Cybersecurity

Project 1 Technical Brief

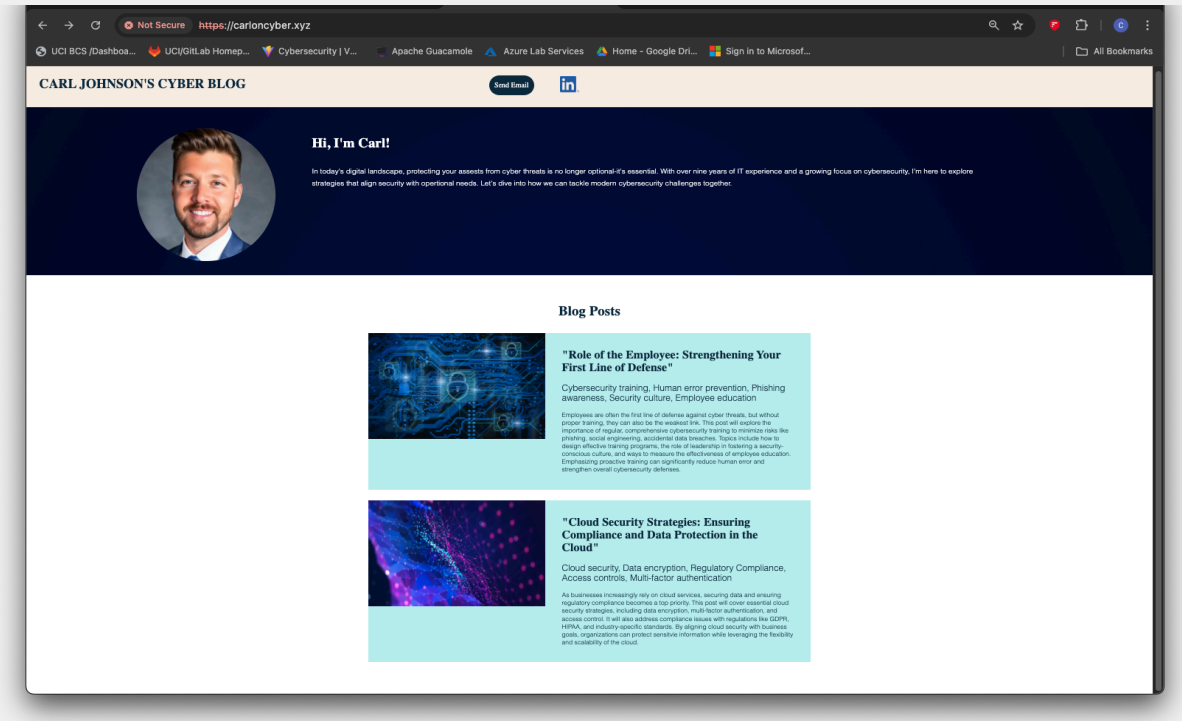
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
Carloncyber.xyz
```

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



CARL JOHNSON'S CYBER BLOG

Send Email

Hi, I'm Carl!

In today's digital landscape, protecting your assests from cyber threats is no longer optional-it's essential. With over nine years of IT experience and a growing focus on cybersecurity, I'm here to explore strategies that align security with opertional needs. Let's dive into how we can tackle modern cybersecurity challenges together.

Blog Posts

"Role of the Employee: Strengthening Your First Line of Defense"

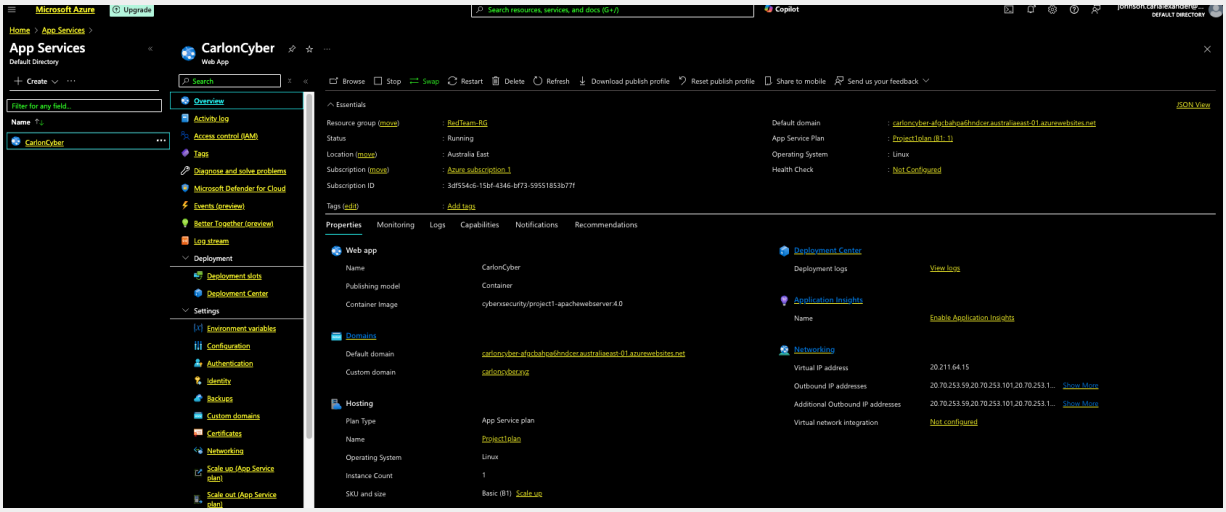
Cybersecurity training, Human error prevention, Phishing awareness, Security culture, Employee education

Employees are often the first line of defense against cyber threats, but without proper training, they can also be the weakest link. This post will explore the importance of regular, comprehensive cybersecurity training to minimize risks like phishing, social engineering, accidental data breaches. Topics include how to design effective training programs, the role of leadership in fostering a security-conscious culture, and ways to measure the effectiveness of employee education. Emphasizing proactive training can significantly reduce human error and strengthen overall cybersecurity defenses.

"Cloud Security Strategies: Ensuring Compliance and Data Protection in the Cloud"

Cloud security, Data encryption, Regulatory Compliance, Access controls, Multi-factor authentication

As businesses increasingly rely on cloud services, securing data and ensuring regulatory compliance becomes a top priority. This post will cover essential cloud security strategies, including data encryption, multi-factor authentication, and access control. It will also address compliance issues with regulations like GDPR, HIPAA, and industry-specific standards. By aligning cloud security with business goals, organizations can protect sensitvie information while leveraging the flexibility and scalability of the cloud.



Day 1 Questions

General Questions

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

