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.

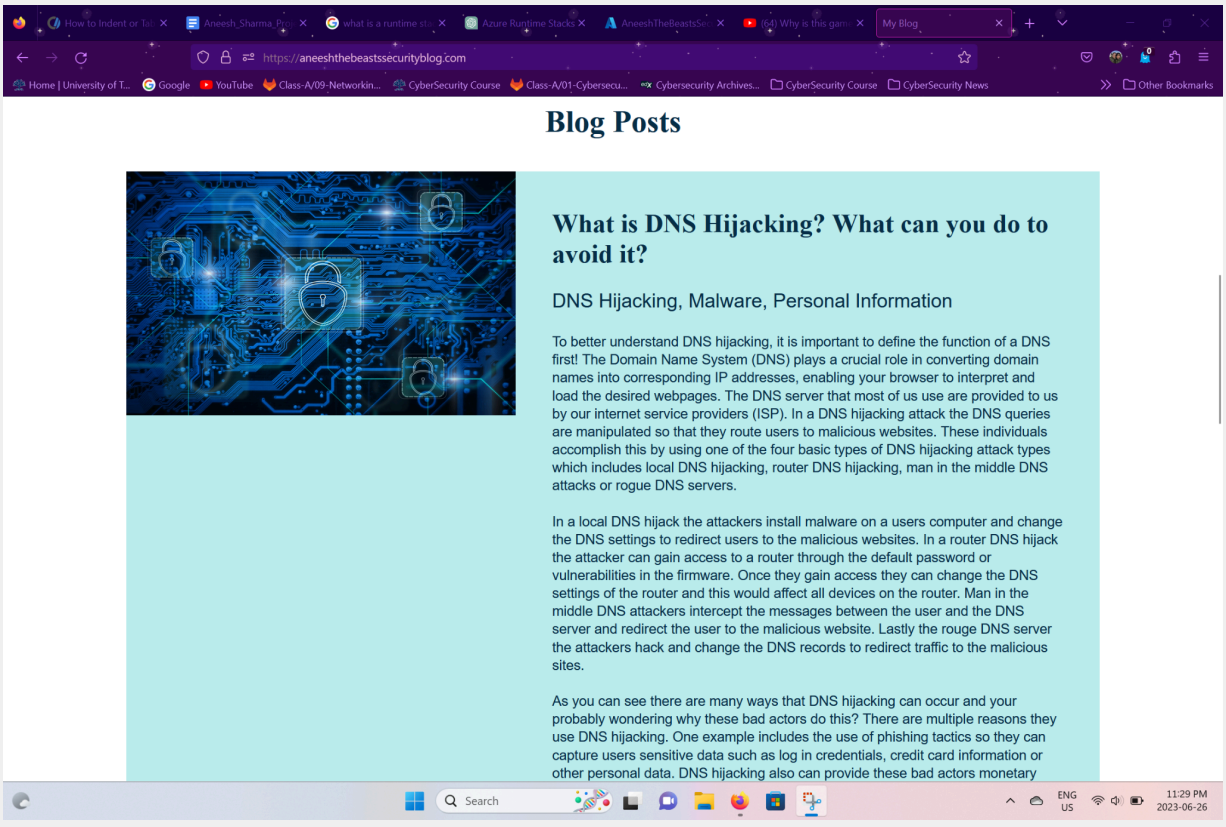
Your Web Application

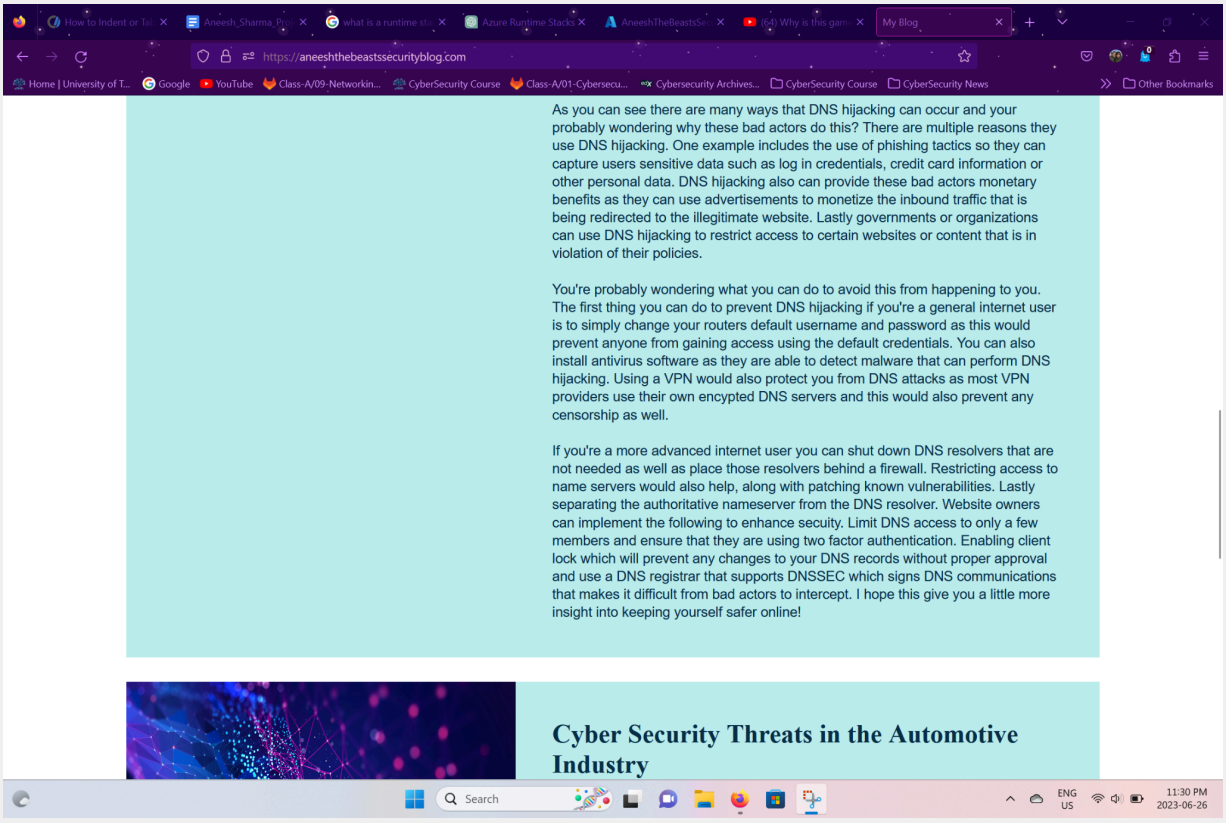
Enter the URL for the web application that you created:

```
aneeshsthebeastssecurityblog.com
```

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


AneeshTheBeasts Security Blog
Send Email
Hi, I'm Aneesh!
I am currently a student and enrolled in the U of T CyberSecurity bootcamp. I decided to take this course because I am interested in changing my current career. I have been passionate about CyberSecurity but have not been able to persue this passion until now.
I will be using this blog to discuss topics that we have discussed in class and also provide insight into current events within the CyberSecurity world. My hope with this blog is to help newcomers understand topics within CyberSecurity as well as inspire others to take a step into this exciting world of CyberSecurity!


