Cybersecurity

Azure-Based Web Infrastructure Enhancement

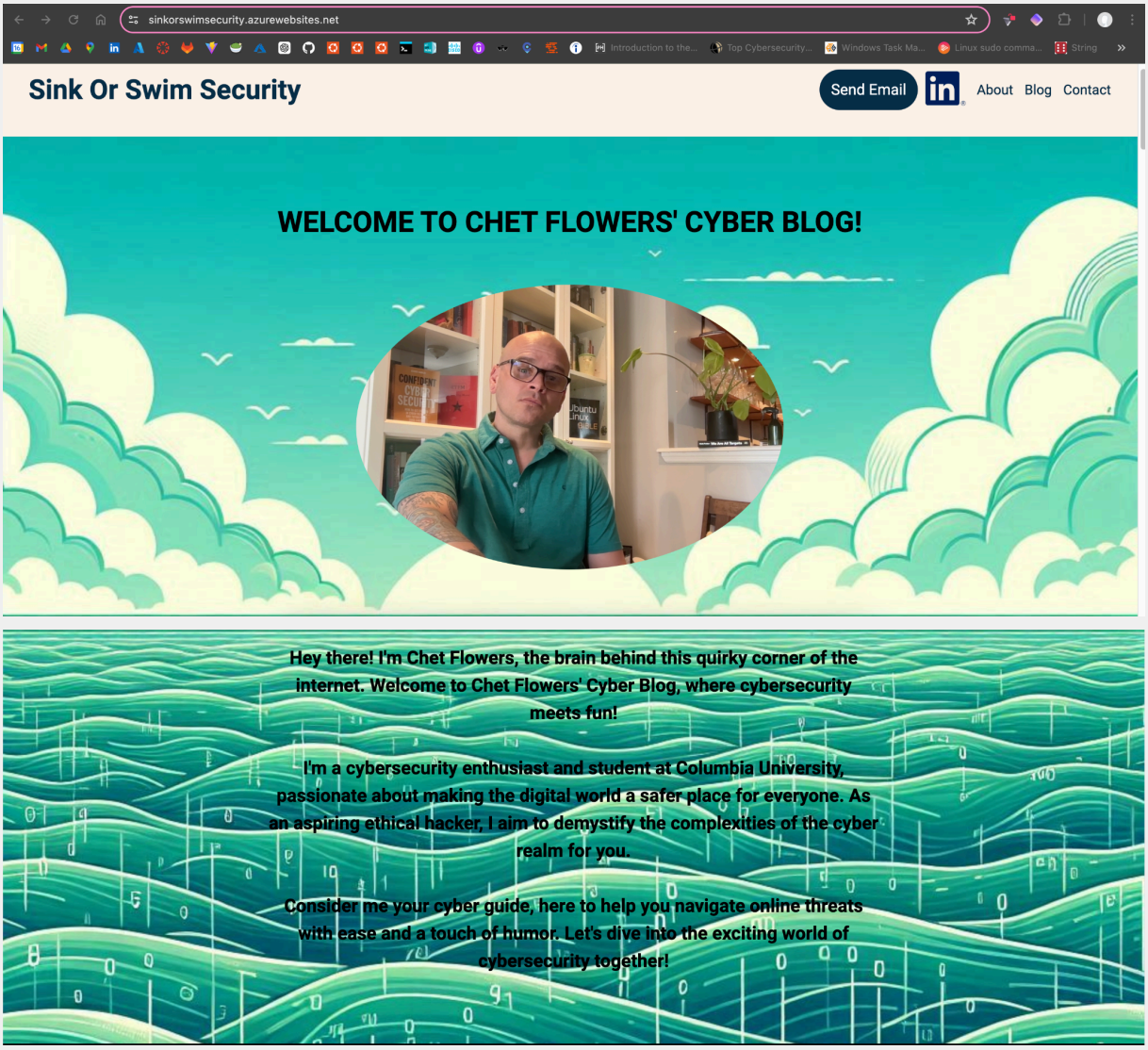
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

