



# 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://josephayehankrahsecurityresume.azurewebsites.net/>

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

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Copy of [MAKE A COPY] Proj... My Blog + Mon Sep 30 7:57PM

josephayehankrahsecurityresume.azurewebsites.net

## JOSEPH ANKRAH'S CYBER BLOG

[Send Email](#)



### Hello World, I'm Joseph!

A resourceful team player offering a dynamic personality and an extensive background working in a professional office in the educational industry. Aptitude in maintaining composure, positive attitude and focus during stressful times. Willingness to learn on and off the job in the ever progressing tech industry. Eager to join forces with a multi-faceted and progressive organization.

## Blog Posts



Chrome File Edit View History Bookmarks Profiles Tab Window Help

Copy of [MAKE A COPY] Proj... My Blog + Mon Sep 30 7:57PM

josephayehankrahsecurityresume.azurewebsites.net

## Blog Posts



### Security Risks of AI technology

#### Artificial intelligence, CIA Triad

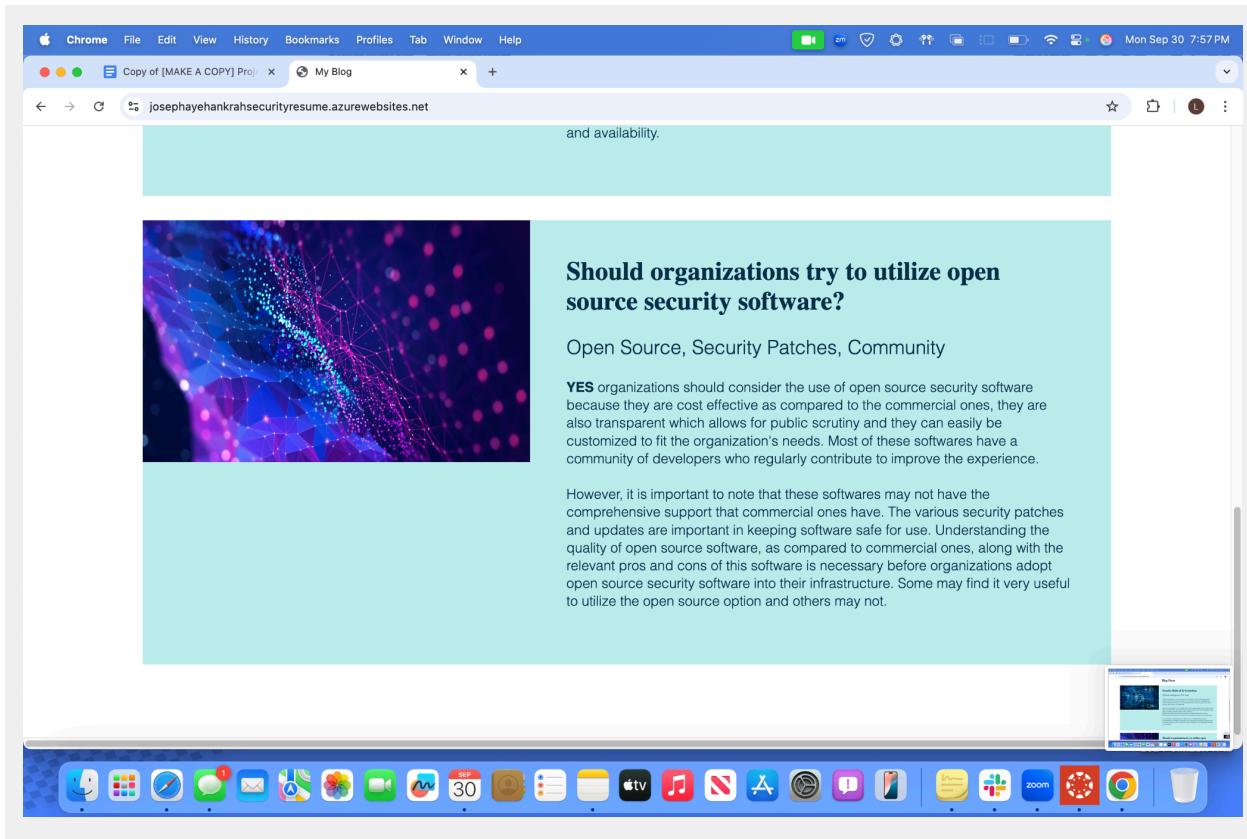
Artificial intelligence has improved a lot of industries, but with its rapid growth comes with a lot of security concerns. As AI is becoming more integrated into critical infrastructures, there is ever more awareness of the consequences these security risks pose to our daily lives.

