Cybersecurity

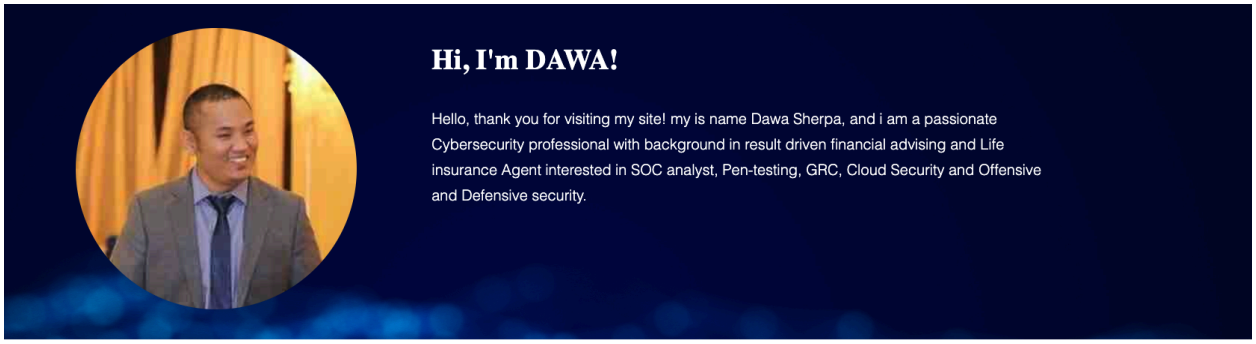
Dawa Sherpa Project 1 Technical Brief

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://dawasherpasecurityresume1-bcaedea4ftfcbcbz.australiaeast-01.azurewebsites.net/]
```



Paste screens

Blog Posts

How Quantum Computing Could Affect Cybersecurity?

Quantum Computing

Quantum computing is poised to revolutionize various sectors, including cybersecurity. As quantum technology advances, it presents both significant risks and potential benefits for digital security. This blog explores how quantum computing could impact current encryption methods, the potential for new security techniques like quantum key distribution, and the steps we need to take to prepare for this transformative technology. From breaking classical encryption to adopting post-quantum cryptographic standards, understanding the implications of quantum computing is crucial for securing our digital future. Quantum computing presents a double-edged sword for cybersecurity. While it poses significant challenges to current encryption methods, it also offers opportunities for developing new, more secure technologies. Preparing for the impact of quantum computing involves adopting new cryptographic standards, enhancing data protection strategies, and investing in emerging security technologies. By staying informed and proactive, we can navigate the challenges of quantum computing and ensure a secure digital future.

hots of you

GRC (Governance, Risk, and Compliance)

GRC

Governance, Risk, and Compliance (GRC) is a strategic approach that integrates the management of governance, risk, and compliance activities within an organization. Governance involves establishing a framework for directing and controlling the organization to achieve strategic objectives and ensure accountability. Risk Management focuses on identifying, evaluating, and mitigating risks that could impact the organization's success. Effective risk management helps prevent disruptions and seizes opportunities for growth. Compliance ensures that the organization adheres to relevant laws, regulations, and internal policies, protecting it from legal issues and penalties. A cohesive GRC framework provides a comprehensive view of potential risks and compliance challenges. It improves decision-making by offering critical insights into organizational risks and regulatory requirements. Streamlining GRC processes enhances operational efficiency and reduces redundancies. Implementing GRC often involves using specialized tools and technologies for monitoring and reporting. Organizations may also seek expert advice to tailor their GRC strategies to their specific needs. The benefits of GRC include better alignment with strategic goals and effective risk mitigation. Overall, GRC is crucial for maintaining integrity, resilience, and sustainable success in a complex business environment.

r website created (Be sure to include your blog posts):

```
[Paste screenshots here]
```

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?

[dawasherpasecurityresume1-bcaedea4ftfcbcbz.australiaeast-01.azurewebsites.net]

Networking Questions

1. What is the IP address of your webpage?

[20.211.64.22]

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

[Sydney, New South Wales, Australia [AU]]

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

