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.

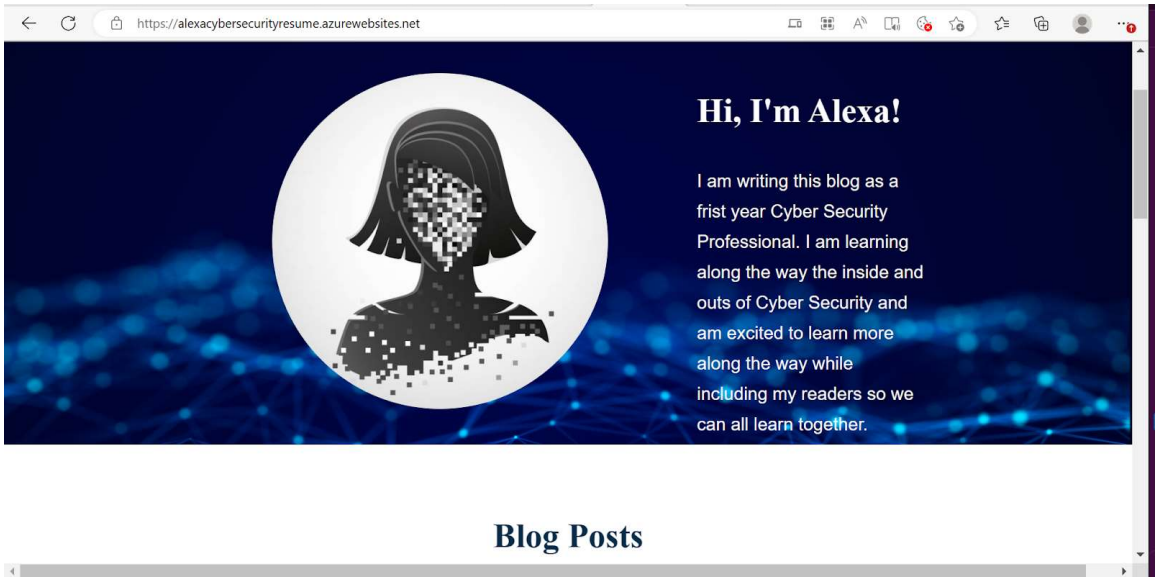
Your Web Application

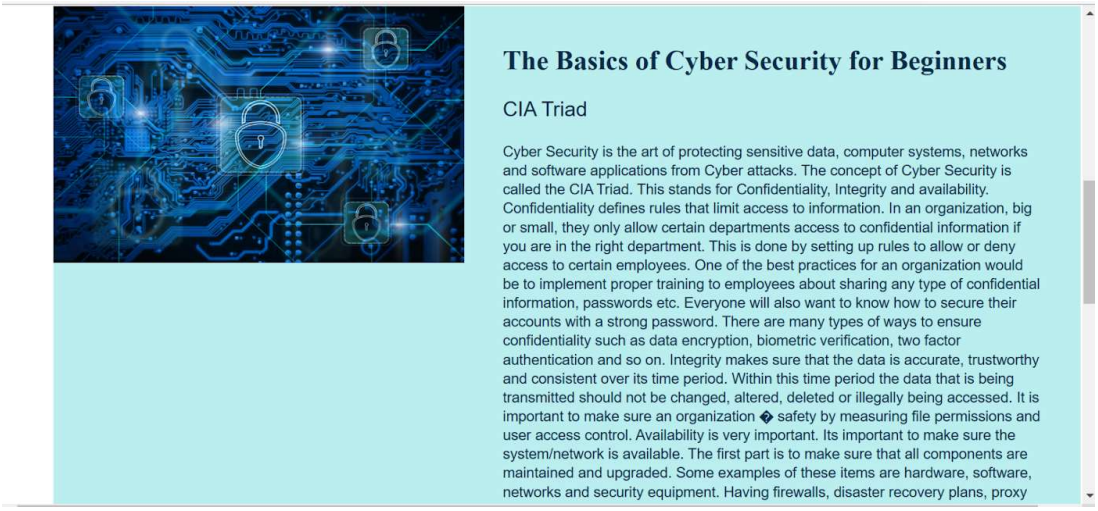
Enter the URL for the web application that you created:

My Resume (alexacybersecurityresume.azurewebsites.net)