```
GoDaddy domain
```

2. What is your domain name?

```
carloncyber.xyz
```

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?

```
City: Sydney, Region: New South Wales, Country: Australia
```

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

```
Non-authoritative answer:
carloncyber.xyz   nameserver = ns74.domaincontrol.com.
carloncyber.xyz   nameserver = ns73.domaincontrol.com.

Authoritative answers can be found from:
ns73.domaincontrol.com  internet address = 97.74.106.47
ns74.domaincontrol.com  internet address = 173.201.74.47
```

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?

```
The runtime stack is PHP 8.2; This means that my web application will
utilize PHP as the back-end programming language to handle
server-side logic, interact with the database, and process requests
from the front end.
```

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

```
Within the “assets” directory, there are various files that are used to
support the web application’s design and functionality. Specifically, there
are files that support visual elements, CSS file formats for font or
```

```
styling, and javascript files for functionality.
```

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

```
Based on the visual design elements, the “assets” directory works on the front end. This is because these elements are associated with presentation and the user interface.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is an organization or individual that uses cloud computing plantform’s services, such as virtual machines, storage, or software.
```

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

```
Access policy is crucial on a key vault due to various aspects, such as; Security, Management, and Policy enforcement. This can be illustrated by security access policies that ensure only authorized users and applications can access sensitive information, management access policies that can be assigned to groups of users for easier management of user permissions, and policy enforcement through the use of enforced rules such as maximum validity period of certificates.
```

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

```
within a key vault, the main differences between keys, secrets and certificates are that keys are used for encryption and decryption, secrets are managed sensitive information such as passwords, and certificates are used for secure communication and identity verification.
```

Cryptography Questions

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

```
The advantages of a self-signed certificate are that they are budget friendly as there is no cost, provide quick issuance, offer control of the creation process, can be used in testing environments, and offer no dependency on outside certification authorities.
```

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

```
The disadvantages of a self-signed certificate are that they lack trust due to inherit trust rules for browsers, no validation for the identify behind the certificate, management complexity for uploading self-signed certs, they provide limited use cases such as testing or instigate a lack of trust for an organization, and no revocation mechanism for updating certs.
```

3. What is a wildcard certificate?

```
A wildcard certification is a single certificate that has a wildcard character in the domain name field as this allows the certificate to secure multiple sub domain names pertaining to the same base domain, but only at the level that is specified with the wildcard character.
```

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 simply due to the fact that there are many vulnerabilities. For example, SSL 3.0 is susceptible to man in the middle attacks because of weak encryption. Microsoft in turn removed SSL 3.0 as a way to prompt more secure methods for users.
```

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, my web application is no longer returning an error on the certificate
```

```
because it is secured with an app managed certificate.
```

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

```
September 23, 2024 thru March 24, 2025
```

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

```
Yes, the intermediate certificate is issued by the root CA, which is
DigiCert Global Root
```

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

```
Yes, the root certificate is issued by DigiCert Global Root CA
```

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

```
Yes, Chrome has a root certificate store that lists DigiCert Global Root CA
```

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

```
Another root in the root store is Amazon Root CA
```

Day 3 Questions

Cloud Security Questions

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

```
Both Azure Web Application Gateway and Azure Front Door are Layer 7 load
balancers designed for HTTP/HTTPS traffic. While they share features like
load balancing, SSL offloading, and traffic management, they differ in scope
and purpose. WAF is regional, focused on application-level routing and
security, while Front Door is global, designed for traffic distribution and
acceleration. Front Door also offers more advanced caching and geo-routing
```

```
capabilities.
```

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

```
SSL offloading is a technique that transfers SSL encryption and decryption
from backend servers to a dedicated load balancer. This will improve
performance, reduce the load on backend servers, enhance security, and
ultimately simplify configuration. Obviously there are associated cons as
well, such as increased costs and potential for a single point of failure.
```

3. What OSI layer does a WAF work on?

```
WAF works on the OSI Application layer 7
```

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

