| 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://andrewbarrycybersecurity.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?

| andrewbarrycybersecurity.azurewebsites.net |
| --- |

### Networking Questions

1. What is the IP address of your webpage?

| 20.211.64.21 |
| --- |

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

| City - The Rocks  State - New South Wales  Country - Australia |
| --- |

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

| sysadmin@vm-image-ubuntu-dev-1:~$ nslookup andrewbarrycybersecurity.azurewebsites.net  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  andrewbarrycybersecurity.azurewebsites.net canonical name = waws-prod-sy3-107.sip.azurewebsites.windows.net.  waws-prod-sy3-107.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-107-a4a2.australiaeast.cloudapp.azure.com.  Name: waws-prod-sy3-107-a4a2.australiaeast.cloudapp.azure.com  Address: 20.211.64.21 |
| --- |

### 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 works on the back end. |
| --- |

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

| **CSS Files** - Cascading Style Sheets contain information regarding the rules and styles that control the HTML aspects of the app such as margins, colours, fonts, spacing, line breaks, positioning etc.  **Image Files** - used on the web app such as the LinkedIn logo and the profile photo of the web app owner. |
| --- |

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

| CSS and image files work on the front end. |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

| A cloud tenant is an individual or an organisation that rents and consumes cloud computing services from a cloud service provider. |
| --- |

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

| An effective access policy is crucial to maintain the confidentiality, integrity and availability of sensitive data and cryptographic keys stored in the vault.   * **Controlled access** - an access policy will allow you to control who can access the resources stored within the vault. The keys stored within the vault are a form of extremely sensitive information and it is important to ensure that no one unauthorised has access to them. * **Least privilege** - an access policy will allow you to ensure that this important principle is met. By clearly outlining specific access permissions within the policy you can ensure that people are not granted access unnecessarily. This will reduce the potential attack surfaces that TAs can target. * **Insider threat** - an access policy will reduce the threat posed by an employee. Without an effective access policy, an employee may access the vault by mistake or with malicious intent. * **Compliance requirements** - many industries that are regulated require stringent security and an access policy can help to show an orgnaisation is taking the correct steps. Even in industries that are not regulated an access policy shows employees, investors and clients that the organisation takes security seriously. * **Auditing & monitoring** - an access policy can also include logging and monitoring procedures that track access to the vault and allow for regular security audits. |
| --- |

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

| **Keys** refers to the cryptographic keys which are used for encryption, decryption, signing and for verifying data.  **Secrets** refers to sensitive data that applications need in order to operate and so should not be exposed in plain text. Azure Key Vault allows secrets to be securely stored and managed, this includes access control and audit trails. Passwords and API keys are two examples of secret that may be stored in a Azure key Vault.  **Certificates** refers to the digital documents that allow us to have confidence in the identity of entities such as servers, clients or individuals and to enable secure communication (such as HTTPS) to be established over a network. Azure Key Vault can help with the secure storage and access of these certificates. |
| --- |

### Cryptography Questions

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

| **Cost-effectiveness** - as the certificate is self-signed it is free to create. Purchasing a certificate from a Certificate Authority (CA) costs money and so a self-signed cert eliminates this expense.  **Speed & simplicity** - self-signed certificates are very simple to create and so can be generated very quickly. An individual or business can generate a cert without the involvement of anyone else and does not need a CA. This makes the whole process fast and simple.  **Security** - while self-signed certs lack the validation of an established CA they still offer encryption capabilities and help to ensure that data transmitted over HTTPS is secured.  **Flexibility** - since the certs are typically generated and signed by the entity they apply to they are extremely flexible in terms of issuance and management. |
| --- |

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

| **Lack of trust** - as self-signed certs are not issued by an established and trusted CA, browsers will not trust them. This will lead to security warnings prior to accessing a site that has a self-signed cert. Many users will choose not to visit a site with a self-signed cert and so this can be a distinct disadvantage, particularly for businesses trying to attract clients.  **Limitations of use** - self-signed certs are not appropriate for public-facing websites due to the reasons outlined above. As a result, they have limited practical use. They may be used for internal use or in testing environments.  **Maintenance challenges** - the managing of self-signed certs can pose challenges, particularly across multiple environments or systems. As each cert is unique to the entity it was generated for, businesses may struggle to maintain consistency and to manage the updating of certs properly.  **Security** - lacking the experience and oversight of a trusted CA means that there is greater potential for security vulnerabilities within self-signed certs. |
| --- |

1. What is a wildcard certificate?

| A wildcard cert is an SSL/TLS cert that allows for the securing of a domain and all its subdomains with just a single cert. Wildcard certs are especially useful for organsiations or businesses that have multiple and/or dynamic subdomains. A wildcard can simplify cert management and cut down the number of certs required. They can be more expensive than standard certs and CAs may impose certain limitations on their usage. |
| --- |

