Cybersecurity

Project 1 Technical Brief

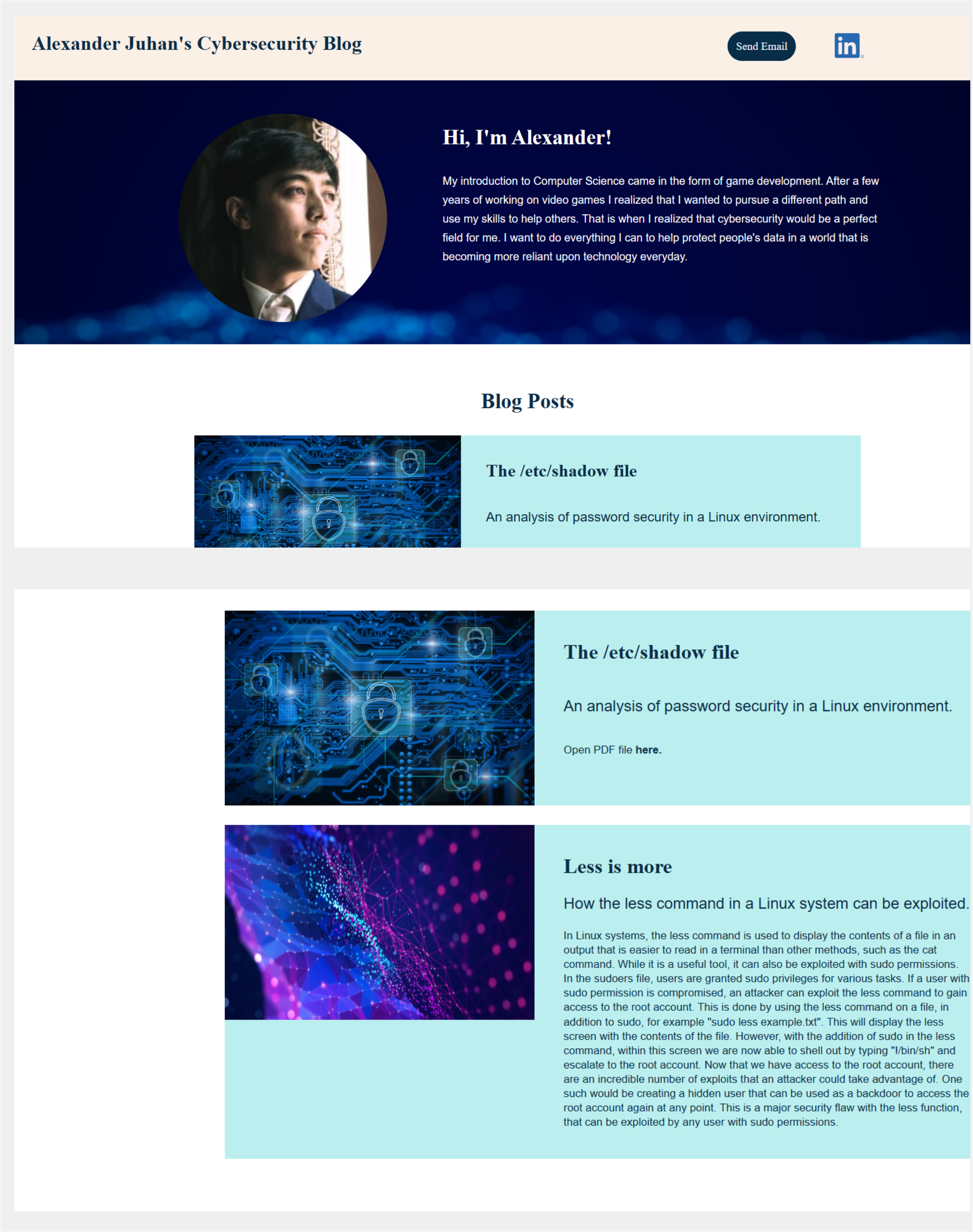
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
My Blog (alexanderjuhansecurityresume.azurewebsites.net)
```

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



Alexander Juhan's Cybersecurity Blog

Hi, I'm Alexander!

My introduction to Computer Science came in the form of game development. After a few years of working on video games I realized that I wanted to pursue a different path and use my skills to help others. That is when I realized that cybersecurity would be a perfect field for me. I want to do everything I can to help protect people's data in a world that is becoming more reliant upon technology everyday.

Blog Posts

The /etc/shadow file

An analysis of password security in a Linux environment.

The /etc/shadow file

An analysis of password security in a Linux environment.

Open PDF file **here.**

Less is more

How the less command in a Linux system can be exploited.

In Linux systems, the less command is used to display the contents of a file in an output that is easier to read in a terminal than other methods, such as the cat command. While it is a useful tool, it can also be exploited with sudo permissions. In the sudoers file, users are granted sudo privileges for various tasks. If a user with sudo permission is compromised, an attacker can exploit the less command to gain access to the root account. This is done by using the less command on a file, in addition to sudo, for example "sudo less example.txt". This will display the less screen with the contents of the file. However, with the addition of sudo in the less command, within this screen we are now able to shell out by typing "!/bin/sh" and escalate to the root account. Now that we have access to the root account, there are an incredible number of exploits that an attacker could take advantage of. One such would be creating a hidden user that can be used as a backdoor to access the root account again at any point. This is a major security flaw with the less function, that can be exploited by any user with sudo permissions.

1st Blog Post PDF link: The etc_shadow file.pdf

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?