```
[Server:        192.168.86.1
Address: 192.168.86.1#53
Non-authoritative answer:
dawasherpasecurityresume1-bcaedea4ftfcbcbz.australiaeast-01.azurewebsites.net       canonical name =
waws-prod-sy3-109.sip.azurewebsites.windows.net.
waws-prod-sy3-109.sip.azurewebsites.windows.net    canonical name =
waws-prod-sy3-109-f656.australiaeast.cloudapp.azure.com.
Authoritative answers can be found from:
australiaeast.cloudapp.azure.com
        origin = ns1-06.azure-dns.com
        mail addr = msnhst.microsoft.com
        serial = 10001
        refresh = 900
        retry = 300
        expire = 604800
]
```

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 back end]
```

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

```
[inside the asset directory there is a css and images folder. Assets
directory contains images and links for website]
```

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 is a customer of the application.]
```

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

```
[An access policy is important on a key vault because it help ensure that
only authorized users and applications can access or manage the secrets,
keys, and certificates stored in the Key Vault, thereby supporting security,
compliance, and effective resource management]
```

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

```
[The difference between keys, secrets and certificates is that certificates
are used in communication to establish trust between parties, secrets are
```

```
sensitive pieces of information that need to be stored securely, keys can be used to encrypt and decrypt data.]
```

Cryptography Questions

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

```
[The advantages of Self-signed certificates are a useful tool in scenarios where cost, speed, and control are important, such as development, testing, and internal use cases]
```

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

```
[The disadvantages of using Self-signed certificates are particularly related to trust, validation, and management.]
```

3. What is a wildcard certificate?

```
[Wildcard certificates are a versatile and cost-effective solution for securing multiple subdomains of a domain with a single certificate]
```

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.

```
[SSL 3.0 isn't provided because it is a known vulnerability]
```

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 because Azure set up a secure SSL certificate]
```

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

```
[Issued On
```

Sunday, August 4, 2024 at 4:40:00 AM
Expires On
Wednesday, July 30, 2025 at 4:40:00 AM]

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

```
[Yes, its Microsoft Azure RSA TLS issuing CA 08]
```

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

```
[Yes, its 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 ]
```

Day 3 Questions

Cloud Security Questions

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

```
[Azure Web Application Gateway and Azure Front Door are both services in
Microsoft Azure that provide traffic management and security features for
web applications, but they serve slightly different purposes and have
distinct features.

Similarities:
    • Both services operate at the application layer(Layer7 Load balancer of OSI model)and
      both route traffic based on HTTP(S) parameter
    • Both services support SSL/TLS termination and can offload SSL decryption.
    • Both services offer integrated Web Application Firewall(WAF) protection.
```

- Both services monitor the health of backend resources and URL based routing.
- Both services distribute incoming traffic across multiple backend resources, improving availability and reliability.

Differences:
- Web application Gateway is regional, ideal for internal applications within a specific Azure region.
- Front Door is global, designed for multi-region , low-latency traffic management.
- Web Application Gateway is a regional resource.
- Front Door is multi regional, including on-premises or other clouds.
- Web Application Gateway has no caching.
- Front Door includes CDN and traffic acceleration
- Web Application Gateway supports HTTP(S) and WebSocket.
- Front Door supports HTTP(S) with URL rewrite and response caching.
- Web Application Gateway is best for advanced regional routing and virtual network integration.
- Front Door is best for global load balancing, fast content delivery and high availability across regions.]

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

[SSL Offloading is the process of decrypting SSL/TLS-encrypted traffic on a load balancer or proxy server instead of on the web server.
Benefits:
- Reduced Server Load: Frees up resources on the web server.
- Simplified Certificate Management:Centralizes SSL management
- Improved Performance:Speeds up response times by offloading encryption tasks
- Enhanced Security: Adds a security layer before traffic reaches backend
- Server.
- Easier Scalability: Simplifies adding or removing servers.

