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://tanvirsecurityblog.azurewebsites.net
```

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

t

TANVIR SHAH'S CYBER BLOG

Send Email

Hi, I'm Tanvir!

Welcome to my cybersecurity blog! I started this blog with the intention of inspiring and teaching others in this line of work. I hope users read my blog and gain some interest in cybersecurity.

Blog Posts

Technology Is Quickly Outgrowing Humans

It is becoming a concerning factor that technology is quickly outgrowing humans at a rapid pace. For one, artificial intelligence is advancing at a speed like no other. It can process and solve algorithms at speeds faster than any human capability. For example, ChatGPT 4.0 can score at least 80% on the bar exam with just one command. Technology has also improved efficiency in food industries by using machines and robots to perform tasks with more precision. A self-serving robot that works as a waiter/waitress in a restaurant is a great example of this. Delivering food to patrons' tables with consistency shows how technology has grown. There are cars now that are fully electric and self-drivable. Using only our devices, we are able to drive these cars and automatically update software throughout the vehicle. Seeing that technology clearly plays a massive role in today's future, it is important that humans do not become any less than technology itself. While humans may have their limits, technology is not limited to any physical restraints which allows it to increase productivity.

Protect Your Network!

Protecting your network is important when you have any kind of sensitive information which may include digital assets. However, there are at least 5 steps we can take in order to prevent any loss and to protect your network. Creating a strong and unique password for all devices and accounts can ensure your network is safe. It is also a good idea to avoid reusing passwords. Using a Two-Factor Authentication tool is also a good idea. By adding a second form of verification such as a cellphone number, users can have a code sent to their devices for verification. Installing regular updates keeps your applications up to date with the latest software and security enhancements. These regular updates usually include the latest patches and bug fixes. Furthermore, by installing Firewalls, you are able to monitor and control network traffic. Firewalls give you the power to block and prevent any unauthorized access. Performing a regular backup helps secure critical data as well. This helps when you suffer a loss of important data during a system failure. By following these steps, you can significantly increase the security of your network and reduce any factors of unauthorized access.

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?

```
tanvirsecurityblog.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.19
```

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

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

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

```
 dig NS tanvirsecurityblog.azurewebsites.net

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> NS
tanvirsecurityblog.azurewebsites.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3785
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;tanvirsecurityblog.azurewebsites.net. IN NS
```

```
;; ANSWER SECTION:
tanvirsecurityblog.azurewebsites.net. 30 IN CNAME
waws-prod-sy3-103.sip.azurewebsites.windows.net.
waws-prod-sy3-103.sip.azurewebsites.windows.net. 1800 IN CNAME
waws-prod-sy3-103-e6e5.australiaeast.cloudapp.azure.com.

;; AUTHORITY SECTION:
australiaeast.cloudapp.azure.com. 60 IN   SOA   ns1-06.azure-dns.com.
msnhst.microsoft.com. 10001 900 300 604800 60

;; Query time: 90 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Jun 24 18:45:57 EDT 2023
;; MSG SIZE  rcvd: 262
```

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
```

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

```
There is an images file and a CSS file.
```

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

```
The CSS file works on the front-end of the site.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
Any group of users that may have a common network access to cloud services.


    Azure tenant: A complete guide to the azure tenant. EDUCBA. (2023,
    March 8). https://www.educba.com/azure-tenant/
```

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

```
This policy would have a restriction on what resources can be accessed and
who can authorize this access.
```

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

```
Keys are cryptographic information stored within a key vault. For example, a
private key is only authorized by someone who has access to it and a public
key can be accessed by anyone. Secrets are a storage for passwords and
private keys. Certificates allow for the owner of the key vault to manage
and store information without accessing private keys.


    BohdanBohdan                    16.4k1515 gold badges7373 silver
    badges6868 bronze badges, BishoyBishoy                    3, Diego
    MendesDiego Mendes                    10.5k22 gold badges3131 silver
    badges3636 bronze badges, & Ryan EfendyRyan Efendy
    4. (1963, February 1). What is difference between Keys and secrets in
    azure key vault?. Stack Overflow.
    https://stackoverflow.com/questions/38277023/what-is-difference-between
    -keys-and-secrets-in-azure-key-vault

    Msmbaldwin. (n.d.). About azure key vault certificates. Microsoft
    Learn.
    https://learn.microsoft.com/en-us/azure/key-vault/certificates/about-ce
    rtificates
```

Cryptography Questions

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

```
It’s completely free and is easy to use.
```

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

```
Most of them are not free and they cannot be revoked.
```

3. What is a wildcard certificate?

```
A wildcard certificate allows us to secure multiple domains and sub-domains.
There is a risk factor in which, if one domain is compromised, then it is
possible the other domains are at risk as well.
```

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 is likely to be vulnerable which may allow users to be compromised
of their important data. Microsoft has also advised that SSL 3.0 should be
disabled to protect consumers.


