| 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://fun-times-blog.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)?

| I selected the Azure free domain. |
| --- |

1. What is your domain name?

| My domain name is fun-times-blog.azurewebsites.net. |
| --- |

### Networking Questions

1. What is the IP address of your webpage?

| The IP address of my webpage is 20.119.16.24. |
| --- |

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

| My IP address is in Washington, Virginia, United States of America. |
| --- |

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

| colin@Colin\_ODonoghue MINGW64 ~  $ nslookup fun-times-blog.azurewebsites.net  Server: UnKnown  Address: 192.168.1.1  Non-authoritative answer:  Name: waws-prod-blu-379-f4e5.eastus.cloudapp.azure.com  Address: 20.119.16.24  Aliases: fun-times-blog.azurewebsites.net  waws-prod-blu-379.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?

| My runtime stack was PHP 8.0 and it works on the back end. |
| --- |

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

| Inside this directory, there are 2 directories. One is called ‘css’ and the other is called ‘images’. Inside ‘css’, there are 2 files called ‘style.css’ and style.css.bak’. Inside ‘images’, there are files that contain \*.jpg files, one png file for the LinkedIn-logo, and a ‘readme’ file. |
| --- |

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

| This works with the front end of the website because these are the styles and images used on the website to design the homepage. |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

| A cloud tenant is a term used to describe a user of a cloud’s framework. A tenant could be either an individual or an entire organization. These users are ultimately using the resources provided by a cloud service provider to configure these resources to meet their needs.  Source:  https://www.redswitches.com/blog/tenant-in-cloud-computing/ |
| --- |

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

| An access policy would be important on a key vault because since these vaults contain important data that should not be easily accessible, one would want the vault to remain secured so that no untrusted person can gain access and use this information in a harmful way. |
| --- |

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

| The differences between keys, secrets, and certificates within a key vault include:  -Keys are used to encrypt and decrypt sensitive data and are created using symmetric or asymmetric keys for data in the key vault.  -Secrets are usually data that involves passwords and credentials for a user that should be kept ‘secret’ inside of the key vault.  -Certificates are used in the verification process of extracting data from the vault and link a name to a public key.  Source:  https://michaelhowardsecure.blog/2021/04/29/the-relationship-between-keys-secrets-and-certificates-in-azure-key-vault/ |
| --- |

### Cryptography Questions

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

| A few advantages of a self-signed certificate include:  -These certificates are more user friendly and do not cost anything to use.  -They are easier to change to the user’s preference by providing a larger key size.  -They are better to use for the purpose of developing and testing websites.  Source: https://www.encryptionconsulting.com/education-center/self-signed-certificates#:~:text=Self%2Dsigned%20Certificates%20are%20simple,saves%20time%20for%20testing%20purposes. |
| --- |

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

| A few disadvantages of a self-signed certificate include:  -They are more risky when opening websites because a security warning page will be prompted including a warning of risk for the user.  -Browsers and operating systems may not trust the certificates.  -There is not a way to find out if this certificate has been exposed if there was an attack on the network.  Source:  https://www.encryptionconsulting.com/education-center/self-signed-certificates#:~:text=Self%2Dsigned%20Certificates%20are%20simple,saves%20time%20for%20testing%20purposes. |
| --- |

1. What is a wildcard certificate?

| A wildcard certificate allows the user to secure unlimited subdomains with 1 certificate (all while saving the user money in the process) while also being granted unlimited reissues of the certificate for other servers.  Source:  https://knowledge.digicert.com/generalinformation/INFO900.html |
| --- |

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 is not provided because in 2014, there proved to be a vulnerability within the SSL version and has now been deemed insecure. The vulnerability allowed for an attacker to decrypt a single client and server’s network traffic and have access to a user’s private account. The data within that a user’s account for a website would be compromised and the attacker could see anything from passwords to cookies. This attack was labeled a ‘POODLE’ attack (which stands for Padding Oracle On Downgraded Legacy Encryption) and it allows the attacker to eavesdrop on communications.  Source:  https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/ |
| --- |

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, my browser is not returning an error for my SSL certificate because my website is secured. |
| --- |

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

| The validity of my certificate is issued on Thursday, March 9, 2023 to expire on Sunday, March 3, 2024. |
| --- |

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

| No, I do not have an intermediate certificate. |
| --- |

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

| The root certificate is DigiCert Global Root G2. |
| --- |

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

| Yes, my browser does have the root certificate in its root store. |
| --- |

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

| One other root CA in my browser’s root store is ‘DST Root CA X3’. |
| --- |

## Day 3 Questions

### Cloud Security Questions

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

| One similarity between Azure Web Application Gateway and Azure Front Door is that they are both load balancers for Layer 7 of the OSI model, which is the Application Layer and works with HTTP and HTTPS. One difference is that these load balancers differ in a certain category of services, as Azure Font Door is non-regional and Azure Web Application Gateway is regional when it comes to services. In other words, Front Door allows us to load balance throughout many regions, while the Application Gateway can only load balance within VMs and containers.  Source:  https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq |
| --- |

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 a way of making it easier for a web server to perform at a high level by passing off the encryption and decryption stage to a machine that will perform the cryptographic task for it. By sending the encrypted data to a device/load balancer, it allows the process of decryption to be completed before it reaches the server. This process is beneficial because now the server is free to perform or handle other tasks without having to waste time decrypting encrypted data. This also enhances the overall performance of a server; since the server is not reliant on performing the encryption stage, it can lead to faster load times for websites.  Source:  https://avinetworks.com/glossary/ssl-offload/ |
| --- |

1. What OSI layer does a WAF work on?

| The OSI Layer that WAF works on is Layer 7, the Application Layer, that handles the communication of networks and applications. |
| --- |

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

| SQL injection is defined as a security vulnerability that allows a user to gain access to unauthorized data by entering a query and using malicious code to tamper with a database. A successful injection begins with bypassing the authentication stage of a web application. Once a threat actor has administrative control of the system, they can change code inside of the database to modify/damage the integrity of data or even delete the data altogether. Threat actors can also implement commands that can lead to sending data to various unauthorized locations for their benefit.  Source:  https://owasp.org/www-community/attacks/SQL\_Injection |
| --- |

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?

| This vulnerability could not impact my website if Front Door wasn’t enabled because a SQL injection requires a user to input a value to return information inside of a query-type format. Since my webpage does not have a text box for a user to input a value, nor does it have any real valuable information in a query that could be private or sensitive for safe keeping, the SQL injection is not a risk for this particular blog site.  Source:  https://www.contrastsecurity.com/glossary/sql-injection |
| --- |

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?

| If I created a custom WAF rule to block all traffic from Canada, it would not allow residents of Canada access to my website. When the rule is applied, it will compare the source IP address coming in to the ones who are allowed access and those who are not within my system. In this case, when this rule is created, it would make sure that IP addresses coming from Canada were not allowed access to my 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 screen shots and completed this document.*
* **YES**

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