



# 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://infosecarnold.com/>

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



## Blog Posts



### Ransomware: Should organizations pay or not?

Ransomware, Payment, Breach

Day after day, week after week, we are hearing more and more companies that have data stolen or leaked due to ransomware attacks. Often, these stories are not surprising. However, when the data that was breached contains valuable personal identifiable information (PII) attackers will attempt to exploit their target for money. This brings up a long debated idea, should organizations pay the ransom? Chris Rock, a professional hacker and co-founder of SIEMonster, a cybersecurity firm argues that organizations should pay the attackers. "They are not just one-time wonders, this is a business for them" Rock states. His idea is founded on the basis that ransomware attackers are fundamentally businessmen conducting valid business. If they release the stolen data after receiving payment, then their credibility goes down and no other organization will pay, he attests. However, others argue that these threat actors are not legitimate businesses and can not be trusted. Many find threat actor organizations to be untrustworthy. Expecting these organizations to follow common sense logic of an actual business is ill advised, according to Black Hills Information Security. Oftentimes, threat actor organizations tear each other apart from the inside. When that happens, what is to stop them from releasing your data anyways? The perfect world answer is that no organizations ever pay the ransomware threat actors. However, the world is not perfect.



### Are humans really the weakest link in security?

Phishing, Human Element

Short answer, yes. The human element of cybersecurity is often thought to be a huge vulnerability. There's a reason that phishing campaigns make up the vast majority of all cybersecurity attacks. According to recent research from IRONSCALES, 81% of global organizations have experienced an increase in phishing attacks since 2020. The type of phishing campaign used varies widely however they all have one thing in common, end users. Social engineering allows threat actors to send phishing emails with a surprising success rate resulting in 241,342 victims in 2020 alone, according to the FBI's Internet Crime Complaint Center (IC3). Recently, security researchers discovered a new phishing campaign targeting military contractors involved in weapon manufacturing. This campaign stood out for its secure C2 infrastructure and multiple layers of obfuscation in the PowerShell stagers. However it did require one thing, a user to download the ZIP attachment. Despite every known and unknown bug and exploit, at the end of the day the user is still the most vulnerable security link.

## Day 1 Questions

### General Questions

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

GoDaddy

2. What is your domain name?

infosecarnold.com

## Networking Questions

1. What is the IP address of your webpage?

```
20.49.104.34
```

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

```
Hampden Sydney  
Virginia  
United States
```

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

```
nslookup -type=NS infosecarnold.com  
Server:  cdns01.comcast.net  
Address:  2001:558:feed::1  
Non-authoritative answer:  
infosecarnold.com      nameserver = ns50.domaincontrol.com  
infosecarnold.com      nameserver = ns49.domaincontrol.com  
ns49.domaincontrol.com internet address = 97.74.104.25  
ns49.domaincontrol.com AAAA IPv6 address = 2603:5:2182::19  
ns50.domaincontrol.com internet address = 173.201.72.25  
ns50.domaincontrol.com AAAA IPv6 address = 2603:5:2282::19
```

## 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  
back end
```

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