Blog Posts
What is DNS Hijacking? What can you do to avoid it?
DNS Hijacking, Malware, Personal Information
To better understand DNS hijacking, it is important to define the function of a DNS first! The Domain Name System (DNS) plays a crucial role in converting domain names into corresponding IP addresses, enabling your browser to interpret and load the desired webpages. The DNS server that most of us use are provided to us by our internet service providers (ISP). In a DNS hijacking attack the DNS queries are manipulated so that they route users to malicious websites. These individuals accomplish this by using one of the four basic types of DNS hijacking attack types which includes local DNS hijacking, router DNS hijacking, man in the middle DNS attacks or rogue DNS servers.
In a local DNS hijack the attackers install malware on a users computer and change the DNS settings to redirect users to the malicious websites. In a router DNS hijack the attacker can gain access to a router through the default password or vulnerabilities in the firmware. Once they gain access they can change the DNS settings of the router and this would affect all devices on the router. Man in the middle DNS attackers intercept the messages between the user and the DNS server and redirect the user to the malicious website. Lastly the rouge DNS server the attackers hack and change the DNS records to redirect traffic to the malicious sites.
As you can see there are many ways that DNS hijacking can occur and your probably wondering why these bad actors do this? There are multiple reasons they use DNS hijacking. One example includes the use of phishing tactics so they can capture users sensitive data such as log in credentials, credit card information or other personal data. DNS hijacking also can provide these bad actors monetary


My Blog
https://aneeshthebeastssecurityblog.com
Home | University of T...
Google
YouTube
Class-A/09-Networkin...
CyberSecurity Course
Class-A/01-Cybersecu...
Cybersecurity Archives...
CyberSecurity Course
CyberSecurity News
Other Bookmarks
As you can see there are many ways that DNS hijacking can occur and your probably wondering why these bad actors do this? There are multiple reasons they use DNS hijacking. One example includes the use of phishing tactics so they can capture users sensitive data such as log in credentials, credit card information or other personal data. DNS hijacking also can provide these bad actors monetary benefits as they can use advertisements to monetize the inbound traffic that is being redirected to the illegitimate website. Lastly governments or organizations can use DNS hijacking to restrict access to certain websites or content that is in violation of their policies.
You're probably wondering what you can do to avoid this from happening to you. The first thing you can do to prevent DNS hijacking if you're a general internet user is to simply change your routers default username and password as this would prevent anyone from gaining access using the default credentials. You can also install antivirus software as they are able to detect malware that can perform DNS hijacking. Using a VPN would also protect you from DNS attacks as most VPN providers use their own encypted DNS servers and this would also prevent any censorship as well.
If you're a more advanced internet user you can shut down DNS resolvers that are not needed as well as place those resolvers behind a firewall. Restricting access to name servers would also help, along with patching known vulnerabilities. Lastly separating the authoritative nameserver from the DNS resolver. Website owners can implement the following to enhance secuity. Limit DNS access to only a few members and ensure that they are using two factor authentication. Enabling client lock which will prevent any changes to your DNS records without proper approval and use a DNS registrar that supports DNSSEC which signs DNS communications that makes it difficult from bad actors to intercept. I hope this give you a little more insight into keeping yourself safer online!
Cyber Security Threats in the Automotive Industry
Search
ENG
US
11:30 PM
2023-06-26


My Blog
https://aneeshthebeastssecurityblog.com
Home | University of T...
Google
YouTube
Class-A/09-Networkin...
CyberSecurity Course
Class-A/01-Cybersecu...
Cybersecurity Archives...
CyberSecurity Course
CyberSecurity News
Other Bookmarks
Cyber Security Threats in the Automotive Industry
Man in the Middle, Authentication, Exploits
When it comes to Cyber Security most people think about attacks on personal devices such as your phone or computer, but these attacks extend beyond just that. Cyber attacks against vehicles have increased 140% since 2020 which is not something most people think about in their day to day lives. With more and more vehicles offering features such as remote start, an app to monitor the car, keyless entry and over the air updates there are alot of threats that we as car owners can face on a daily basis.
As electric vehicles have become inceasingly popular there has been a subsequent expansion in the number of charging stations located around cities. These charging stations however, pose as a target for cyber attacks. Many of these stations communicate via cellular signals which makes them vulnerable to man in the middle attacks. In these attacks a bad actor will intercept data that is being communicated from the charging station. A skilled hacker could then use this exploit to bring down an entire system of charging points, they could remotely control these charging points and use them to infect the system with malware. These charging points also communicate to the customer via an app which could lead personal information being stolen or remote apps being installed on the clients device.
As the automotive industry has expanded and more cars come with connected infotainment systems which is another security risk. This system is always online and constantly sharing information to the users phone or a database where updates to the vehicle are provided, if this system is not properly protected user information could be exposed and the vehicle can also be at risk. The infotainment systems provide a path to the cars electronic control unit allowing some skilled individuals remote access to the car which would allow it to be easily stolen and any customer data linked to the car to be exposed.
Keyless car thefts have also increased overtime and have been exploited at a staggering rate. This type of attack is a great example of a man in the middle attack
Search
ENG
US
11:30 PM
2023-06-26