Sensitive Data Breaches: AI models often rely on large datasets which may contain Personal Information. Data breach and unauthorized access to these datasets may lead to data theft, identity theft or other violations.  
Intellectual Property: AI may have access to valuable intellectual property. Protecting these models from breach and unauthorized access is very necessary.

As AI becomes integrated into our daily lives, it is essential that security vulnerabilities are mitigated. Individuals and businesses must have the opportunity to harness the power of AI, while ensuring we safeguard its confidentiality, integrity and availability.

Should organizations try to utilize open





## 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?

The screenshot shows the Azure portal interface for a Web App named "JosephAyehAnkrahSecurityResume". The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Microsoft Defender for Cloud, Events (preview), Better Together (preview), Deployment, Settings (with Environment variables, Configuration, Authentication, and Identity), and a search bar at the top.

The main content area is titled "Custom domains" and displays the configuration for managing custom domains assigned to the app. It includes fields for "IP address" (set to 13.70.72.33) and "Custom Domain Verification ID" (set to B328F8D5DDB2004ACC3272A8CD98AC9A7FD93DD06C05...). There are buttons for "Add custom domain", "Buy App Service domain", and "Delete". A table lists the current custom domain entry:

Custom domains	Status	Solution
josephayehankrahsecurityresume.azurewebsites.net	✓ Secured	-

The URL "josephayehankrahsecurityresume.azurewebsites.net" is also displayed at the bottom of the page.

## Networking Questions

1. What is the IP address of your webpage?

13.70.72.33

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?

```
Last login: Thu Sep 26 21:20:40 on ttys000
[josephankrah@MacBookPro ~ % nslookup -type=NS josephayehankrahsecurityresume.azurewebsites.net
Server:      2600:1702:1560:c410::1
Address:     2600:1702:1560:c410::1#53

Non-authoritative answer:
josephayehankrahsecurityresume.azurewebsites.net      canonical name = waws-pr
od-sy3-037.sip.azurewebsites.windows.net.
waws-prod-sy3-037.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-0
37.australiaeast.cloudapp.azure.com.

Authoritative answers can be found from:
australiaeast.cloudapp.azure.com
origin = ns1-06.azure-dns.com
mail addr = msnhst.microsoft.com
serial = 10001
refresh = 900
retry = 300
expire = 604800
minimum = 60

josephankrah@MacBookPro ~ %
```

No NS records available for my website but the parent domain “australiaeast.cloudapp.azure.com” has an NS record which is 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?

PHP8.2 - works on backend

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

CSS files and images for the web app. CSS defines the design and outline of the webpage.

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

Front end because the HTML outlines the webpage, the CSS designs the layout.

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

A cloud tenant is an instance of a cloud service that is dedicated to a specific customer or organization without a cloud service provider's platform.

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

It contains very sensitive and secret keys, certificates and information that may affect a company. Access policies would ensure only the right people are able to access it

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

Keys are used to access resources on a system

Certificates are used to verify and authenticate validity of a Website or a resource and also used to encrypt traffic between a client and a server

Secrets are information or data that are sensitive and need to be protected.

### Cryptography Questions

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

1. It is cost effective
2. Quick and easy to set up and implement
3. You have full control of the certificate.

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

Most browsers and applications may not trust self signed certificates. They do not provide the same level of security as the commercially issued ones.

