|  |
| --- |
| 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://thejonathanhite.info |

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)?

|  |
| --- |
| GoDaddy @ $3.99 for the first year |

1. What is your domain name?

|  |
| --- |
| thejonathanhite.info |

### Networking Questions

1. What is the IP address of your webpage?

|  |
| --- |
| 20.119.0.37 |

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

|  |
| --- |
| It shows a Microsoft Datacenter in Tappahannock, VA, USA |

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

|  |
| --- |
| It confirms that the IP address of the Domain thejonathanhite.info is in fact 20.119.0.37 |

### 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 works on the back end to handle the processes of the site. |

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

|  |
| --- |
| This contained the basic files to compose the website, including the index.html file as well as the style templates (ie font, background colors, etc). |

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

|  |
| --- |
| This would again be a part of the back end processes, as these are stored files being retrieved when the site is loaded. |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

|  |
| --- |
| A person or company that’s leasing/subscribing online resources. |

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

|  |
| --- |
| Because only the owner/administrator should have access to the vault. A malicious actor could gain access and swap keys, compromising the security and integrity of the site, leading to redirection attacks or worse. |

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

|  |
| --- |
| The keys themselves are what’s used for encrypting/decrypting and verifying data coming/going to the site. The certificates legitimize the site and are created with the keys. Secrets is a location that can be used to store sensitive data such as passwords or other key information. |

### Cryptography Questions

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

|  |
| --- |
| It’s quick and easy to get |

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

|  |
| --- |
| It’s basically meaningless and won’t be recognized as legitimate by popular browsers |

1. What is a wildcard certificate?

|  |
| --- |
| It covers the domain as well as all the subdomains |

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 is an old protocol where as TLS 1.0, 1.1, and 1.2 are newer and provide a better security layer. |

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?

|  |
| --- |
| Not anymore, the managed certificate shows the proper lock symbol in Chrome. |

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

|  |
| --- |
| Issued 6/6/23, valid through 12/6/23, issued by GeoTrust Global |

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

|  |
| --- |
| No, there was no other certificates showing in the details tab in Chrome |

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

|  |
| --- |
| Yes, the main certificate that the site is currently binded to. |

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

|  |
| --- |
| After checking through the “Manage Device Certificates” and Trusted Root Certificate Authorities menu in Chrome, it does not appear that the certificate was saved. Coincidentally, there was another certificate saved by GeoTrust Global that expired May 2022, but it was not the same one issued for my site. |

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

|  |
| --- |
| Currently there is a 20-year Root Certificate for GlobalSign, due to expire on 3/18/29. |

## Day 3 Questions

### Cloud Security Questions

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

|  |
| --- |
| Both have security features such as firewalls, |

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

|  |
| --- |
| This is a service that removes the burden of processing incoming SSL encryption normally going to a server to a separate device. This speeds up the process and frees up traffic to the server. |

1. What OSI layer does a WAF work on?

|  |
| --- |
| A Web Application Firewall operates at the Application level (duh), as it is done via software instead of a separate device. |

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

|  |
| --- |
| For SQL injection, a WAF managed rule could ensure that all submitted data is inspected to avoid anything suspicious, such as suspicious characters or code. |

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?

|  |
| --- |
| Not currently, as I do not have anything that code could be injected to, such as a guest book or other form with a submit button. |

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?

|  |
| --- |
| Technically yes, assuming they’re incoming from a Canadian IP address. If they were using a VPN or were somehow connecting from a non-Canadian IP address they’ll have no trouble viewing the site. |

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.* ***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.