SOURCES FOR BLOG: Top Cybersecurity Threats [2023] (sandiego.edu)
An Introduction to Cyber Security Basics for Beginner (geekflare.com)

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


https://alexacybersecurityresume.azurewebsites.net
Hi, I'm Alexa!
I am writing this blog as a frist year Cyber Security Professional. I am learning along the way the inside and outs of Cyber Security and am excited to learn more along the way while including my readers so we can all learn together.
Blog Posts


The Basics of Cyber Security for Beginners
CIA Triad
Cyber Security is the art of protecting sensitive data, computer systems, networks and software applications from Cyber attacks. The concept of Cyber Security is called the CIA Triad. This stands for Confidentiality, Integrity and availability. Confidentiality defines rules that limit access to information. In an organization, big or small, they only allow certain departments access to confidential information if you are in the right department. This is done by setting up rules to allow or deny access to certain employees. One of the best practices for an organization would be to implement proper training to employees about sharing any type of confidential information, passwords etc. Everyone will also want to know how to secure their accounts with a strong password. There are many types of ways to ensure confidentiality such as data encryption, biometric verification, two factor authentication and so on. Integrity makes sure that the data is accurate, trustworthy and consistent over its time period. Within this time period the data that is being transmitted should not be changed, altered, deleted or illegally being accessed. It is important to make sure an organization safety by measuring file permissions and user access control. Availability is very important. Its important to make sure the system/network is available. The first part is to make sure that all components are maintained and upgraded. Some examples of these items are hardware, software, networks and security equipment. Having firewalls, disaster recovery plans, proxy

servers and a proper backup solution will help when it comes to Denial of Service (DoS) attacks.

Common Cyber Treaths/Attacks in 2023

Attacks, Threats

As technology improves so do the Cyber Threats/Attacks. In this section we will be talking about some of the Cyber threats/attacks in 2023. It may seem like you know how to prevent these attacks that are being listed but the hackers are getting smarter. Phishing attacks are when an email is sent to you that looks legitimate but when you click on it that email for example what happens is that you end up clicking a link that goes back to the attackers computer and they are now able to access your information and will end up getting access to the organizations network and systems.. Employers in most organizations set up annual training around these different types of attacks. Hackers are aware that these training's are happening which makes them come up with different ways to conduct phishing attacks. Cyber-Physical Attacks are where the hackers are targeting physical places/objects. For Example there is an ongoing threat where water treatment facilities, electrical grids, transportation systems etc. are being targeted. The next type of vulnerability is Privacy Concerns with connected cars and semi-automated vehicles. With

talking about some of the Cyber threats/attacks in 2023. It may seem like you know how to prevent these attacks that are being listed but the hackers are getting smarter. Phishing attacks are when an email is sent to you that looks legitimate but when you click on it that email for example what happens is that you end up clicking a link that goes back to the attackers computer and they are now able to access your information and will end up getting access to the organizations network and systems.. Employers in most organizations set up annual training around these different types of attacks. Hackers are aware that these training's are happening which makes them come up with different ways to conduct phishing attacks. Cyber-Physical Attacks are where the hackers are targeting physical places/objects. For Example there is an ongoing threat where water treatment facilities, electrical grids, transportation systems etc. are being targeted. The next type of vulnerability is Privacy Concerns with connected cars and semi-automated vehicles. With technology improving so are cars. They are starting to make all electrical cars and working on driver-less ones as well. It was estimated that by 2020 90% of new cars will be connected to the internet. For hackers this means another opportunity to steal sensitive data and harm drivers. This is done by exploiting vulnerabilities in the insecure system. We will see an increase in the number of connected cars and in the number and severity of system vulnerabilities as manufacturers rush to market with the high-technology automobiles.

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?

