



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://abibsecurityresume.azurewebsites.net/>

ABIB SUBBA'S CYBER BLOG

Send Email



Hi, I'm Abib!

Hello, I'm Abib! a cyber analyst passionate to design web application using Azure's free domain, coding, learning, and contributing to innovative tech projects. With a wealth of knowledge in cybersecurity and technology, I'm here to provide you with expert insights and answers to your burning questions in the digital realm.

Blog Posts



Blog Post 1: "Are humans really the weakest link in security?"

Human error can compromise security.

Humans are frequently identified as the weakest link in security due to their susceptibility to social engineering attacks and their potential for making mistakes. In many security breaches, attackers exploit human vulnerabilities, such as falling for phishing emails or divulging sensitive information unknowingly. Despite advanced technology and robust security measures, human error remains a prevalent cause of security incidents. Training and awareness programs are essential to mitigate these risks, emphasizing the importance of cybersecurity best practices. Nevertheless, it's crucial to recognize that humans can also be a strong asset in security when adequately educated and motivated to follow protocols and remain vigilant. Therefore, while humans may indeed represent a weak point in security, they can also become a powerful defense with the right knowledge and awareness.



Blog Post 2: "Ransomware"

Should organizations pay or not?

Paying the ransom may provide a quick solution to regain access to critical data, but it also fuels the criminal enterprise. Moreover, there's no guarantee that paying will result in data recovery or prevent future attacks. It's essential for organizations to prioritize prevention, strong cybersecurity measures, and robust backups. The decision to pay should be a last resort, carefully evaluated in consultation with law enforcement and cybersecurity experts, considering the potential legal and ethical ramifications. Ultimately, the best defense against ransomware is a proactive one, focusing on prevention and resilience rather than relying on paying criminals.

Day 1 Questions

General Questions

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

Azure free domain

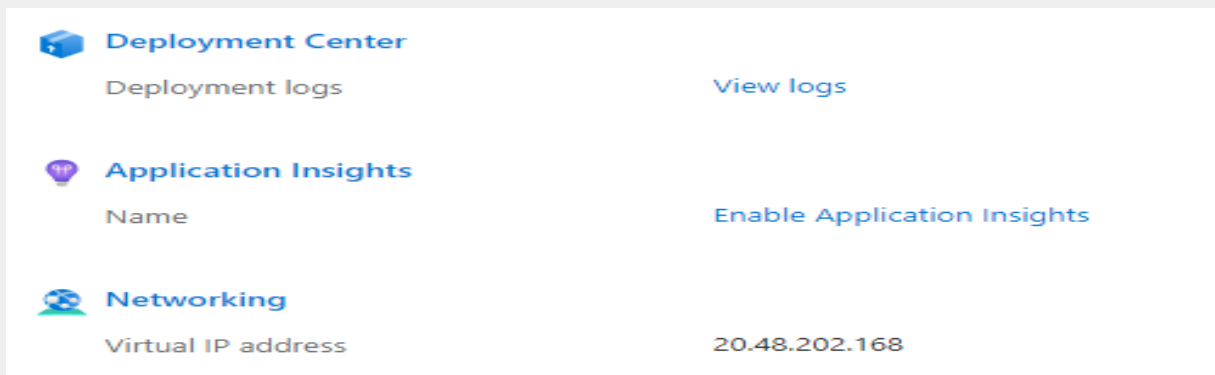
2. What is your domain name?