Since it is not comparably secure, it is prone to Man-in-the-middle attacks

### 3. What is a wildcard certificate?

It is a certificate that can be used to secure multiple domains under the same root domain

### 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.

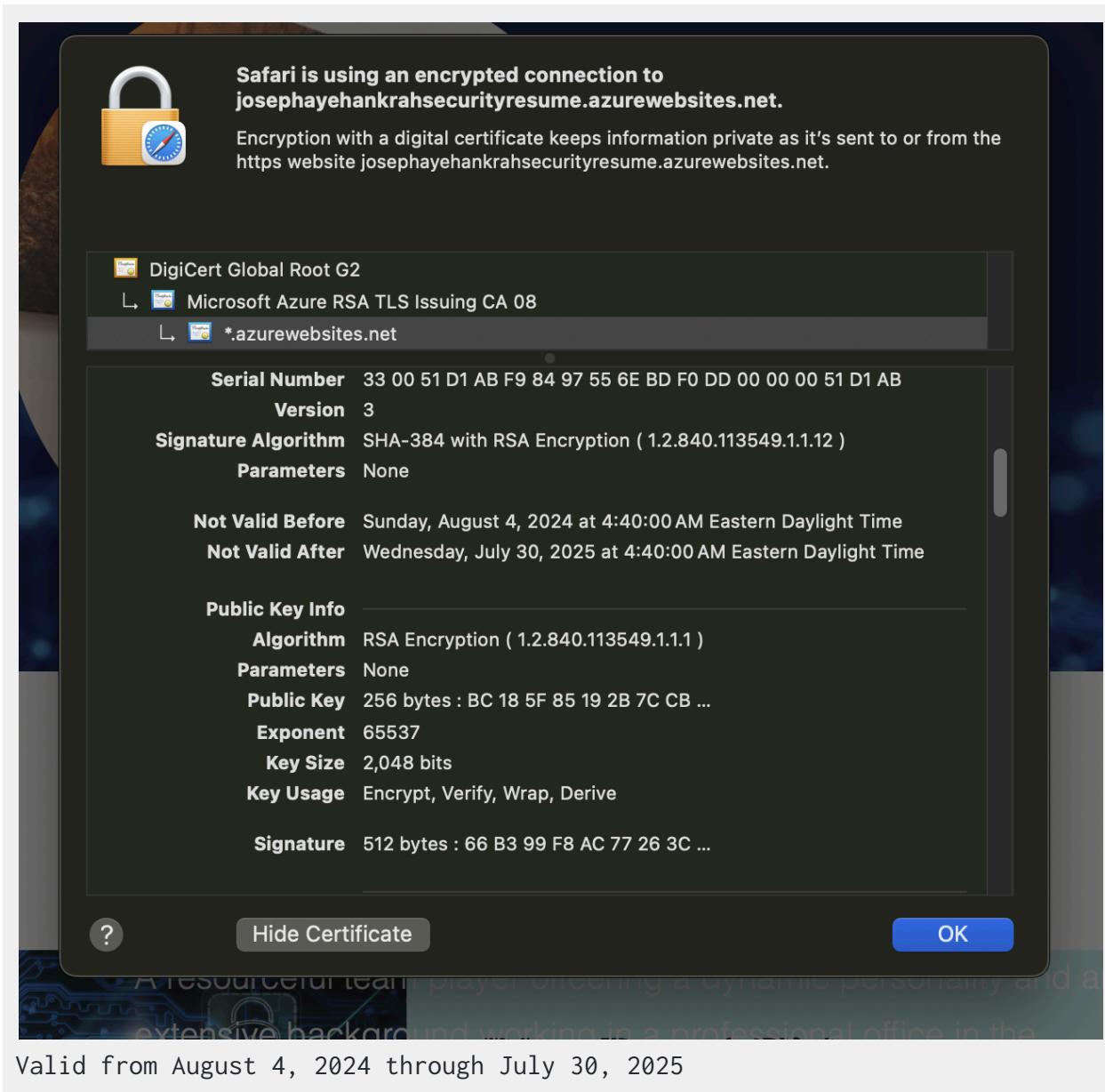
Azure does not use SSL 3.0 because of its known security vulnerabilities. POODLE (Padding oracle attack) and BEAST (Bleichenbacher's block cipher attack) can be used by an attacker to decrypt encrypted traffic over SSL 3.0

### 5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

- Is your browser returning an error for your SSL certificate? Why or why not?

No because the browser recognises the certificate as valid because it recognized the certificate provider in the root certificate store.

