Cybersecurity

Project 1 Technical Brief

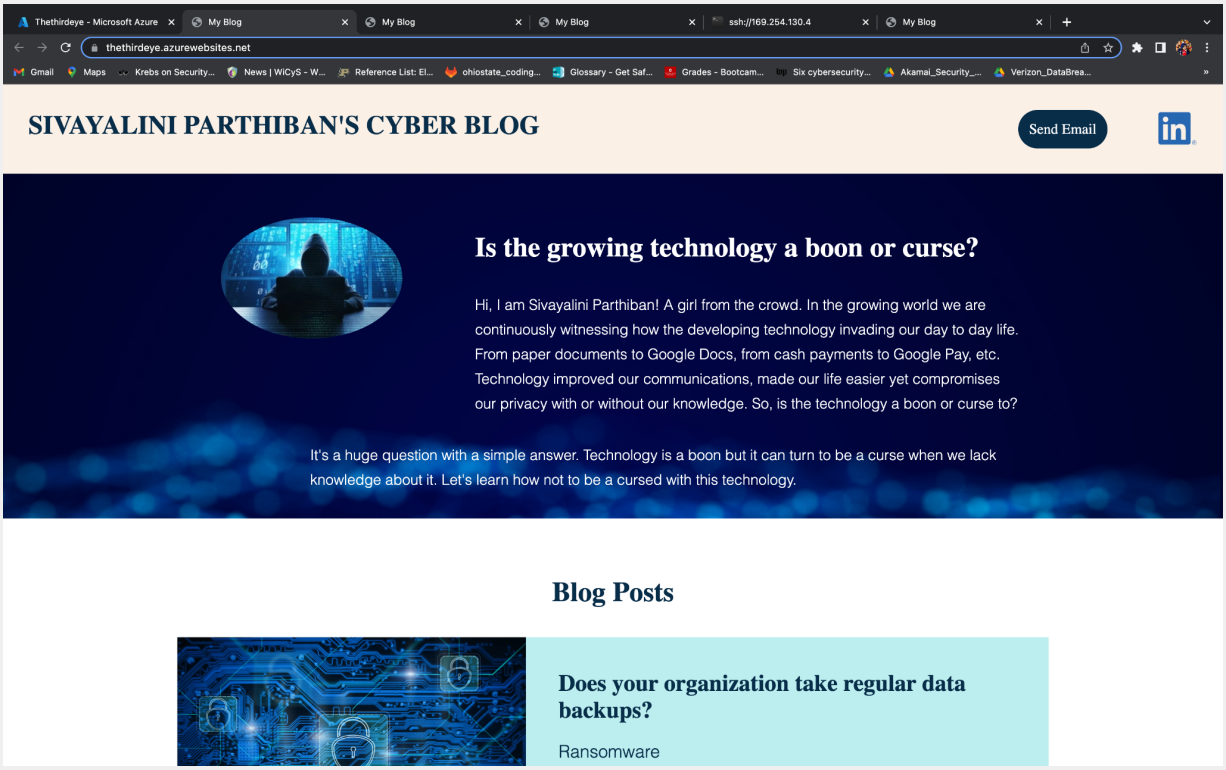
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

https://thethirdeye.azurewebsites.net

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


Thethirdeye - Microsoft Azure
My Blog
My Blog
My Blog
ssh://169.254.130.4
My Blog
thethirdeye.azurewebsites.net
Gmail
Maps
Krebs on Security...
News | WiCyS - W...
Reference List: El...
ohiostate_coding...
Glossary - Get Saf...
Grades - Bootcam...
Six cybersecurity...
Akamai_Security_...
Verizon_DataBrea...
SIVAYALINI PARTHIBAN'S CYBER BLOG
Send Email
Is the growing technology a boon or curse?
Hi, I am Sivayalini Parthiban! A girl from the crowd. In the growing world we are continuously witnessing how the developing technology invading our day to day life. From paper documents to Google Docs, from cash payments to Google Pay, etc. Technology improved our communications, made our life easier yet compromises our privacy with or without our knowledge. So, is the technology a boon or curse to?
It's a huge question with a simple answer. Technology is a boon but it can turn to be a curse when we lack knowledge about it. Let's learn how not to be a cursed with this technology.
Blog Posts
Does your organization take regular data backups?
Ransomware