abibsecurityresume.azurewebsites.net

Networking Questions

1. What is the IP address of your webpage?

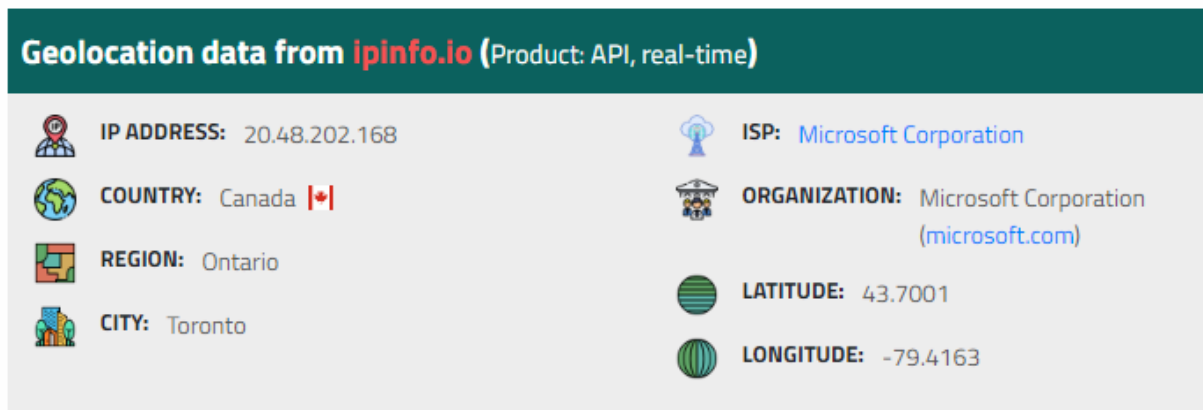
20.48.202.168












The screenshot shows the Azure portal interface. On the left, there are three icons: a blue cube for 'Deployment Center', a purple shield for 'Application Insights', and a blue globe for 'Networking'. The 'Networking' section is selected, showing a 'Virtual IP address' with the value '20.48.202.168'. There are also links for 'View logs' and 'Enable Application Insights'.

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

Toronto, Ontario, Canada



The screenshot shows the geolocation data for the IP address 20.48.202.168 from ipinfo.io. The data is presented in a table-like format with icons and text. The location is Toronto, Ontario, Canada. The ISP is Microsoft Corporation. The latitude is 43.7001 and the longitude is -79.4163.

Geolocation data from ipinfo.io (Product: API, real-time)	
 IP ADDRESS: 20.48.202.168	 ISP: Microsoft Corporation
 COUNTRY: Canada 	 ORGANIZATION: Microsoft Corporation (microsoft.com)
 REGION: Ontario	 LATITUDE: 43.7001
 CITY: Toronto	 LONGITUDE: -79.4163

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

ns1-06.azure-dns.com

Note: CP command `<nslookup -type=ns abibsecurityresume.azurewebsites.net>`

```
Command Prompt
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vbond>nslookup -type=ns abibsecurityresume.azurewebsites.net
Server: cdns01.comcast.net
Address: 2001:558:feed::1

Non-authoritative answer:
abibsecurityresume.azurewebsites.net canonical name = waws-prod-yt1-057.sip.azurewebsites.windows.net
waws-prod-yt1-057.sip.azurewebsites.windows.net canonical name = waws-prod-yt1-057-4c85.canadacentral.cloudapp.azure.com

canadacentral.cloudapp.azure.com
primary name server = ns1-06.azure-dns.com
responsible mail addr = msnhst.microsoft.com
serial = 10001
refresh = 900 (15 mins)
retry = 300 (5 mins)
expire = 604800 (7 days)
default TTL = 60 (1 min)

C:\Users\vbond>
```

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 chosen was PHP 8.2. It works on the back end of a web application.

Home > App Services >


Create Web App


Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *  Azure subscription 1

Resource Group *  RedTeam [Create new](#)

Instance Details


Need a database? [Try the new Web + Database experience.](#) 

Name * abibsecurityresume
  The app name abibsecurityresume is not available .azurewebsites.net

Publish * ☒ Code ☐ Docker Container ☐ Static Web App

Runtime stack * PHP 8.2

Operating System * ☒ Linux ☐ Windows

Region * Canada Central
  Not finding your App Service Plan? Try a different region or select your App Service Environment.

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

There are 2 subdirectories named `css` and `images`.

The `css` assets are used to define styles for web pages, including the design, layout and variations in display for various devices and screen sizes. And `images` directory store images that are used by the website.

```
root@5f96633c3803:/# cd /var/www/html
root@5f96633c3803:/var/www/html# ls
assets index.html index.html.save index.html.save.1 index1.html.bak index2.html.bak index3.html.bak
root@5f96633c3803:/var/www/html# cd assets
root@5f96633c3803:/var/www/html/assets# ls
css images
root@5f96633c3803:/var/www/html/assets#
```

