



# Cybersecurity

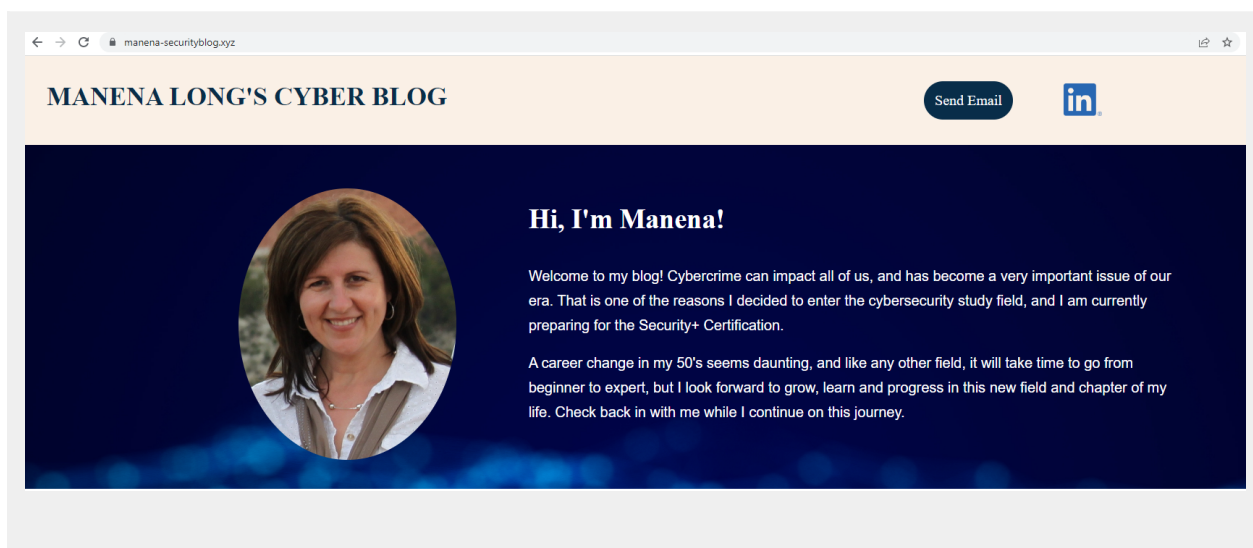
## Project 1 Technical Brief

### Your Web Application

Enter the URL for the web application that you created:

<https://manena-securityblog.xyz>

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



## Blog Posts



### Why cybersecurity is important and how it impacts your everyday life

cybercrime, hacked

It is vital to understand that cybercrime can impact all of us and that anyone can become the target of hackers with malicious intentions. We live in a digital world, which means our work lives, personal lives, and finances have all begun gravitating toward the world of the internet, mobile computing, and electronic media. Unfortunately, this makes us more vulnerable than ever to malicious attacks, invasions of privacy, fraud, and other attacks. That is why it's crucial to learn more about the ways that cybersecurity impacts your everyday life and how to stay safe from hackers and cyber criminals. Here are some ways to help you improve the security of your digital world.

1. Set up automatic updates on your cell phone. Operating system updates offer security fixes and patches that make your device more secure.
2. Practice good password selection. The ideal strong password is between 8 and 12 characters and includes upper- and lower-case letters, at least one number, and a unique character (such as !?, @)
3. Beware of suspicious email links or attachments. The majority of all malware payloads are delivered via email. These suspicious files can seem legitimate and can be disguised as something you may be interested in. Never click on links from senders you are unfamiliar with.
4. Use two-factor authentication whenever you can. Also commonly referred to as 2FA, two-factor authentication requires two different types of verification before you're given access to an account.
5. Use a VPN. See the next post.

It is important to do as much as possible to prevent yourself from becoming a victim – which is what all the best practices outlined above are all about.



### Do I really need a VPN?

VPN, private network

We live in a world where our online activities leave digital footprints. Every website we visit, where we are, how much we spend, and what cards we pay with. All this data is valuable to companies, and they want to get as accurate information about us as they possibly can. VPN stands for 'virtual private network' – a service that protects your privacy online and conceal your browsing information. It creates an encrypted tunnel for your data and protects your online identity. Instead of showing your IP address, your VPN will teleport your connection to a server in the country that you choose to connect to and show an IP address originating in that location. This way, the VPN works as a protection layer, encrypting all the data that travels through it. If you connect to a lot of public Wi-Fi hotspots, you never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity. A VPN connection protects your online identity by hiding your IP address and keeping your personal information safe. A VPN is not a cure-all, but the more the internet is present in our lives, the more we can benefit from using one.