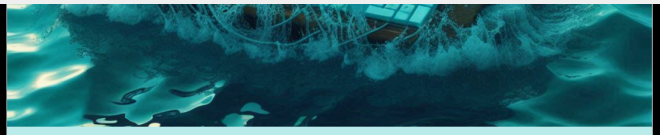
Enter the URL for the web application that you created:

```
https://sinkorswimsecurity.azurewebsites.net/
```

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


sinkorswimsecurity.azurewebsites.net
Sink Or Swim Security
Send Email
About
Blog
Contact
WELCOME TO CHET FLOWERS' CYBER BLOG!
Hey there! I'm Chet Flowers, the brain behind this quirky corner of the internet. Welcome to Chet Flowers' Cyber Blog, where cybersecurity meets fun!
I'm a cybersecurity enthusiast and student at Columbia University, passionate about making the digital world a safer place for everyone. As an aspiring ethical hacker, I aim to demystify the complexities of the cyber realm for you.
Consider me your cyber guide, here to help you navigate online threats with ease and a touch of humor. Let's dive into the exciting world of cybersecurity together!

BLOG POSTS



Unraveling the Mystery of Cryptography: Unlocking Secrets in Plain Sight

Cryptography - Encryption - Decryption

Hey there! Have you ever wanted to send secret messages that only you and your friend could understand? Well, cryptography is the magical art of doing just that! It's like creating a secret code, but way cooler because it involves math and technology.

Imagine you have a super-secret message you want to send to your friend across the world. You could just write it down, but what if someone intercepts it? That's where cryptography comes in. It's like putting your message in a locked box before sending it. Even if someone finds the box, they can't open it without the key.

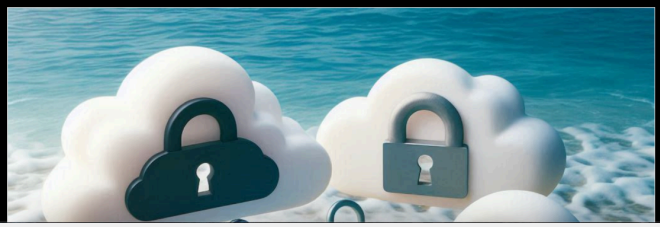
One of the most famous types of cryptography is called 'encryption.' It's like turning your message into a secret code that only the intended recipient can decode. Think of it like turning 'HELLO' into 'URYYB' using a special algorithm.

But wait, there's more! Cryptography isn't just about sending secret messages. It's also crucial for keeping your online transactions safe. Ever wonder how your credit card information stays secure when you buy stuff online? You can thank cryptography for that!

Here's a cool fact: cryptography has been around for centuries! Ancient civilizations used secret codes to communicate during wars and negotiations. Even Julius Caesar used a simple substitution cipher to send confidential messages!

Today, cryptography is more advanced than ever. We use complex algorithms and mathematical principles to keep our data safe from hackers and cybercriminals. It's like building an impenetrable fortress around our digital world.

So next time you send a message or buy something online, remember the invisible shield of cryptography that's keeping your information safe and sound. It's like having your own secret superpower in the digital age!



Navigating the Cloud: Keeping Your Data Safe and Sound

Cloud - Security - Encryption

Hey, tech-savvy pals! Let's talk about cloud security - it's like keeping your digital stuff safe in the sky!

So, what's the cloud anyway? Think of it as a virtual storage space where you can keep all your photos, documents, and cat videos. But just like your impenetrable art safe, you want to make sure it's locked up tight so no one gets sticky fingers!

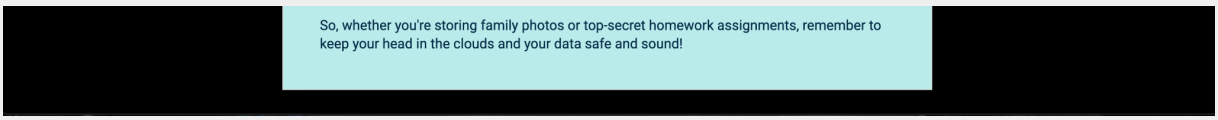
First things first, when you upload something to the cloud, it's like sending your stuff on a digital journey. It travels through the internet to reach its destination - a data center somewhere out there in the world. That's why it's super important to encrypt your data before it takes off!

