Cybersecurity

Project 1 Technical Brief

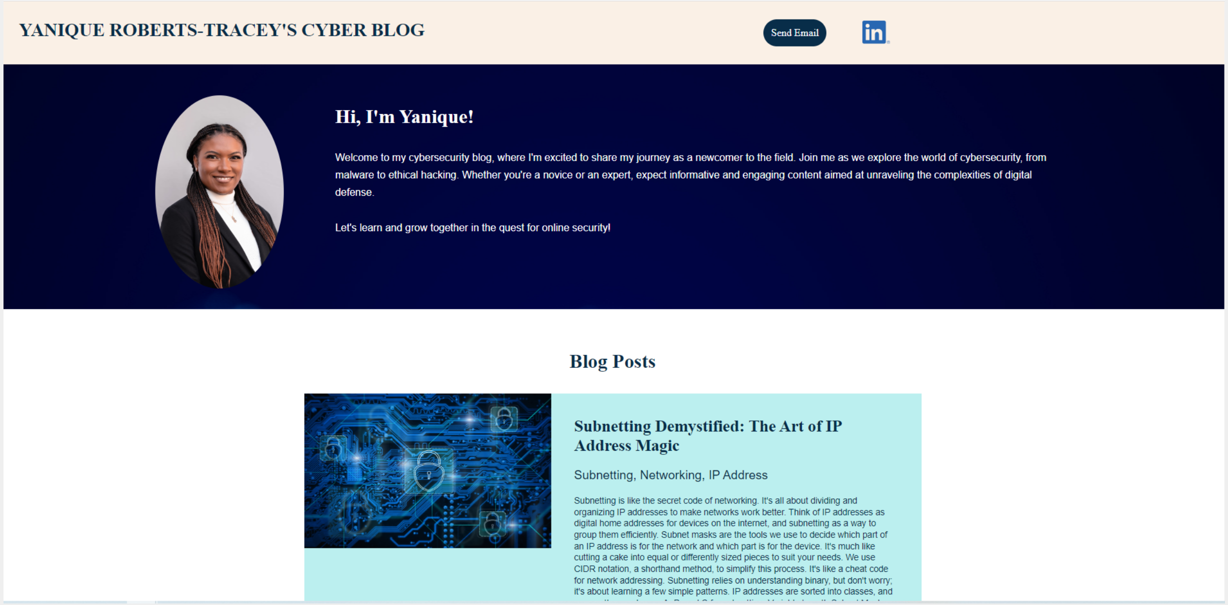
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://traceysecurityblog.azurewebsites.net/
```

Paste screenshots of your website created (Be sure to include your blog posts):



YANIQUE ROBERTS-TRACEY'S CYBER BLOG

Hi, I'm Yanique!

Welcome to my cybersecurity blog, where I'm excited to share my journey as a newcomer to the field. Join me as we explore the world of cybersecurity, from malware to ethical hacking. Whether you're a novice or an expert, expect informative and engaging content aimed at unraveling the complexities of digital defense.

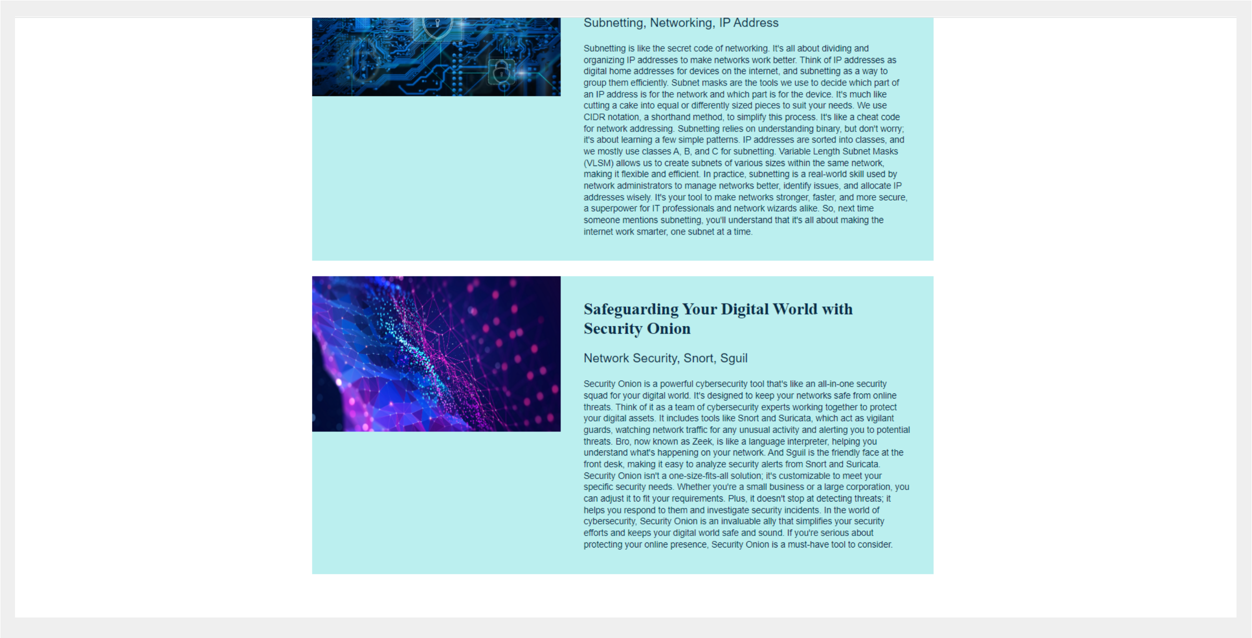
Let's learn and grow together in the quest for online security!

Blog Posts

Subnetting Demystified: The Art of IP Address Magic

Subnetting, Networking, IP Address

Subnetting is like the secret code of networking. It's all about dividing and organizing IP addresses to make networks work better. Think of IP addresses as digital home addresses for devices on the internet, and subnetting as a way to group them efficiently. Subnet masks are the tools we use to decide which part of an IP address is for the network and which part is for the device. It's much like cutting a cake into equal or differently sized pieces to suit your needs. We use CIDR notation, a shorthand method, to simplify this process. It's like a cheat code for network addressing. Subnetting relies on understanding binary, but don't worry; it's about learning a few simple patterns. IP addresses are sorted into classes, and



Subnetting, Networking, IP Address

Subnetting is like the secret code of networking. It's all about dividing and organizing IP addresses to make networks work better. Think of IP addresses as digital home addresses for devices on the internet, and subnetting as a way to group them efficiently. Subnet masks are the tools we use to decide which part of an IP address is for the network and which part is for the device. It's much like cutting a cake into equal or differently sized pieces to suit your needs. We use CIDR notation, a shorthand method, to simplify this process. It's like a cheat code for network addressing. Subnetting