an undetected malicious bot being allowed access could overload my traffic, drag down my performance, harvest information, or turn the machines behind my site into a zombie in a botnet. |
| --- |

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. A VPN or proxy could be used to conduct activity via an IP that is not sourced to Canada, and thus evade a block by region. |
| --- |

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.