```
alexanderjuhansecurityresume
```

Networking Questions

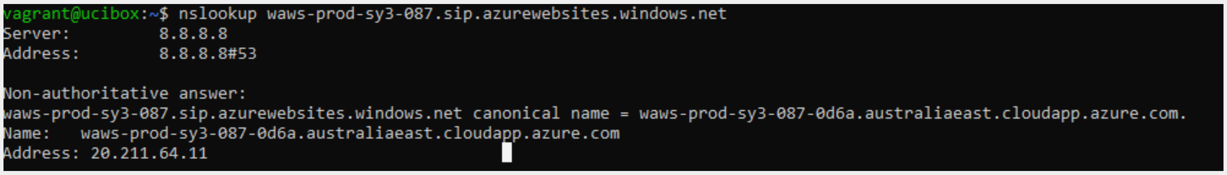
1. What is the IP address of your webpage?

```
20.211.64.11
```

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?



```
vagrant@ucibox:~$ nslookup waws-prod-sy3-087.sip.azurewebsites.windows.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
waws-prod-sy3-087.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-087-0d6a.australiaeast.cloudapp.azure.com.
Name:   waws-prod-sy3-087-0d6a.australiaeast.cloudapp.azure.com
Address: 20.211.64.11
```

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 8.1, backend
```

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

```
HTML assets help the page display. This can include images, as well as
applications that help perform specific tasks.
```

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

```
HTML deals with the front end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A partition in a cloud environment that isolates and secures resources.
```

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

```
Access policies will ensure that Key Vaults are as secure as possible.
```

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

```
Secrets are passwords, keys are cryptographic keys generated by algorithms,
and certificates are key pairs that allow access to data.
```

Cryptography Questions

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

```
Cost-efficiency. Speed and ease of access for testing purposes. Zero
dependencies.
```

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

Browsers and OSs will not recognize them. Risky for use in transactions dealing with highly sensitive data such as financial information. Susceptible to man-in-the-middle attacks.

3. What is a wildcard certificate?

A key that can be used with multiple sub-domains, as opposed to individual keys for each sub-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 poses a major security threat. MS disabled it to be safe.

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, I used the free azure created site, so the SSL certificate was generated for me by MS.

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

03/14/2022 - 03/09/2023

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

MS Azure TLS Issuing CA 01

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

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.

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?

Both are layer 7 load balancers. Gateway is a regional service, while Front Door is non-regional.

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 a process that removes SSL encryption from incoming traffic. This process relieves the usage of resources from a web server, and uses the resources of a dedicated server.

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 attacks allow hackers to inject malicious code onto a web server. This injection triggers the back-end to execute the code that was injected, and can allow access to restricted data. This malicious code can spread malware to clients visiting the site.

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?

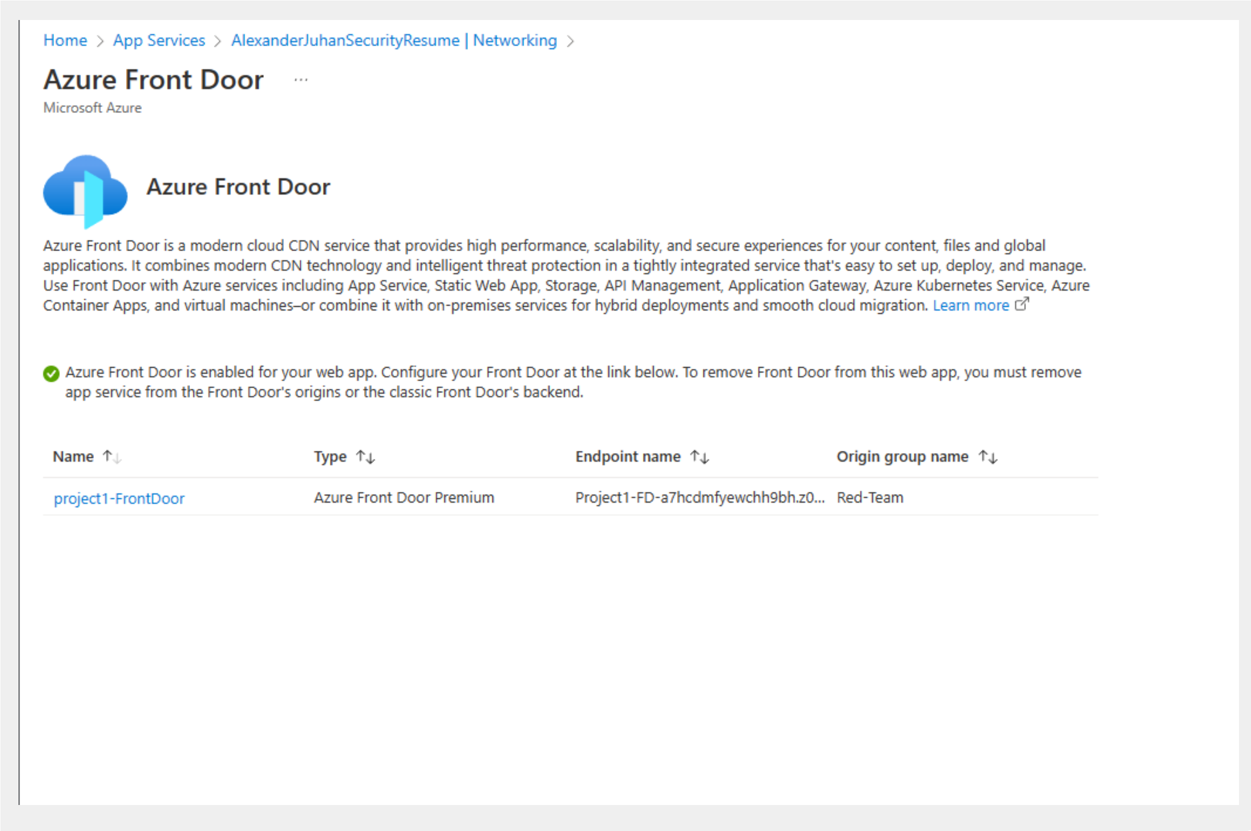
No, not at the moment. There is not any sensitive data that can be breached on my website, such as financial information. Additionally, there are not any fields available for text input that would allow for SQL injection in the first place.