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 has been largely deprecated in favor of its successor TLS. While SSL is still in use it has declined significantly due to major and well-publicised security vulnerabilities and weaknesses. TLS addresses the shortcomings of SSL and so it is strongly recommended that people migrate away from using SSL. By not offering SSL Azure is clearly encouraging clients to adopt TLS. |
| --- |

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?

| My browser is not returning an error as my SSL certificate has been created by a trusted Certificate Authority. |
| --- |

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

| Issued On  Wednesday, 13 March 2024 at 01:36:42  Expires On  Saturday, 8 March 2025 at 01:36:42 |
| --- |

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

| My intermediate certificate is Microsoft Azure RSA TLS Issuing CA 07  An intermediate certificate sits between a website's certificate and its root certificate and is used to further enhance security by creating a chain of trust. Rather than directly signing end-entity certificates with the root certificate, CAs use intermediate certificates to sign end-entity certs. |
| --- |

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

| My root certificate is DigiCert Global Root G2.  A root certificate is a self-signed cert issued by a CA which is used to sign other certificates such as intermediate certs. Browsers have preinstalled lists of root certs from established CAs. If the browser encounters a root cert which is contained on this list it will trust the cert and allow a connection to be established with that website. |
| --- |

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

| Yes, my browser has the DigiCert Global Root G2 certificate. |
| --- |

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

| Entrust 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?

| **Similarities**   * Both reside in front of the web application to protect it * Both work on the Application Layer of the OSI model * Both use a load balancer as their primary solution * They can protect against web vulnerability attacks by incorporating a web application firewall * They have additional features such as URL path-based routing and SSL/TLS termination   **Differences**   * Web Application Gateway is more of a regionally focussed tool, it is best suited to protect a web app in a single region in your cloud environment. * Azure Front Door is more of a globally focused tool, it is better suited when you have a variety of regions in your cloud environment. |
| --- |

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 process where the task of encryption and decryption of an SSL/TLS connection is handled prior to the data reaching the destination server. The task is ‘offloaded’ from the destination server and handled by another dedicated service or device such as Web Application Gateway or Front Door.  **Benefits**   * **Reduction in server load** - offloading of SSL/TLS encryption/decryption can can significantly reduce the workload a destination server has to deal with.This improves server performance and scalability as the server can focus solely on processing application logic. * **Improved performance** - devices that handle SSL/TLS offloading are often optimised to perform this task and may execute the process faster than the server. These faster responses lead to an overall improvement in how the application as a whole performs. * **Simplified certificate management** - certificates are usually installed and managed on the offloading device/service rather than on individual servers. This simplifies the process of cert management such as renewal and deployment and can also help reduce the risk of misconfigurations and errors related to certs. * **Flexibility** - SSL/TLS offloading allows for uniform application of security policies regardless of where an application is hosted (on prem, cloud, hybrid). Offloading can also take place at the edge of an organisation’s network. This enhances security by detecting and mitigating threats before the traffic reaches the internal network. |
| --- |

1. What OSI layer does a WAF work on?

| Application Layer (7) |
| --- |

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

| SQL Injection Attack - is an attack where a Threat Actor (TA) identifies and exploits vulnerabilities in a web application. The TA uses input fields or parameters in a way that the app designer did not intend by injecting malicious SQL queries and interacting with the web app’s database.  The TA will:   * Identify an input field or parameter where user-supplied data is incorporated into SQL queries without being properly sanitised or validated. * Craft a malicious SQL command or payload that will be entered in the vulnerable input field. * Concatenate the malicious SQL command with a legitimate SQL query and enter this in the vulnerable input field, forming a query the web application designer/owner did not intend. * The altered query is executed and the database server behaves in a way the app designer had not intended.   This can result in unauthorised access to data, avoidance of authentication rules, deletion or modification of data and records and in a worst-case scenario the total compromise and loss of the underlying server. SQL attacks can bring about significant reputational and financial losses. |
| --- |

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, without Front Door enabled my website could be vulnerable to this type of attack.  If Front Door wasn’t enabled my website would be directly exposed to the internet and would not have the benefit of the security features (including all the WAF rules) it provides. Front Door adds an additional layer of protection by acting as a reverse proxy, inspecting traffic and applying security policies. Without Front Door all incoming requests would be routed directly to the server and so attackers could send malicious SQL queries directly to the server. If the website’s code is vulnerable to SQL injection a TA could then exploit this vulnerability. |
| --- |

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?

| Theoretically, if you create a custom WAF to block all traffic from Canada then anyone attempting to access your website from a Canadian IP should be blocked.  However, there are some issues which must be considered.  **VPN and proxy servers** - users with a Canadian IP can bypass the WAF by using either a VPN or a proxy server which will mask the true location of their IP.  **IP geolocation accuracy** - the databases used to determine the geographic location of IP addresses are not always completely accurate. This could lead to some people in Canada being able to view the website and may also lead to some people outside of Canada being blocked from accessing the 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.