My Resume (alexacybersecurityresume.azurewebsites.net)

Networking Questions

1. What is the IP address of your webpage?

```
alexa@DESKTOP-TF4DFTH MINGW64 ~
$ nslookup alexacybersecurityresume.azurewebsites.net
Server:  modem
Address:  192.168.0.1

Non-authoritative answer:
Name:    waws-prod-blu-373-0ed5.eastus.cloudapp.azure.com
Address:  20.119.0.23
Aliases:  alexacybersecurityresume.azurewebsites.net
          waws-prod-blu-373.sip.azurewebsites.windows.net
```

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

```
Tappahannock, Virginia, United States
```

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

```
alexa@DESKTOP-TF4DFTH MINGW64 ~
$ nslookup alexacybersecurityresume.azurewebsites.net
Server:  modem
Address:  192.168.0.1

Non-authoritative answer:
Name:    waws-prod-blu-373-0ed5.eastus.cloudapp.azure.com
Address:  20.119.0.23
Aliases:  alexacybersecurityresume.azurewebsites.net
          waws-prod-blu-373.sip.azurewebsites.windows.net
```

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 8.0

Backend

SOURCE: PHP, .NET, JAVA, Backend Technologies Development (openxcell.com)
```

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

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

```
Front End

SOURCE:The Difference Between Front-End vs. Back-End | ComputerScience.org
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
The sharing of computing resources in a private or public environment that
```

```
is isolated from other users and kept secret

Source: Google
```

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

```
This determines whether a given security principal, namely a user,
application or user group can perform different operations on Key Vault
secrets, keys and certificates

Source: Google
```

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

```
Keys:in Azure key vault an RSA or an Elliptic Curve (EC) key which are both
asymmetric algorithms.

Secrets: is anything thats sensitive that not an asymmetric key or a
certificate such as An 256-bit AES symmetric key, a database connection
string and kubernetes secret and an application token

Certificates: the job of a certificate is to bind a name to a public key

Source: The Relationship Between Keys, Secrets and Certificates in Azure Key
Vault | Michael's Security Blog (michaelhowardsecure.blog)
```

Cryptography Questions

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

```
Opportunity for unlimited certificate generation.
No payment required for the signature
Quick initiation. No need to pend the response of the certification center

Source: Google
```

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

```
User personal data set at risk  Source: Google
Permanent “unknown publisher” warning
Data security is not guaranteed
Lack of user trust resulted from the absence of a certification center signature
Possible errors in the certificate appearance and displaying in case it failed to be generated correctly.

Source: How to create self-signed SSL certificate and why you need it (serpstat.com)
```

3. What is a wildcard certificate?

```
A public key certificate which can be used with multiple sub-domains of a domain. The principal use for securing web sites with HTTPS but are also applications in many other fields.

Source: Google
```

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.

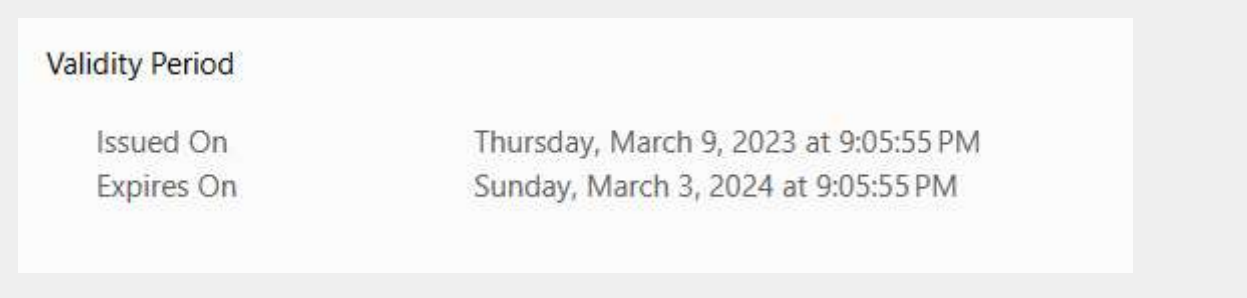
```
This is to ensure the safety of users. Microsoft completely disabled SSL 3.0 in Azure Websites by default to protect customer from the vulnerability.

Source: Google
```

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
```

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



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

```
No- because we are using the free domain
```

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

```
Yes because we are using azurewebsites.net certificate
```

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

```
For some reason i do not see it listed and im not sure what happened
```

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

```
Secure Trust CA
```

Day 3 Questions

Cloud Security Questions

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

Similarities: both support session affinity

Azure Web Application Gateway: can direct affinitize the traffic to the same server within the cluster

Azure Front Door:can direct subsequent traffic from a user session to the same cluster or backend in a given region

SOURCE: Azure Front Door - Frequently asked questions | Microsoft Learn

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

SSL Offloading: the process of removing the SSL-based encryption from incoming traffic to relieve a web server of the processing burden of decrypting and/or encrypting traffic sent via SSL.