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 would block most Canadians from accessing the site. The WAF rule uses a geolocation feature, and would limit access from any Canadian IP addresses.However, there are ways around this method, such as using a VPN.

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

    a. Azure Front Door enabled



Home > App Services > AlexanderJuhanSecurityResume | Networking >

Azure Front Door ...

Microsoft Azure

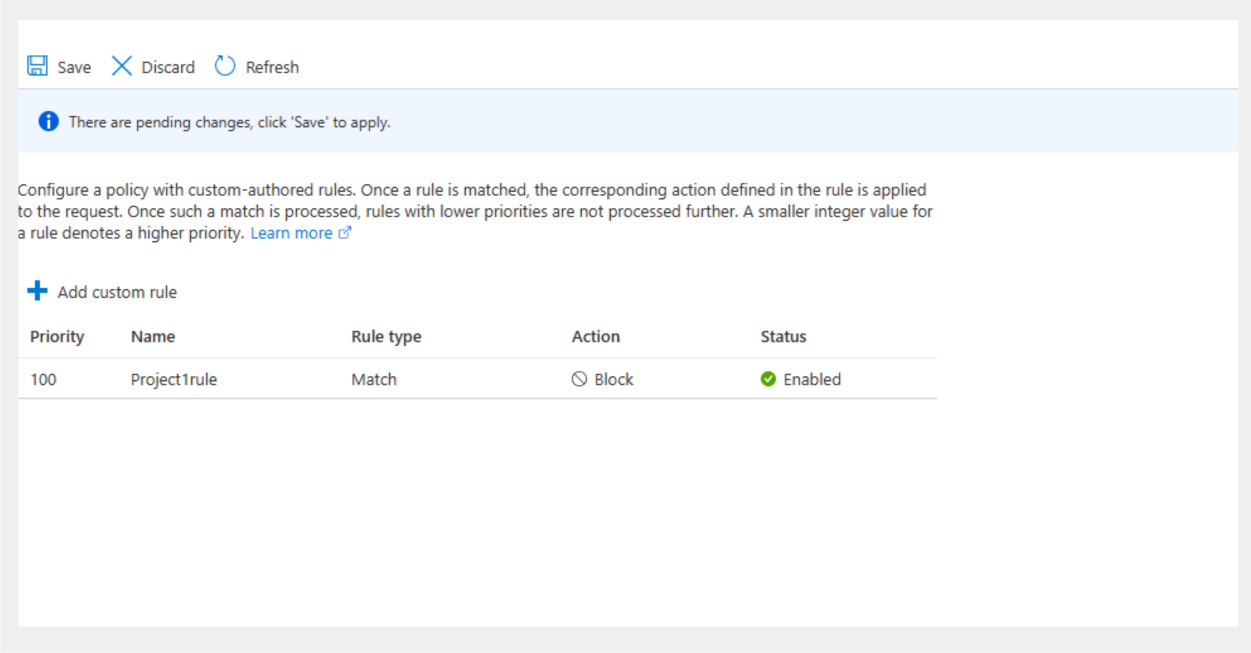
Azure Front Door

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 ↑↓
project1-FrontDoor	Azure Front Door Premium	Project1-FD-a7hcdmfyewchh9bh.z0...	Red-Team

b. A WAF custom rule



ⓘ 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

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**