3.What OSI layer does a WAF work on?

[A Web Application Firewall (WAF) works at Layer 7 of the OSI model, which is where apps like websites live. It analyzes things like web traffic

```
(HTTP/HTTPS requests) to protect against attacks like SQL injection and
cross-site scripting. Essentially, it focuses on the data being sent to your
app]
```

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

```
[SQL injection is a type of attack where someone tries to trick a website
into running malicious SQL commands. For example, they might input something
sneaky into a search box to access or alter data in a database that they
shouldn't. A WAF rule for SQL injection looks for these suspicious patterns
in web traffic and blocks them to keep the data safe]
```

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, without Azure Front Door (or another WAF), my website could be
vulnerable to SQL injection attacks. If there's a flaw in my site's code
that allows SQL injection, attackers could exploit it to access or alter my
database. Front Door helps protect against this by filtering out malicious
traffic before it gets to my site, reducing the risk of such attacks]
```

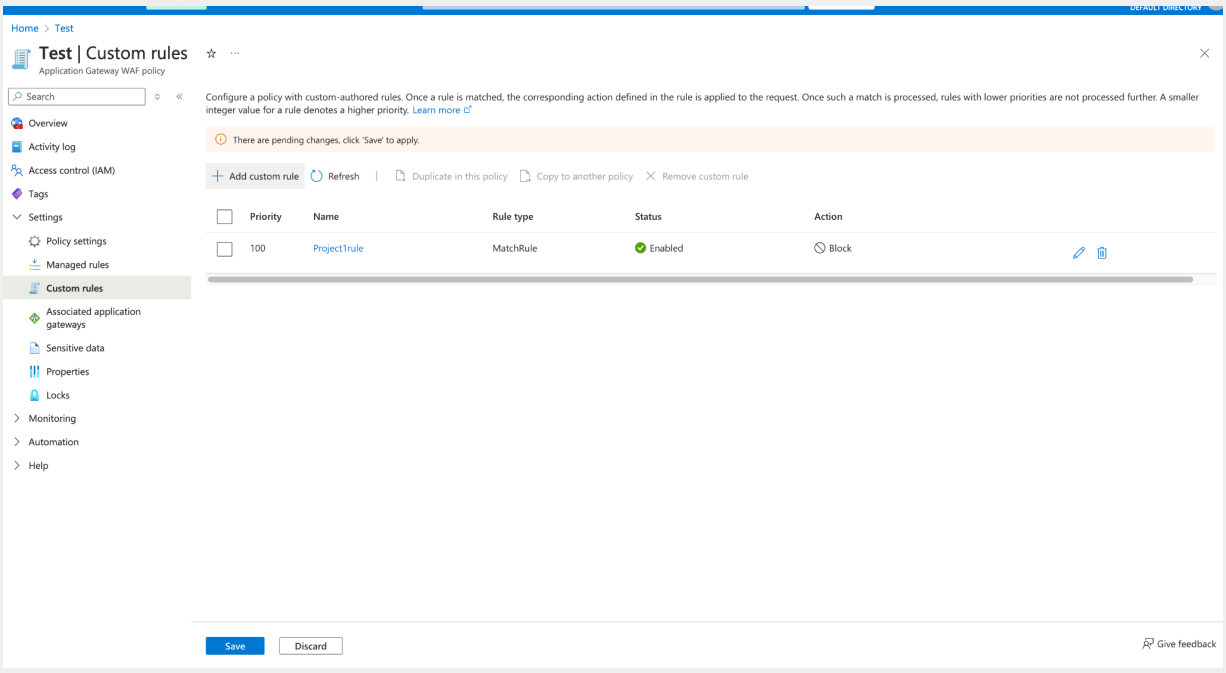
6.Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

```
[Yes, if you set up a rule to block all traffic from Canada, people in
Canada won't be able to access your website. The rule tells the WAF to block
any requests coming from Canadian IP addresses, so it would effectively
block everyone in Canada from getting to your site]
```

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

a. 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 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