Encryption is like putting your data in a magic box with a secret code only you and your pals know. So even if someone intercepts your data on its journey through cyberspace, they won't be able to peek inside without the key.

But wait, there's more! Cloud providers also use fancy security measures like firewalls and access controls to keep the bad guys out. It's like having a team of digital bodyguards protecting your precious data 24/7.

Now, let's talk about passwords. You wouldn't leave your front door unlocked, right? Well, the same goes for your cloud accounts. Make sure you use strong, unique passwords and never share them with anyone - not even your bestie!

Oh, and don't forget about backups! Just like making copies of your favorite video game, backing up your data ensures you won't lose everything if something goes wrong in the cloud.



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?

```
azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.15
```

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?

```
Server: 168.63.129.16
IP Address: 168.63.129.16#53
```

Web Development Questions

1. When creating your web app, you select a runtime stack. What was it? Does it work on the front end or the back end?

```
PHP 8.2
Back end
```

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

```
/CSS: This directory contains cascading style sheet (CSS) files used for
styling web pages. CSS is responsible for controlling the layout,
formatting, and visual appearance of HTML elements on a webpage.

/images: This directory usually contains image files used in the web
application. These images could include logos, icons, product images, or any
other graphical elements displayed on the website.
```

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 refers to an individual or organization that uses cloud
computing services provided by a cloud service provider.
```

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

```
Implementing access policies on a key vault is essential for maintaining the confidentiality, integrity, and availability of sensitive data and cryptographic keys stored within the vault, while also ensuring compliance with regulatory requirements and best security practices.
```

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

```
Keys are used for cryptographic operations, secrets are used for authentication and access control, and certificates are used for establishing identity and enabling secure communication.
```

Cryptography Questions

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

```
Self-signed certificates offer simplicity, cost-effectiveness, and flexibility.
```

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

```
Self-signed certificates' drawbacks include a lack of trust in web browsers and other applications. They are vulnerable to man-in-the-middle attacks due to a lack of validation and verification.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a type of SSL/TLS certificate that is used to secure a domain and all its subdomains with a single certificate.
```

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.

```
SL 3.0 is not provided as an option for binding certificates in Azure because it is an outdated and insecure protocol that has known vulnerabilities. SSL 3.0 uses POODLE which is a security risk to HTTP
```

```
cookies and other encrypted data. SSL 3.0 is obsolete.
```

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. The SSL was generated by Azure and is a managed certificate.
```

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

```
Issued On: Tuesday, March 12, 2024, at 9:36:42 PM
Expires On: Friday, March 7, 2025, at 8:36:42 PM
```

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

2	Sent by server	Microsoft Azure RSA TLS Issuing CA 07 Fingerprint SHA256: 724247794951c93f3e41711617e95ce143263e3196c345a1da78f6639749ec03 Pin SHA256: Mfmoi2wKbxJCpl54JB7B+PPNkO8dRO51Bpbp+Gu4aFg= RSA 4096 bits (e 65537) / SHA384withRSA

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

3	In trust store	DigiCert Global Root G2 Self-signed Fingerprint SHA256: cb3ccbb76031e5e0138f8dd39a23f9de47ffc35e43c1144cea27d46a5ab1cb5f Pin SHA256: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY= RSA 2048 bits (e 65537) /

```
SHA256withRSA
```

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

```
Yes, it is labeled “In trust store”
```

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

```
GeoTrust Global 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 services provide traffic management capabilities, such as load balancing and URL-based routing.
- Both support SSL termination to handle HTTPS traffic.
- Both services are designed to handle high traffic volumes and scale according to demand.

Differences -

- Gateway is for regional load-balancing and application delivery.
- Front Door is for global load-balancing and application delivery.
- Gateway supports URL-based routing, SSL termination, and sticky sessions.
- Front Door is more advanced in routing features such as split TCP dynamic site acceleration, and anycast protocol for the fastest delivery.
- Gateway is used with Azure Application Insights, Firewall, and Traffic Manager.
- Front Door integrates with global services like Azure CDN and Azure Traffic Manager for more complex routing scenarios.
```

