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://intruderbware.azurewebsites.net/
```

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

Blog Posts

Ransomware-Why We Shouldnt Pay

ransomware, cybersecurity, protecting networks, security

We should think twice before paying bad actors ransomware because if they dont get paid for their efforts, then they will stop or slow down their efforts to breach businesses. According to blockchain data platform Chainalysis, ransomware revenue "plummeted" from $765.6 in 2021 to at least $456.8 in 2022. According to their data, it is due in part to businesses opting to not pay bad actors. This is music to my ears! More businesses today are also reserving budget money to protecting and securing their networks. I believe that by allocating resources to mitigate risk far outways the risk of not protecting assets and data. Customers are valueable and ensuring their personal information remains safe and confidential should be at the forefront of every business.

Fraudulent Emails-seeing an increase in activity

trends, remote workforce, phishing

As I get my cup of coffee and open my mail every morning, I have to go through the mundane task of reviewing "urgent" emails or "thank you for your order" and most recently "your banking information has been compromised." My heart rate increases until I realize they are just fraudulent emails. After spending wasted time on researching and investigating, I delete and go on with my day working on important tasks and activities. I have noticed an influx of fraudulent emails and texts on a daily basis. This is becoming very distractive during work as I have to concentrate and move very fast throughout the day. I may feel rushed and worried that I havent investiaged the email long enough to take action. Im sure others are feeling this burden as well. According to Justin Headley (Senior Manager in Warren Averett's Security, Risk and Controls Group), social-engineering attacks and phishing emails is still the primary method for threat actors to gain access to organizations. (https://www.bizjournals.com/birmingham/news/2023/03/13/table-of-experts-cybersecurity.html). It seems that this trend is only getting worse. Companies should insure they have proper education for their employees and constant communication on latest trends and issues. Along with engaging with outside vendors to help securing their network, educating employees will go a long way in tackling this ever growing issue.

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?

```
intruderbware.azurewebsites.net
```

Networking Questions

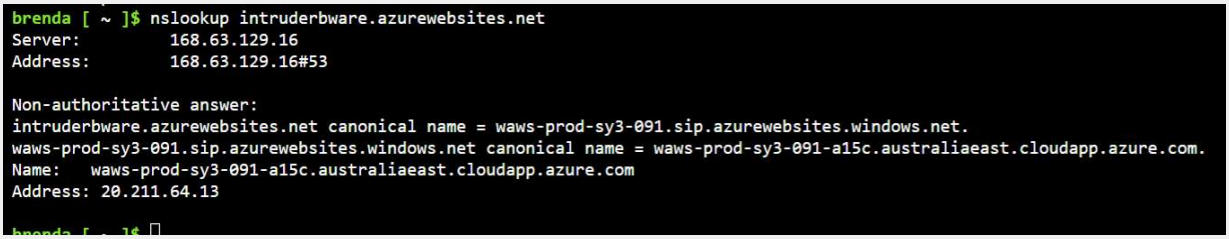
1. What is the IP address of your webpage?

```
20.211.64.13
```

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

```
 Falls Church, VA USA
```

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



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?

Picked PHP 8.2 runtime stack. The run time stack is a scripting language used for web creation. In our case, we are using PHP. PHP is considered a platform for backend scripting.

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

Assets are the images,stylesheets and fonts for the website. They are non code files that are directly copied to the “build” output. (docusaurus.io/docs/static-assets)

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

Front end as this is everything we can see on the website and things that dont change, like my font or picture. css folder links to html code.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

For cloud offerings,the tenant is the regional location that houses the servers that are providing cloud services.

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

It determines whether a given service principal, namely an application or user group, can perform different operations on Key Vault secrets, keys, and certificates. (ttps://stackshare.io/azure-key-vault-access-policy)

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

Keys are cryptographic as they can be generated using differ algorithms. Certificates are built on top of keys and secrets and add an automated feature like auto rotation. Secrets are those things such as passwords and secure storage and database connection strings.

