



Securing Cloud Applications

Technical Report

Web Application Overview

Screenshots of the created website (read blog posts!!):

LUKE THURSTON'S CYBER BLOG

Send Email

 LinkedIn logo



Image 1

Something to Write Home About

Pen Testing

Among the inner circles of cybersecurity experts there are a number of topics that make sense to discuss loudly (if not effectively). But for someone looking at Cybersecurity from the outside, many of the conversations and discussion topics may appear weighty and overcomplicated. To remedy this gap, I wanted to take the chance to spell out the rationale behind why someone would spend 8-12 hours a day trying to 'capture a flag' or 'stegan-o-gra-fi' an image. You see to a cybersecurity analyst the world consists of only one type of object - DATA! The problem is that most data is incredibly insecure. This means it can be accessed or modified by bad actors with little programming acumen. In other words, hackers, foreign governments, and rogue employees have plenty of motive and opportunity to launch cyber attacks. If businesses are able to communicate securely with the employees in their network and members of the government are able to store data in systems that are not vulnerable, they will pay a high reward to those who ensure it stays that way. As a result, you see long strains of complicated encryption methods that use advanced mathematics to deter attackers. If it were possible to quickly identify and patch the holes in a cyber system, you would not have to pay a Pen Tester to dream up any and every way to access the data on file or bring down your network. But alas, the dream of a perfectly secure computer is (at this point) only a mirage.



Phase 1 - Build

General Considerations

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

Azure free domain

2. What is your domain name?

<https://lukessecurityresume.azurewebsites.net/>

Networking Questions

1. What is the IP address of your webpage?

13.77.50.113

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

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

	Test	Result
✓	HTTP Connect	200 OK
✓	HTTP Filter	
✓	HTTP Delay Check	Success - response in 932 ms
✓	HTTPS Certificate Check	
✓	HTTPS Certificate Expiration	

[dns lookup](#) [smtp diag](#) [blacklist](#) [http test](#)
Reported by [mxtoolbox.com](#) on 1/8/2024 at 9:45:08 PM, just for you. [Transcript](#)

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?

The runtime stack I selected was PHP 8.2 and it's a back-end stack. The reason it's a backend stack is because it gets interpreted by a backend server.

Source:

<https://www.quora.com/Is-PHP-primarily-a-front-end-or-back-end-language-Why#:~:text=PHP%20is%20considered%20a%20%E2%80%9Cbackend,%E2%80%9Cfrontend%E2%80%9D%20client%20side%20browser.>

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

The `assets` directory has the `css` files as well as the image files. `CSS` stands for cascading style sheets and is responsible for the layout and formatting of the webpage. The images folder is simply a collection of the images displayed on the site.

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

The `CSS` and image files contained in the subdirectories of the `assets` folder

are front-end. (Backend has to do with storing the data in a database. In other words there would be backend framework files - for example, express, angular, etc.)

Phase 2 - Secure

Cloud Technology

1. What is a cloud tenant?

According to loginradius.com, “Tenancy in cloud computing refers to the sharing of computing resources in a private or public environment that is isolated from other users and kept secret.” There can be a single tenant or a multi-tenant set up. With one tenant, each tenant has an individual database. With multiple tenants, there is still one application, but it is shared among multiple businesses. ([loginradius](https://loginradius.com), Understanding the Difference Between Single-Tenant and Multi-Tenant Cloud)

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

It determines what operations a user, group, or application can perform on secrets, keys, and certificates in the key vault. (learn.microsoft.com, Assign a Key Vault access policy)

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

In general we can think of keys (api keys, cryptographic keys, etc.) as being used to transform plain text to cipher text (encryption) or cipher text to plain text (decryption). Such keys can either be openly distributed (in which case, they are called public keys) or only shared with a select group of people (private keys).

On the other hand, we know from our project slides that a secret is “anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.”

We also know from our project slides that “SSL certificates are used to validate the authenticity of a web application and to assist with encrypting

the user's traffic between the client and the server.”

To summarize these differences, we can say that in a key-vault, the keys and certificates are types of secrets, but that secrets are a larger class of items that could include other data such as passwords and so forth.

