



# 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://matthewdrumondesecurityresume-bydxh0gggmh8chgn.australiaeast-01.azurewebsites.net/>

→ Decommissioned

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

## MATTHEW DRUMONDE'S CYBER BLOG

[Send Email](#)



### Hi, I'm Matthew!

I am a recent graduate of Toronto Metropolitan University, holding a Bachelor of Commerce in Business Technology Management with a 3.9 GPA. I have gained experience in areas such as cybersecurity integration, business development, and technological solutions through internships and projects. I excel at utilizing AI tools and cloud services to enhance productivity, as well as possess strong technical skills in data analysis.

## Blog Posts

## Blog Posts



### Ransomware: Should Organizations Pay or Not?

#### Ransomware

Ransomware attacks are becoming an increasing worry for groups all around the world, usually pushing them to make essential choices: should they pay or not. Paying the ransom might appear as the fastest method to get back access to coded data, but it brings big risks and moral worries. Firstly, there's no confirmation that online criminals will give back access after getting payment, which could cause possible monetary loss with resolution of the issue. Also, if you pay ransoms, it encourages attackers. This might cause more attacks and make your organization a target again in the future. Alternatively, if no payment is made it can lead to extended periods of non-functioning systems, significant financial deficits and damage to reputation when confidential data gets exposed. Enterprises need to balance the cost of system reconstruction and potential losses against ransom payments. Besides that, numerous cybersecurity professionals along with law enforcement bodies advise not paying since this could add up toward overall earnings from ransomware attacks hence inciting more culprits into participating in such actions. Instead of depending on payment for a solution, groups should put prevention first by using strong security steps like regular backups, training of employees and high-level threat finding. Good plans to respond to incidents and working with cybersecurity companies can lessen the effect if an attack happens. At the end, deciding whether or not to pay is difficult but good preparation can help organizations avoid being trapped into making that decision from the start.



## Are Humans really the weakest link in security?

### Humans, Weakest, Security

The saying, humans are the weakest link in security, is often mentioned in cybersecurity talks, but how true is it? Certainly, human mistakes contribute greatly to security breaches - via phishing tricks, weak passcodes, or wrong setups. However, putting all the fault on humans simplifies this problem too much. In fact, people can either be a risk or an asset depending upon how companies control and give power to their employees. A key cause why people are viewed as the most fragile link is due to modern security systems being so complex. If employees do not get enough training, they could unintentionally make mistakes that damage security. But, by giving regular learning opportunities, creating awareness programs and having easy-to-understand security rules, companies can greatly decrease the chance of human errors happening. Furthermore, solid security isn't only connected to technology; it is also about developing a sense of security in the culture. If workers comprehend their duty in defending the company, they can transform into an interactive part of the safeguard system by noticing phishing trials or stating doubtful activity. Conversely, pointing fingers at individuals for all breaches could dishearten employees and cause more disconnect and lower awareness regarding safety procedures. To sum up, although human mistakes contribute notably to security violations, it is overly simple to label humans as the weakest link. Given appropriate training, instruments and a culture of safety consciousness, people can change from being a threat to security into one of the most robust protectors against cyber dangers.

## 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?

<https://matthewdrumondsecurityresume-bydxh0gggmh8chgn.australiaeast-01.azurewebsites.net/>

### Networking Questions

1. What is the IP address of your webpage?

20.211.64.21

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

Sydney, Australia, New South Wales

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

ns1-06.azure-dns.com.

## 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 selected was PHP 8.2. PHP is primarily a back-end technology.

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

In my `/var/www/html/assets` directory, there are CSS files and images. The purpose of CSS files is to give style to the front end part of my web application by setting how things like texts, buttons or layouts appear to users. The images are used for creating visual aspects such as logos, icons or other graphic elements.

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

These work on the front end

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

It is essentially a virtual environment within a cloud platform's infrastructure that allows users or organizations the ability to manage their own resources securely and independently

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

It is important to a key vault because it defines and controls who has the ability to access sensitive keys, secrets, and certificates, ensuring only authorized parties can access this data

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

Keys are used for encrypting, decrypting and signing data. Secrets are arbitrary strings of sensitive info like passwords that need to be securely stored. Certificates contain public keys and are used for SSL/TLS encryption to secure communications between servers and clients. Certificates often include both a private and a public key and are basically used to authenticate identities.

