| 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://forrestsecurity.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?

| [ForrestSecurity] |
| --- |

### Networking Questions

1. What is the IP address of your webpage?

| [20.119.16.56] |
| --- |

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?

| [Server: KVD21.lan  Address: 192.168.12.1  Non-authoritative answer:  Name: waws-prod-blu-565-b607.eastus.cloudapp.azure.com  Address: 20.119.16.56  Aliases: forrestsecurity.azurewebsites.net  waws-prod-blu-565.sip.azurewebsites.windows.net  ] |
| --- |

### 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 8.2, it primarily works on the back end but can be used in front end development] |
| --- |

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

| [Inside of assets there were two directories: css and images. Css contained two files style.css and style.css.bak. The style.css file contained the information regarding how the web page was displayed. This included font sizes, background colors, margins,and other details on how things would be displayed on the webpage. Style.css.bak is a backup of the original style.css file.  The images directory contained specific jpeg files could be used on the website.] |
| --- |

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?

| [A cloud tenant is a user who is using computing resources on cloud space] |
| --- |

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

| [Access policies are important on key vaults because they allow users, applications, or user groups to alter the key vault. Permissions can be set based on the policy that is enacted.] |
| --- |

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

| [Keys are the cryptographic string (public and private) used to encrypt information and then authenticate information. Secrets store private information such as passwords. In secrets the information is encrypted and an identifier is created so it can be recovered at a later time. A certificate includes two items, a certificate (which contains the public key and X.509 certificate metadata) and a private key. Certificates are imported to the Key Vault and then bound to a web application.] |
| --- |

### Cryptography Questions

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

| [An advantage of a self-signed certificate is that you create it which makes it fast and free. They are also typically easier to customize and have no other dependencies upon other certificates.] |
| --- |

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

| [A disadvantage of a self-signed certificate is that browsers and operating systems do not trust them because they are not issued by a trusted third-party. Another disadvantage is that it may not be as secure as third-party certificates. This leads to the self-signed certificate being viewed as untrustworthy.] |
| --- |

1. What is a wildcard certificate?

| [A wildcard certificate is a certificate that has a wildcard (\*) in the domain name. This allows multiple sub-domains to be attached to the same 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.

| [TLS versions 1.0 through 1.2 are upgrades to SSL 3.0. SSL 3.0 has known security issues and was deprecated in 2015.] |
| --- |

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 there is not an error for the certificate. The certificate was issued by a trusted third-party.] |
| --- |

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

| [The validity on the certificate is Tuesday, March 12 2024 through Friday, March 7 2025.] |
| --- |

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

| [No, there is not an intermediate 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] |
| --- |

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

| [Baltimore CyberTrust Root] |
| --- |

## Day 3 Questions

### Cloud Security Questions

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

| [The similarities between Azure Front Door and Web Application Gateway are that they are load balancers that operate in layer 7, and manage application traffic. The setup for each is similar and both have WAF integration. The differences between the two are that Front Door is global and Gateway is regional. ] |
| --- |

1. What is SSL offloading? What are its benefits?

| [SSL offloading is when SSL encryption and decryption tasks are moved from your server to a separate device. The benefit of this is it optimizes the performance of your server by freeing up resources.] |
| --- |

1. What OSI layer does a WAF work on?

| [WAF operates in OSI layer 7.] |
| --- |

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

| [Structured Query Language (SQL) Injection is when code is injected in to modify or retrieve data from SQL databases.] |
| --- |

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?

| [No, there are no databases or locations for SQL to run on the application. ] |
| --- |

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. If they are using their own personal IP address they will not be able to access the website, but if they use a VPN they could change their location to allow access.] |
| --- |

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

**YES**

* ***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.