    BetaFred. (n.d.). Microsoft Security advisory 3009008. Microsoft Learn.
    https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/2
    015/3009008?redirectedfrom=MSDN
```

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’s free domain provides a SSL certification.
```

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

```
Issued on Thursday, March 9, 2023 at 10:05:55 PM.
Expires on Sunday, March 3, 2024 at 10:05:55 PM.
```

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

```
Microsoft Azure TLS Issuing CA 02
```

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?

```
No, my browser does not have the root certificate in its root store because
the site was stored on a remote server.
```

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

```
*.azurewebsites.net
```

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 Gateways and Azure Front Door are both load balancers.
The difference between these two is that Azure Web Application Gateway is
used globally. Meanwhile, Azure Front Door remains regional.

     Duongau. (n.d.). Azure front door - frequently asked questions. Azure
Front Door - Frequently asked questions | Microsoft Learn.
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq
```

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 a tool that redirects incoming encrypted information
towards a load balancer. There are a few benefits which include performance
improvements, less latency and also helps to increase security of websites.
```

3. What OSI layer does a WAF work on?

```
A WAF works on Layer 7.
```

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

```
A SQL Injection is an exploit that targets the database of a server by
injecting a malicious code. This code allows a user to retrieve data that
someone normally would not have access to.
```

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?

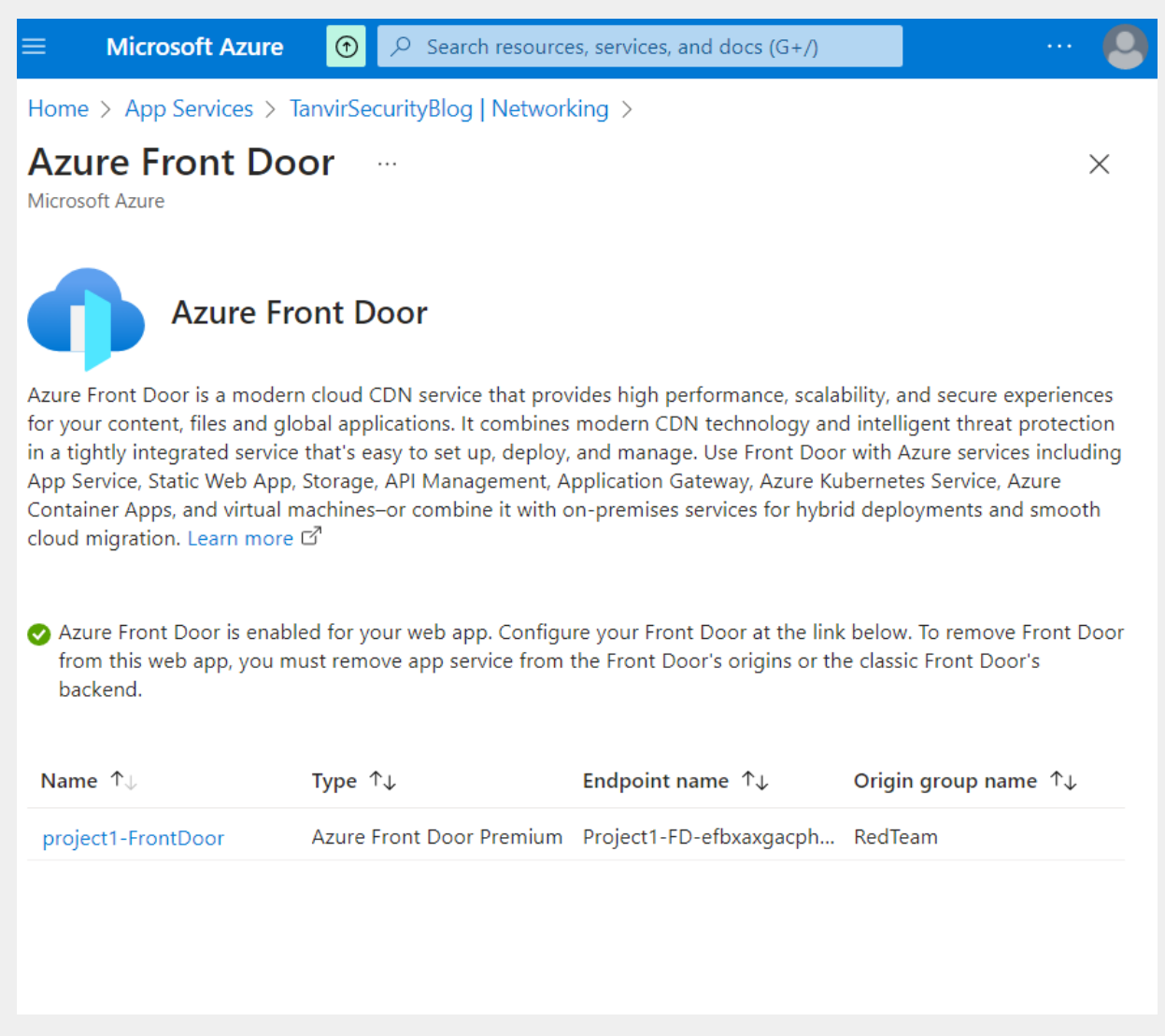
```
If a SQL injection-based attack were to happen against my website, nothing
would happen even if Front Door was not enabled. This is because my website
is not attached to my database.
```