## Cryptography Questions

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

The advantages of SSL certificates include being cost-effective (they are free), quick to generate (can be created instantly), full control (you created it so you manage it yourself).

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

The disadvantages of SSL certificates include lack of trust (not trusted by browsers because they are not issued by a trusted certificate authority), no identity validation (there is no third-party verification, and therefore self-signed certificates don't verify the identity of the website or organization, meaning they are vulnerable to man in the middle attacks), limited use cases (unsuitable for public-facing or production websites where trust and security are essential for users).

### 3. What is a wildcard certificate?

It is a type of SSL/TLS certificate that secures a domain and all of its subdomains with one single certificate. It uses a wildcard character to cover any subdomain under the main domain eliminating the need for a certificate for each subdomain

### 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 it is an outdated and insecure protocol, that has known vulnerabilities. This caused modern platforms to upgrade, leaving SSL 3.0 no longer supported.

### 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, as the Azure hosting site has provided this certificate for me.

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

Sunday, August 4, 2024 at 4:40:00 AM to Wednesday, July 30, 2025 at 4:40:00 AM

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

Microsoft Azure RSA TLS issuing CA 08

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

DigiCert Global Root G2

- 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.

ISRG Root X1

## Day 3 Questions

### Cloud Security Questions

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

Similarities include load balancing, SSL termination, URL-based routing, Security features, health monitoring

Differences include: Web Application Gateway in Azure is a regional Layer 7 load balancer. It's made to control traffic within one specific region of Azure and comes with functions such as path-based routing along with an integrated Web Application Firewall (WAF).

Azure Front Door acts as a worldwide traffic controller that enhances the flow of data across various regions. It provides routing based on latency, caching, and global failover for distributed applications with high performance.

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

SSL offloading is the process of decrypting SSL/TLS traffic on a dedicated device or service (e.g., load balancer, application gateway) before it reaches the backend servers, this is able to shift the burden of encryption/decryption from the servers to the device handling the offloading

Benefits: reduced server load, improved scalability, simplified certificate management, better performance, and enhanced security

### 3. What OSI layer does a WAF work on?

OSI layer 7 - the application layer where HTTP and HTTPS traffic are handled, allowing the WAF to filter incoming/outgoing web traffic

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

#### SQL Injection

SQL Injection is a kind of vulnerability in web applications. It happens when an attacker changes a query going to the database by adding harmful SQL code into entry fields. This could let the intruder circumvent authentication, obtain or alter sensitive information, get rid of it entirely and even perform administrative tasks on the database.

#### Example:

An aggressor can possibly input a sequence such as ' OR '1'='1' -- into the sign-in form. It's possible that it modifies the query to always provide true result, and thus allow improper entry.

#### WAF Protection:

A WAF identifies and stops SQL injection tries by checking incoming data for patterns or inputs that are similar to SQL injection signatures. This can include efforts to change the syntax of SQL, use frequent keywords in SQL, or incorporate special characters like quotation marks or comment signs.

### 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 the website doesn't have the right process of validating input or if it uses SQL queries that are dynamic without escaping input, it can be exposed to SQL injection. If there is no Front Door or a WAF, the safety of this site totally depends on coding practices which would have to be secure (e.g., queries with parameters). Without strong measures in place, your webpage may encounter danger; otherwise, while it could be safe enough as is - having a WAF adds an additional safeguard level.



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?

Stopping all internet requests from Canada by utilizing a personalized WAF rule doesn't automatically imply that people living in Canada can't get to your website. This is due to the fact that the WAF rule usually stops requests based on where the IP address tied with the incoming request comes from geographically.

Why someone in Canada might still access the website:

VPN or Proxy Services: For people in Canada, they can get around the block. This is possible by using a VPN or proxy service. These services send their online traffic through servers located in different countries. It then seems like they are not inside Canada.