relies on understanding binary, but don't worry; it's about learning a few simple patterns. IP addresses are sorted into classes, and we mostly use classes A, B, and C for subnetting. Variable Length Subnet Masks (VLSM) allows us to create subnets of various sizes within the same network, making it flexible and efficient. In practice, subnetting is a real-world skill used by network administrators to manage networks better, identify issues, and allocate IP addresses wisely. It's your tool to make networks stronger, faster, and more secure, a superpower for IT professionals and network wizards alike. So, next time someone mentions subnetting, you'll understand that it's all about making the internet work smarter, one subnet at a time.

Safeguarding Your Digital World with Security Onion

Network Security, Snort, Sguil

Security Onion is a powerful cybersecurity tool that's like an all-in-one security squad for your digital world. It's designed to keep your networks safe from online threats. Think of it as a team of cybersecurity experts working together to protect your digital assets. It includes tools like Snort and Suricata, which act as vigilant guards, watching network traffic for any unusual activity and alerting you to potential threats. Bro, now known as Zeek, is like a language interpreter, helping you understand what's happening on your network. And Sguil is the friendly face at the front desk, making it easy to analyze security alerts from Snort and Suricata. Security Onion isn't a one-size-fits-all solution; it's customizable to meet your specific security needs. Whether you're a small business or a large corporation, you can adjust it to fit your requirements. Plus, it doesn't stop at detecting threats; it helps you respond to them and investigate security incidents. In the world of cybersecurity, Security Onion is an invaluable ally that simplifies your security efforts and keeps your digital world safe and sound. If you're serious about protecting your online presence, Security Onion is a must-have tool to consider.

Day 1 Questions

General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

```
Azure free domain
```

2. What is your domain name?