Cryptography

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

The chief benefits of using self-signed certificates are that they require no fee and are relatively fast to set up. Other advantages include:

Advantages of a Self-Signed SSL Certificate

- Self-signed SSL certificates are free.
- They're suitable for internal (intranet) sites or testing environments.
- They encrypt the incoming and outgoing data with the same ciphers as any other paid SSL certificate.

Source: <https://sectigostore.com/page/what-is-a-self-signed-certificate/>

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

The main problem with self-signed certificates is that they are not trusted in most root stores. In other words, you may be able to add them to your own root store, but if someone from outside your network or on another device tries to access your material, their browser will throw a “Your connection is not private” error.

Other disadvantages include:

Disadvantages of a Self-Signed SSL Certificate

- No browsers and operating systems **trust** self-signed certificates.
- The browsers will **not show visual indicators of trust** like a padlock symbol and HTTPS in front of the domain name.
- Your websites visitors have to proceed through a security warning page with error messages like “**error_self_signed_cert**” or “**sec_error_untrusted_issuer**” or “**err_cert_authority_invalid**” to access your content. This means that the users must manually click on the “Accept Risk” button to open your website.
- Warning pages drastically **affect the traffic** on your website. If visitors don’t feel safe on your site, they’re bound to leave. This means they’re more likely to visit a competitor’s website and you could **lose business**.
- **People feel cautious** about sharing their personal information (such as credit card numbers, bank details, passwords, date of birth, phone number, email addresses, physical address, etc.) when a website is labeled as “**not secure**.”
- It’s easy for attackers to make self-signing certificates to perform **man-in-the-middle (MitM) attacks**. So, once the users bypass the security warning, they’re exposed to data theft and cyberattacks.
- Self signed certificates are **highly risky** for a website that offers paid subscriptions/memberships handles tax information or health records of users, accepts donations/charity or fundraising online or has an eCommerce facility.

Source: <https://sectigostore.com/page/what-is-a-self-signed-certificate/>

3. What is a wildcard certificate?

According to digicert, a wildcard certificate is “a single certificate with a wildcard character (*) in the domain name.” This allows multiple sub domains to be included with this certificate. For example, the certificate used for my blog was called *.azurewebsites.net. This applies because my full domain name is <https://lukessecurityresume.azurewebsites.net/>.

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.

Generally speaking, Transport Layer Security (TLS) is a protocol that is an upgraded version of Secure Socket Layer (SSL). According to ssl2buy.com, TLS 1.0, “was [an] upgrade of SSL v.3.0 released in January 1999.” In other words, SSL 3.0 is outdated and TLS versions 1.0, 1.1, and 1.2 patched vulnerabilities present in that older software protocol.

Source: <https://www.ssl2buy.com/wiki/ssl-vs-tls>

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?


Since I chose the free azure option, my certificate was pre-selected for me and there is no error when loading the page.



However, to follow along with the exercise, the certificate used at <https://self-signed.badssl.com/> does in fact return an error:

Not secure


https://self-signed.badssl.com



Your connection is not private

Attackers might be trying to steal your information from **self-signed.badssl.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

