Cybersecurity

Project 1 Technical Brief

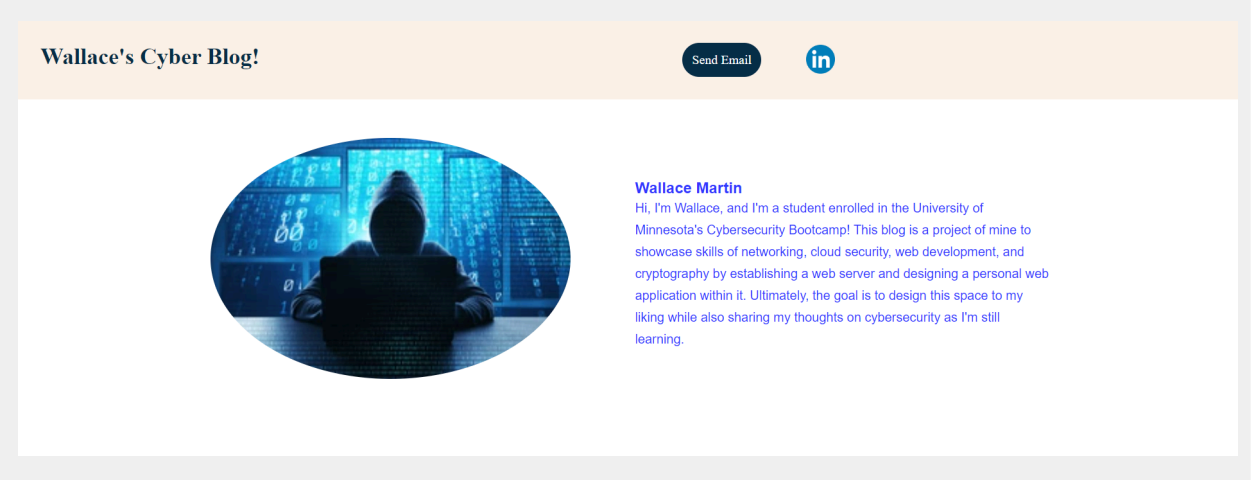
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

https://martinwallacesecurity.azurewebsites.net/

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



Blog Posts

Insomniac Games' Line of Defense Against Ransomware

Ransomware, Ransomware Attack, Cybersecurity, Insomniac Games, Sony, Playstation

Ransomware is a malicious software that's designed to block access from a computer system until a sum of money is paid. In many cases, the defenders are put into a bind and don't have a choice but to comply. In an era comprised of digital assets, ransomware has become a common issue for organizations. Not only can an organization's proprietary assets become compromised, but so can the data of its employees and users. This was the fate of Sony subsidary Insomniac Games. Back in November 2023, a cataclysmic data breach hit Insomniac. Since being acquired by Sony in 2019, Insomniac is most well known nowadays for their work on Playstation videogame series such as Ratchet & Clank and Marvel's Spider-Man. The severity of this leak and the contents that were taken, which can now be seen by the public cannot be understated. Sensitive information that belonged to employees, source code for existing games, documents containing release dates for games years away, the studio was pretty much cracked open for anyone to see. The Insomniac Games leak really puts into perspective how devastating these ransomware attacks can be on businesses, and why the need to invest in cybersecurity defenses is so important. All in all, as we continue to build our digital infrastructures that need an online connection, these ransomware threats will become even more common, so we have to be ready for it.

What Should we Expect From AI in Cybersecurity?

AI, Artificial Intelligence, Cybersecurity, Automation

It feels like no matter where you get your information from, AI is the talk of the town when it comes to advancements in our working industries. At some point, we have to come to terms with that some tasks will get replaced as these AI programs get smarter and smarter. While this puts a number of jobs at stake, I feel cybersecurity is a field that will never truly be able to function on its' own without human judgement. When it comes to cybersecurity, advanced AI seems like a no brainer for organizations to want to invest in it. If we can allocate AI to do tasks they are capable of and bring more manpower into more high-end development tasks that require human analysis to verify for any shortcomings or mistakes, I think it can help improve current security practices and bring out more strategies to help against attackers. While lower-end jobs may fizzle out, I think qualified security professionals will still thrive, maybe even moreso as AI can be a valuable tool to gather and assess information on topics we may be unfamiliar with. On the other hand, the added inclusion of advanced AI in recent years can be a double-edged sword in the realm of security. A very real issue that is starting to crop up is cybercriminals using AI themselves to carry out malicious objectives. For example, as AI improves, the algorithms hackers use to decipher a user's password(s) improves exponentially. With access to quicker and more accurate password guessing, this is a quickfire way to get access to someone's information. While we should inform the public about strong ways to defend their data, ultimately, as security professionals, it is our responsibility to find the best use cases for AI so that we can still be prepared to defend against whatever new strategies attackers throw at us and our users.

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?

```
martinwallacesecurity
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.15
```

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?

```
Domain name, TTL 1100, and nsname
```

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 8.2, back end
```

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

```
Images, css files, fonts, positioning of UI. Pretty much the components of
what we, the users see on the websites we visit
```

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?

```
User(s) who may share server resources in a private or public environment
that non tenants cannot access
```

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

```
Because it determines whether a given security principle can perform
different operations on key vault secrets, keys, and certificates
```

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

```
Keys - A string of characters used within an encryption algorithm for
altering data so that it appears random

Secrets - Private pieces of information, act as keys to unlock protected
resources or sensitive information

Certificates - File used to confirm the authenticity, identity, and
reliability of a website or web application
```

Cryptography Questions

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

```
They can quickly be created and carried out for testing. This can be useful
when developments need to be made fast and need to set up secure connections
without the need for waiting for certificate authority.
```

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

```
They can come with security risks such as the lack of trust validation which
```

```
may turn users away due to a warning message, or because users must manually verify and trust these self signed certificates and apply them to their systems themselves, so less technical users may be lost on what to do.
```

3. What is a wildcard certificate?