2. What is SSL offloading? What are its benefits?

```
SSL Offloading (aka SSL Termination) is the process of decrypting
SSL-encrypted traffic at intermediary devices before it reaches the web
server (ie. Load Balancers, Proxy Servers or application gateways.

Benefits -
- Reduces CPU load by freeing up web servers to be able to handle more
requests. Creates faster response times.
- Management is amplified and consistent by centralizing the process on the
offloading device. Helps with updating and renewing certificates.
- New servers do not need to be configured for SSL because the offloading
device handles all the encryption/decryption, making scalability easier.
- The offloading device can include additional security features like WAF's
(Web Application Firewalls) and intrusion detection systems for extra
security. Protects against DDoS attacks.
- Centralized management can make it easier to maintain and audit policies.
```

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.

```
WAF rule 933140: PHP Injection Attack: I/O Stream Found
This rule detects instances where an I/O stream is found in network traffic,
indicating a possible attack.
PHP injection attacks involve injecting malicious PHP code into web
applications.
The rule generates an alert to notify administrators.
```

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 isn't enabled and this WAF rule isn't in place, my website
could be impacted by PHP Injection Attacks. Without the protection provided
by the WAF rule, malicious actors could exploit vulnerabilities in the
website's code that allow them to inject and execute malicious PHP code.
This could lead to various consequences such as unauthorized access, data
```

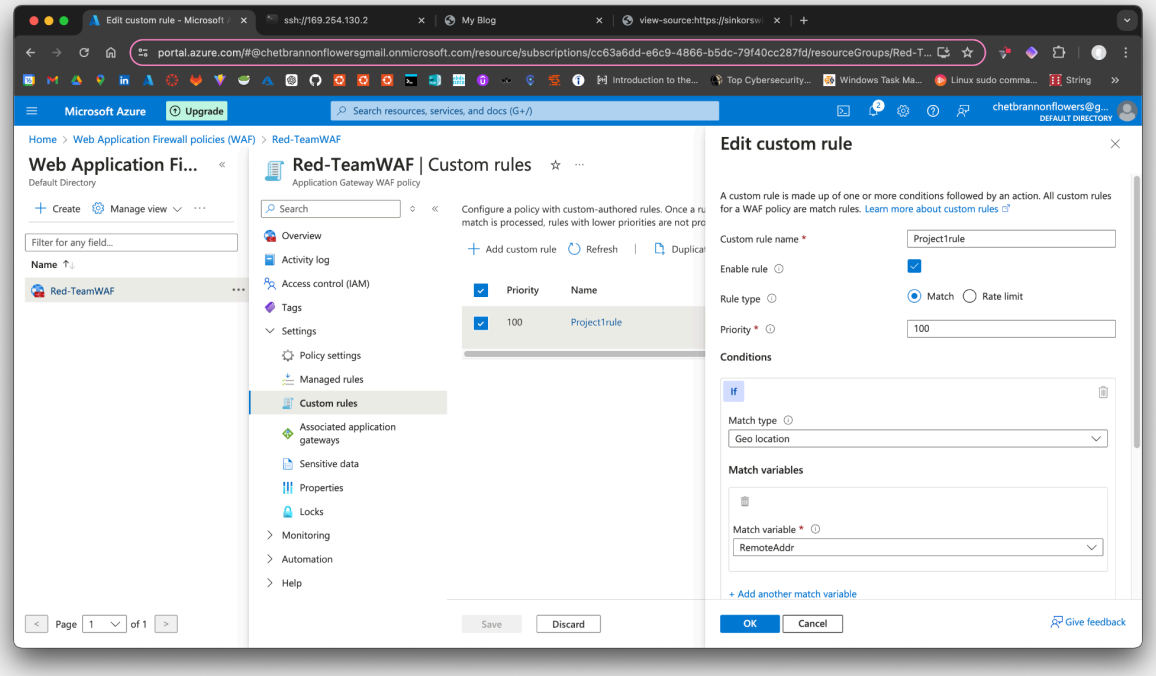
theft, data manipulation, or even complete compromise of your website and server.

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?

Using VPNs: By connecting to a VPN server in another country, users can change their apparent IP address.
Web Proxies: Using web proxies can similarly alter the perceived origin of their requests.
Mobile Networks: Users on mobile networks with dynamically assigned IP addresses might occasionally be assigned non-Canadian IPs.

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

    a. 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*