



Cybersecurity

Project 1 Technical Brief

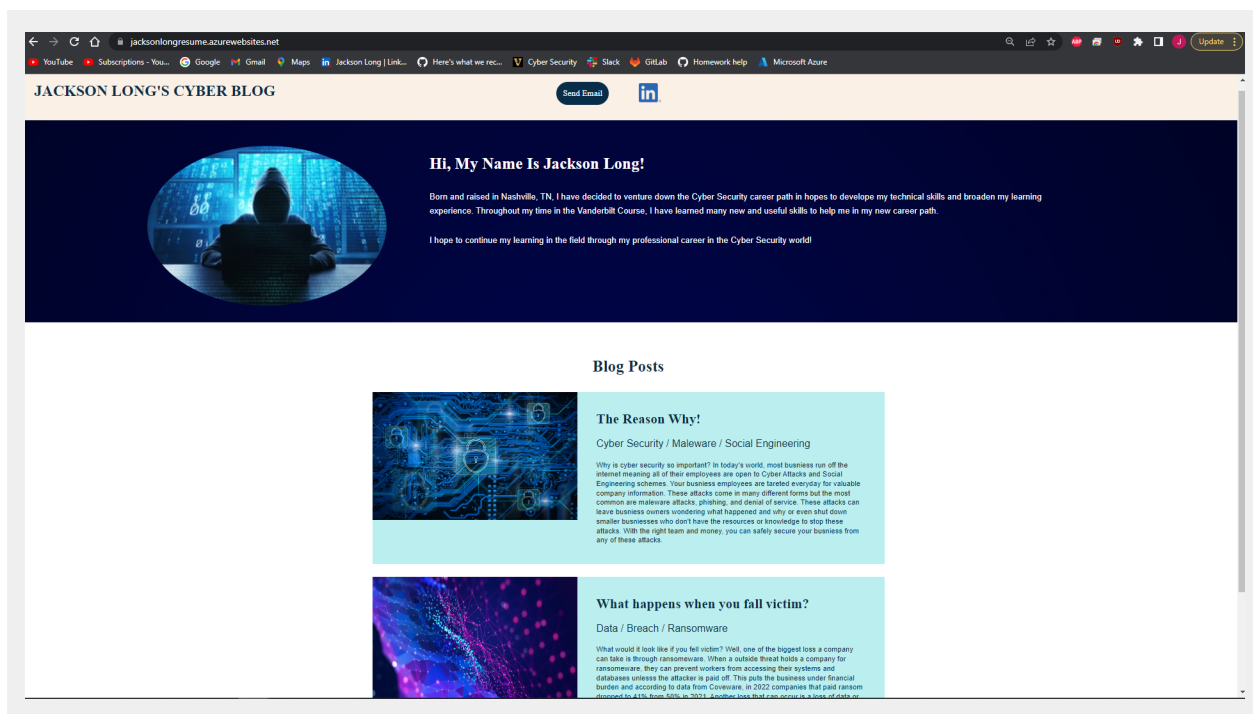
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

[<https://jacksonlongresume.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?

[jacksonlongresume.azurewebsites.net]

Networking Questions

1. What is the IP address of your webpage?

[20.211.64.13]

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?

```
MINGW64/c/Users/Jacks
Jacks@DESKTOP-BDLJFPU MINGW64 ~
$ nslookup -type=NS jacksonlongresume.azurewebsites.net
Server: dsldevice6.attlocal.net
Address: 2600:1700:39a0:9100::1

Non-authoritative answer:
jacksonlongresume.azurewebsites.net canonical name = waws-prod-sy3-091.sip.azurewebsites.windows.net
waws-prod-sy3-091.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-091-a15c.australiaeast.cloudapp.azure.com

australiaeast.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)

Jacks@DESKTOP-BDLJFPU MINGW64 ~
$
```

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 8.0 & Back End]

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

[The files that configure the original webpage]

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 customer who purchases cloud computing resources]

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

[To prevent unauthorized users from having access to the vault]

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

[Cryptographic keys that support multiple key types and algorithms]

Secrets- provides secure storage such as passwords and database connection strings

Certificates- Managing keys, it regenerates or rotates keys periodically.]

Cryptography Questions

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

[Simple to modify or customize, no payment required, Quick initiation]

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

[Data security is not guaranteed, user personal data set at risk]

3. What is a wildcard certificate?

[a public key certificate which can be used with multiple sub-domains of a domains]

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.

[To ensure the safety of the users. SSL 3.0 was a major vulnerability observed in Azure machines and websites. It was not limited to one or two types of machines, but all websites and windows VMs got vulnerable]

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?

[The certificate is self-signed: Some websites use self-signed SSL certificates instead of a certificate issued by a trusted certificate authority. In this case, the browser will warn the user that the connection is not secure, but the user may choose to proceed anyway]

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

[Issued On
Tuesday, December 27, 2022 at 3:12:39 PM
Expires On
Friday, December 22, 2023 at 3:12:39 PM]

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

[Microsoft Azure TLS Issuing CA 105 is our intermediate certificate]

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]

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

[Redmond]

Day 3 Questions

Cloud Security Questions

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

[Both Front Door and application gateway are on layer 7 (HTTP/HTTPS) load balancers, but front door is a non-regional service and App gateway is a regional service]

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

[It is the process of removing the SSL based encryption from incoming traffic that a web server receives to relieve it from decryption data. It takes care of the encryption/decryption process on a separate device so it doesn't affect the web servers performance.]

