|  |
| --- |
| 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://www.robkupper.com |

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 |

1. What is your domain name?

|  |
| --- |
| robkupper.com |

### Networking Questions

1. What is the IP address of your webpage?

|  |
| --- |
| 20.119.16.44 |

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

|  |
| --- |
| Country:United States State/Region:Virginia City:Washington |

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

|  |
| --- |
| A **TypeDomain NameTTLAddress**  Arobkupper.com600  20.119.16.44[Check IP Blacklist](https://dnschecker.org/ip-blacklist-checker.php?query=20.119.16.44)  **Owner:** Microsoft Corporation   [WHOIS](https://dnschecker.org/ip-whois-lookup.php?query=20.119.16.44) [AS8075](https://dnschecker.org/asn-whois-lookup.php?query=AS8075) NS **TypeDomain NameTTLCanonical Name**  NSrobkupper.com3600  ns41.domaincontrol.com. (97.74.100.21[Check IP Blacklist](https://dnschecker.org/ip-blacklist-checker.php?query=97.74.100.21))  **Owner:** GoDaddy.com LLC   [WHOIS](https://dnschecker.org/ip-whois-lookup.php?query=97.74.100.21) [AS44273](https://dnschecker.org/asn-whois-lookup.php?query=AS44273)  NSrobkupper.com3600  ns42.domaincontrol.com. (173.201.68.21[Check IP Blacklist](https://dnschecker.org/ip-blacklist-checker.php?query=173.201.68.21))  **Owner:** GoDaddy.com LLC   [WHOIS](https://dnschecker.org/ip-whois-lookup.php?query=173.201.68.21) [AS44273](https://dnschecker.org/asn-whois-lookup.php?query=AS44273) SOA **TypeDomain NameTTLPrimary NSResponsible Email**  SOArobkupper.com3600ns41.domaincontrol.com.dns.jomax.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. A runtime stack is a collection of hardware and software components that work together to deliver a service. In this case, the service is the web app that lets us publish our webpage. It includes both frontend and backend servers but also includes storage, database, Network services, and the like, depending on what is needed for the specific web app. |

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

|  |
| --- |
| The CSS file, which provides the formatting and style for the web page to interpret how the HTML is displayed, colors, fonts, text size… There is also a “images” directory where images used by the template are stored and a .DS\_Store file. I am not 100%, but after some research, the.DS\_file appears to be something related to macOS. I first moved it and tested the functionality of the file then deleted it after it had no effect. |

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

|  |
| --- |
| The front end as it deals with the display of the page. |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

|  |
| --- |
| It is a user that shares access to resources in the cloud. It could be either a single or multi-tenant group and is either in a public or private cloud. |

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

|  |
| --- |
| Key vaults are the keys to the kingdom and as such restricting access to the individual keys based on both strict need and security concerns is prudent. |

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

|  |
| --- |
| Keys are used to encrypt data.  Secrets are used to store sensitive info like passwords, connection strings, bitcoin wallets…  Certificates are securing the website, signing code… |

### Cryptography Questions

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

|  |
| --- |
| It is easy to produce. |

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

|  |
| --- |
| It does not provide much assurance to users of the site. A third-party certificate from a trusted source does. |

1. What is a wildcard certificate?

|  |
| --- |
| A wildcard certificate is a type certificate that supports multiple 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.

|  |
| --- |
| There are significant vulnerabilities to 3.0 certs. |

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. I was able to update it to a Microsoft managed cert which is accepted by most browsers as secure. |

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

|  |
| --- |
| 2024-01-30 to 2024-07-29 |

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

|  |
| --- |
| It is not. I can not issue certificates on behalf of a domain. I have a End-Entity Cert. |

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

|  |
| --- |
| No |

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

|  |
| --- |
| It does. |

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

|  |
| --- |
| Amazon Root CA 4 |

## Day 3 Questions

### Cloud Security Questions

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

|  |
| --- |
| They both manage traffic, Support SSL Termination, and protect against common threats. The Gateway will only protect a single region where it operates, Front Door operates on the edge of Microsoft’s network and can protect all regions. |

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

|  |
| --- |
| They take the decryption work off of the webserver improving its performance. |

1. What OSI layer does a WAF work on?

|  |
| --- |
| It operates on the Application Layer (7). |

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

|  |
| --- |
| SQL injection is an attack that uses unprotected input boxes that are used to retrieve information for a SQL database. In this attack a non-intended input is used to build a query to return other than intended results and access data not intended by the developers. |

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 is no database on my site. It is a static site that provides information through HTML code only. |

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?

|  |
| --- |
| The site could still be accessed by people in Canada through the use of a VPN, IP Forwarding, or by using Tor. |

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.