Cybersecurity

Project 1 Technical Brief

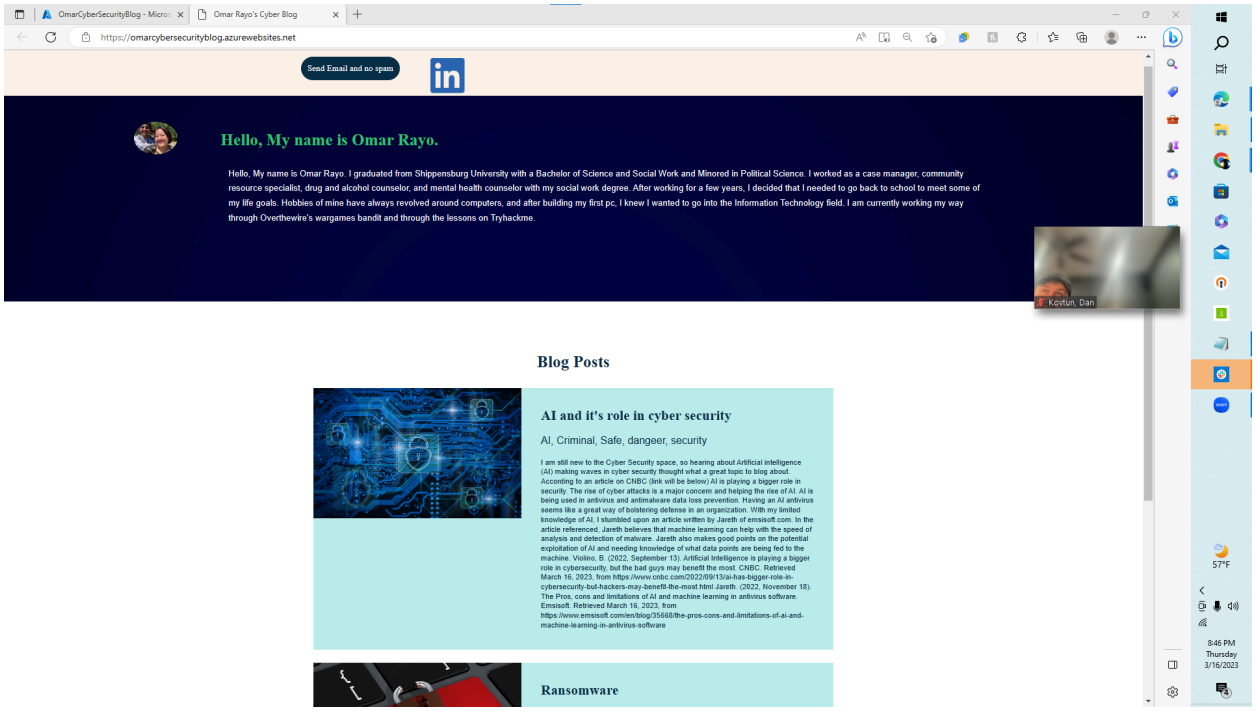
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://omarcybersecurityblog.scm.azurewebsites.net
```

Paste screenshots of your 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
```

2. What is your domain name?

```
omarcybersecurityblog.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.11
```

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

```
Australia, New South Wales, Sydney
```

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

waws-prod-sy3-087.sip.azurewebsites.windows.net	1800	waws-prod-sy3-087-0d6a.australiaeast.cloudapp.azure.com (20.211.64.11)

omarcybersecurityblog.azurewebsites.net	30	waws-prod-sy3-087.sip.azurewebsites.windows.net (waws-prod-sy3-087-0d6a.australiaeast.cloudapp.azure.com.)

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?

> Runtime is a piece of code that implements portions of a programming language's execution model. In doing this, it allows the program to interact with the computing resources it needs to work. Also it is a back end process.

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

```
index.html
```

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

```
This works with both but when editing the back end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

   ```
   Tenancy in cloud computing refers to sharing of computing resources in a
   private or could be public environment that is isolated from other users.
   ```

```
It is a SaaS which then divides into two types: single-tenant or
multi-tenant.
```

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

```
It determines whether a given security principal, namely a user, application
or user group, can perform different operations on Key Vault secrets, keys,
and certs. Having people that need accesses to it only have access to it
allows for no secrets to be stolen or resources taken.
```

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

```
Keys: supports many different types of keys and algorithms, and enables the
use of software-protected and HSM-protected keys.
Secrets: Provides secure storage of secrets such as passwords and data bases
connection strings.
Certificates: Support Certificates which are built on top of keys and
secrets and add an automated renewal feature. Keep in mind when a
certificate is created an addressable key and secret are also created with
the same name.
```

Cryptography Questions

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

```
Self-signed certificates are easy to make, free to use, and fast. They are
great in development/testing environment and internal network websites.
There are zero dependencies on other for the issuance of cert. Also not
having it publicly available will not allow others who are looking for ways
into your website more known attack vectors.