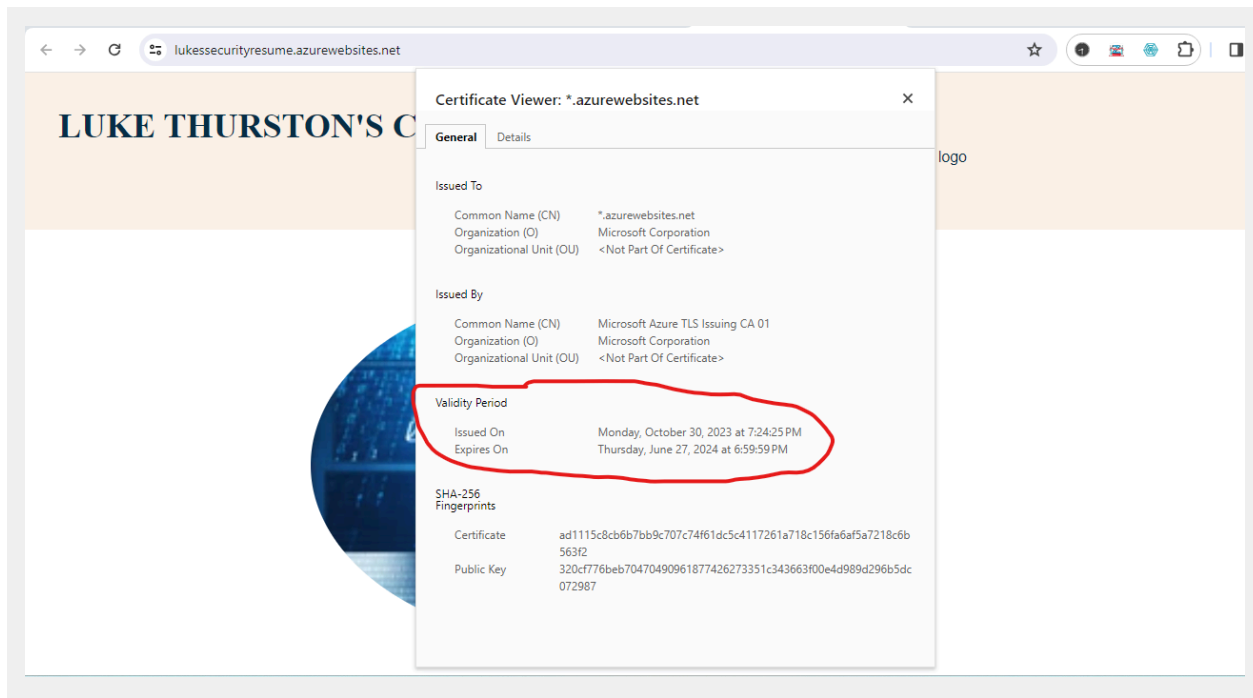
 To get Chrome's highest level of security, [turn on enhanced protection](#)

Advanced

Back to safety

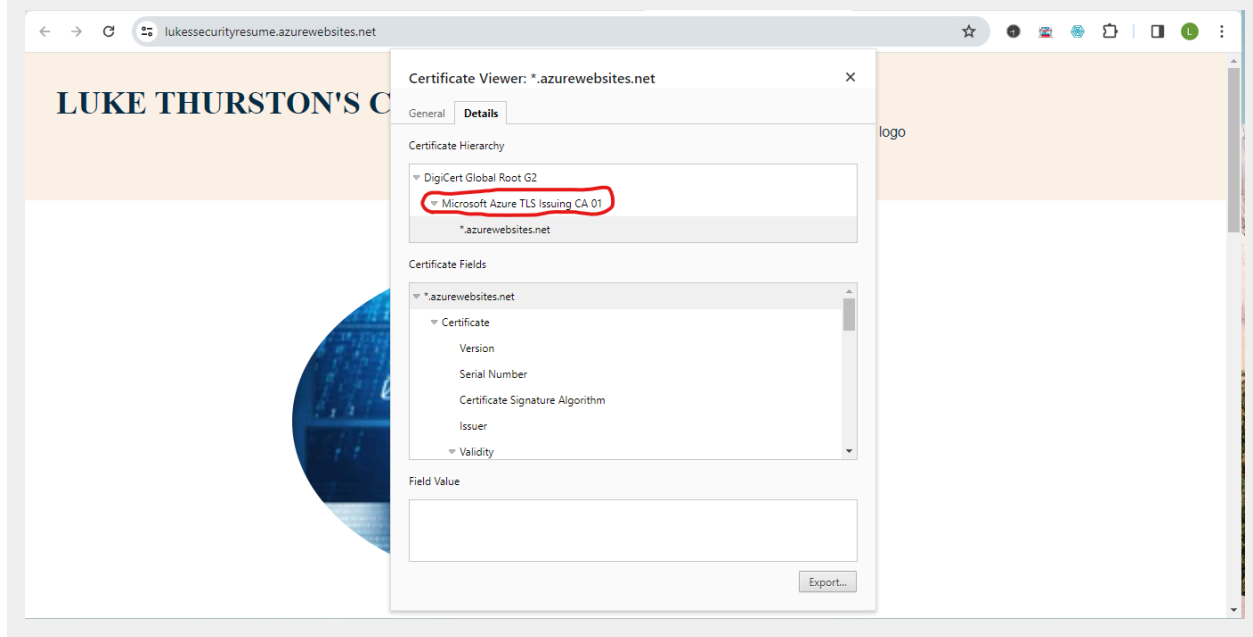
The reason for this is that the certificate at the second website is not issued by a trusted certificate authority.