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



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

Microsoft Azure RSA TLS Issuing CA 08 from Microsoft

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

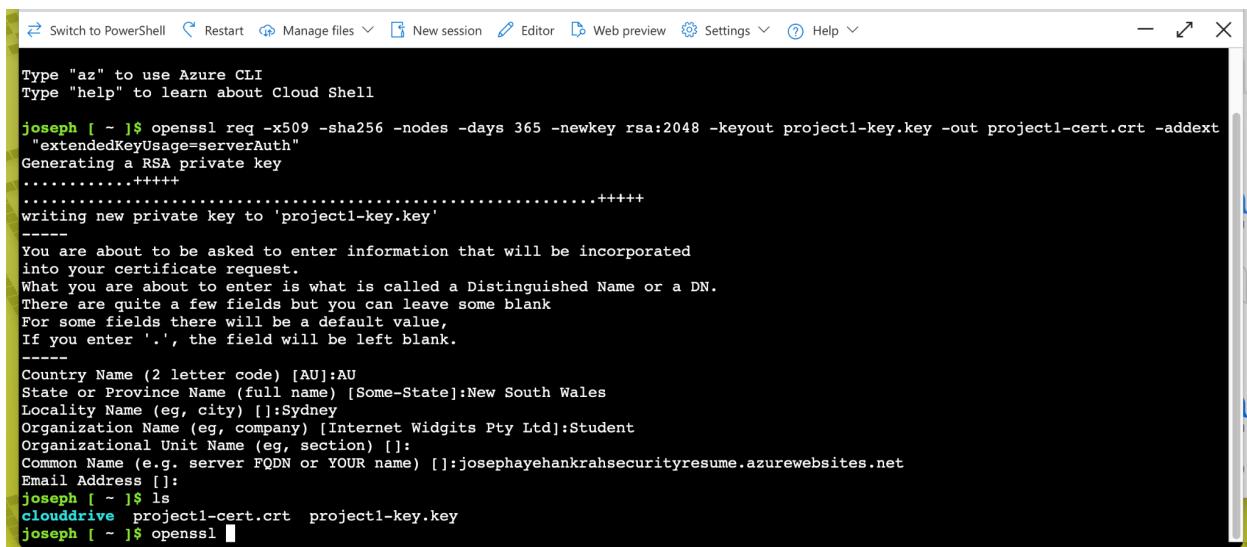
DigiCert Global Root G2. from DigiCert Inc

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

Yes it does.

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

GTS Root R1.

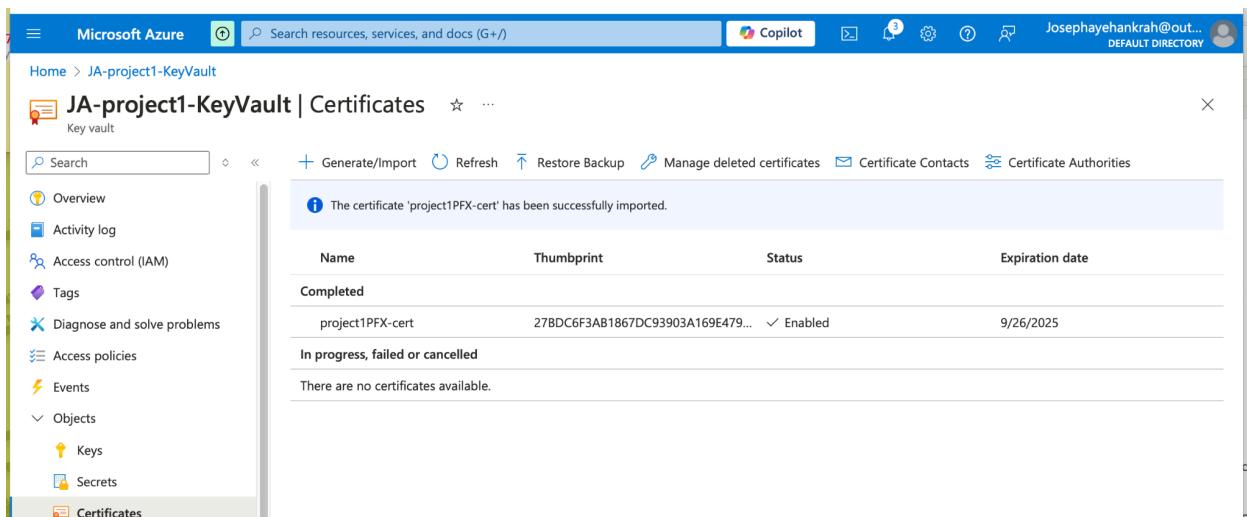


```
Switch to PowerShell Restart Manage files New session Editor Web preview Settings Help

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

joseph [ ~ ]$ openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout project1-key.key -out project1-cert.crt -addext "extendedKeyUsage=serverAuth"
Generating a RSA private key
.....+++++
writing new private key to 'project1-key.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:New South Wales
Locality Name (eg, city) []:Sydney
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Student
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:josephayehankrahsecurityresume.azurewebsites.net
Email Address []:
joseph [ ~ ]$ ls
clouddrive project1-cert.crt project1-key.key
joseph [ ~ ]$ openssl
```