```
traceysecurityblog.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.21
```

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

```
Australia East
```

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

```
Server:  mynetwork.home
Address:  192.168.2.1

Non-authoritative answer:
Name:    waws-prod-sy3-107-a4a2.australiaeast.cloudapp.azure.com
Address:  20.211.64.21
Aliases:  traceysecurityblog.azurewebsites.net
          waws-prod-sy3-107.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?

```
Back-end
```

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

```
Inside the “/var/www/html” directory, there is a subdirectory named
“assets.” This directory contains two additional subdirectories, “css” and
“images.” The “css” directory holds Cascading Style Sheets (CSS) files,
which are used to define the presentation and styling of web content. The
“images” directory is used to store image files that are used on the
website, such as pictures, icons, or other graphical elements. These
directories, “css” and “images,” are important to building and designing web
pages.
```

3. 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?

A cloud tenant refers to an individual or organization that uses cloud computing resources, such as virtual servers, storage, or applications, from a cloud service provider. These resources are typically accessed and managed through the cloud provider's infrastructure, allowing tenants to leverage the benefits of cloud technology without owning or maintaining physical hardware. In cloud computing, a single-tenant setup gives one customer dedicated computing resources for exclusive use. On the other hand, a multi-tenant architecture allows multiple customers to share common computing resources while maintaining high security and isolation (Nidhi, 2023).

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

A Key Vault access policy defines which users, applications, or groups can perform various operations on the cryptographic assets stored within the vault, playing a vital role in managing access, ensuring data security, and meeting regulatory requirements (Assign a key Vault access policy (legacy), 2023).

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

-Keys: support various key types and algorithms and can be either software-protected or HSM-protected. They are essential for tasks like encryption, decryption, signing, and verifying digital signatures.

-Secrets: are used to securely store sensitive information, including passwords, API keys, and connection strings, offering enhanced security and access control.

-Certificates: are built on keys and secrets and feature automated renewal. They are primarily used for securing communication and authentication, often for SSL/TLS encryption on websites and applications (Azure Key Vault keys, secrets and certificates overview, 2023).

Cryptography Questions

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

According to Bisson (2023), the following are advantages of a self-signed certificate:

Cost-Effective: They are budget-friendly because there are no expenses involved in obtaining them from a certificate authority (CA).

Ease of Use: Self-signed certificates can be quickly generated and implemented, which makes them well-suited for short-term or localized settings.

Unlimited Availability: Developers and application owners have the freedom to create as many certificates as required without being constrained by external factors or teams.

Internal Applications: Self-signed certificates are particularly valuable for internal systems, private networks, and testing environments where the focus is on encryption rather than the need for external trust validation.

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

According to Bisson (2023), the following are disadvantages of a self-signed certificate:

Trust Validation Absence: Self-signed certificates lack trust validation because they aren't issued by established certificate authorities (CAs). Consequently, web browsers and client applications often trigger warnings, urging caution for users.

Security Risk: Compromised self-signed certificates can be problematic, as attackers can use them to impersonate the certificate owner, potentially leading to security breaches and fraud.

Manual Trust Setup: Users need to manually establish trust in self-signed certificates by adding them to their trust stores. This process demands technical expertise and can be inconvenient, particularly for non-technical users.

3. What is a wildcard certificate?

A wildcard certificate is a single SSL/TLS certificate that uses a wildcard character (*) in the domain name, allowing it to secure multiple subdomains under the same base domain. For instance, a wildcard certificate for *.(domainname).com can be used to secure subdomains like www.(domainname).com, mail.(domainname).com, and store.(domainname).com, along with any other subdomains under (domainname).com, making it a versatile and efficient option for securing various subdomains (What is a Wildcard Certificate?, 2022-2023).

4. 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.