3. What OSI layer does a WAF work on?

[Layer 7]

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

[SQL injection occurs when you ask a user for input and instead the user gives you an SQL statement that you will unknowingly run on your 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?

[If a Front Door was not enabled, then the website would be exposed to these

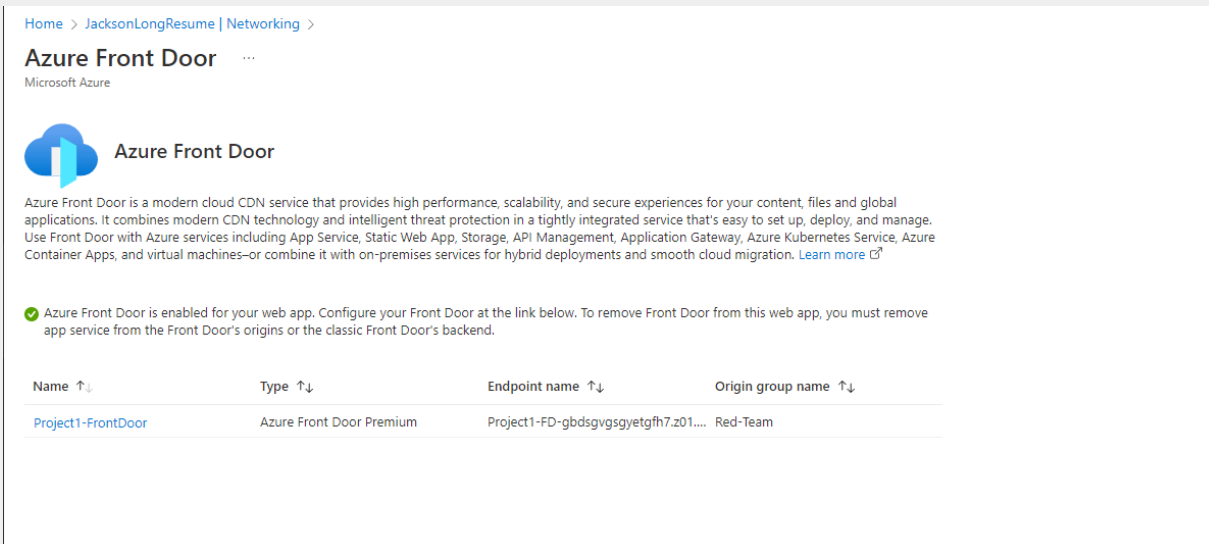
attacks]

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, the only way they could access it would be through a VPN]

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

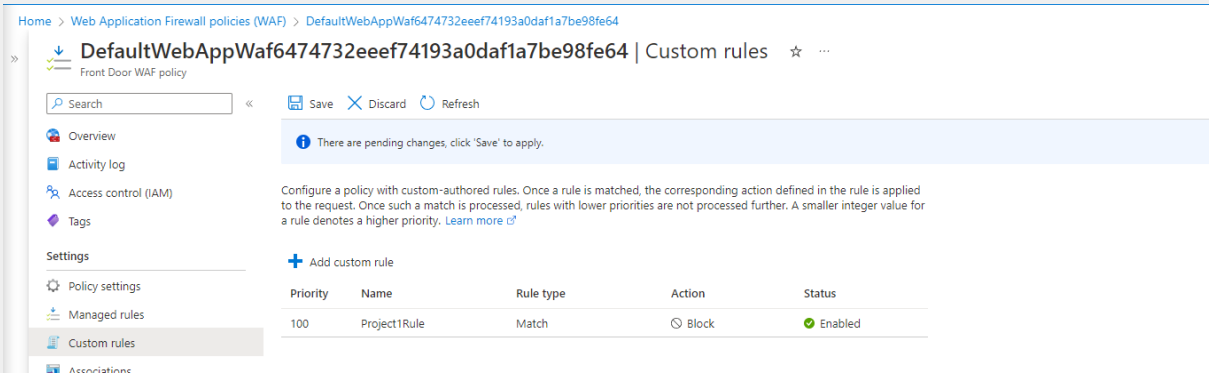
- a. Azure Front Door enabled



The screenshot shows the Azure Front Door page in the Azure portal. The breadcrumb navigation is "Home > JacksonLongResume | Networking > Azure Front Door". The page title is "Azure Front Door" with a Microsoft Azure logo. Below the title, there is a description of Azure Front Door as a modern cloud CDN service. A green checkmark icon indicates that Azure Front Door is enabled for the web app. Below this, there is a table with columns: Name, Type, Endpoint name, and Origin group name. The table contains one row: "Project1-FrontDoor", "Azure Front Door Premium", "Project1-FD-gbdsgvgsgyetgh7.z01....", and "Red-Team".

Name	Type	Endpoint name	Origin group name
Project1-FrontDoor	Azure Front Door Premium	Project1-FD-gbdsgvgsgyetgh7.z01....	Red-Team

- b. A WAF custom rule



The screenshot shows the Azure WAF Custom rules page. The breadcrumb navigation is "Home > Web Application Firewall policies (WAF) > DefaultWebAppWaf6474732eeef74193a0daf1a7be98fe64". The page title is "DefaultWebAppWaf6474732eeef74193a0daf1a7be98fe64 | Custom rules". There is a search bar and buttons for Save, Discard, and Refresh. A message states: "There are pending changes, click 'Save' to apply." Below this, there is a description of how to configure a policy with custom-authored rules. A table shows the custom rules with columns: Priority, Name, Rule type, Action, and Status. The table contains one row: "100", "Project1Rule", "Match", "Block", and "Enabled".

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. Yes*
- ***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*