## Creation of the self-signed SSL certificate



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and user information. Below the navigation bar, the URL 'Home > JA-project1-KeyVault' is visible. The main content area is titled 'JA-project1-KeyVault | Certificates'. On the left, a sidebar lists various vault management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies, Events, Objects (Keys, Secrets, Certificates), and Metrics. The 'Certificates' option is selected. A message box at the top right of the main content area states, 'The certificate 'project1PFX-cert' has been successfully imported.' Below this message, a table displays the imported certificate details:

Name	Thumbprint	Status	Expiration date
Completed			
project1PFX-cert	27BDC6F3AB1867DC93903A169E479...	✓ Enabled	9/26/2025
In progress, failed or cancelled			
There are no certificates available.			

## Uploading and adding the self-signed SSL certificate to Azure key vault

## Day 3 Questions

### Cloud Security Questions

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

They are both load balancing and traffic management services that azure offers

They are similar in a way that they both manage traffic flow, they distribute traffic across multiple backend servers to improve system performance. They also integrate well with Azure services such Azure App services and Virtual machines.

The difference is mainly on how they are individually used. Azure Web App Gateway is primarily used with web apps while the azure front door is good for both web apps and also content delivery networks.

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

It is a technique that is used to improve the performance and security of web applications by offloading processor intensive tasks of SSL or TLS ( encryption and decryption) to a hardware or software module.

It allows for the web server to focus on serving web content which massively reduces server load.

3. What OSI layer does a WAF work on?

It works at the 7th layer of the model. It inspects HTTP/HTTPS traffic and filters the unwanted packets.

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

	Action	Rule name	Anomaly score	Status	Protocol
<input checked="" type="checkbox"/>	9...	HTTP Request Smuggling Attack	9	Enable	REQUEST-921-PROTOCOL
<input type="checkbox"/>	9...	HTTP Response Splitting Attack	9	Enable	REQUEST-921-PROTOCOL

HTTP request smuggling attack: it is an attack that injects malicious requests by exploiting the vulnerabilities in a web server and application. It confuses the web server and application to expose data or to behave in an undesired way.

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 be impacted by this attack because the web app has not been hardened against such attacks. After that security rules have been configured to allow public http traffic, any attacker could exploit that.

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. It means that no one with a Canadian IP address can access my website because the rule blocks all traffic from Canada unless the person uses a vpn to access the website.

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

The screenshot shows the Microsoft Azure WAF Policy Create blade for a policy named 'Project1test'. The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, Settings (Policy settings, Managed rules, Custom rules selected), Sensitive data, Properties, Locks, Monitoring, Automation, and Help. The main area displays the 'Custom rules' configuration. A modal window titled 'Add custom rule' is open, showing the rule definition: 'Custom rule name \* Project1rule', 'Rule type Match', 'Priority \* 100', and a condition 'if Geo location RemoteAddr'. Below the modal, the main table lists one rule: 'Priority 100, Name Project1rule, Rule type MatchRule, Status Enabled, Action Block'. A message at the top of the main area says 'There are pending changes, click 'Save' to apply.'

## 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