# Day 1 Questions

## General Questions

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

GoDaddy

2. What is your domain name?

Manena-securityblog.xyz

## Networking Questions

1. What is the IP address of your webpage?

20.119.8.24

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

Washington, Virginia, USA

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

```
$ nslookup -type=NS manena-securityblog.xyz
```

```
Server: UnKnown
```

```
Address: 192.168.1.1
```

```
Non-authoritative answer:
```

```
manena-securityblog.xyz nameserver = ns66.domaincontrol.com
```

```
manena-securityblog.xyz nameserver = ns65.domaincontrol.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?

PHP 7.4 ; Back end

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

Two directories named “css” and “images”  
Inside these directories are css files and images that are used for the presentation of the web pages.

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

Front end

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

A cloud tenant is a customer who purchases cloud computing resources. This could be an individual user, a group of users, or an entire department or company.

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

Access policies on a key vault are of high importance. Access control dictates who is allowed to access the secure information and what actions a particular user or group is allowed to perform over the keys, secrets, and certificates. Through authentication and authorization, the access policy makes sure security principals are who they say they are and that only authorized users or groups have access to the key vault.

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

Key: Cryptographic materials like RSA and EC keys, used to encrypt and decrypt data are stored in the key vault.

Certificate: SSL certificates can be created and stored in the key vault. Certificates show the authenticity of a website. Certificates build on top of keys and secrets. They have a thumbprint that is used to bind a name to a public key.

Secrets: Provides secure storage for anything that needs tightly controlled access like passwords, API keys, and database connection strings.

## Cryptography Questions

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

Self-signed certificates are free. They do offer encryption and are suitable for internal network websites or testing/development environments.

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

A self-signed certificate is not secure. No browser will trust a self-signed certificate and will display a warning page to the website visitor.

It is easy for attackers to create self-signed certificates to perform attacks.

Self-signed certificates are not signed by a trusted authority.

3. What is a wildcard certificate?

Wildcard certificates are single certificates (SSL/TLS) with a wildcard character (\*) in the domain name field. This allows the certificate to authenticate and provide HTTPS encryption to a website and all of its subdomains under the same base 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.

There is a vulnerability in the SSL 3.0 protocol. This vulnerability allows a man-in-the-middle attacker to decrypt the ciphertext. Microsoft disabled SSL 3.0 in Azure Websites to protect customers from this vulnerability.

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 error is returned. I created and bound a secure, trusted SSL certificate to my web app.

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

9/13/2022 - 3/14/2023

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

Yes, GeoTrust Global TLS RSA4096 SHA256 2022 CA1

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

Yes, DigiCert, Inc

- 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.

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?

### Similarities:

Front Door and Web Application Gateway both work on layer 7 of the OSI model.

They both reside in front of the web application to protect it.

Both can incorporate a WAF (web application firewall).

They both act as load balancers and are viable options for securing web applications.

They both have additional features such as URL path-based routing and SSL/TLS termination.

### Differences:

Front Door is a non-regional service. It can load balance across regions and is suited when you have several regions in a cloud environment.

Application Gateway is a regional service. It can load balance and protect between VM's/containers etc. within a single region in the cloud.

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

SSL (Security Socket Layer) offloading takes place by placing a device, like a load balancer, between the browser and the server to handle encryption, decryption, and security tasks.

There are two forms of SSL offloading:

1. SLL termination: Data gets encrypted or decrypted by a device, depending on which direction the data is traveling. For incoming traffic, the SSL encryption is removed and the web server receives the decrypted information.

Benefits: Reduces the workload and processing burden on the web server and helps improve the server speed.

2. SLL bridging: Decrypting of incoming data, inspecting it for malicious code, and then re-encrypting it before sending it on to the web server.

Benefits: Data remains encrypted during the entire transmission process. It protects the server from malware, corrupted data, SQL injections, and other common web-application attacks and enhances the stability of the website.

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

Layer 7 - Application Layer

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

SQL injection Attack: A SQL attack consists of the insertion of a SQL query via the input data from the client to the application. SQL injection occurs when unintended data enters a program from an untrusted source. The data is used to dynamically construct a SQL query.

A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database, and in some cases issue commands to the operating system.

If the Web App Firewall detects unauthorized SQL code in a user request, it either transforms the request, to render the SQL code inactive, or blocks the request.

### 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, because user input channels are the main vector for SQL injection attacks. My website does not have any user input options.

### 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 someone who resides in Canada does not use a VPN, they will not be able to access my website. If a user uses a VPN, they might be able to access my website because their IP address can show as originating from a different country, even if they live in Canada.


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



a. Azure Front Door enabled

Home > App Services > Manena-SecurityBlog | Networking >


## Azure Front Door ...




### Azure Front Door

Azure Front Door Service is Microsoft's highly available and scalable web application acceleration platform and global HTTP performance for your end-users. Use Front Door with Azure services including Web/Mobile Apps, Cloud Services and Virtua

---



Azure Front Door is configured for your web app

[project1-MSCFrontDoor](#) 

b. A WAF custom rule

project1MSCFrontDoorf2328e5918344bae828bbd41c38c772a | Custom rules ☆ ...

Front Door WAF policy

Search << 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	Project1rule	Match	Block	Enabled

## 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*