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

This works on the front end of my website.

```
root@5f96633c3803:/var/www/html/assets/images# ls
Background.jpg Image1.jpg Image2.jpg LinkedIn-logo.png RobertSmith-profile.jpg readme
root@5f96633c3803:/var/www/html/assets/images#
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

It is a virtual container that utilizes cloud computing resources and services (public or private) by the customers in the cloud. Each tenant operates within its own isolated environment based on their specific needs and requirements.

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

Key Vault secrets can be given access policies either by user or application to control and restrict who can access and manage cryptographic assets within a key vault, enhancing security.

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

Keys: They are cryptographic keys used for encryption, decryption, and cryptographic operations to secure data at rest and in transit.

Secrets: They are any sensitive information that needs to be stored securely, such as passwords, connection strings, or APIs keys used for authentication and authorization purposes.

Certificates: They are digital documents that contain information about the identity of an entity, such as a person or organization used for securing communication through SSL/TLS protocols.

Cryptography Questions

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

Self-signed certificates are easy to create, quick issuance, free, and cost-effective for testing but lack third-party validation.

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

They aren't trusted by web browsers, causing security warnings, making them not suitable for production environments.

3. What is a wildcard certificate?

A type of digital certificate that is used to secure multiple subdomains under a single domain like - "*.google.com", "*.badssl.com", "*.azurewebsites.net" would secure "www.example.com", "blog.example.com". With a wildcard certificate, a single certificate can be used to secure any number of subdomains, as long as they are all under the same root domain.

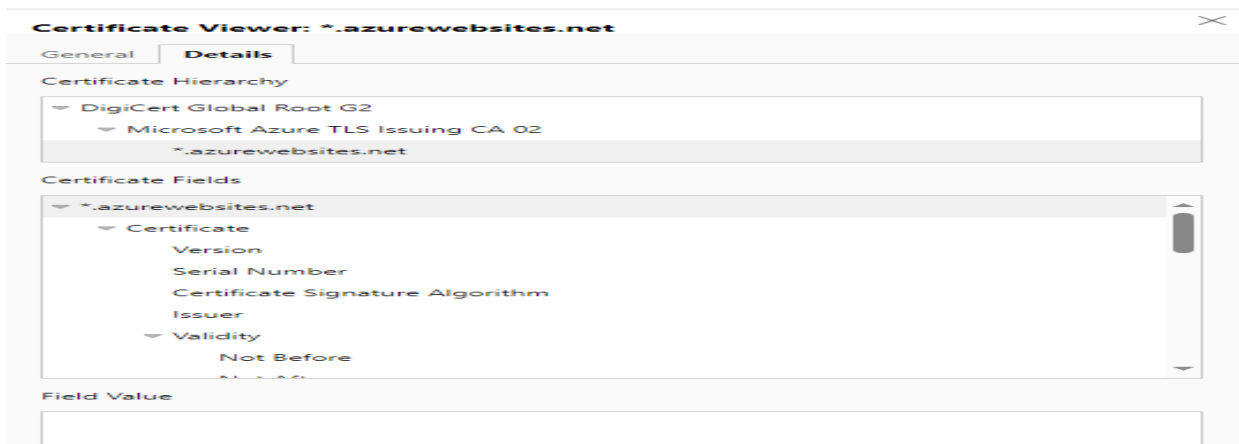
4. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn't provided.

SSL 3.0 is an outdated and insecure protocol due to security vulnerabilities, making it unsuitable for use in modern web applications.

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 certificate on my webpage is secured from the Azure hosting site.



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

Friday, July 21, 2023 at 3:56:12 PM to Sunday, July 20, 2025 at 3:56:12 PM.

Certificate Viewer: *.badssl.com

General Details

Issued To

Common Name (CN)	*.badssl.com
Organization (O)	BadSSL
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	*.badssl.com
Organization (O)	BadSSL
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Friday, July 21, 2023 at 3:56:12 PM
Expires On	Sunday, July 20, 2025 at 3:56:12 PM

Fingerprints

SHA-256 Fingerprint	52 95 7E DD 56 4F 07 D9 A4 AD FF C1 78 3D 72 2F 2D 46 D9 F6 8B 9D 96 FD EC FA 58 66 16 7E ED 0D
SHA-1 Fingerprint	1D B8 69 1E B3 C4 52 9E 6A BE E4 1B F3 54 74 A5 C7 A3 BA 8E

