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://marko-cyberlounge.azurewebsites.net/
```

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

```
[Paste screenshots here]
```

My Blog

marko-cyberlounge.azurewebsites.net

MARKO JOVANOVIC'S CYBERSECURITY LOUNGE

Send Email

Hi, I'm Marko!

Graduating from York University in 2012, I found myself building airplanes for Bombardier Aerospace. Next, I was integrating home automation systems. It is here where I developed my 'Cyber Paranoia'. This is where my Cyber Journey begins. Join me as we explore the world of CyberSecurity together! Now sit back, relax, and welcome to The CyberSecurity Lounge!

Blog Posts

My Blog

marko-cyberlounge.azurewebsites.net

How Secure is our Data?

Data storage; hackers; information; breach

A few years ago, after contracting the Covid-19 virus, I was offered the opportunity to partake in a genetic study with the goal of better understanding how Covid-19 affects different people. It sounded fascinating, and I did feel a small urge to help out in whatever small way that I could. On top of that, I would receive the results of my genetic study, which would include fascinating information on my genetic heritage, as well as potentially useful information on any sort of genetic disease risks that I may have, or may be a carrier of. People pay lots of money to get this sort of information about themselves, and here I am being offered it for free!

Ultimately what stopped me from going through with it were the warnings in the user agreement: We cannot guarantee the confidentiality of your genetic information. They went on to describe how they go about separating any identifiable information from the results, so even if the data does fall into the wrong hands, in theory they wouldn't be able to connect it to the owner. At the same time, however, they acknowledged that this is not a fail-proof technique, and that it is possible, even likely, that techniques and technologies will be developed in the future where hostile actors could deduce such information. How could this affect me, an insignificant individual, was my first thought. Perhaps insurance companies that provide health coverage, or life insurance policies, could get their hands on this sort of information, potentially affecting the rate I would pay for such services.

Which brings me to my main question: If we really knew how insecure our data is, would it stop us from providing it in the first place? The people using Ashley Madison for extramarital affairs, if they understood the risk of having their identities and infidelities exposed, would they still use it? Most people wouldn't provide their confidential information, let alone financial info, to untrusted websites and entities. But what about those large organizations that we rely on to survive in the modern age (as opposed to social media where we willingly post information about ourselves, to be used to make profit for those companies)? Banks, hospitals, government departments, all already store ever increasing amounts of private

My Blog

marko-cyberlounge.azurewebsites.net

age (as opposed to social media where we willingly post information about ourselves, to be used to make profit for those companies)? Banks, hospitals, government departments, all already store ever increasing amounts of private data. Data that in the wrong hands could have a severe material impact on an individual's life and well-being. We are reminded of this by such events as the LifeLab hack in Canada, where personal medical data of up to 15 million Canadians may have been compromised! Only after the attack did LifeLabs hire cybersecurity experts to secure the system and determine the scope of the attack. Amateurs! As individuals, what are our options? Do we stop getting medically tested? That would be preposterous! Do we go back to only hardcopy data, after decades of trying to go digital? That, too, sounds unrealistic.