Blog Post 1 Sources:

1. Imperva. (2019). *What is a DNS Hijacking | Redirection Attacks Explained | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/dns-hijacking-redirection/
2. Lexie. (2022, September 28). *What is DNS Hijacking and How to Prevent it? | ExpressVPN Blog*. Home of Internet Privacy. https://www.expressvpn.com/blog/dns-address-hijacking-explained/

Blog Post 2 Sources:

1. Nuspire, T. (2022, November 15). *Examining the Top 5 Automotive Cybersecurity Threats*. Security Boulevard. https://securityboulevard.com/2022/11/examining-the-top-5-automotive-cybersecurity-threats/
2. *As Cyber Attacks on Cars Rise, So Does Related Cybersecurity*. (2022, September 7). GovTech. https://www.govtech.com/transportation/as-cyber-attacks-on-cars-rise-so-does-related-cybersecurity
3. *The top 8 Cybersecurity threats facing the automotive industry heading into 2023*. (2023, May 16). Cybersecurity.att.com. https://cybersecurity.att.com/blogs/security-essentials/the-top-8-cybe

```
rsecurity-threats-facing-the-automotive-industry-heading-into-2023

I plan on remaking my blog after the project is graded to properly cite the sources used within the article and have a page dedicated to sources used in the posts that I make.
```

Day 1 Questions

General Questions

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

```
GoDaddy
```

2. What is your domain name?

```
AneeshTheBeastsSecurityBlog
```

Networking Questions

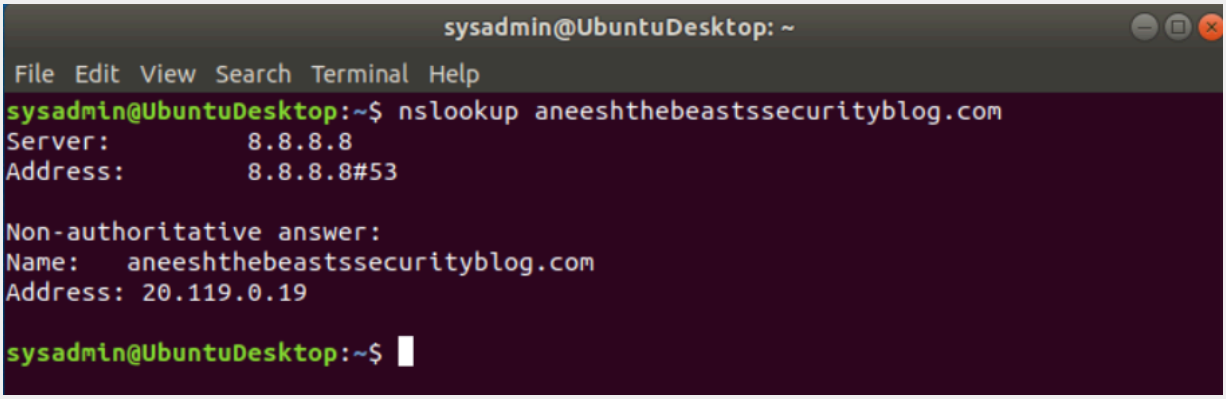
1. What is the IP address of your webpage?