```
Assets contains the web assets that the the website uses on the front end of
```

the application

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?

A user who purchases cloud resources

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

An access policy determines what user or group of users can perform what operations on Key Vault secrets, keys, and certificates.

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

Keys: enables the use of software-protected and HSM-protected keys  
Secrets: Provide secure, encrypted, storage of passwords and database connection strings.  
Certificates: add on an automated renewal feature

### Cryptography Questions

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

Fast, free, easy to issue

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

Do not provide any trust value. Most common web browsers will not trust them

### 3. What is a wildcard certificate?

A certificate with a wildcard (\*) allows the certificate to secure multiple sub domains 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.

To protect customers from the known design vulnerability in the way SSL 3.0 handles block cipher mode padding

### 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. The SSL certificate is signed by azure, a trusted CA

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

Expiration date: 7/6/2023

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

Yes: GeoTrust Global TLS RSA4096 SHA256 2022 CA1

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

Yes: DigiCert Global Root CA

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

Yes

CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US

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

CN=Certigna Root CA,OU=0002 48146308100036,O=Dhimyotis,C=FR

## Day 3 Questions

### Cloud Security Questions

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

Similarities: Reside in front of your web application for protection - Layer 7 of OSI - Is a load balancer - can use a WAF - URL path based routing - SSL/TLS termination

Differences: Web Application Gateway is more regional. It protects a web app in a single region in your cloud.

Azure Front Door is more global. It is better suited for when you have a variety of regions in a cloud environment.

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

A separate load balancer that removes the SSL based encryptions from incoming web traffic in order to reduce strain from the web server.

3. What OSI layer does a WAF work on?

OSI layer 7

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

SQL injection is when an attacker inserts malicious SQL code into a web request in order to modify or extract data. The WAF SQL rule would inspect for malicious SQL code.

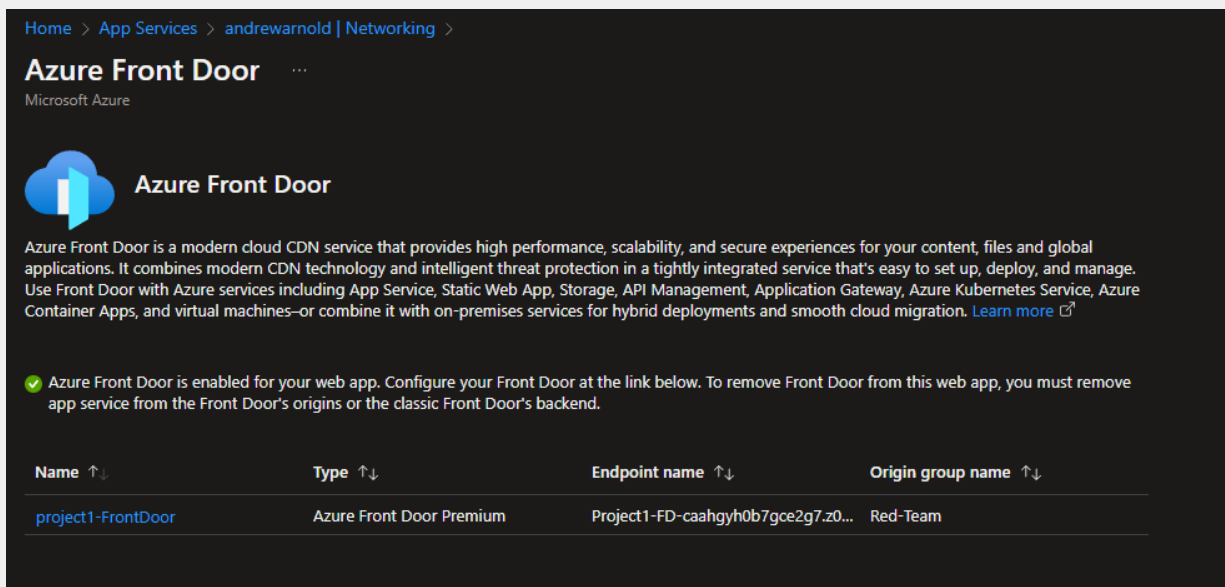
5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn't enabled? Why or why not?

No, because my current website does not have any way to insert SQL code.

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, people in Canada can access the website. They can access the website if they have a VPN or a way to change their geolocation.


7. Include screenshots below to demonstrate that your web app has the following:
- a. Azure Front Door enabled



Home > App Services > andrewarnold | Networking >

## Azure Front Door

Microsoft Azure

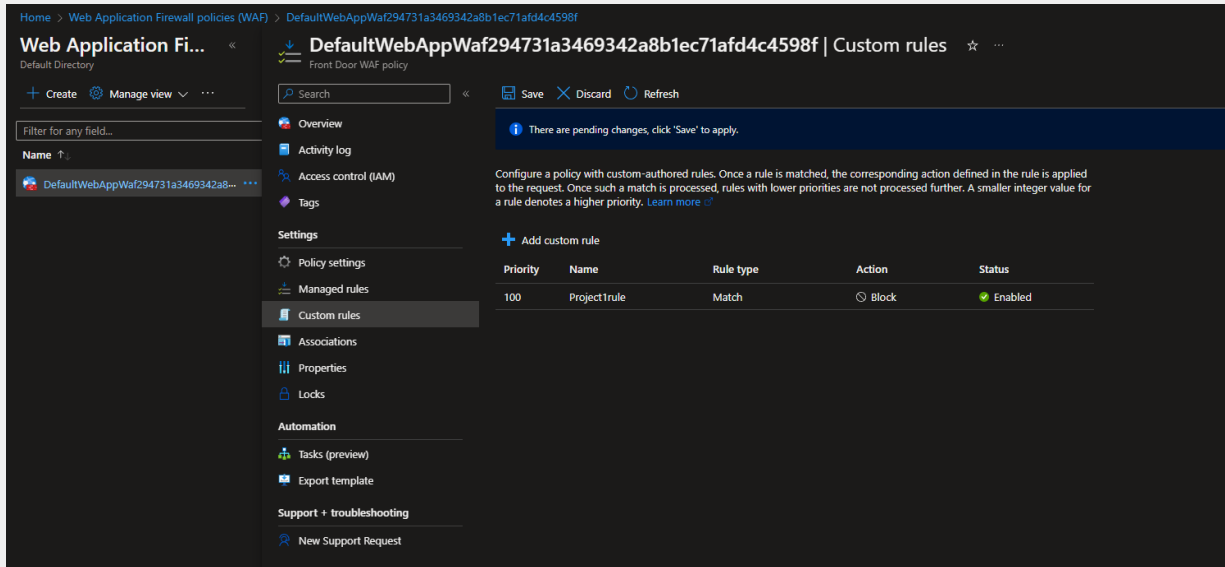
 **Azure Front Door**

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 ↑↓
<a href="#">project1-FrontDoor</a>	Azure Front Door Premium	Project1-FD-caahgyh0b7gce2g7.z0...	Red-Team

- 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**