Thethirdeye - Microsoft Azure | My Blog | My Blog | My Blog | ssh://169.254.130.4 | My Blog

thethirdeye.azurewebsites.net

Gmail Maps Krebs on Security... News | WiCyS - W... Reference List: El... ohiostate_coding... Glossary - Get Saf... Grades - Bootcam... Six cybersecurity... Akamai_Security_... Verizon_DataBrea...

Blog Posts

Does your organization take regular data backups?

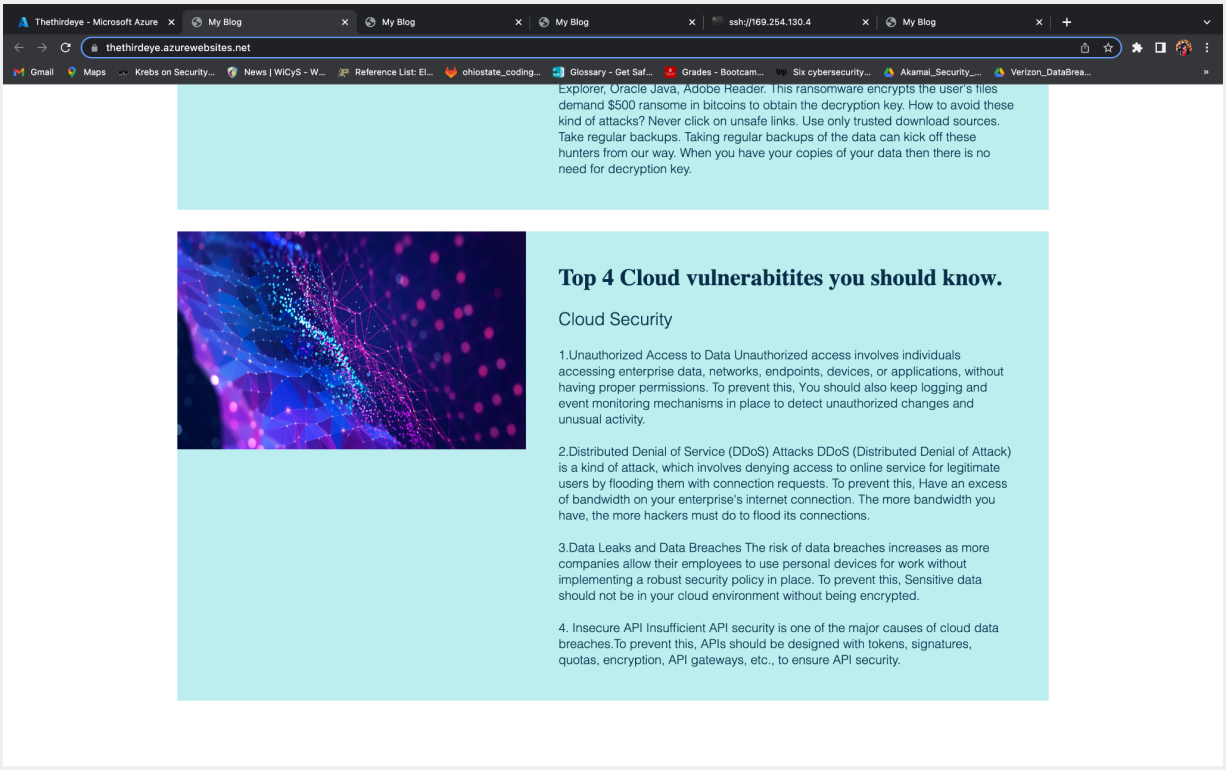
Ransomware

What is ransomware? Ransomware is a malicious software that blocks the system access, then encrypts the files or system untill the victim pays the ransome in exchange of the decryption key. This malicious software can enter your system through emails, pop-ups, messages, etc. TeslaCrypt is the popular ransomware discovered in the beginning of the 2015. It was spread by the Angular and Nuclear browser exploit kits. Exploit kits are efficient tools for cybercriminals to distribute thier malware. These kits patched vulnerabilities in web technologies like Internet Explorer, Oracle Java, Adobe Reader. This ransomware encrypts the user's files demand $500 ransome in bitcoins to obtain the decryption key. How to avoid these kind of attacks? Never click on unsafe links. Use only trusted download sources. Take regular backups. Taking regular backups of the data can kick off these hunters from our way. When you have your copies of your data then there is no need for decryption key.

Top 4 Cloud vulnerabitites you should know.

Cloud Security

1.Unauthorized Access to Data Unauthorized access involves individuals accessing enterprise data, networks, endpoints, devices, or applications, without having proper permissions. To prevent this, You should also keep logging and event monitoring mechanisms in place to detect unauthorized changes and unusual activity.



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?

```
thethirdeye
```

Networking Questions

1. What is the IP address of your webpage?

```
20.49.104.34
```

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

```
East US
```

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

```
Server:192.168.0.1
Address:192.168.0.1#53

Non-authoritative answer:
thethirdeye.azurewebsites.net canonical name =
waws-prod-blu-249.sip.azurewebsites.windows.net.
waws-prod-blu-249.sip.azurewebsites.windows.net canonical name =
waws-prod-blu-249-ce93.eastus.cloudapp.azure.com.
Name: waws-prod-blu-249-ce93.eastus.cloudapp.azure.com
Address: 20.49.104.34
```

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 stack defines the technology stack used to develop the app.Its is
Backend.
```

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

```