Cryptography Questions

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

Advantage is cost savings as the person creating the certificate issues the cert, vs a third party trusted certificate authority. It is signed by using a private key. Another advantage is its fast, Dont have to wait for a third party CA to issue a cert. They are also good for dev/test environments and internal websites. (https://www.encryptionconsulting.com/education-center/self-signed-certificates/)

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

A self-signed certificate is not privately or publicly certified by a CA. Might not be considered as secure as a trusted CA. Another disadvantage is some browsers and O/S's do not trust self signed certificates. There will always be an "at risk" message before going forward into the website. Sometimes that will deter people from advancing. Per Encryption Counseling, self-signed certificates are highly risky for transaction or financial-related websites that handle memberships, subscriptions and users become vulnerable to data theft and other cyberattacks when attackers create self-signed certificates that can be used in man-in-the-middle (MITM) attacks. (https://www.encryptionconsulting.com/education-center/self-signed-certificates/)

3. What is a wildcard certificate?

A wildcard certification is a public key certificate that can be used to protect subdomains inside a domain. Its not acquired from a trusty CA. Multiple subdomains can be hard to manage, but with a wildcard certificate, you can secure many subdomains efficently. It can also save you money.

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 disabled by default in Windows Azure Pack because of the security vulnerability CVE-2014-3566 "Poodle" explained in Microsoft Security Advisory 3009008. (https://learn.microsoft.com/en-us/previous-versions/azure/windows-server-azure-pack/mt125373(v=technet.10))

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 I have the free version of Azure which already provided a certificate. I will answer the questions analyzing the mock self-signed certificate.

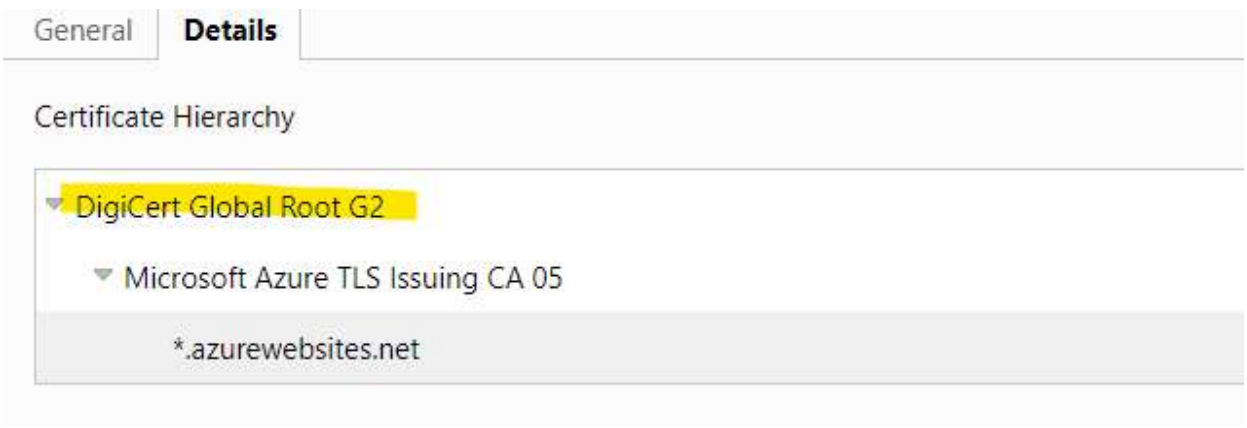
    b. What is the validity of your certificate (date range)?

It is active until 3/14/2023-3/13/2024

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

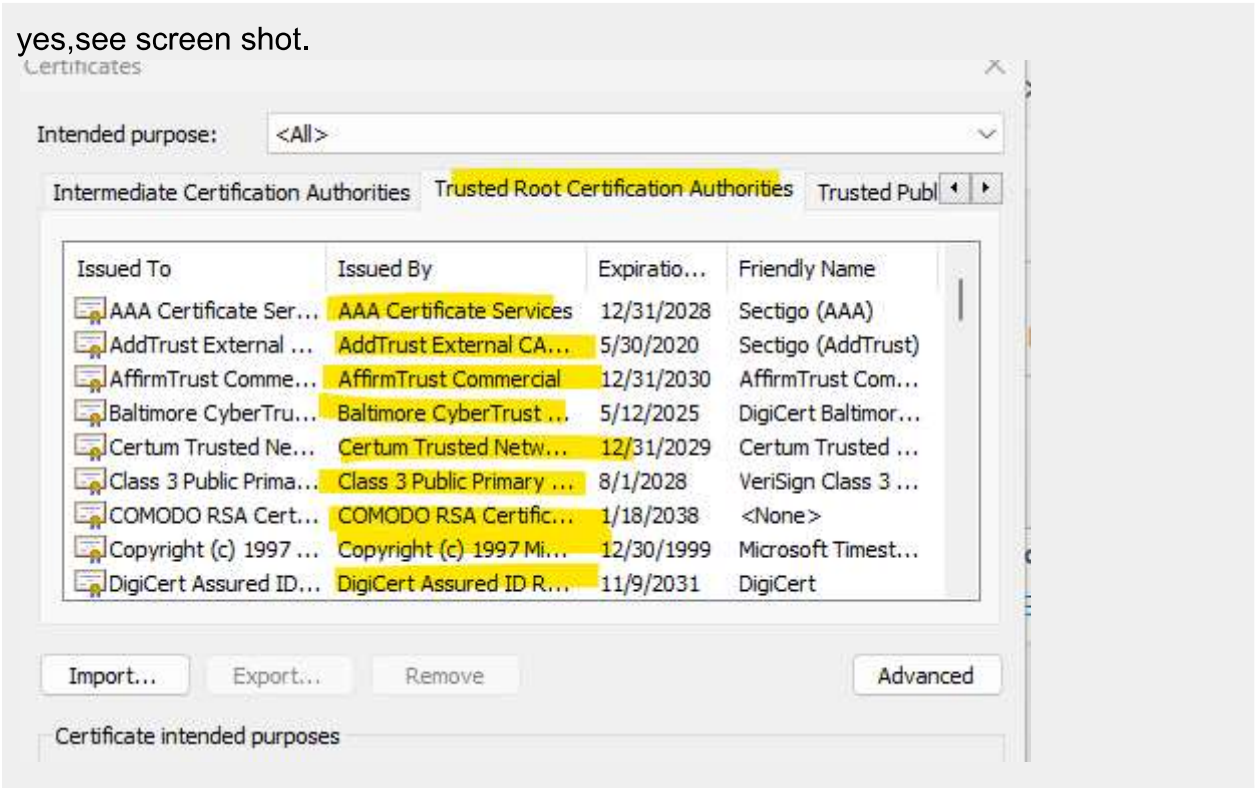
Yes, my blog website has an intermediate certificate, see screen shot.

    d. Do you have a root certificate? If so, what is it?
    Yes, see the cert for my blog website. Azure has a DigiCert Glbal Root G2 and Azure TLS issuing CA 05

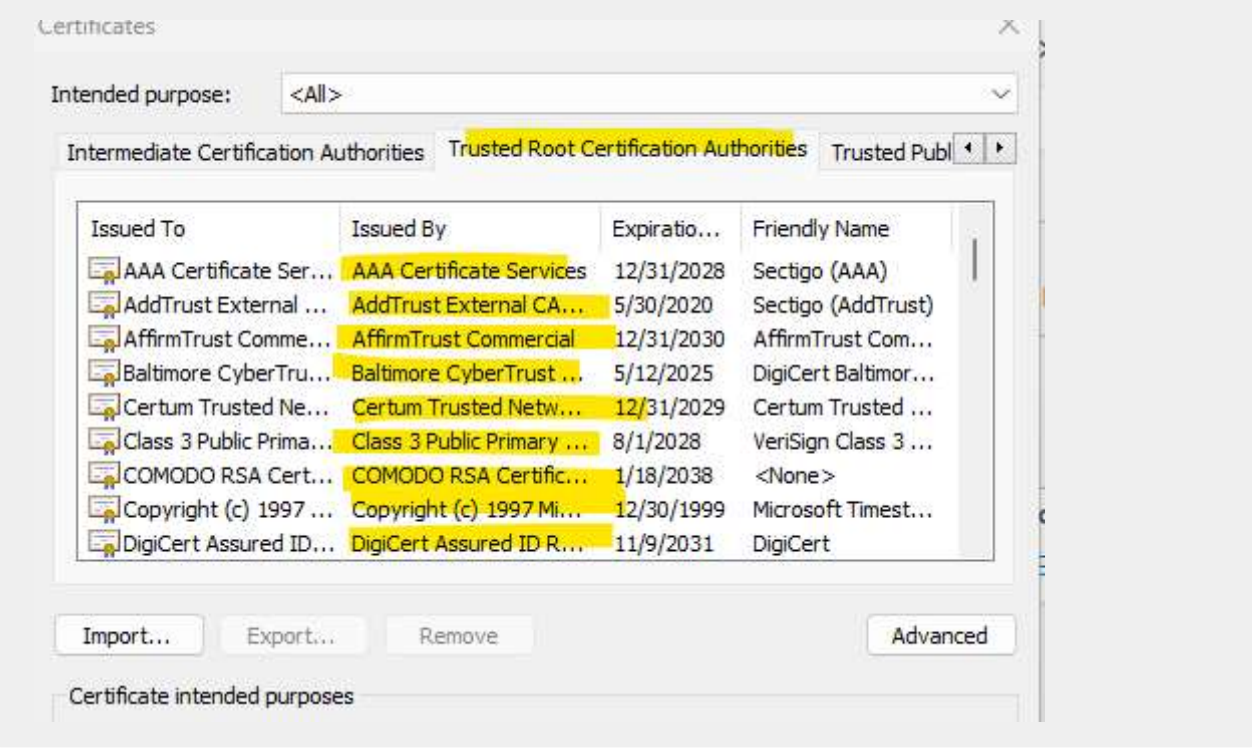


e. Does your browser have the root certificate in its root store?