Info:https://www.encryptionconsulting.com/education-center/self-signed-certi
ficates/
```

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

```
Some disadvantages are that browsers and os will not trust the cert. They
are also highly risky for transactions.Users become vulnerable to data theft
and other cyberattacks when attackers create self-signed certificates that
can be used in man-in-the-middle (MITM) attacks
```

3. What is a wildcard certificate?

```
This type of SSL/TLS certificate allows you to secure your main domain and
an unlimited number of subdomains under your main domain with just one
single certificate.

info:https://sectigo.com/ssl-certificates-tls/wildcard?utm_term=+wild%20+car
d%20+certificates&utm_campaign=Sectigo%20Retail_SSL_US&utm_source=adwords&ut
m_medium=ppc&hsa_acc=9165095309&hsa_cam=2046696154&hsa_grp=74035559244&hsa_a
d=581419584209&hsa_src=g&hsa_tgt=kwd-309691797750&hsa_kw=+wild%20+card%20+ce
rtificates&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjwtsCgBhDEARIsAE7R
Yh1D499I_RZtU_DK6L6k5VYE-ITzXWi1iB07zfHd9q0OSBp40GTRFXQaAjRFEALw_wcB
```

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 reason why SSL 3.0 is disable is because a known vulnerability came out
that would make all VM's and websites vulnerable. So by default all machines
have SSL 3.0 disabled.

info:https://redmondmag.com/articles/2015/01/09/ssl-3-in-azure-storage.aspx
```

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 domains come with SSL certificates.
```

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

```
3/14/2023 to 3/14/2024 We have a data range of a year.
```

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

```
Yes, it is a stand in for root certificate. They are used to sign the SSLs
for the customers install and maintain the chain of trust.
```

```
info: https://www.godaddy.com/help/what-is-an-intermediate-certificate-868
```

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

```
A root SSL cert is a certificate issued by a trusted Cert Auth (CA). A
trusted entity is some who auth to verify someone is who they say they are.

info:https://support.dnsimple.com/articles/what-is-ssl-root-certificate/
```

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

```
Yes Chrome has has a root store which contains the sets of Certificates
Chrome trusts by default.
```

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

```
Certum CA
```

Day 3 Questions

Cloud Security Questions

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

```
The similarities between Azure Web Application is that both reside in the
front of your web application in order to protect it. They both work on the
Layer 7. Their primary solution is a load balancer. Their primary solution
is a load balancer. They can incorporate a web application firewall to
protect against web attacks. They have additional features such as URL
path-based routing and SSL/TLS termination.

The Difference between Azure Web Applications is that WAG is more regional
and is best suited to protect a web application in a single region in your
cloud. The Azure Front Door is more global and is better suited when you
have a variety of regions in a cloud environment.
```

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

```
SSL offloading relieves a web server of the processing burden of encrypting
and decrypting traffic sent via SSL. All web browser is compatible with SSL
security protocol, making SSL traffic common. The processing is offloaded to
a separate server designed specifically to perform SSL acceleration or SSL
termination.


The information received
from:https://avinetworks.com/glossary/ssl-offload/#:~:text=SSL%20offloading%
20relieves%20a%20web,SSL%20acceleration%20or%20SSL%20termination.
```

3. What OSI layer does a WAF work on?

```
According to Cloudflare, “A WAF is a protocol layer 7 defense in (in the OSI
model) and is not designed to defend against all types of attacks.
```

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

```
According to L7defense.com a SQL (Structured Query Language) injection match
conditions specifies the web request portion that you want to verify WAF,
such as the Address or the query string. If an access control list is
created, you will specify whether requests contain the malicious SQL code
you want to allow or block.
```

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?