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

Yes, Microsoft Azure TLS Issuing CA 02.

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

Yes, DigiCert Global Root G2

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

Yes, It is GTS Root R1.

Certificate Viewer: *.google.com

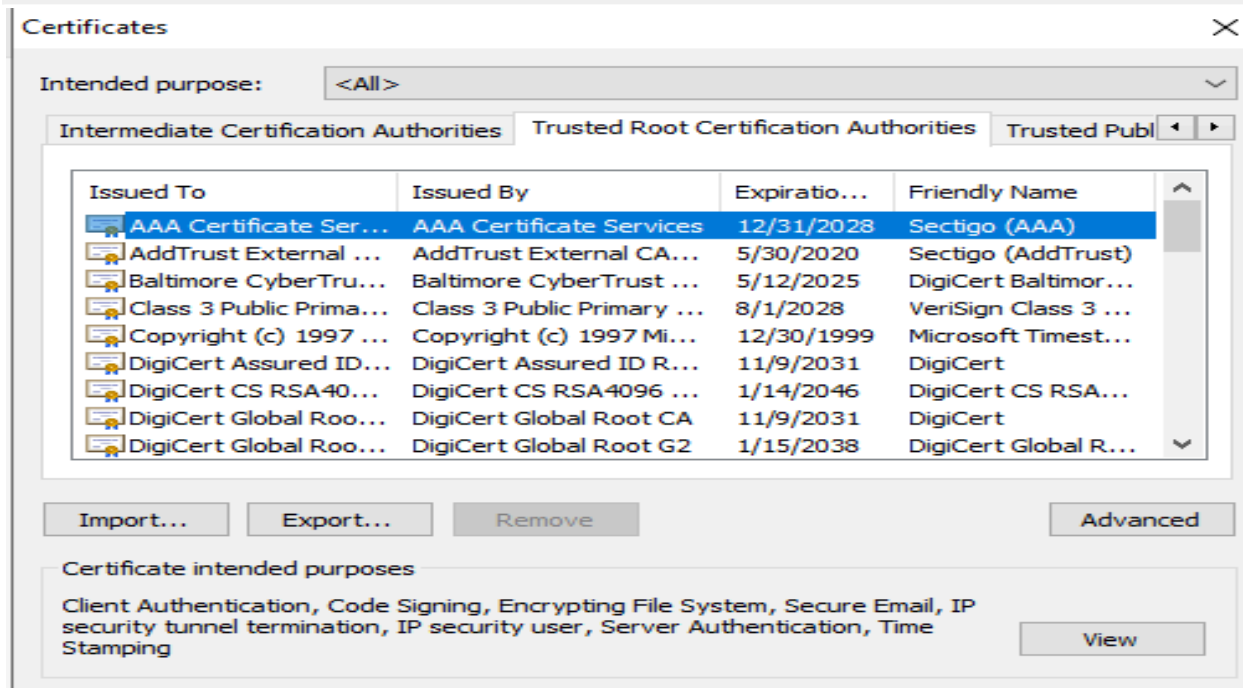
General **Details**

Certificate Hierarchy

- ▼ GTS Root R1
 - ▼ GTS CA 1C3
 - *.google.com

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

AAA Certificate Services



Day 3 Questions

Cloud Security Questions

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

Azure Web Application Gateway & Azure Front Door

Similarities:

- Both work on the Application Layer 7 of the OSI model.
- They offer Web Application Firewall (WAF) for enhanced security.
- Their primary solution is a load balancer.
- Both reside in front of your web application in order to protect it.

- Suitable for URL path-based routing and SSL/TLS termination securing web applications within a region.

Differences:

Azure Web Application Gateway is designed specifically for web applications and provides advanced application delivery capabilities in a single region in your cloud.

Azure Front Door is a global, scalable, and available service that provides intelligent routing and load balancing capabilities at the DNS level in a cloud environment.

:

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 handling SSL/TLS encryption and decryption outside of web servers, typically by dedicated components like Azure Web Application Gateway or Azure Front Door.

Benefits are reduced server load speed time, simplified performance, enhanced security, centralized certificate management, and used as a load balancer for serving web traffic using different servers.

3. What OSI layer does a WAF work on?

Web Application Firewall (WAF) typically operates to work at the Application Layer, which is the Layer of the OSI Layer 7.

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

SQL injection: A type of Web Application attack where malicious SQL queries are injected into input fields to extract data from 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?

Yes, it could be now and in the future. Front Door protection, as well as other security features such as DDoS protection, can help mitigate the risk of SQL injection and other web application vulnerabilities. I will never say a website is 100% secure.

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?

If I create WAF rules to block all traffic from Canada, then yes, anyone who tried to access my website from a Canadian IP address to gain access would be blocked from accessing my website.

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


- a. Azure Front Door enabled

Azure Front Door enabled - Screenshot.

Home > [abibsecurityresume](#) | [Networking](#) >

Azure Front Door

Microsoft Azure



Azure Front Door

Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. Use Front Door with Azure services including App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines—or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more](#)