The SSL 3.0 protocol is not provided due to its vulnerability to a man-in-the-middle attack known as “POODLE” (Padding Oracle on Downgraded Legacy Encryption). Although this type of attack requires forcing the use of SSL 3.0, it can lead to information disclosure. Microsoft has taken active measures to remove SSL 3.0 support from its products, including Internet Explorer, Windows Server, Azure services, and Office 365, to enhance security. In general, the industry has deprecated SSL 3.0 in favor of more secure TLS versions like 1.0, 1.1, and 1.2, prioritizing the protection of data exchanged between clients and web servers (Mackie, 2015).

5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

    a. Is your browser returning an error for your SSL certificate? Why or why not?

No. The browser did not return an error for the SSL certificate. It was issued by a trusted/recognized organization, Microsoft and is therefore part of a trusted chain of certificates.

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

August 1, 2023 at 5:55:22 AM to June 27, 2024 at 7:59:59 PM

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

The SSL certificate, “Microsoft Azure TLS Issuing CA 01,” is an intermediate certificate issued by Microsoft Azure. This intermediate certificate is used to sign and issue SSL/TLS certificates for Azure services and domains, including those with the “*.azurewebsites.net” domain.

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

DigiCert Global Root G2

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

Yes

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

AAA Certificate Services
Sectigo (AAA) - COMODO RSA Certification Authority

Day 3 Questions

Cloud Security Questions

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

According to the article, Comparing Azure Front Door vs Application Gateway: What’s the Difference? (2023), the following are similarities and differences between Azure Web Application Gateway and Azure Front Door:

Similarities:
- Both offer global load balancing for improved availability and responsiveness.
- They support SSL termination, reducing the load on backend servers by handling SSL/TLS encryption.
- Both can be equipped with a Web Application Firewall (WAF) to protect against web vulnerabilities.
- They provide advanced traffic routing and management capabilities for

```
directing traffic to different backend resources.

Differences:
- Azure Web Application Gateway is designed for application-level load
balancing and web traffic management, making it suitable for web
applications, while Azure Front Door serves as a content delivery network
(CDN) for content, APIs, and microservices.
- Azure Front Door has a wider global reach with more points of presence
(PoPs) for global content delivery.
- Azure Front Door uses anycast-based routing for lower latency, while Azure
Web Application Gateway uses unicast-based routing.
- Azure Front Door offers additional security features, including Front Door
Managed Rules and Threat Intelligence.
- Azure Web Application Gateway integrates well with Azure Kubernetes
Service (AKS), while Azure Front Door is broader in its support for content
delivery and API management.
```

2. 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 offloading SSL/TLS encryption and
decryption tasks from web servers to dedicated devices or services,
providing several benefits. These benefits include reduced server load,
improved performance, simplified certificate management, enhanced security
with measures like Web Application Firewalls, scalability for handling
increased traffic, and flexibility to adapt to changing security and
performance needs. In Azure services like Azure Web Application Gateway and
Azure Front Door, SSL offloading is a valuable feature that enhances web
application performance, simplifies certificate management, and adds a layer
of security for secure and high-performance content delivery to end users
(SSL Offloading, 2023).
```

3. What OSI layer does a WAF work on?

```
Application Layer (Layer 7)
```

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