```
I believe that my current website is not vulnerable even if the Front Door
was enabled. For an SQL is a method for inserting SQL queries into the input
fields through the SQL database underlying the system. I have no area where
they would be able to input PHP that can be used to write the command.
```

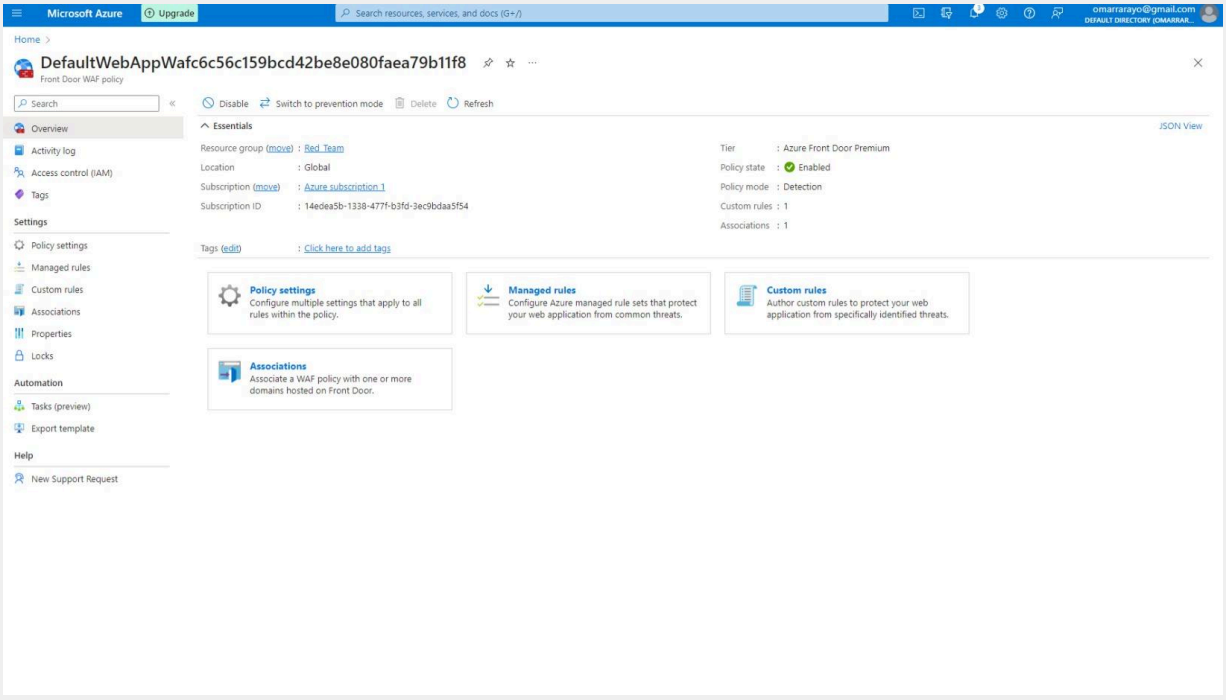
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

They would still be able to enter the website unless I set the priority of the first rule create to allow Canada. If the new rule is set to 100 and the old rule is set to 101 the yes it would block traffic.

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

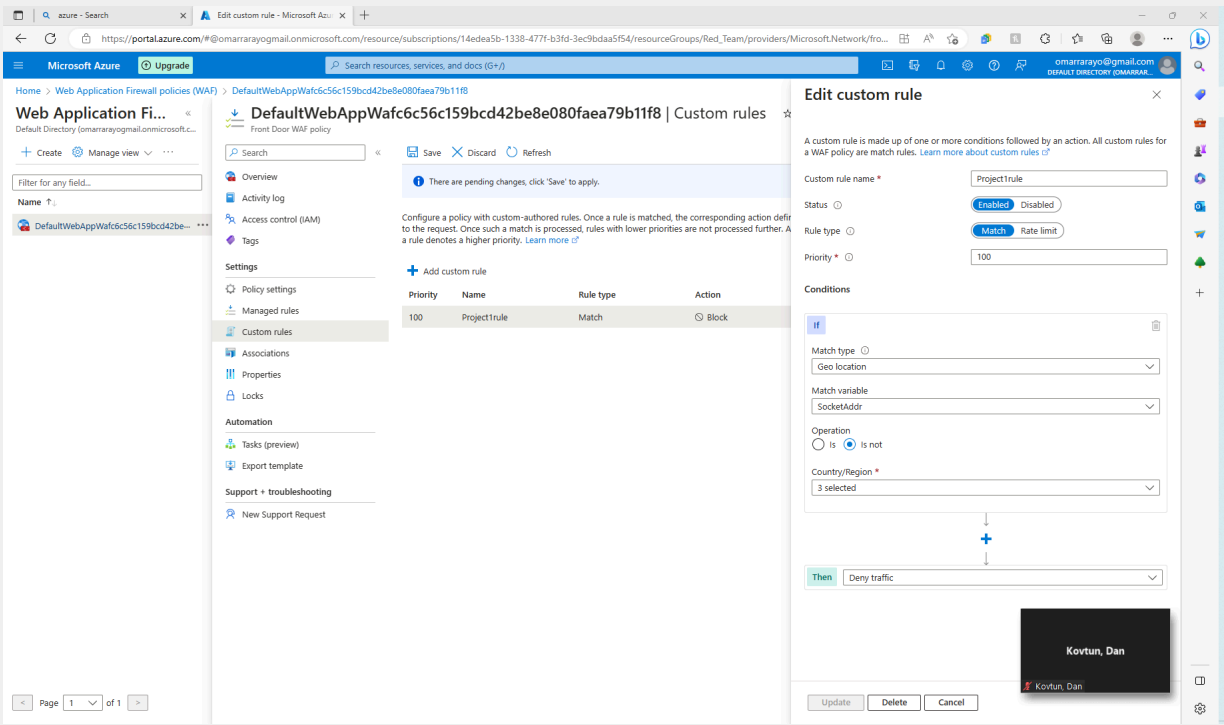
    a. Azure Front Door enabled

[Paste screenshot here]



    b. A WAF custom rule

[Paste screenshot



here]

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.*