It has css and images which used for styling the 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 is essentially a customer who purchases cloud computing
resources. This could be an individual user, a group of users, or an entire
department or company.
```

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

```
A key vault access policy is important because it grants the azure app
subscription access to the key vaults. It determines whether a given
Security principal can perform different operations on key Vault secrets,
keys and certificates.
```

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

```
Secrets:It provides secure storage of passwords and database connection
strings.
Certificates: It provides information about the source of certificates
issuer, credentials and other details. It supports certificates that are
built on top of other features of key vault like keys and secrets and add an
automated renewal.
Keys: Cryptographic material is imported/generated when a service requests
the key vault into Key Vault.An authorized cloud service can request the key
Vault perform one or more cryptographic operations with a key on its behalf.
```

Cryptography Questions

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

- It is free, fast and easy to use.

- They are suitable for internal network websites and development or testing environments.
- Encryption and decryption of the data is done with the same ciphers used by paid SSL certificates.

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

- Self-signed certificates aren't trusted by browsers because they are generated by our own server. You can tell if a certificate is self-signed if a CA is not listed in the issuer field.
- SSL certificates are difficult to revoke.
- SSL certificates never expire.

3. What is a wildcard certificate?

Using wildcard certificate we can secure an unlimited number of subdomains pertaining to the same base domain. A SSL/TLS Wildcard certificate is a single certificate with a wildcard character (*) in the domain name field.

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.

Microsoft completely disabled SSL 3.0 in Azure Websites by default since to protect its customers from vulnerabilities.

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. It doesn't return error because the SSL certificate is active and the connection is secure.

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

12/02/2022 to 12/02/2023

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

```
No I don’t have an intermediate certificate it is a cross-signed
certificate.
```

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

```
Yes, I do have a root certificate, it is a self signed certificate .
```

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.