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



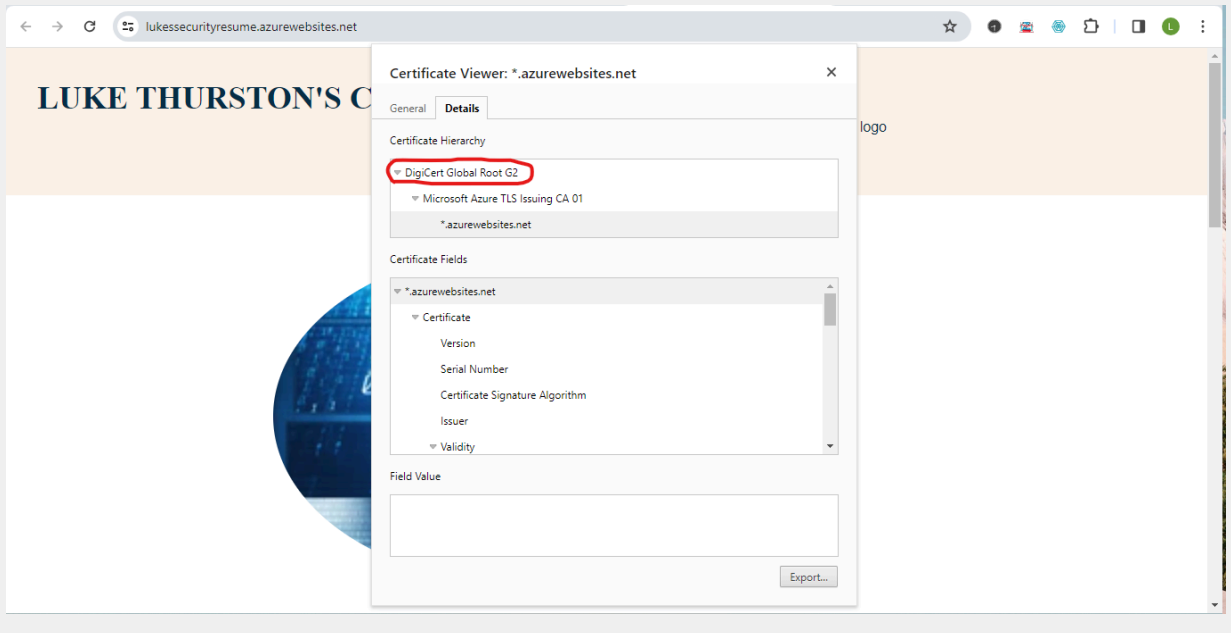
c. Do you have an intermediate certificate? If so, what is it?

Yes, it's **Microsoft Azure TLS Issuing CA 01** as circled below:



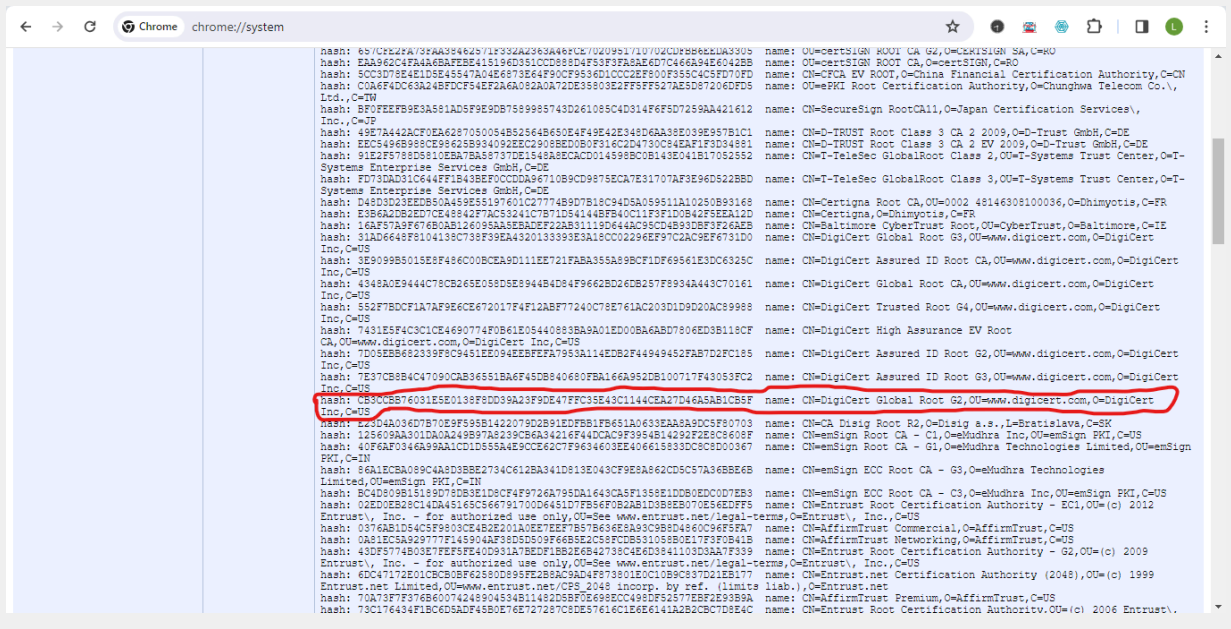
d. Do you have a root certificate? If so, what is it?

Yes, its **DigiCert Global Root G2** as circled below:



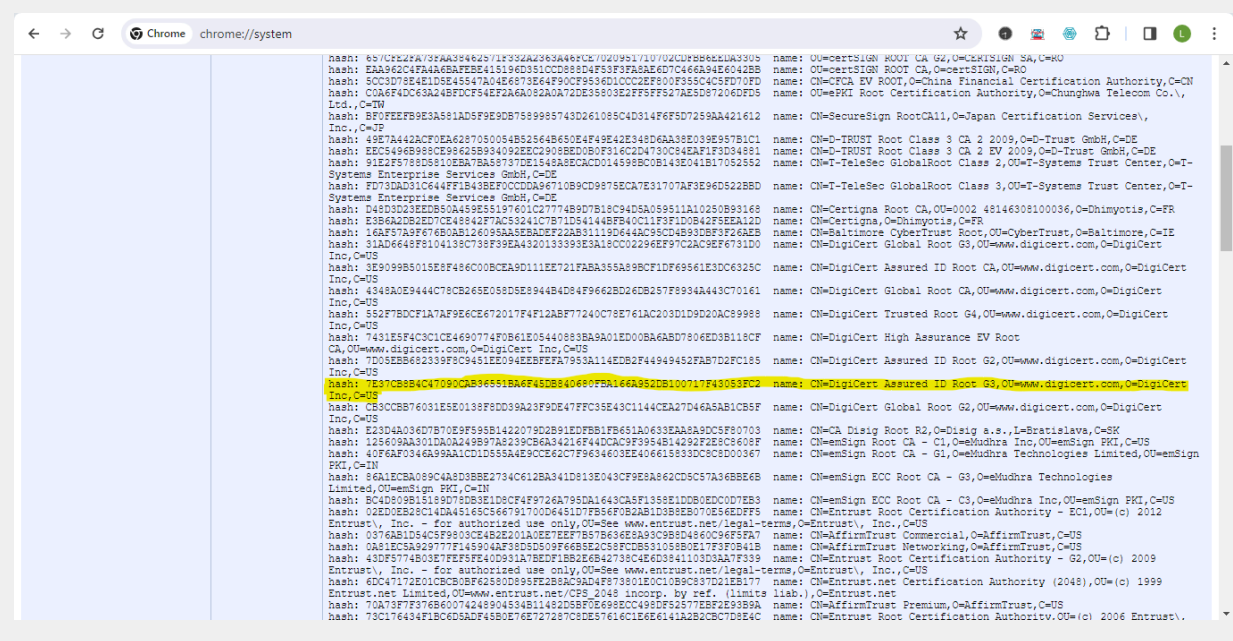
e. Does your browser have the root certificate in its root store?