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?

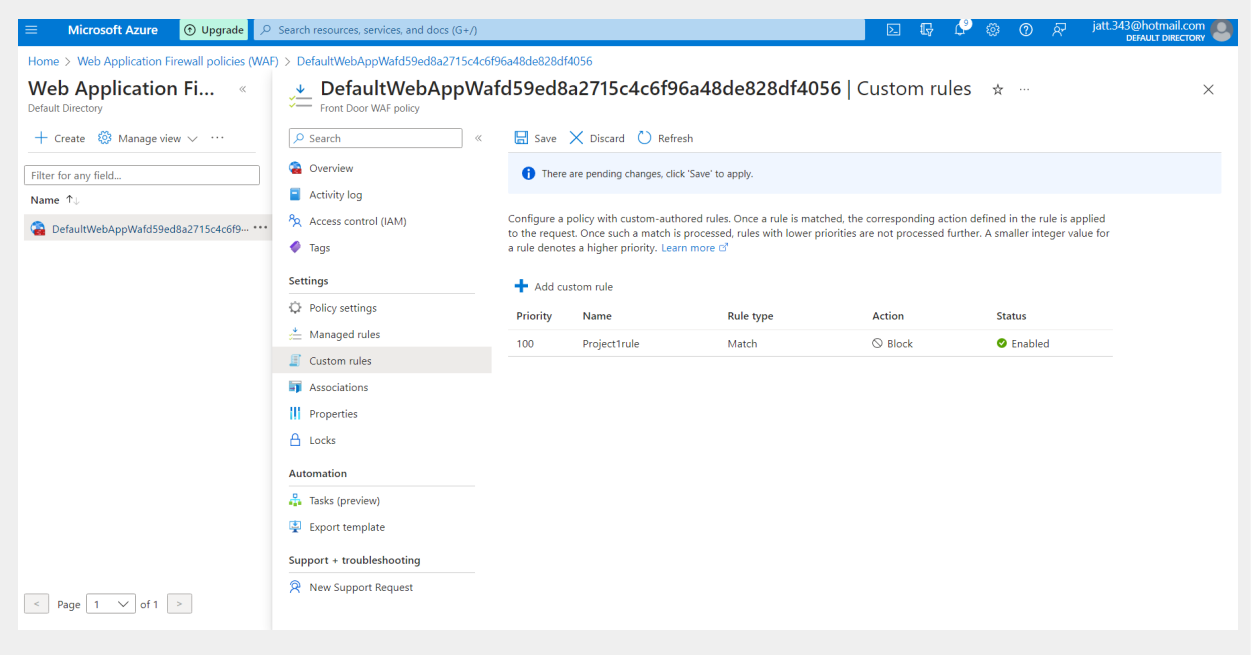
```
Yes, anyone who lives in Canada would not be able to access my website. This
is simply because the WAF rule would block anyone with a Canadian IP address
to gain access to my website.
```

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

    a. Azure Front Door enabled



b. 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***