| 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:

| chrissecurityresume.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)?

| Free Domain |
| --- |

1. What is your domain name?

| chrissecurityresume.azurewebsites.net |
| --- |

### Networking Questions

1. What is the IP address of your webpage?

| 20.115.232.12 |
| --- |

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

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

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

| $ nslookup chrissecurityresume.azurewebsites.net  Server: 2607:f428:ffff:ffff::1  Address: 2607:f428:ffff:ffff::1#53  Non-authoritative answer:  chrissecurityresume.azurewebsites.net canonical name = waws-prod-mwh-117.sip.azurewebsites.windows.net.  waws-prod-mwh-117.sip.azurewebsites.windows.net canonical name = waws-prod-mwh-117-fe6a.westus2.cloudapp.azure.com.  Name: waws-prod-mwh-117-fe6a.westus2.cloudapp.azure.com  Address: 20.115.232.12 |
| --- |

### 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 7.4, backend |
| --- |

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

| Inside that directory, it contained the assets for the wen app, such as images and a .css file that specifies the layout |
| --- |

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

| Front end |
| --- |

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

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

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

| implementing access policies on a key vault is vital for protecting sensitive data, ensuring compliance, and managing permissions effectively within an organization. |
| --- |

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

| * **Keys** are used for cryptographic operations. * **Secrets** store sensitive information securely. * **Certificates** bind identities to public keys and facilitate secure communications. |
| --- |

### Cryptography Questions

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

| Advantages  1. **Cost-Effective**: Self-signed certificates can be created without purchasing a certificate from a Certificate Authority (CA), making them a free option for securing communications. 2. **Easy to Create**: They are straightforward to generate using tools like OpenSSL, making them accessible for developers and system administrators. 3. **Control**: Organizations have full control over the certificate creation process, including the key length, expiration dates, and associated metadata. 4. **Testing and Development**: Self-signed certificates are useful in testing and development environments where the overhead of obtaining a CA-signed certificate is unnecessary. 5. **Internal Use**: For internal applications or services where external trust is not required, self-signed certificates can be adequate and efficient. |
| --- |

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

| 1. **Trust Issues**: Browsers and applications typically do not trust self-signed certificates by default, leading to warning messages that can confuse users and impact the user experience. 2. **Lack of Verification**: Self-signed certificates do not provide any verification of the identity of the organization or individual behind them, making them less secure for public-facing services. 3. **Management Overhead**: In larger organizations, managing self-signed certificates can become cumbersome, especially if they need to be distributed and trusted across multiple devices or users. 4. **Risk of Man-in-the-Middle Attacks**: Without a trusted CA, self-signed certificates are more susceptible to impersonation, as attackers could potentially create their own self-signed certificates. 5. **Limited Use Cases**: They are generally unsuitable for public-facing services, as users and browsers may reject them due to lack of trust, hindering access to the service. |
| --- |

1. What is a wildcard certificate?

| wildcard certificate is a type of SSL/TLS certificate that allows you to secure multiple subdomains of a single domain with a single certificate. It uses a wildcard character (usually an asterisk, \*) in the domain name to specify that it can cover all 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 3.0 is not provided in Azure or other modern web environments primarily due to significant security vulnerabilities that have been discovered over the years. 1. Security Vulnerabilities  * **POODLE Attack**: SSL 3.0 is vulnerable to the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack, which allows attackers to decrypt parts of the data being transmitted over SSL connections. This exploit takes advantage of the way SSL 3.0 handles padding.  2. Obsolete Protocol  * SSL 3.0 is considered an outdated protocol. The Internet Engineering Task Force (IETF) officially deprecated SSL 3.0 in 2015, recommending that organizations transition to more secure protocols.  3. Increased Security Standards  * Modern security standards prioritize encryption protocols that provide stronger security mechanisms, such as TLS (Transport Layer Security). TLS versions 1.1 and 1.2 include improvements in cryptographic algorithms and mechanisms that significantly enhance security compared to 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, because we secured it with an app service managed cert |
| --- |

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

| Issued On  Sunday, August 4, 2024 at 5:16:32 AM  Expires On  Wednesday, July 30, 2025 at 5:16:32 AM |
| --- |

* 1. 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. |
| --- |

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

| Yes, a root certificate is issued by a trusted certificate authority. |
| --- |

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

| Yes, Digicert |
| --- |

* 1. 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

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

| Choosing between Azure Web Application Gateway and Azure Front Door depends on your specific application needs—whether you require regional management and application security (Web Application Gateway) or global performance optimization and scalability (Azure Front Door) |
| --- |

1. What is SSL offloading? What are its benefits?

| SSL offloading can significantly enhance the performance, manageability, and security of web applications, making it a valuable practice for organizations that handle SSL traffic. |
| --- |

1. What OSI layer does a WAF work on?

| A Web Application Firewall (WAF) primarily operates at the **application layer**, which is Layer 7 of the OSI model. |
| --- |

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

| SQL injection is a type of vulnerability where attackers can manipulate an app’s SQL queries by injecting malicious scripts into fields that interact with an app’s database so the attacker can read or modify the data. |
| --- |

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, if the WAF wasn’t enabled, an attacker could directly exploit the vulnerability by injecting malicious SQL commands |
| --- |

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?

| Yes, it would virtually block all traffic but if someone were to use a VPN they would be able to access the website. |
| --- |

1. Include screenshots below to demonstrate that your web app has the following:
   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.