✓ Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove app service from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
Frontdoor-project1	Azure Front Door Premium	FD-project1-gudpaqcraaguc7ax.z01...	Red-Team

Home > Web Application Firewall policies (WAF) > DefaultWebAppWaf023c5c05942647fe9105379b1d040742

Web Application Firewall policies (WAF)

DefaultWebAppWaf023c5c05942647fe9105379b1d040742 | Managed rules

Front Door WAF policy

Assign Manage exclusions Refresh Enable Disable Change action

Search

Filter for any field...

Name ↑

DefaultWebAppWaf023c5c05942647fe9...

Overview

Activity log

Access control (IAM)

Tags

Settings

Policy settings

Managed rules

Custom rules

Associations

Properties

Locks

Automation

<input checked="" type="checkbox"/>	921110	HTTP Request Smuggling Att...	Block on Anomaly	Enabled
<input type="checkbox"/>	921120	HTTP Response Splitting Attack	Block on Anomaly	Enabled
<input type="checkbox"/>	921130	HTTP Response Splitting Attack	Block on Anomaly	Enabled
<input type="checkbox"/>	921140	HTTP Header Injection Attack...	Block on Anomaly	Enabled
<input type="checkbox"/>	921150	HTTP Header Injection Attack...	Block on Anomaly	Enabled
<input type="checkbox"/>	921160	HTTP Header Injection Attack...	Block on Anomaly	Enabled
<input type="checkbox"/>	921151	HTTP Header Injection Attack...	Block on Anomaly	Enabled
<input type="checkbox"/>	921190	HTTP Splitting (CR/LF in requ...	Block on Anomaly	Enabled
<input type="checkbox"/>	921200	LDAP Injection Attack	Block on Anomaly	Enabled
<input type="checkbox"/>	930100	Path Traversal Attack (/../)	Block on Anomaly	Enabled
<input type="checkbox"/>	930110	Path Traversal Attack (/../)	Block on Anomaly	Enabled
<input type="checkbox"/>	930120	OS File Access Attempt	Block on Anomaly	Enabled
<input type="checkbox"/>	930130	Restricted File Access Attempt	Block on Anomaly	Enabled

b. A WAF custom rule

A WAF custom rule - Screenshot.

Home > Web Application Firewall policies (WAF) > DefaultWebAppWaf023c5c05942647fe9105379b1d040742

Web Application Firewall policies (WAF)

DefaultWebAppWaf023c5c05942647fe9105379b1d040742 | Custom rules

Front Door WAF policy

Save Discard Refresh

Search

Filter for any field...

Name ↑

DefaultWebAppWaf023c5c05942647fe9...

Overview

Activity log

Access control (IAM)

Tags

Settings

Policy settings

Managed rules

Custom rules

Associations

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	Project1Rules	Match	Block	Enabled

DefaultWebAppWaf023c5c05942647fe9105379b1d040742 | Custom rules

Front Door WAF policy

Save Discard Refresh

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	Project1Rules	Match	Block	Enabled

FTPS should be required in web apps ...

 Exempt  View policy definition  Open query

Severity

 High

Freshness interval

 30 Min

Tactics and techniques

 Credential Access +1

^ Description

Enable FTPS enforcement for enhanced security

^ Remediation steps

Manual remediation:

To ensure enforcement of FTPS only for your web app:

1. Go to the App Service for your API app
2. Select Configuration, and go to the General Settings tab
3. In FTP state, select FTPS only.

For more information, visit here: <https://aka.ms/deploy-ftp>

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