yes,see screen shot.



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



Day 3 Questions

Cloud Security Questions

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

Both are networking management load balancers. They help manage web traffic to web applications on layer 7. Similarities include -
SSL/TLS termination, SSL Offloading, auto scaling, redundant zones, static IP, multiple site hosting, URL based routing, and HTTP/2 traffic native support is the similarities. .
Differences include-Front Door is a **global** load balancer while Application Gateway is a **regional** load balancer. This means that Front Door is better suited if you have multiple regions in your cloud and your priority is to route traffic to the most efficient endpoint.
Application Gateway is better for those who need deeper control over how traffic is balanced within the same region. You can write rules that govern exactly how Application Gateway distributes traffic within a regional application environment. (https://www.techtarget.com/searchcloudcomputing/tip/Pick-a-load-balancer-Azure-Front-Door-vs-Application-Gateway) You can also use both tools together.

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

SSL offloading relieves the server burden by terminating the encryption-decryption task by sending the traffic to a third party security device. This helps free up the server so it only has to read plain text. The appliance is set between the client's browser and the server. This ADC will receive client requests, decrypt the traffic and finally, send it to the server. A few benefits are that SSL offloading will accelerate SSL and increase performance on the server. It also ensures that the websites and applications are secured as it protects against threats like DDoS and man in the middle. It also balances the loads so one server is not getting exhausted or getting overburdened.
(https://arraynetworks.com/)

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.

The rules that Azure Web Application Firewall uses to detect and prevent common exploits are created, maintained, and updated by Microsoft's security team. If a rule changes, Microsoft updates Azure Web Application Firewall automatically. In a web form field, the attacker inserts text that will trick the server into running SQL commands. These commands allow the attacker to access sensitive data. Azure Web Application Firewall creates a barrier of non trust between a web app and its user input. Azure Web Application Firewall assumes that all input is potentially malicious, so it sanitizes the input. Sanitizing can mean removing dangerous text elements, such as SQL comment indicators (and, or, > <). Even while doing the sanitation, no harm will be done to the backend data.
(https://learn.microsoft.com/en-us/training/modules/introduction-azure-web-application-firewall/2-what-is-azure-web-application-firewall)

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?