```
SQL injection - Prevents malicious SQL code from being injected into a web
application, potentially allowing an attacker to manipulate data, steal
sensitive information or gain unauthorized access to a database.
```

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?

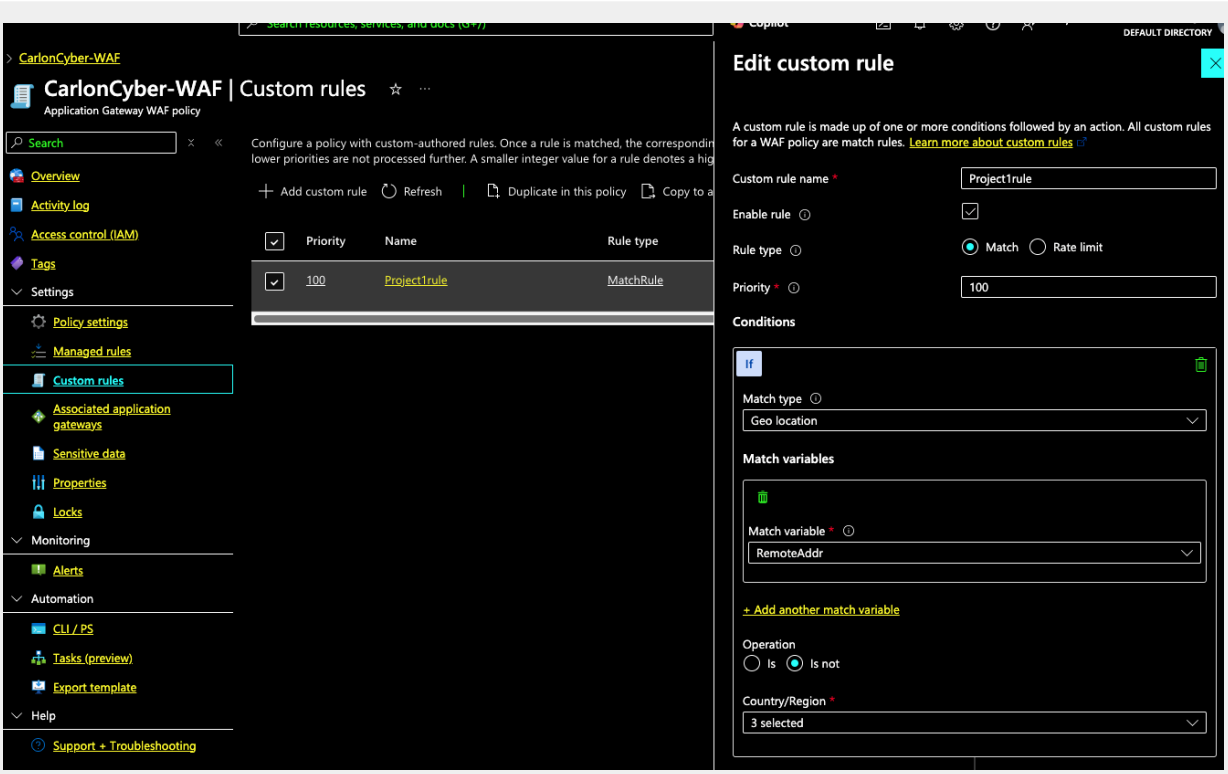
```
No, an SQL injection on my current website would not be considered
vulnerable to this type of attack because this is a static HTML website.
```

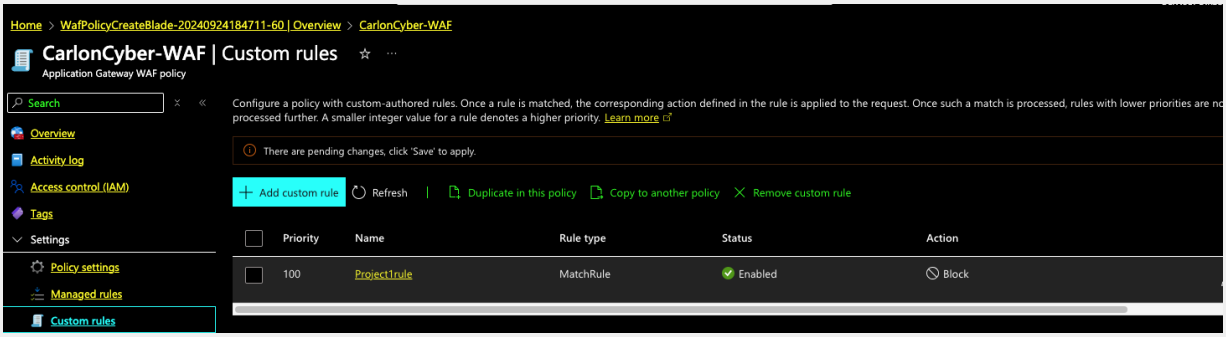
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

```
Yes, creating a custom WAF rule to block all traffic from Canada would mean
any IP residing within that country would not be able to access my website.
An alternative to reaching my site would be through the use of a VPN to mask
their Canadian IP.
```

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*