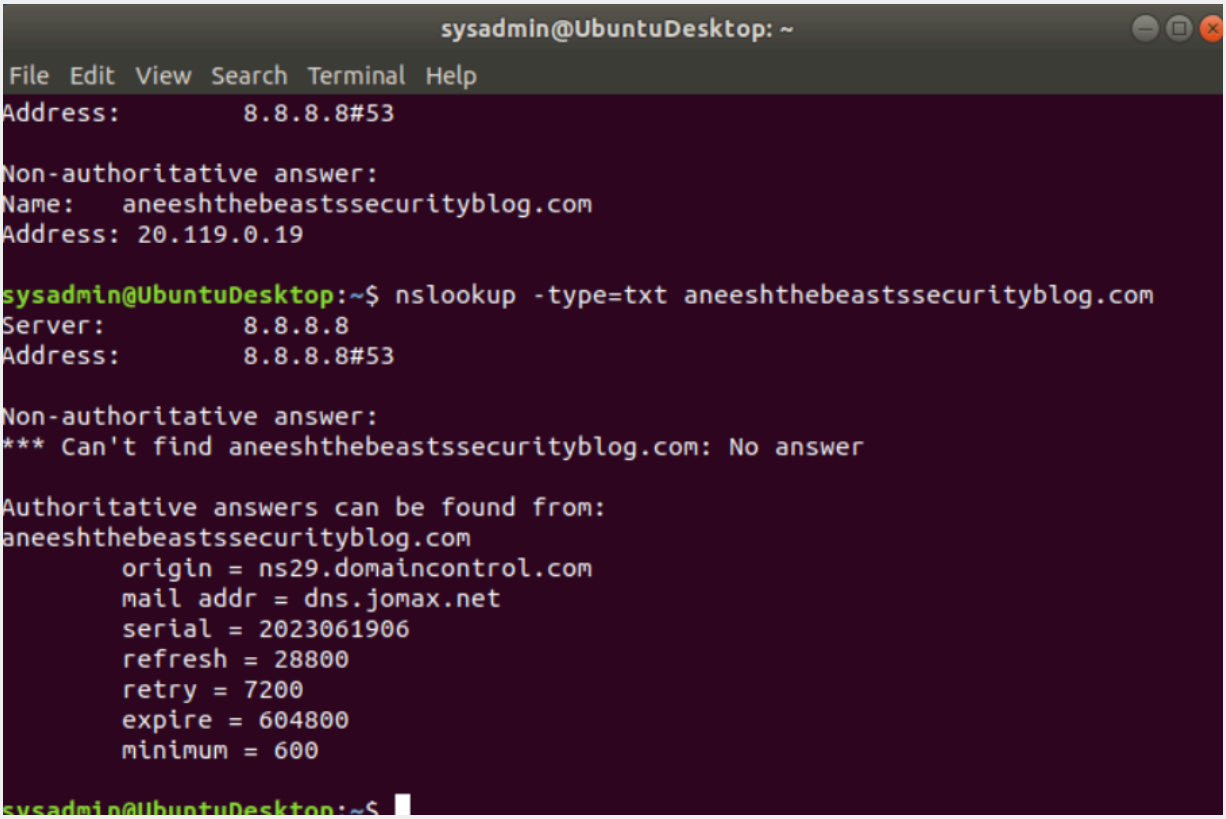
```
20.119.0.19
```

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

```
City= Washington
State= Virginia
Country= USA
```

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





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 and it works on the back end.
```

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

```
Inside the asset's directory, there is a folder called CSS and images. The CSS file contains rules on how HTML elements should be displayed on the web browser. The image's folder contains images to be displayed on the web browser.
```

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

```
This works on the front end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is an individual or organization that uses a cloud computing service that is provided by a cloud service provider.

