|  |
| --- |
| 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.

Josh Schauert - Project 1

**Your Web Application**

Enter the URL for the web application that you created:

<http://sf4cybersec.xyz/>

**Day 1 Questions**

**General Questions**

* What option did you select for your domain (Azure free domain, GoDaddy low-cost domain, Azure premium domain)?

|  |
| --- |
| Go Daddy |

* What is your domain name?

|  |
| --- |
| SF4CyberSec.xyz |

**Networking Questions**

* What is the IP address of your webpage?

|  |
| --- |
| 20.211.64.7 |

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

|  |
| --- |
| Sydney, New South Wales, Australia |

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

|  |
| --- |
| $ nslookup sf4cybersec.xyz  Server: dsldevice6.attlocal.net  Address: 2600:1700:52c0:b160::1  Non-authoritative answer:  Name: sf4cybersec.xyz  Address: 20.211.64.7 |

**Web Development Questions**

* 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 7.4 , Backend |

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

|  |
| --- |
| The CSS assets, CSS is used to define styles for your web pages, including the design, layout and variations in display for different devices and screen sizes  There is also an Images directory storing images used by the website |

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

|  |
| --- |
| Front End |

**Day 2 Questions**

**Cloud Questions**

* What is a cloud tenant?

|  |
| --- |
| Its a computer architecture that allows customers to share computing resources in the cloud. ( Public or Private ) |

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

|  |
| --- |
| Because it allows / restricts access( Permissions ) separately to keys , secrets or certificates |

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

|  |
| --- |
| Keys support multiple key types and algorithms , Secrets provide secure storage for passwords and database connection strings, Certificates are built on top of keys and secrets with an added auto renew feature. |

**Cryptography Questions**

* What are the advantages of a self-signed certificate?

|  |
| --- |
| They are free is the biggest advantage. They are suitable for internal network websites and testing and development environments |

* What are the disadvantages of a self-signed certificate?

|  |
| --- |
| They are risky because they have no validation from any third party authority. ( Usually a Trusted SSL Certificate Company ) |

* What is a wildcard certificate?

|  |
| --- |
| It is a single certificate with a wildcard character in the domain name field. This allows the certificate to secure multiple sub domain names pertaining to the same base domain. |

* 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.

|  |
| --- |
| It is not provided to ensure the safety of users. Microsoft completely disabled ssl 3.0 in Azure websites by default to protect customers from the POODLE vulnerability |

* After completing the Day 2 activities, view your SSL certificate and answer the following questions:
* Is your browser returning an error for your SSL certificate? Why or why not?

|  |
| --- |
| No, Because we secured it with a app service managed certificate |

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

|  |
| --- |
| Not Before Thu, 30 Jun 2022 00:00:00 GMT  Not After Fri, 30 Dec 2022 23:59:59 GMT  So from June 30th 2022 to December 30th 2022 |

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

|  |
| --- |
| Yes, Its issued by DigiCert, Inc.  Certificate Authorities issue an “intermediate root” with a private key which makes it trusted. |

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

|  |
| --- |
| Yes I do.  A root certificate is issued by a Trusted certificate authority. A trusted certificate authority is an entity thats entitled to verify someone is who they say they are. |

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

|  |
| --- |
| Yes it does ( digicert, INC. ) |

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

|  |
| --- |
| 1.Comodo RSA Code Signing CA  2. Go Daddy Secure Certificate Authority - G2  3. Microsoft Azure TLS Issuing CA 01 |

**Day 3 Questions**

**Cloud Security Questions**

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

|  |
| --- |
| Similarities: Both are load balancers on OSI Layer 7  Both Reside in front of the web application  Differences: Front Door is global, Application gateway is regional. Front Door can load balance between your different scale units/clusters/stamp units across regions, Application Gateway allows you to load balance between your VMs/containers etc. that is within the scale unit. |

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

|  |
| --- |
| SSL offloading is the process of removing the SSL-based encryption from incoming traffic to relieve a web server of the processing burden of decrypting and/or encrypting traffic sent via SSL. The processing is offloaded to a separate device designed specifically for SSL acceleration or SSL termination. Benefits of SSL offloading are as follows:   * Boost the page load speed time * Faster response from the Web server * Better web server performance * Enhance the stability of website * Auto-scaling the web servers during the peak hours of traffic * Use as a load balancer for serving web traffic using different servers. |

* What OSI layer does a WAF work on?

|  |
| --- |
| Layer 7 , Application Layer |

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

|  |
| --- |
| Path Traversal Attack = The Path Traversal attack technique allows an attacker to access files, directories, and commands that potentially reside outside the root directory |

* 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 it could, based on what I found, The only way to effectively defend against directory traversal attacks is to carefully write the code of the website or web application and use user input sanitization libraries. |

* 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?

|  |
| --- |
| Yes it does with the exception of if the user attempting to access your site from Canada is using a VPN to gain access |

* Include screenshots below to demonstrate that your web app has the following:
* Azure Front Door enabled

|  |
| --- |
|  |

* 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 the project has been graded.*

YES

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