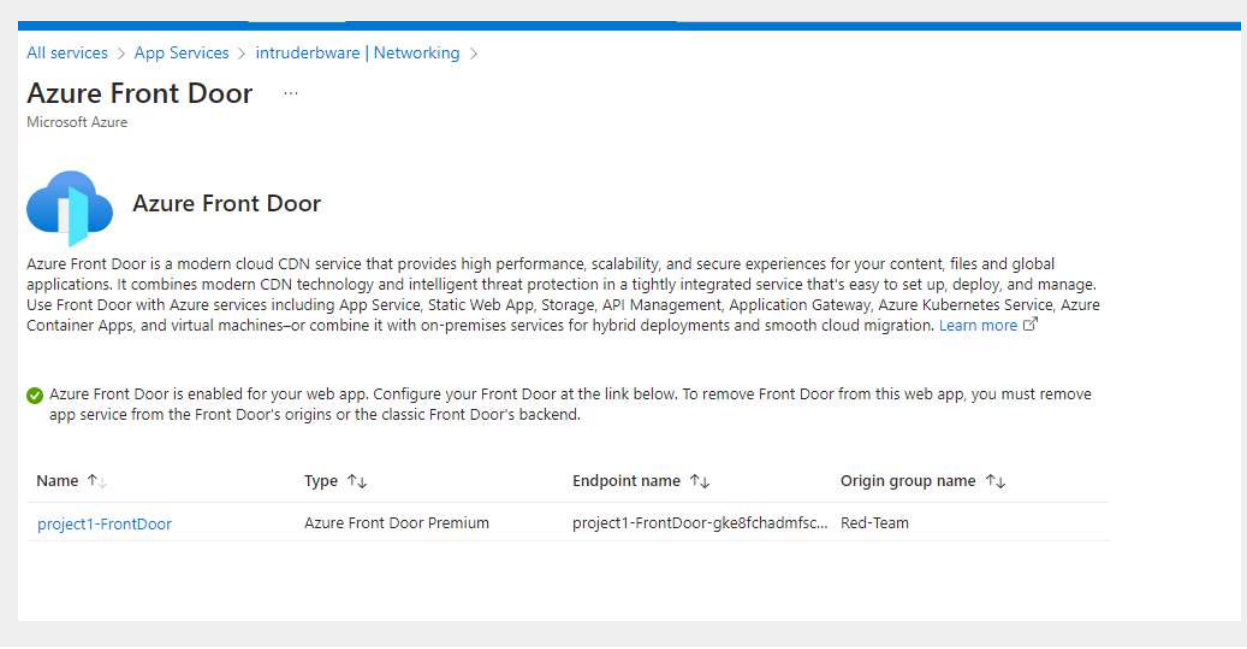
No because I dont have a field form for log in or contact me form. Nothing can be “submitted”.

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?

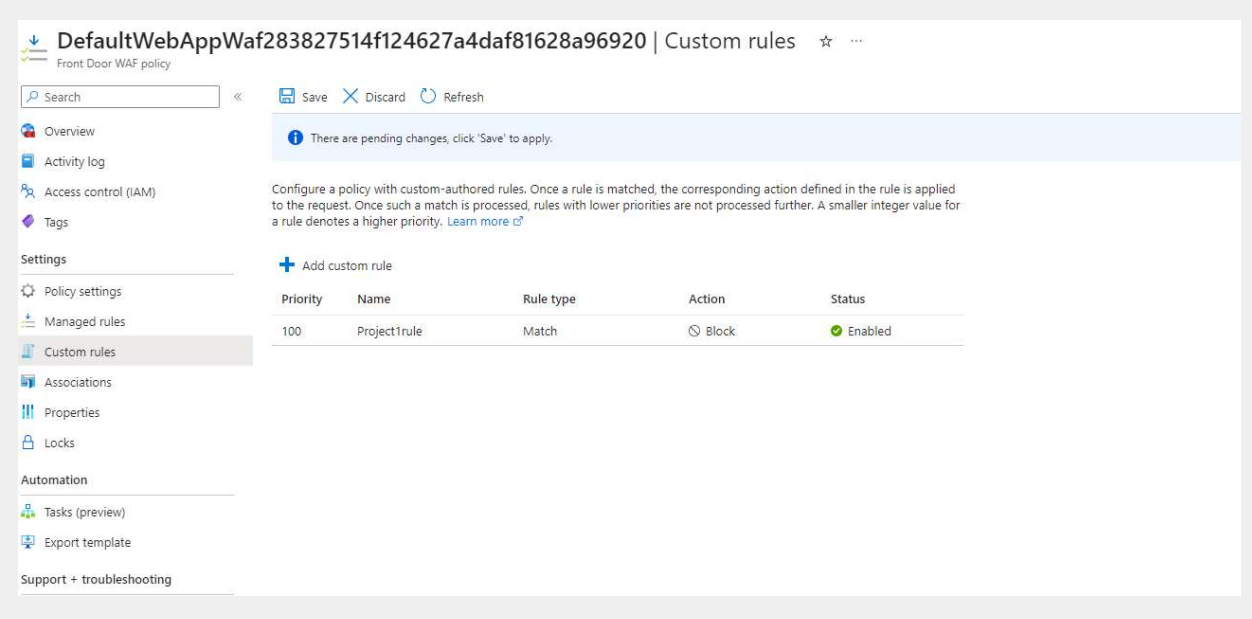
Hypothetically, No one from Canada would be able to access my website because we would block all traffic (rule) originating from Canada. After this rule is put into place, no one could come in through Canada, however,, a bad actor can obtain a VPN that shows originating from England (example) and tunnel into my website.

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.* ***yes***