Arguably more harrowing is the discovery that adversaries routinely hack into our government departments, such as the military, to harvest personal information of personnel. ISIS apparently was able to gather personal information of US drone pilots; Russian and Chinese hackers have targeted the personal information of US Air Force pilots. Lots can be done with this info, such as targeting these people for sensitive information that they have access to, or more harrowingly, sending assassins to eliminate these valuable personnel in the event of an escalation of hostilities. A young individual, with dreams of flying airplanes or helicopters, might see the military as a good starting point to develop those skills, and get paid at the same time. Are they thinking of the possibility that they could one day end up on a potential hit-list of our adversaries? I doubt it.

The exponentially increasing amount of data that is digitized and stored in databases, mixed with the growing labour shortage of cybersecurity professionals, results in an alluring environment for cyber criminals and hostile state actors. Knowing that, along with my own experiences of evaluating the significance of the personal information that I put out there, has developed a sense of "cyber paranoia" within me, and was a main motivation for entering the world of cybersecurity. As the saying goes, "just because you're paranoid doesn't mean they aren't after you". Perhaps the question we should ask ourselves isn't how secure our data is, rather should we expect it to be secure over time, especially as it appears we are trending towards a more hostile world?

My Blog

marko-cyberlounge.azurewebsites.net

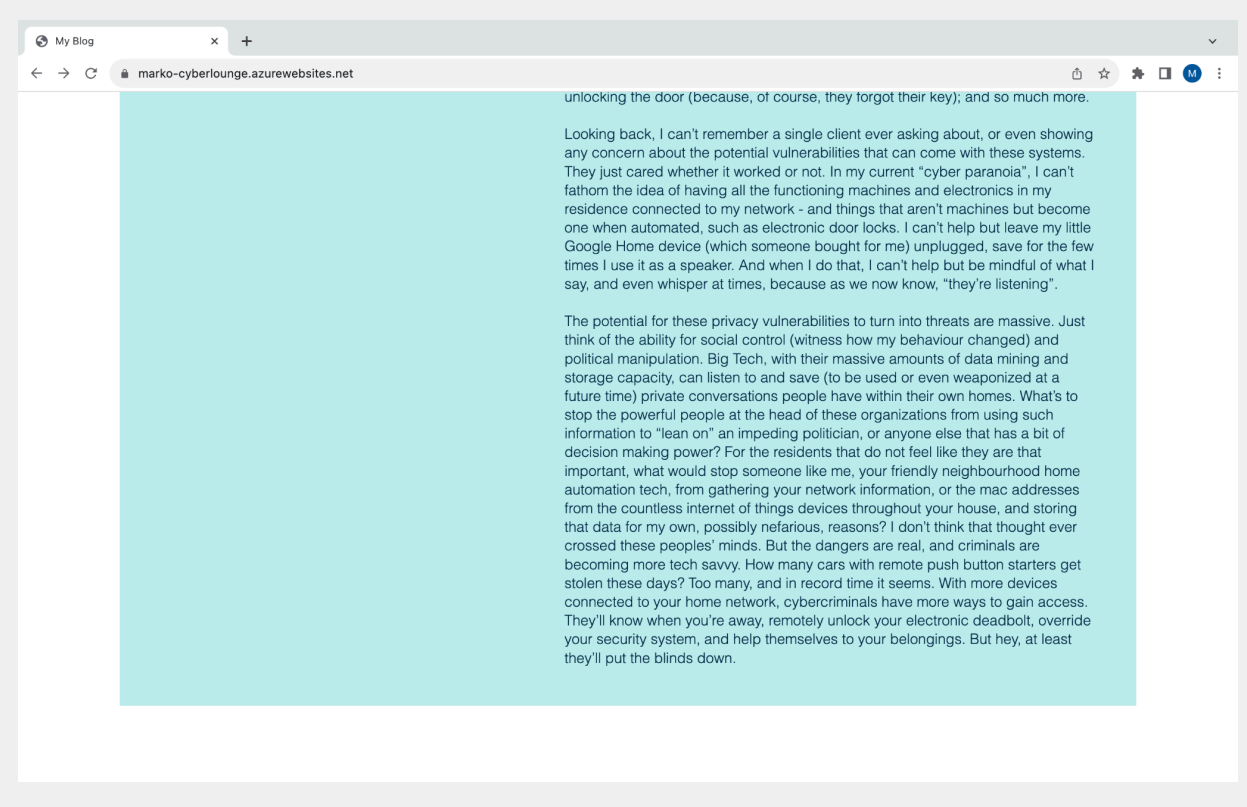
Would You Want a Home Automation System?

Internet of things; home automation; networks; Big Tech

The Internet of Things applications have grown massively over the last decade. In Toronto, where I live, I used to be involved with integrating some applications with home automation systems in private homes. It seemed like anyone that was half-way well-off (and you need to be to buy a house here) that was building a new custom house, or renovating an older one, was getting some level of home automation installed and integrated in their residence. I always looked at it as more of a luxury item that wasn't really "needed", however, I gradually came to appreciate its benefits: sensors that help regulate the temperature (colder when no one is home, and warmed up just in time for their arrival), leading to more efficiency; ability to control house fixtures, like blinds, when you're on vacation, making it look like someone is home (or, for those that have watched the Home Alone movies, to make sure the garage is closed - and that you didn't forget anybody!); making sure your kids can get in the house after school by remotely unlocking the door (because, of course, they forgot their key); and so much more.

Looking back, I can't remember a single client ever asking about, or even showing any concern about the potential vulnerabilities that can come with these systems. They just cared whether it worked or not. In my current "cyber paranoia", I can't fathom the idea of having all the functioning machines and electronics in my residence connected to my network - and things that aren't machines but become one when automated, such as electronic door locks. I can't help but leave my little Google Home device (which someone bought for me) unplugged, save for the few times I use it as a speaker. And when I do that, I can't help but be mindful of what I say, and even whisper at times, because as we now know, "they're listening".

The potential for these privacy vulnerabilities to turn into threats are massive. Just think of the ability for social control (witness how my behaviour changed) and political manipulation. Big Tech, with their massive amounts of data mining and storage capacity, can listen to and save (to be used or even weaponized at a future time) private conversations people have within their own homes. What's to



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?