```
A certificate that can secure multiple sub domain names pertaining to 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.

```
SSL 3.0 is outdated and no longer secure because of a vulnerability known as POODLE, which hackers can exploit to obtain serious information about users like passwords and cookies
```

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 it has been properly configured and the ssl certificate is still operating within the validity period
```

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

```
10/31/2023 - 06/27/2024
```

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

```
Microsoft Azure TLS Issuing CA 02
```

    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.

```
CN=Amazon Root CA 4,O=Amazon,C=US
e35d28419ed02025cfa69038cd623962458da5c695fbdea3c22b0bfb25897092
```

Day 3 Questions

Cloud Security Questions

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

```
They are both load balancers for http and https traffic. However, Gateway is a regional service that balances requests within a region, meanwhile Front Door is a global service that can distribute requests across different regions.
```

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

```
SSL offloading does the encryption/decryption process on a different device so that it doesn't compromise the performance of the web server
```

3. What OSI layer does a WAF work on?

```
7
```

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

```
SQL injection - inspects for malicious SQL code, since attackers may try to insert malicious SQL code into web requests in order to do things like modify your database or extract its data
```

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?

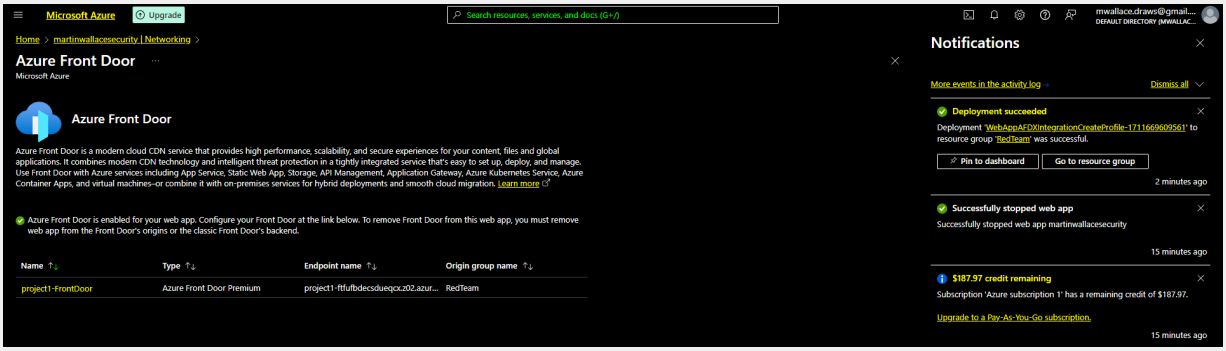
```
Yes, my website would be negatively impacted with the exclusion of WAF, since http traffic would go unmonitored. This gives hackers an opportunity to perform an attack.
```

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?

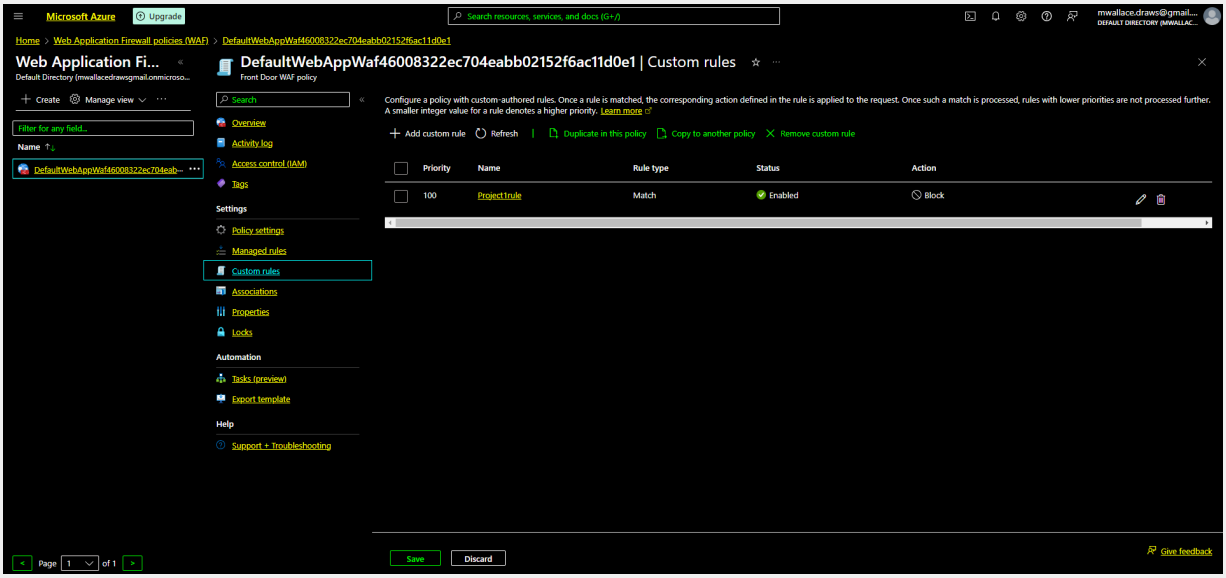
```
Yes, if they are trying to access the website on an IP address that is identified as a Canadian IP address. If they are on a VPN however, it's a different story.
```

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

    a. Azure Front Door enabled



    b. A WAF custom rule



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.*