Mobile Networks or Dynamic IPs: There may be instances where users are given IP addresses that do not accurately represent their actual location. Additionally, they might use mobile networks with registered IP addresses attributed to another area.

Edge Nodes of CDN: If a website utilizes a content delivery network (CDN), it might seem like requests are coming from the edge servers of the CDN. These could be situated in another country.

So, although the regulation can obstruct majority of Canadian IPs, it cannot assure complete prevention for all users who are physically present in Canada.

7. Include screenshots below to demonstrate that your web app has the following:
  - a. A WAF custom rule

## Add custom rule



If



Match type ⓘ

Geo location



### Match variables



Match variable \* ⓘ

RemoteAddr



+ Add another match variable

Operation



Is



Is not

Country/Region \*

3 selected



+ Add new condition


Then

Deny traffic



Add

Cancel

 Give feedback

## Add custom rule



A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. [Learn more about custom rules](#)

Custom rule name \*

Project1rule



Enable rule ⓘ



Rule type ⓘ



Match



Rate limit

Priority \* ⓘ

100



### Conditions

If



Match type ⓘ

Geo location



#### Match variables



Match variable \* ⓘ

RemoteAddr



+ [Add another match variable](#)

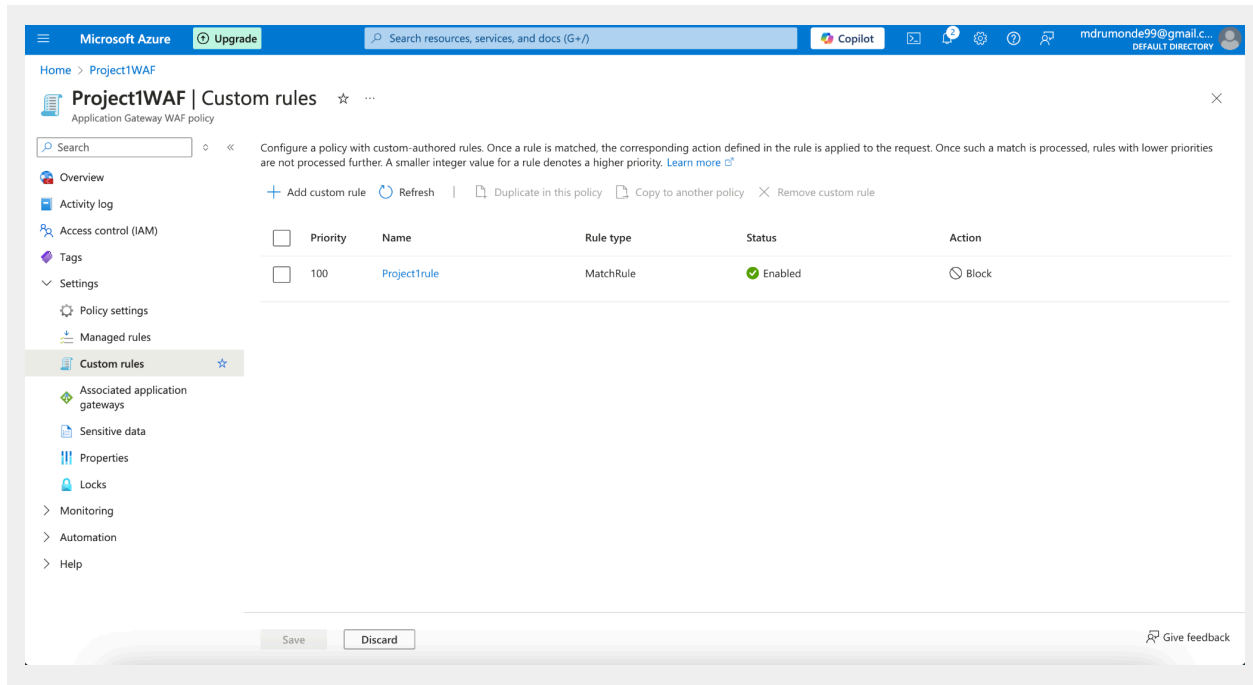
Operation

Add

Cancel



Give feedback



## 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