```
marko-cyberlounge.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.119.0.23
```

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

```
Washington, Virginia, United States
```

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

```
Server:           192.168.2.1
Address:    192.168.2.1#53
Non-authoritative answer:
marko-cyberlounge.azurewebsites.net canonical name =
waws-prod-blu-373.sip.azurewebsites.windows.net.
waws-prod-blu-373.sip.azurewebsites.windows.net canonical name =
waws-prod-blu-373-0ed5.eastus.cloudapp.azure.com.
Name: waws-prod-blu-373-0ed5.eastus.cloudapp.azure.com
Address: 20.119.0.23
```

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
It works on the back end.
```

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

```
Inside of assets, there are two directories: css and images.
Within the css directory, there is a file (style.css) that contains a set of
formatting characteristics that define how to exhibit the html components -
that is, how the user will view the different items on the webpage.
Within the images directory, various images used in the html file are stored
here, such as pictures, the background, logos, etc.
```

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?

```
The client/organization that owns and manages specific instances on the
cloud service. It allows them to share computing resources in a public or
private cloud, with the data of each tenant being isolated, and thus
invisible to other tenants.
```

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

```
Since the key vault contains secrets that need to be securely stored, it is
important to control who and/or what has access to and the ability to
perform different operations on the contents of the key vault (keys,
secrets, and certificates).
```

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

```
Encryption Keys within the key vault are asymmetric, and can be generated or
imported. They are used to encrypt and decrypt data. What makes using the
keyvault more secure than just using code is the fact that the private key
never leaves the vault. This way, the keyvault allows us to use the keys
without actually seeing them, keeping our secrets and certificates more
secure than they otherwise would be when making connections between
different users and servers.

A secret is anything that is sensitive that is not an asymmetric key or a
certificate. Examples can be database connection strings, application
tokens, passwords, etc.

Certificates are used to establish an encrypted path to a website. They
validate the authenticity of a website using a chain of trust. They use the
public key cryptography (within the keyvault) to establish a secure
```

connection between the browser and the server.

Cryptography Questions

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

They are more simple to modify or customize. They are more appropriate for development and testing environments, as well as for websites on an internal network.

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

The lack of trust validation. This would make the viewer of the website less likely to input any important or personal information, such as credit card info to make a purchase.
There is a greater risk of compromise.
Furthermore, users must manually verify and trust these self-signed certificates by adding them to their trust stores. It is probable that many regular users would not even know what this means or how to do it.

3. What is a wildcard certificate?

Indicated by the wildcard character '*', these certificates are used to secure multiple primary domains and their first-level subdomains.

Some benefits include saving time and money, since it is more efficient and cost-effective to use a single wildcard certificate instead of multiple standard certificates. Furthermore, wildcard certificates have increased flexibility since they are used to secure multiple subdomains, which is helpful if subdomains need to be added or removed later on.

One of the big drawbacks is it creates a security risk. Due to a single shared private key being used for all the subdomains, in the event that it is compromised, all other subdomains on the same certificate become vulnerable. Also, wildcard certificates are difficult to keep track of across many servers. Should a certificate expire somewhere without being renewed, it can restrict access for users to the domains and subdomains they require access to.

