



# Cybersecurity

## Project 1 Technical Brief

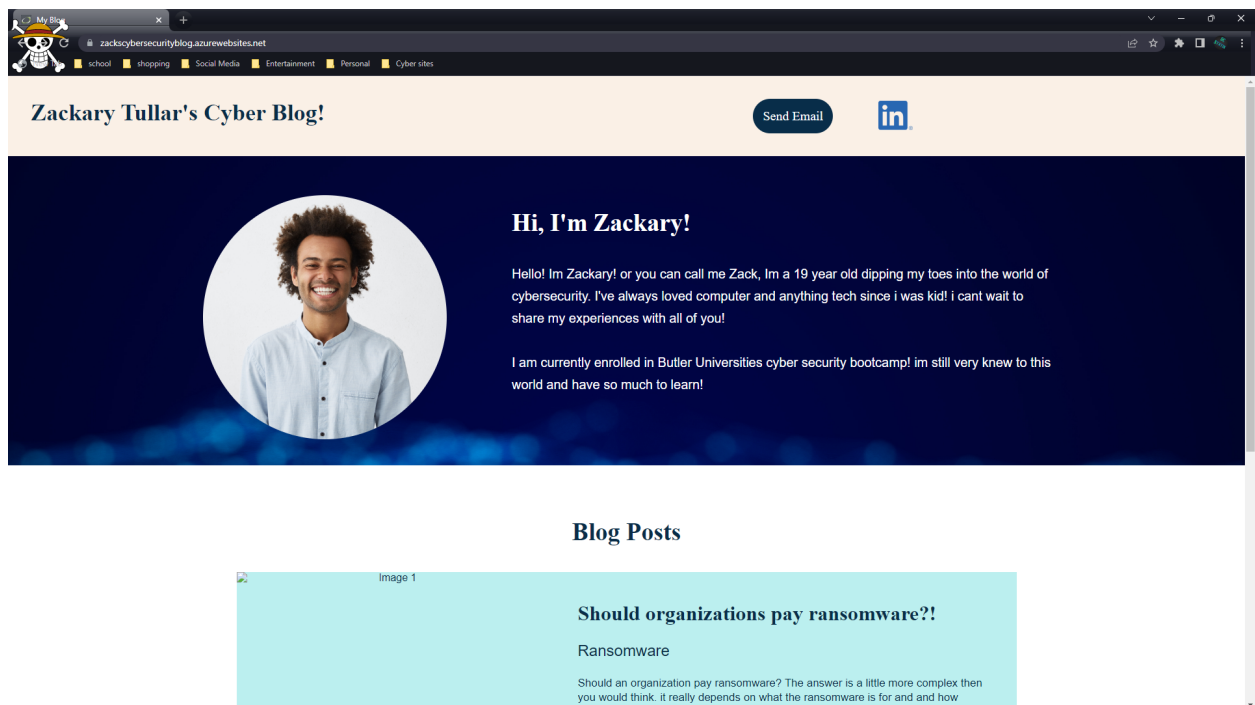
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

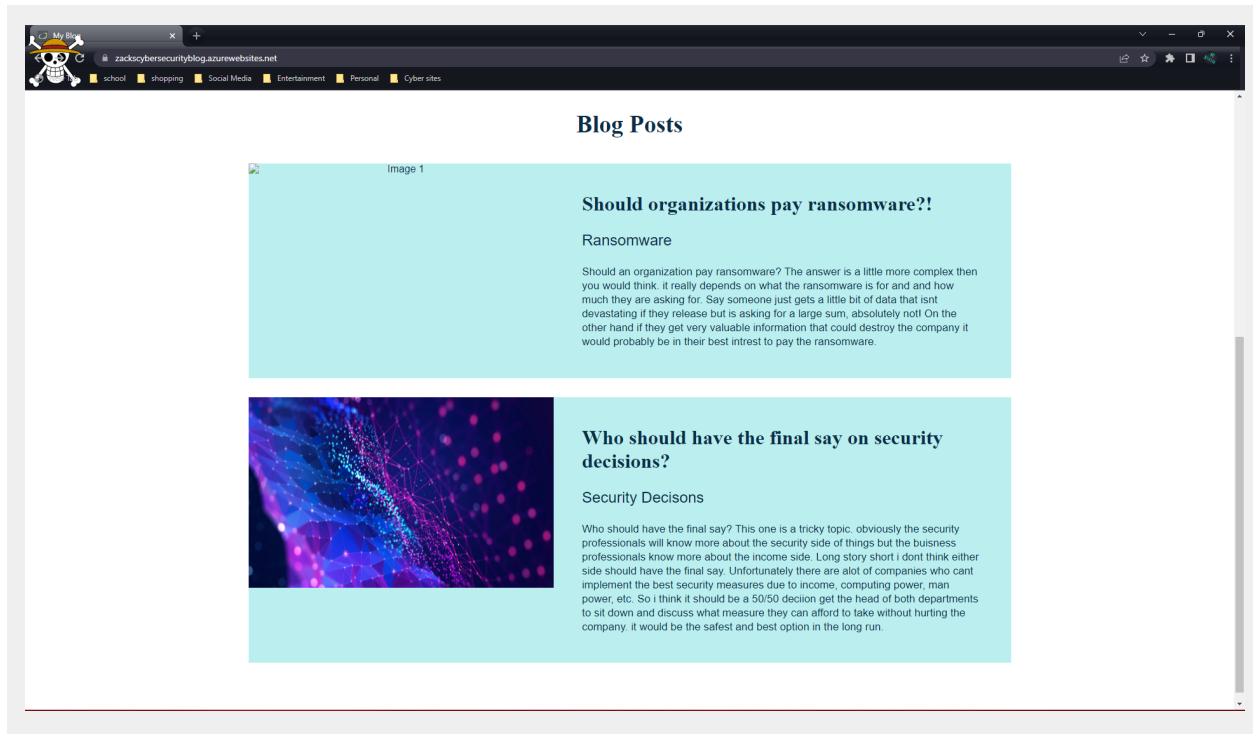
### Your Web Application

Enter the URL for the web application that you created:

<https://zackscybersecurityblog.azurewebsites.net/>

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





## 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?

ZacksCyberSecurityBlog

### Networking Questions

1. What is the IP address of your webpage?

20.118.56.8

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

Martinsville, Indiana United States

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

Server: www.routerlogin.com

Address: 10.0.0.1

Non-authoritative answer:

Name: waws-prod-dm1-313-e626.centralus.cloudapp.azure.com

Address: 20.118.56.8

Aliases: zackscybersecurityblog.azurewebsites.net  
waws-prod-dm1-313.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 7.3]

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

Inside assets has two directories css and images

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

This works with the front end providing images to the website

## Day 2 Questions

### Cloud Questions

### 1. What is a cloud tenant?

Cloud Tenant is the named subdomain assigned to Customer on the Platform.

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

It would be important so not just anybody can access it.

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

Keys are basically give you the access to whatever its for but without the certificates you will only be able to see so little.

## Cryptography Questions

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

They are fast and easy to use.  
Flexible and customizable  
Developers wont be dependent on others.

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

If compromised its a serious risk.  
Security teams lack visibility and control over certificates  
They cant be revoked by a ca

### 3. What is a wildcard certificate?

Its a public key certificate that can be used on multiple subdomains

### 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.

Because there was an industry-wide vulnerability in 3.0 called POODLE so they disabled support for it.

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 because the certificate is valid.

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

The certificate is valid from current-March 9th, 2023

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

No

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

No

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.

Blizzard Battle.net Local Cert

## Day 3 Questions

### Cloud Security Questions

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

Azure Front door uses path based load balancing. Azure web application gateway goes a little further within their virtual network. Their functionality is similar with load balancing though.

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

SSL offloading is the process of removing the SSL based encryption from incoming traffic that a web server receives to relieve it from decryption of data. It lightens the load of the burden of encrypting and decrypting so it won't be as compute intensive.

3. What OSI layer does a WAF work on?

It works on OSI layer 7.

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

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.

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 vulnerability. They could easily steal all the data I may have stored on the website. By entering malicious commands into web forms because it's unsecured.

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. People could easily get around the WAF rule using a proxy or a VPN changing the location they are trying to access it from.

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

### a. Azure Front Door enabled

The screenshot shows the Azure Front Door configuration page for a resource named 'Project1Endpoint-gvd9afbdcfhd9an.z01.azurefd.net'. The page is divided into two main sections: 'Routes' and 'Security policy'.

**Routes Section:**

Routes	Domains	Origin group	Status	Provisioning state
default-webapp-route	1 selected	project1OriginGroup	Enabled	Succeeded
Project1Endpoint-gvd9afbdcf...				

**Security policy Section:**

Name	Domain state
default-webapp-security-...	-
DefaultWebAppWafba...	-
1 association	-
Project1Endpoint-gv...	Enabled

The screenshot shows the 'Essentials' page for the Azure Front Door resource 'Project1-FrontDoor'. It displays various details and properties.

**Essentials Section:**

Property	Value
Resource group (move)	Cyber_Group
Status	Active
Location	Global
Subscription (move)	Azure subscription 1
Subscription ID	8398e4fd-76a1-44db-aae5-0b30008a5cc4
Tags (edit)	Click here to add tags
Name	Project1-FrontDoor
Pricing Tier	Azure Front Door Premium
Front Door ID	eb81f4f6-3c8f-4786-995b-3401257f64fb
Origin response timeout	60 Seconds

**Properties Section:**

Property	Value
Endpoint hostname	Project1Endpoint-gvd9afbdcfhd9an.z01.azurefd.net
Security policy	default-webapp-security-policy-ZacksCyberSecurityBlog-2d117dde
Web application firewall	DefaultWebAppWafba5cb7f298284351b23d2988901e32d1
Origin group name	project1OriginGroup

### b. A WAF custom rule

DefaultWebAppWafba5cb7f298284351b23d2988901e32d1 | Custom rules

Front Door WAF policy

Search

Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Policy settings

Managed rules

Custom rules

Associations

Properties

Locks

Automation

There are pending changes, click 'Save' to apply.

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. [Learn more](#)

Add custom rule

Priority	Name	Rule type	Action	Status
100	project1Rule	Match	Block	Enabled

Microsoft Defender for Cloud | Overview

Showing subscription 'Azure subscription 1'

Search

Subscriptions What's new

General

Overview

Getting started

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems

Cloud Security

Security posture

Regulatory compliance

Workload protections

Management

Environment settings

Security solutions

Workflow automation

1 Azure subscriptions

0 Assessed resources

0 Active recommendations

-- Security alerts

Security posture

0/0 Unassigned recommendation

0/0 Overdue recommendations

Secure score

0% SECURE SCORE

Azure -

AWS -

GCP -

Explore your security posture >

Regulatory compliance

No compliance assesment

Improve your compliance >

Workload protections

Inventory

Unmonitored VMs

0 All VMs are monitored

## 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**