```
CN=Amazon Root CA 1,O=Amazon,C=US
```

Day 3 Questions

Cloud Security Questions

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

```
Similarities and Differences:-
Layer 7 traffic can be managed by both Application gateway and front door.
Difference between both is  Front Door is a global load balancer while
Application Gateway is a regional service load balancer. Front Door is
better suited in the following situations where we can use multiple regions
within our cloud and When the priority is to route traffic to the most
efficient endpoint.
Application Gateway is better suited for those who want more control over
how traffic is balanced within the same region. We can write rules to
control how application gateway distributes traffic within a regional
environment. It helps when we need to load balance between individual
virtual machines.

We can create an Application Gateway and Front Door using Azure Portal.
```

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

```
SSL offloading helps with encryption/decryption process on a separate SSL proxy device placed between the browser and the server and so it won’t affect the web server’s performance. The SSL offloading device is known as the application-specific integrated circuit processor, a proxy or a load balancer.

Data is not compromised because the data is encrypted during the transmission process.
Server is not compromised, it helps server by saving it from common web application attacks.
```

3. What OSI layer does a WAF work on?

```
Layer 7
```

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

```
HTTP response splitting is a form of web application vulnerability, resulting from the failure of the application or its environment. It occurs when data enters a web app through an untrusted source or when a HTTP response header sent to a web user is not validated for malicious characters. It can be used to perform cross site scripting attacks, cross-user defacement, web cache poisoning, and similar exploits.

WaF HTTP response splitting rules protect the web app from this attack.
```

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, It could impact the site even if the front door is enabled or not, because the front door provides fast, reliable, and secure access between
```

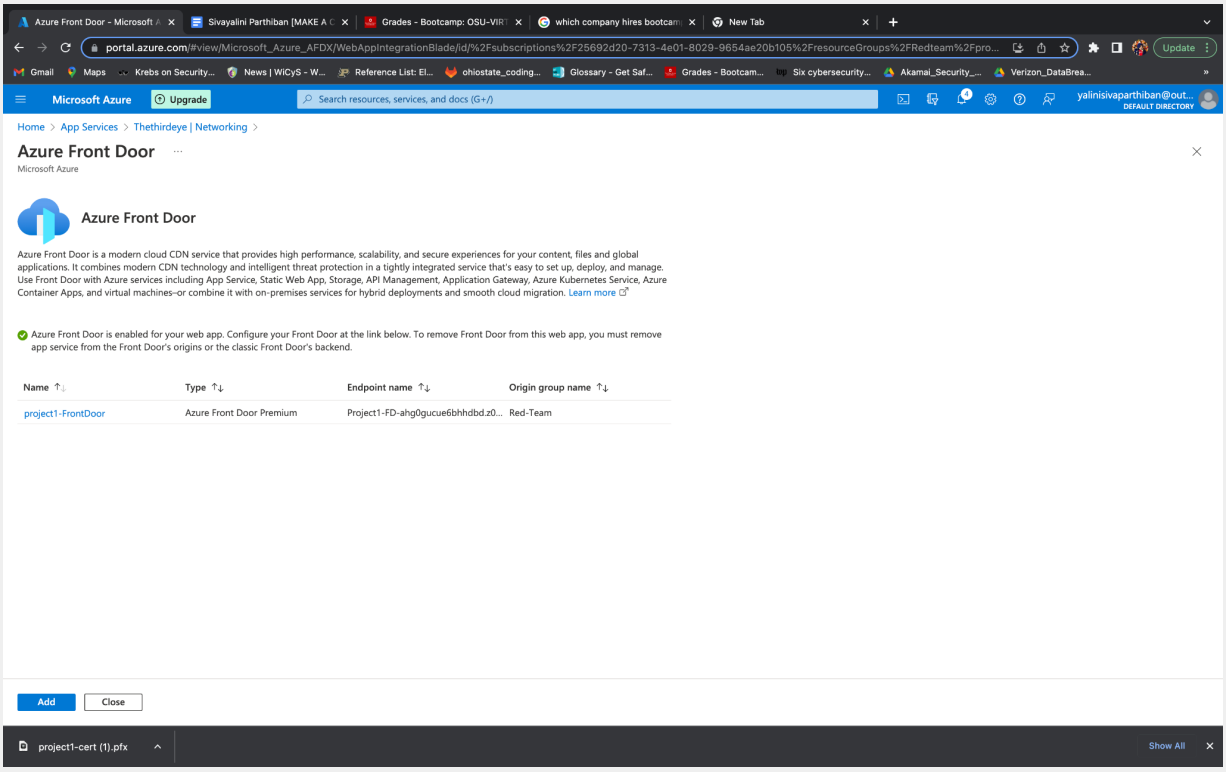
your users and your applications static and dynamic web content across the globe but it can’t block the website from the HTTP response splitting attack.