Yes, by navigating to **chrome://system** we can see that **DigiCert Global Root G2** is listed in the names of trusted authorities:



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

Another Certificate Authority in the list of authorities would be **DigiCert Assured ID Root G3** as highlighted below:



Phase 3 - Protect

Cloud Security

1. Azure Web Application Gateway and Azure Front Door

According to Microsoft, both are “load balancers for HTTP/HTTPS traffic, but ... Front Door is a global service that can distribute requests across regions, while [Azure Web] Application Gateway is a regional service that can balance requests within a region.”

Source: <https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq>

2. A primary feature of the Web Application Gateway and Front Door is “SSL Offloading.”

AppViewX offers a very intuitive explanation of SSL offloading as follows: “SSL offloading means that all HTTPS traffic is decrypted on the Load

Balancer and passed to the backend servers in plain HTTP. This means all layer 7 actions are completed on the traffic before passing it to the backend hosts.”

Additionally, the benefits of SSL offloading can be summarized below:

Benefits of SSL Offloading

- The SSL offloader unit offloads the SSL handshaking task that involves both encryption and decryption—the two main tasks that bog down the computing power of the web application.
- The device completes the handshaking of SSL quicker than the web server. This results in smooth loading of the website and faster processing of requests at the end of the web application.
- It may also aid in HTTPS inspection, reverse proxy, traffic control, persistence of cookies, etc., depending on what kind of SSL load balancer you have installed at your end.
- HTTPS inspection is another most important point to use for SSL load-balancer. We understand how important encryption is, but it is a double-edged sword – attackers could be hiding and encrypting malicious code.

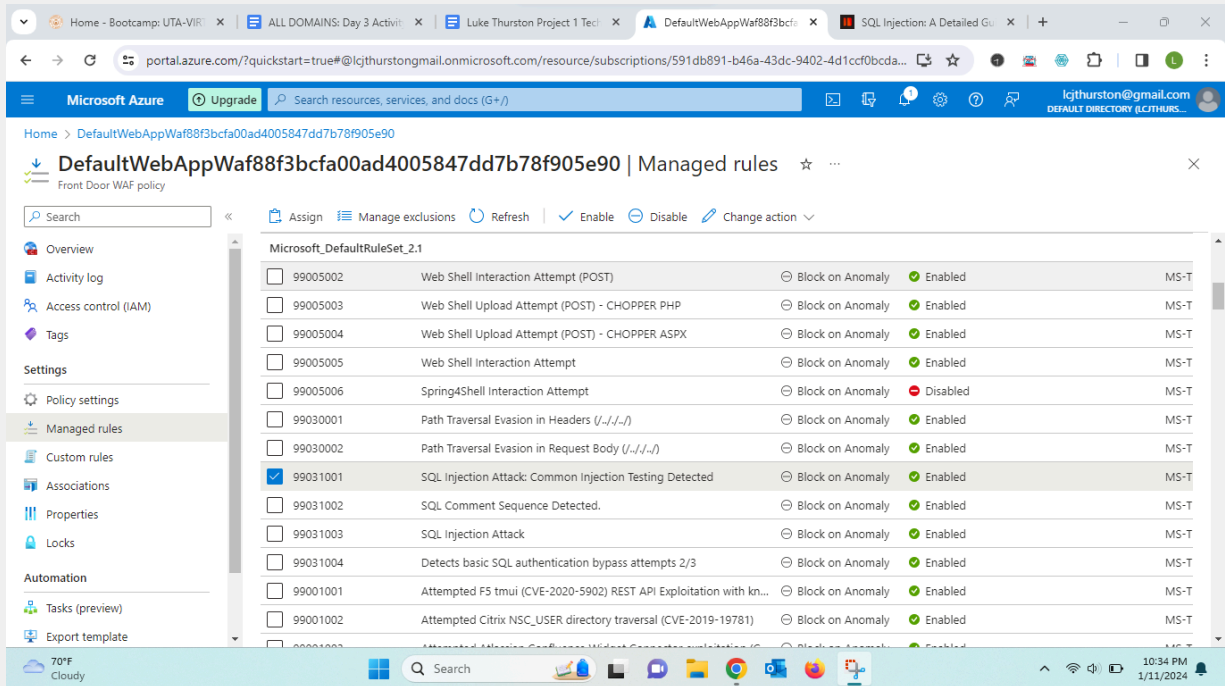
Source:

<https://www.appviewx.com/blogs/the-benefits-of-offloading-ssl-certs-on-f5-devices-and-how-to-automate-it/#:~:text=SSL%20offloading%20takes%20care%20of,tan%20on%20the%20web%20server.>

3. What OSI layer does a WAF work on?

A Web Application Firewall (WAF) works on layer 7 of the OSI model (i.e. the application layer) because it helps prevent web applications from attacks such as XSS (Cross Site Scripting) and SQL Injection.

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



The rule highlighted in the image above (i.e. blue checkmark) will scan for common signatures of SQL queries on the web app. Namely, if a client is requesting information that does not align with what the majority of other clients request, this rule will block such request from going through successfully.

- 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?

Absolutely - SQL Injection is a very common way to insert commands into a website that come across as plain text. When this text gets read by the backend, it can execute commands that were never intended by the developer of the site.

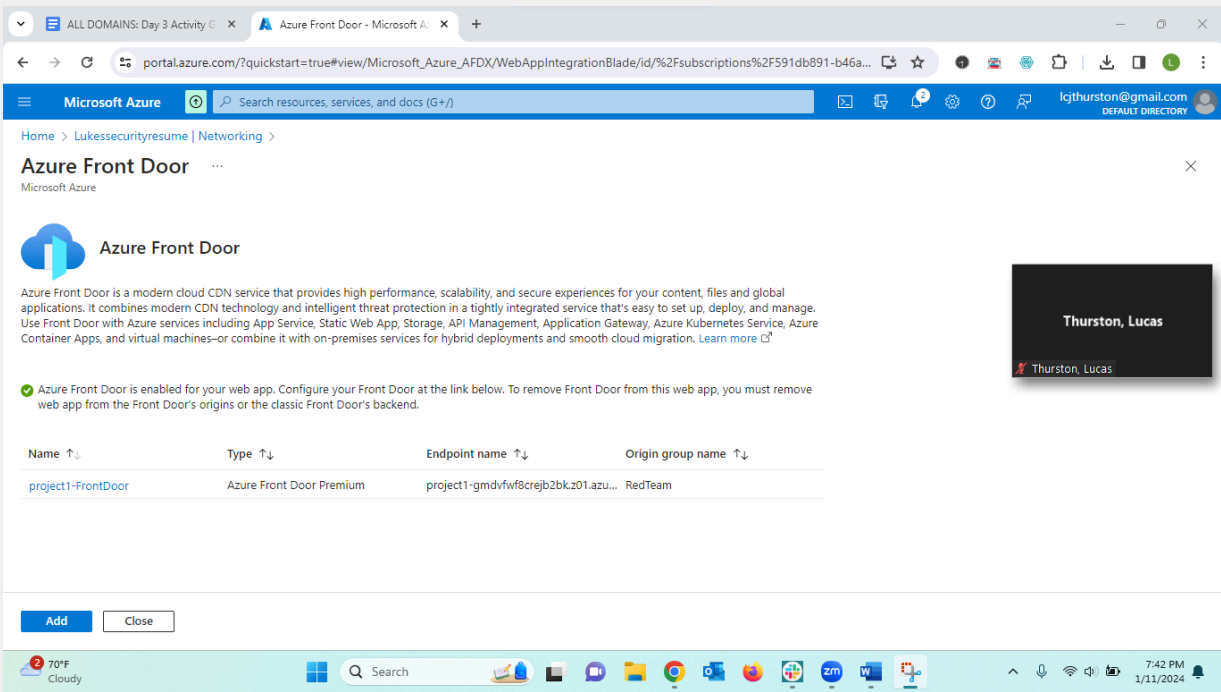
- Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

Persons in Canada could still access the website if they used an IP address that didn't originate from Canada. There are many ways to spoof an IP address, but the simplest would be having a virtual machine with a

non-Canadian IP access the website.