```
A SQL injection attack involves inserting malicious SQL code into an
```

application's input fields, potentially compromising the database's security and allowing unauthorized access, data extraction, manipulation, and more. These attacks target web applications that rely on databases, making e-commerce sites and login pages common victims. Web Application Firewalls (WAFs) employ SQL injection managed rules to identify and block these attacks by analyzing requests and responses for suspicious patterns. Detecting SQL injection attempts, WAFs can take actions like request blocking or notifying administrators, safeguarding against this prevalent and hazardous web application vulnerability (Kingthorin, 2023).

5. 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, the website could be impacted by SQL injection even if Azure Front Door wasn't enabled. Azure Front Door is primarily a content delivery and load balancing service and may not provide specific protection against SQL injection attacks.

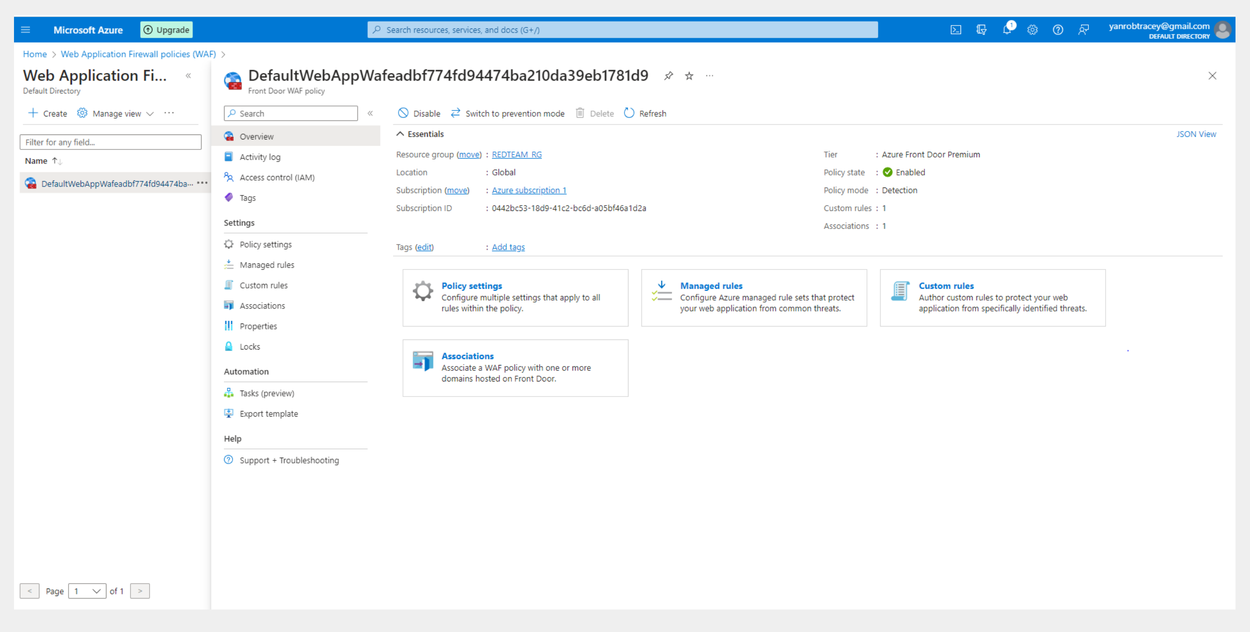
Azure Front Door is not a specific protection against SQL injection. The vulnerability arises at the application level due to inadequate input validation and sanitation. Whether you use Azure Front Door or not, safeguarding your website from SQL injection is primarily dependent on implementing proper security practices within your application. These practices include input validation, parameterized queries, and utilizing built-in security controls and firewalls.

6. 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, if you create a custom Web Application Firewall (WAF) rule to block all traffic from Canada, anyone residing in Canada would not be able to access the website. This is because the WAF rule would prevent their requests from reaching your website's server, effectively blocking their access. This blocking is based on geolocation data in the IP address, which the WAF uses to identify the traffic's origin.

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

   a. Azure Front Door enabled



DefaultWebAppWafeadbf774fd94474ba210da39eb1781d9

Front Door WAF policy

Resource group (move)	: REDTEAM_RG
Location	: Global
Subscription (move)	: Azure subscription 1
Subscription ID	: 0442bc53-18d9-41c2-bc6d-a05bf46a1d2a
Tags (edit)	: Add tags