Gupta, D. (n.d.). Single-tenant vs Multi-Tenant Cloud [infographic]: Loginradius blog. loginradius. https://www.loginradius.com/blog/identity/single-tenant-vs-multi-tenant/
```

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

```
Access policy would be important on a key vault because it would help ensure security and proper management of cryptographic keys and secrets. Access policies would allow only a certain group of people access, which would prevent any unauthorized access.


Msmbaldwin. (2023, March 8). Assign an Azure Key Vault access policy (CLI). Microsoft Learn. https://learn.microsoft.com/en-us/azure/key-vault/general/assign-acces
```

```
s-policy?tabs=azure-portal
```

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

```
Certificates are utilized in communication to establish trust between
parties, while secrets, are confidential pieces of information that require
secure storage. Keys are used to encrypt and decrypt data.

The Relationship Between Keys, Secrets and Certificates in Azure Key Vault.
(2021, April 29). Michael's Security Blog.
https://michaelhowardsecure.blog/2021/04/29/the-relationship-between-keys-se
crets-and-certificates-in-azure-key-vault/
```

Cryptography Questions

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

```
The advantage of a self-signed certificate is that they are free and easy to
issue. They are good for development/testing environments and internal
network websites. Self-signed certificates are also easy to modify and
customize, and they are able to carry more metadata. Since they are self
generated, it saves time in terms of testing because you don't have to rely
on other issuing authorities.

Puneet. (2020, September 23). What is a Self-Signed Certificate? Advantages,
Disadvantages & Risks. Encryption Consulting.
https://www.encryptionconsulting.com/education-center/self-signed-certificat
es
```

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

```
The disadvantage of a self-signed certificate is that they are not trusted
by browsers and when visiting the website it would display a prompt that
would tell you to accept risk when visiting. They are also very risky for
websites that deal with any transactions or financial information. The
challenge with self-signed certificates is that the lack of visibility makes
it hard to keep track of them compared to certificates issued by a
certificate authority. Lastly, it is hard to tell if a self-signed
certificate has been hacked if the business network is compromised.
```

Puneet. (2020, September 23). *What is a Self-Signed Certificate? Advantages, Disadvantages & Risks*. Encryption Consulting. https://www.encryptionconsulting.com/education-center/self-signed-certificates

3. What is a wildcard certificate?

A wild card certificate is a certificate that has a wildcard in its name. This certificate is able to secure multiple subdomains that relate to the base domain.
What is a Wildcard Certificate? (n.d.). Knowledge.digicert.com. https://knowledge.digicert.com/generalinformation/INFO900.html

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 not provided because there is a known vulnerability that was discovered, and it has been depreciated since June 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?

When using the certificate that I created on my own, the browser is retuning an error because the certificate is not issues by a certificate authority that makes the site secure.
When I use the current certificate that azure set up, then it returns no errors and works like normal.

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

The validity of the certificate that azure set up
Issued: 2023-06-16T00:00:00+00:00
Expiration: 2023-12-16T23:59:59+00:00

The validity of the self-made certificate is

```
Issued: 2023-06-19T23:19:01+00:00
Expiration: 2024-06-18T23:19:01+00:00
```

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

```
GeoTrust Global TLS RSA4096 SHA256 2022 CA1
This is the intermediate certificate on the website that I have created.
```

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

```
DigiCert Global Root CA
This is the root certificate on my website.
```

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

```
Yes, my browser has the root certificate in its root store.
```

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

```
One other root CA that is available in my browser is COMODO CA Limited
```

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 Gateway and Azure Front Door
is that they are both layer 7 HTTP/HTTPS load balancers, and the difference
between both is that Front Door is a non-regional service and Application
Gateway is a regional service.

duongau. (n.d.). Azure Front Door - Frequently asked questions.
Learn.microsoft.com. Retrieved June 27, 2023, from
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 refers o the procedure of eliminating SSL-based encryption
from incoming traffic directed towards a web server. This helps reduce the
burden on the server by eliminating the need for decryption of data.

What is SSL Offloading? Definition and Related FAQs. (n.d.). Avi Networks.
https://avinetworks.com/glossary/ssl-offload/
```