Benefits: the SSL offloader unit offlaods the SSL handshaking tasks that bog down the computing power of the web application. 2. The device completes the handshaking of the SSL quicker than the web server. 3. It may also help aid in HTTPS inspection, reverse proxy, traffic control and persistence of cookies, etc. this will depend on what kind of SSL load balancer you have installed at your end.

SOURCE for SSL Offloading: What is SSL Offloading? | F5

SOURCE for benefits: Benefits of Offloading SSL (certs) on F5 Devices, and How to Automate it (appviewx.com)

3. What OSI layer does a WAF work on?

Layer 7

Source: What is a WAF? | Web Application Firewall explained | Cloudflare

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

Directory Traversal: a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files. This is also known as a path traversal.

SOURCE:Directory Traversal: Vulnerability and Prevention | Veracode

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?

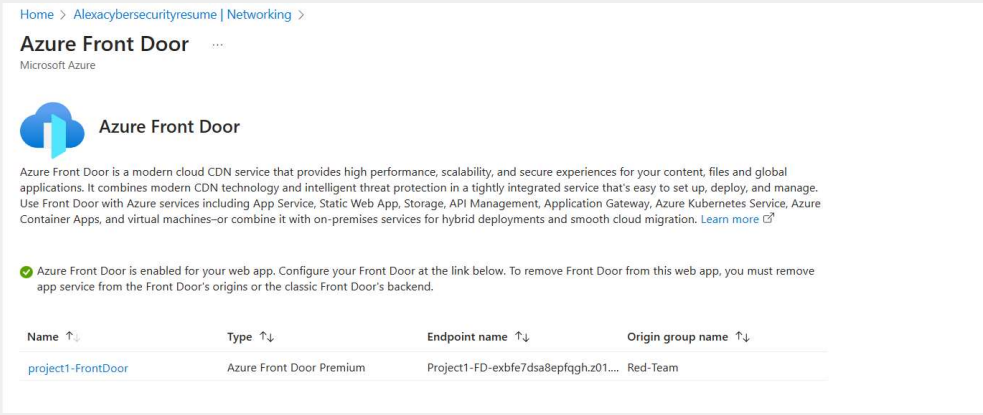
```
I believe it wouldn't necessarily be a threat as my website wouldnt contain
any documents that are important or and stored user names/passwords.
```

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?

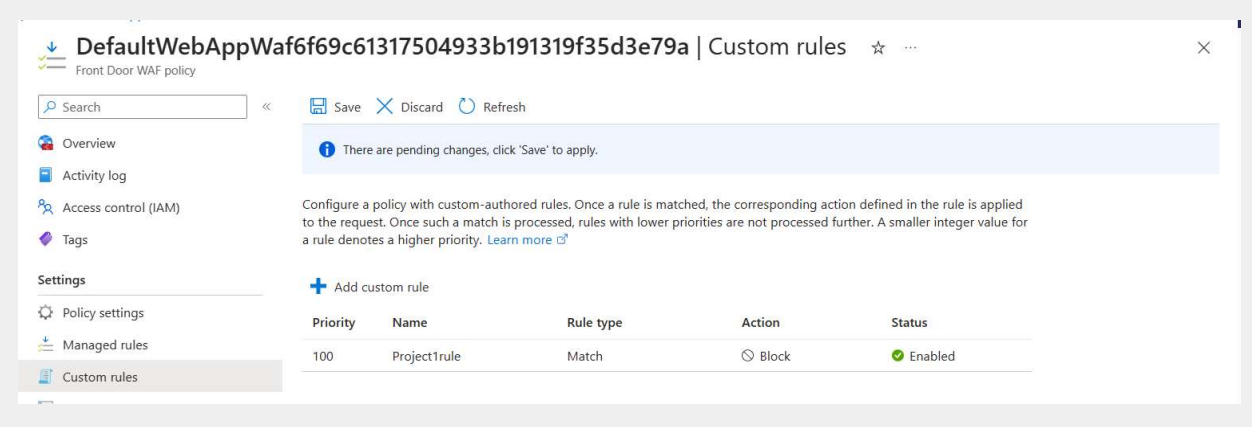
```
No because it will only block Canadian IP addresses- there is no way to know
if the person resides in Canada they can only go based off of IP addresses.
```

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*

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.