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?

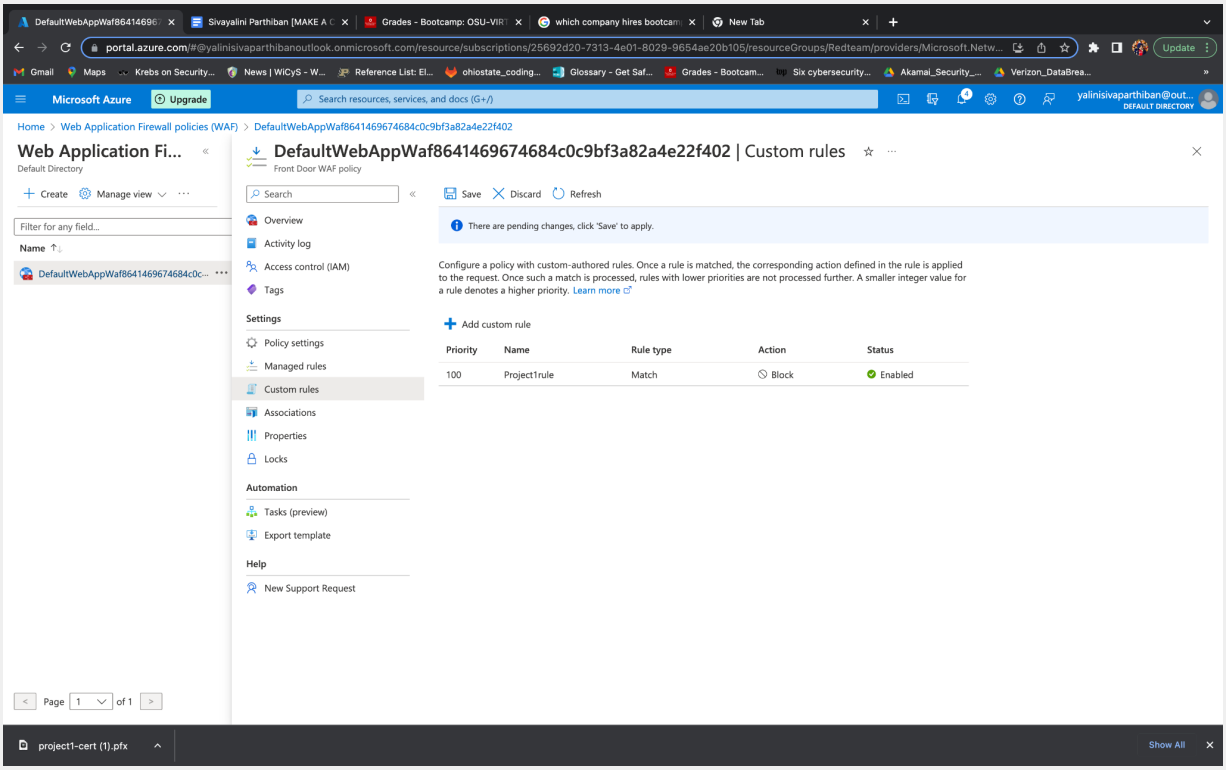
Yes,anyone from canada can’t access the site if it blocks all the traffic from canada unless they hide their identity using vpn.

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. YES*