3. What OSI layer does a WAF work on?

```
It works on layer 7 defence
```

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

```
The purpose of a SQL injection rule statement is to detect and prevent the
presence of malicious SQL code. SQL injection attacks occur when attackers
intentionally insert harmful SQL code into web requests. This code can be
used to manipulate or extract sensitive data from the database. Hence, an
SQL injection rule statement is designed to identify and mitigate such
attacks, safeguarding the integrity and security of your system.

SQL injection attack rule statement - AWS WAF, AWS Firewall Manager, and AWS
Shield Advanced. (n.d.). Docs.aws.amazon.com.
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-typ
e-sqli-match.html
```

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?

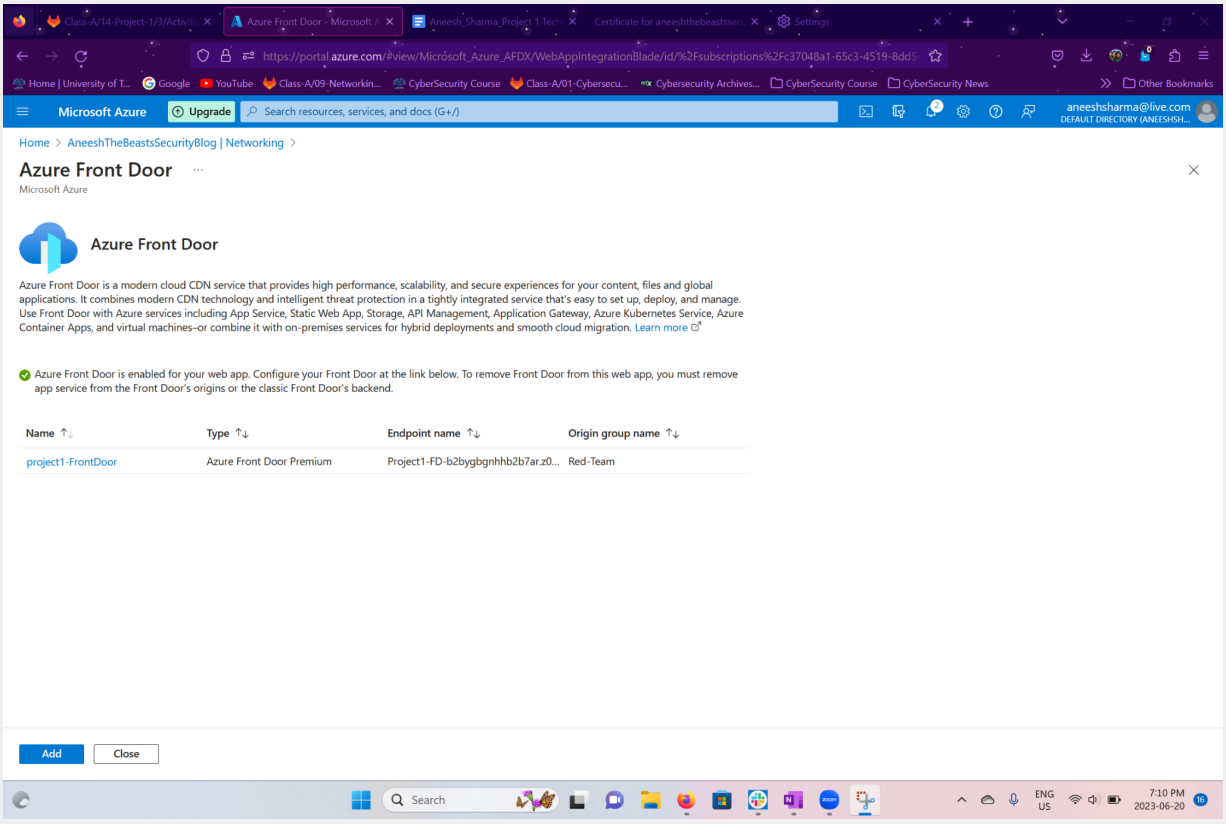
```
If front door was no enabled, it wouldn't have an impact because my WAF
rules would still block SQL injections.
```

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?