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

a. Azure Front Door enabled



Home > Lukesecurityresume | Networking >

Azure Front Door

Microsoft Azure

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](#)

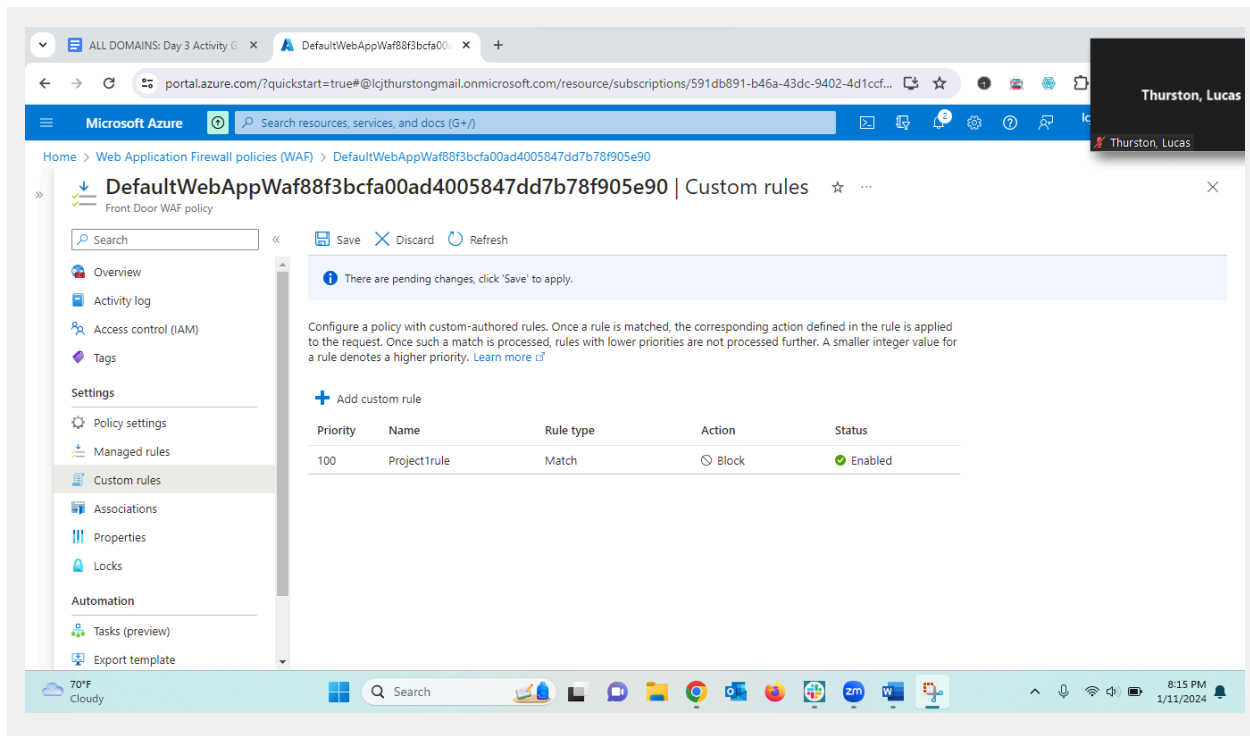
✓ Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove web app from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
project1-FrontDoor	Azure Front Door Premium	project1-gmdvfwf8crejb2bk.z01.azu...	RedTeam

[Add](#) [Close](#)

70°F Cloudy Search 7:42 PM 1/11/2024

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.
- ***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