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.

```
Microsoft disabled SSL 3.0 in order to protect its customers from a design
vulnerability that allows for man-in-the-middle attacks known as POODLE.
```

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, it is not because my webpage has a valid certificate that is enabled
from the Key Vault. My browser trusts the certificate because it has been
issued by an official/trustworthy company (DigiCert (root) and Microsoft
Azure (intermediate)).
Also, the certificate is not out of date (expires: June 27, 2024).
```

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

```
Tuesday September 5, 2023 @ 8:21:24 PM
to
Thursday June 27, 2024 @ 7:59:59 PM
```

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

```
Yes, it is Microsoft Azure TLS Issuing CA 01
```

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

```
Yes, it is 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.

```
Apple Root CA - G2
```

Day 3 Questions

Cloud Security Questions

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

```
Both reside in front of the web application in order to protect it; both work on Layer 7 (application layer) of the OSI model; both provide load balancing functions across a web service; they can both implement a web application firewall (WAF) in order to protect against web vulnerability attacks; both have additional features such as SSL/TLS termination and URL path-based routing.

The key difference between the two is that the Web Application Gateway is used more regionally, and is best suited to protect a web application in a single region in the cloud. On the other hand, the Azure Front Door is more global and better suited when there are multiple regions in a cloud environment.

We used Azure Front Door for our project because it is less expensive, and easier to implement.
```

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

```
SSL offloading, sometimes referred to as load balancing, is the implementation of processors whose task is limited to performing the functions required for SSL/TSL (i.e. the handshake and the encryption/decryption), which frees up processing power for the application or website to run more efficiently.
Some benefits include saving resources for the application servers to run their primary functions, making it faster for the users even if there is increased traffic. Also, depending what load balancer is being used, it can help with HTTPS traffic inspection, which is especially important for larger organizations.
```

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 managed rule will block this attack if it detects
attempts to exploit the SQL databases. It does this by monitoring network
traffic on the application layer (layer 7), and inspects and blocks requests
for potentially malicious signatures, patterns, and character sequences that
are characteristic of SQL injection attempts.
```

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 there are no user input fields to inject the malicious SQL
statement located anywhere within the website as it is currently designed.
```

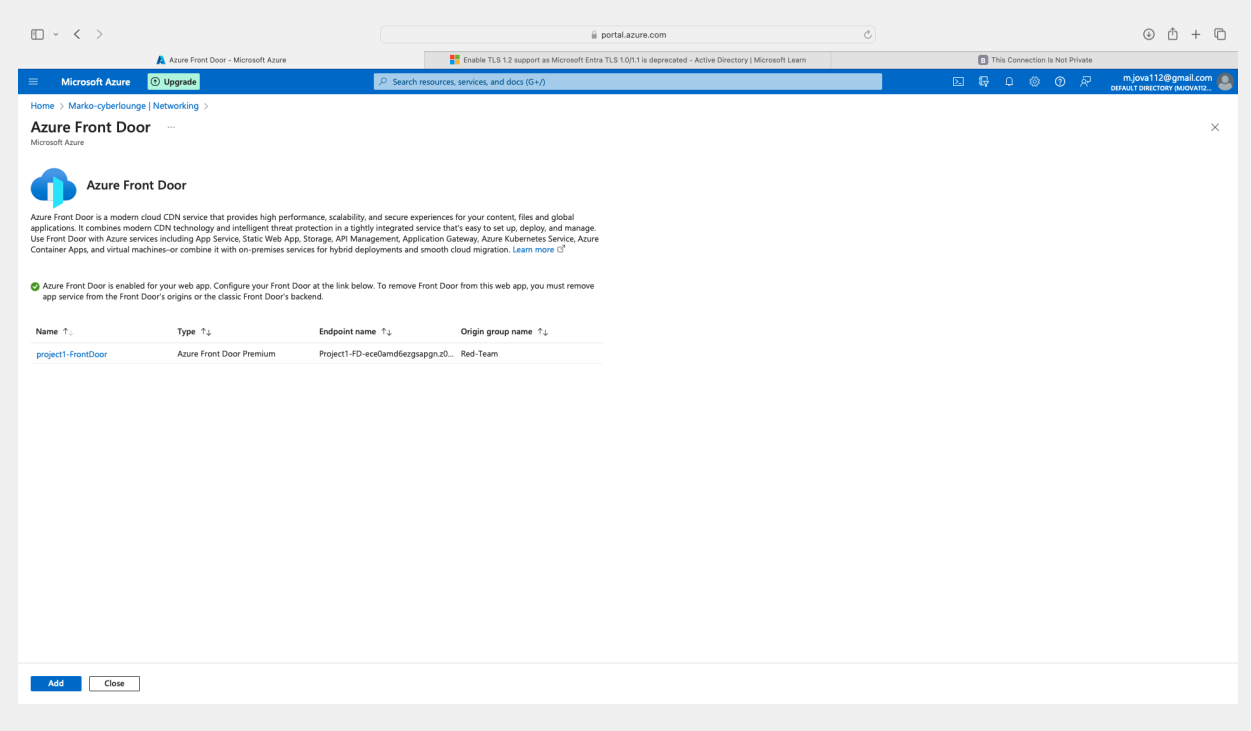
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

```
No, because someone could use a VPN to circumvent the WAF rule by making it
appear that they reside in a country that is not blocked by the rule.
```