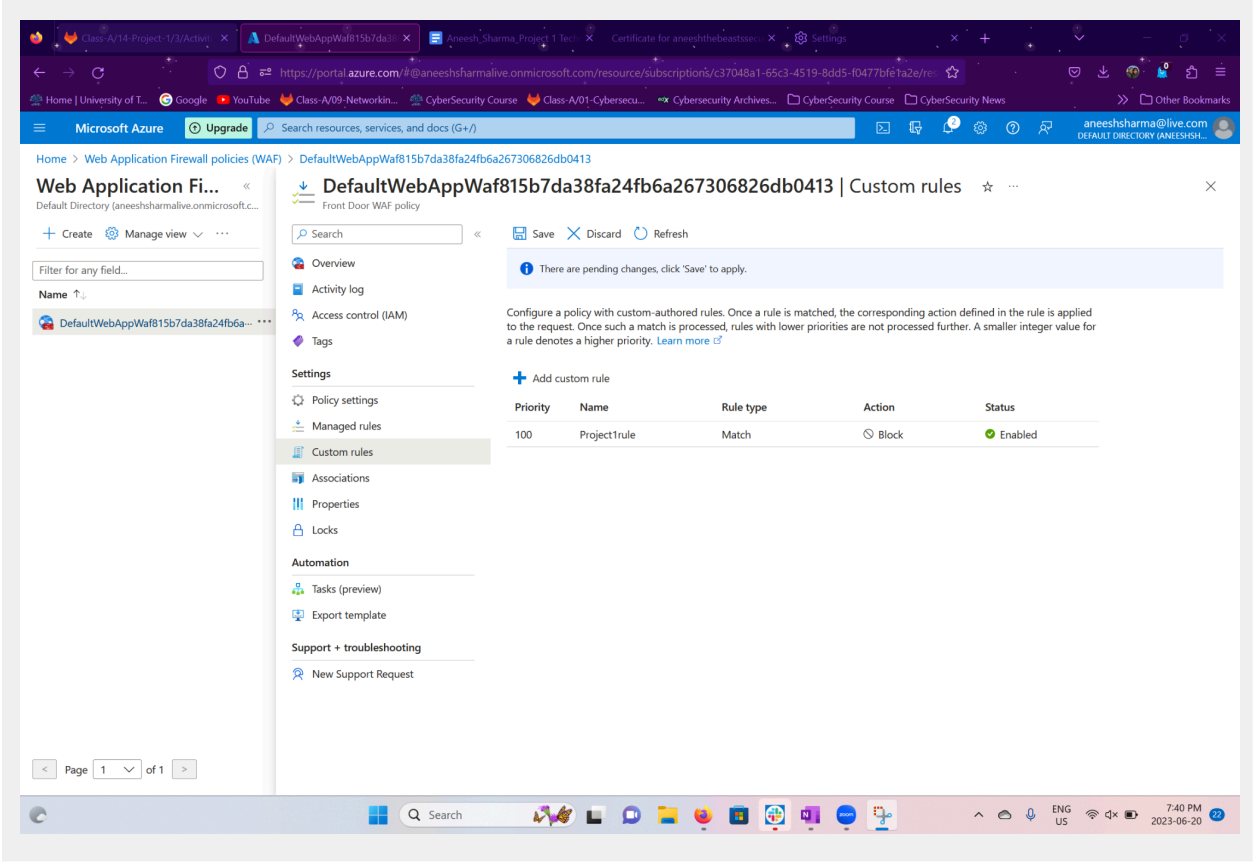
```
No, this wouldn't be true because the WAf rule is blocking Canadian
addresses, but there is no way to check if the user lives in Canada. The
individuals could be using a VPN to mask their IP address.
```

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.*
- *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.*