Tier	: Azure Front Door Premium
Policy state	: ✓ Enabled
Policy mode	: Detection
Custom rules	: 1
Associations	: 1

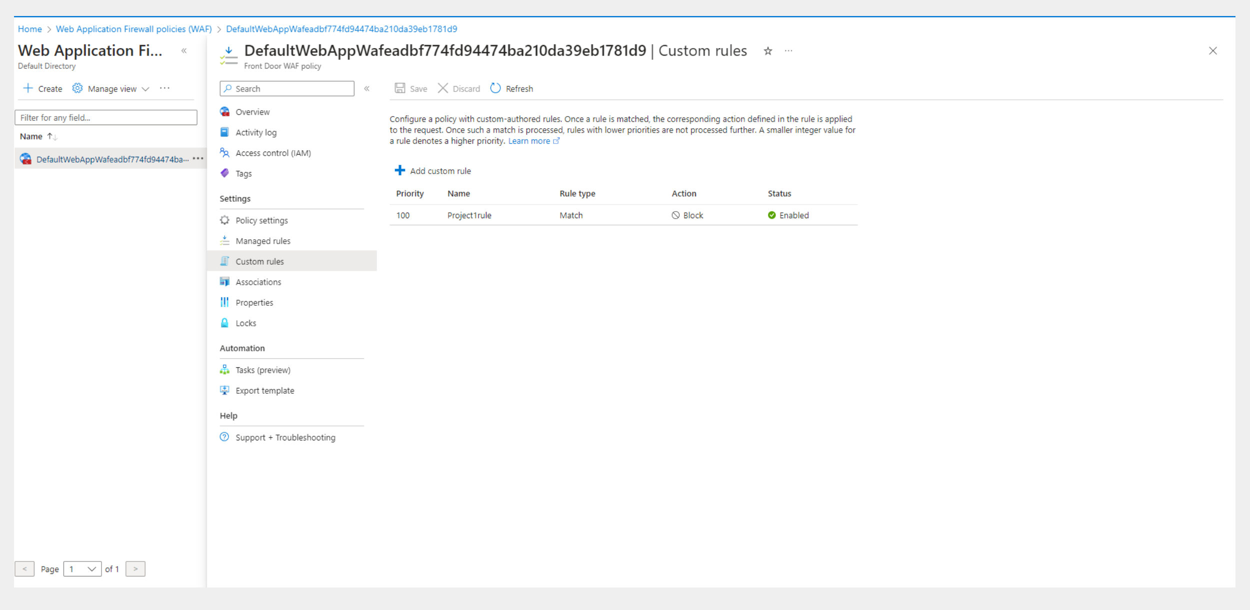
Policy settings
Configure multiple settings that apply to all rules within the policy.

Managed rules
Configure Azure managed rule sets that protect your web application from common threats.

Custom rules
Author custom rules to protect your web application from specifically identified threats.

Associations
Associate a WAF policy with one or more domains hosted on Front Door.

b. A WAF custom rule



DefaultWebAppWafeadbf774fd94474ba210da39eb1781d9 | Custom rules

Front Door WAF policy

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. Learn more

Priority	Name	Rule type	Action	Status
100	Project1rule	Match	⊘ Block	✓ Enabled

References

Assign a Key Vault access policy (legacy). (2023). Microsoft Ignite https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal

Azure Key Vault keys, secrets and certificates overview. (2023). Microsoft Ignite https://learn.microsoft.com/en-us/azure/key-vault/general/about-keys-secrets-certificates

Bisson, D. (2023). What are self-signed certificates? Risks and benefits. *Venafi* https://venafi.com/blog/self-signed-certificates-cyber-criminals-can-quickly-turn-strength-vulnerability/

Comparing Azure Front Door vs Application Gateway: What's the Difference? (2023). Myres Training https://myrestraining.com/blog/azure/comparing-azure-front-door-vs-application-gateway-whats-the-difference/#

Mackie, K. (2015). Microsoft disabling SSL 3.0 in azure storage next month https://redmondmag.com/articles/2015/01/09/ssl-3-in-azure-storage.aspx

Nidhi. (2023). What Is a Tenant in Cloud Computing? The Pros and Cons of Being a Tenant in Cloud Computing. RedSwitches https://www.redswitches.com/blog/tenant-in-cloud-computing/

Kingthorin. (2023). SQL injection. OWASP https://owasp.org/www-community/attacks/SQL_Injection

SSL Offloading. (2023). AVI Networks https://avinetworks.com/glossary/ssl-offload/#:~:text=SSL%20offloading%20relieves%20a%20web,SSL%20acceleration%20or%20SSL%20termination

What is a Wildcard Certificate? (2022-2023). Digicert. *Knowledge base* https://knowledge.digicert.com/generalinformation/INFO900.html

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 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.*