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

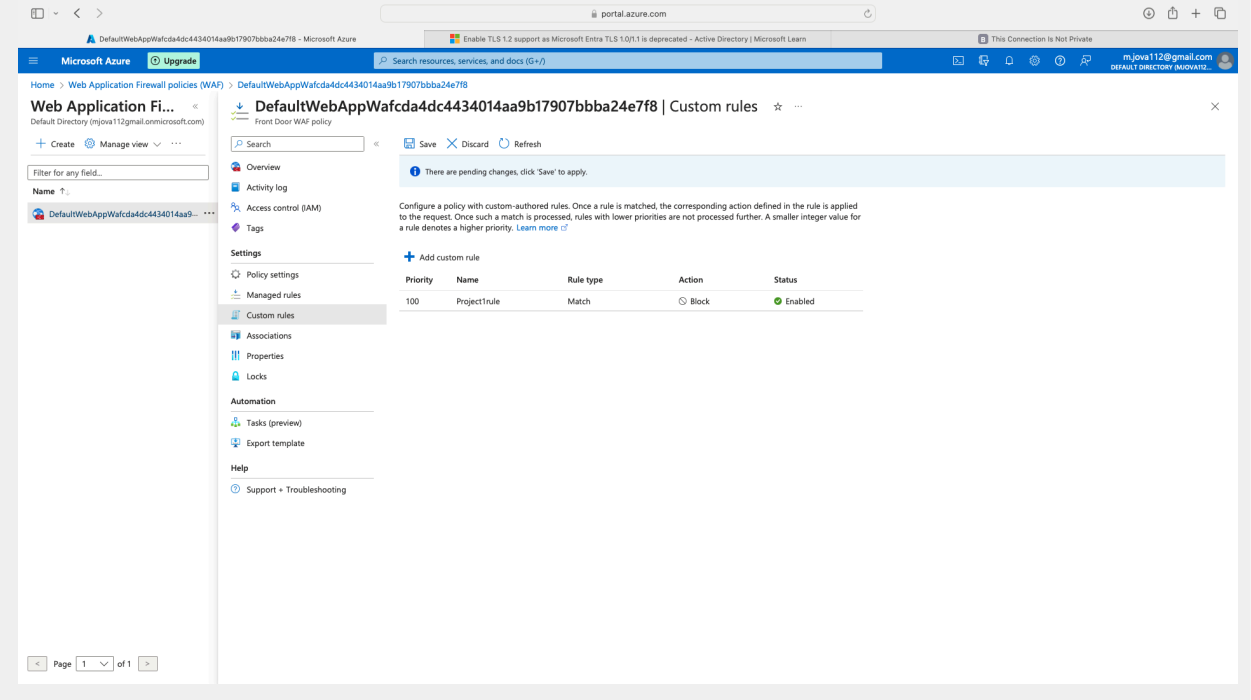
    a. Azure Front Door enabled

```
[Paste screenshot here]
```



b. A WAF custom rule

[Paste screenshot here]



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