



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://ryanknowssecurity.com>

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

Ryan Uliss's Cyber Blog

Send Email






Hi, I'm Ryan!

Helping people secure their personal information has always been a passion of mine. I love helping people out of tough situations and giving the people that I work with peace of mind. I am currently undergoing education to further my knowledge of the complex world of CyberSecurity. Previously, I have several years of fraud prevention and assistance experience with major companies such as Yelp, Uber, and TransUnion. Nothing quite puts a smile on my face like assisting a nervous or scared customer who is a victim of fraud and showing that these situations, while tough, can be overcome with proper prevention and security techniques. Feel free to check in here regularly for the new developments within the CyberSecurity world. Don't hesitate to reach out directly with any questions, concerns, or topics you would like me to cover specifically.

Blog Posts



Employment Fraud is Real?

Fraud, Employment, LinkedIn, Cybersecurity



Employment Fraud is Real?

Fraud, Employment, LinkedIn, Cybersecurity

Yes! Employment fraud is real and is happening to people in this country every day. This may not be the first type of fraud that comes to mind when we think of 'Identity Theft', as one tends to think about credit card or loan fraud. But yes, we are starting to see a trend where fraudsters are using the credentials and identities of other people in order to gain employment and a paycheck. Now why might somebody do this? Well, there are a number of different reasons, the most obvious would be to gain employment, and payment from, an organization they do not have the qualifications to apply for on their own. There is also the benefit of receiving the benefits of a paycheck without having to deal with taxes and the IRS. Usually, the way an individual will become aware that they are a victim, is when they are contacted by the IRS about income they obtained from a company they never worked at, or a state that they never worked in. Luckily, companies that are hiring are becoming more aware of this fraud trend, and working towards verification techniques to confirm that the person they are interviewing is who they say they are. Linked In has also recently added additional information to its user's pages, now allowing us to view when the account was created, when it was last updated, and whether or not the account has been verified via email. So for all of you looking to break into a new field and start with a new company, be aware that these risks are out there, go out of the way to verify your Linked In account, in order to avoid any confusion, and review your tax information thoroughly in order to confirm no other unrecognized sources of income are being reported with your Social Security Number! Should you become aware of anything of this nature on your file, contact the IRS for resolution immediately.



What is Pig Butchering?

Scams, Cryptocurrency, Pig Butchering

Pig Butchering, a scary sounding name for an even scarier fraud trend currently on the rise. Pig Butchering revolves around scamming individuals through a combination of cryptocurrency investments and dating apps. The way this usually works is that fraudsters will hunt for victims on popular dating apps, and prey on people who are looking to find another special somebody. The scam begins innocently enough, with the fraudster gaining the trust of the victim through flirtatious conversation. This eventually leads to the fraudster convincing the victim to send them money as an investment on a Cryptocurrency exchange app. Once the money is deposited, the app displays, inaccurately, a large financial gain on the investment, luring the victim into a false sense of security and financial gain. Once the victim decides it is time to withdraw, the fraudster withdraws all funds from the account, and cuts off all conversation with the victim. Sometimes, the app will explain that they can receive their funds by paying a large tax on the account, but even individuals who paid this tax were again cut off from all conversation, and the funds never recovered. This is a particularly cruel way to scam an individual, as they are usually innocent hard working people just looking for love, yet they can have their entire financial livelihood uprooted. Studies show that most of these 'Pig Butchering' accounts come from China. They also suggest that a lot of the fraudsters are themselves victims of human trafficking and are forced into this work by their captors, a very scary thought. This is a perfect example that shows just how fraud can pop up anywhere, and how widespread this type of theft can be across the globe. For anybody currently on these dating apps, beware of the risks associated, take necessary precautions, and don't end up a butchered pig!

Day 1 Questions

General Questions

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

Go Daddy

2. What is your domain name?

www.ryanknowssecurity.com

Networking Questions

1. What is the IP address of your webpage?

20.119.0.29

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: homeportal
Address: 2600:1700:4180:1aa0: :1

Non-authoritative answer:
Name: ryanknowssecurity.com
Address: 20.119.0.29

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 stack we selected was a back end source code written in PHP to assist with the layout and design of the website from the creator's side.

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

This contains the specifics of the website, for example border and margin sizes as well as fonts displayed.

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

Front end as it affects the viewer/customer side and the front facing website.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

An organization that provides cloud computing services. 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.

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

It allows for only approved individuals to make any edits or changes to the key vault. A key vault access policy determines whether a given security principal, namely a user, application, or user group, 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: Support multiple key types and algorithms, and enables the use of software-protected and HSM-protected keys.

Secrets - Provide secure storage of secrets, such as passwords and database

connection strings.

Certificates - Built on top of keys and secrets and add an automated renewal feature.

Cryptography Questions

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

They are simple to modify or customize. They can carry more metadata or have greater key sizes. There are zero dependencies on others for the issuance of certificates, which saves time for testing purposes.

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

They do not provide any trust value, so are mostly useless in establishing identity assurance. They also cannot be revoked.

3. What is a wildcard certificate?

A public key certificate which can be used with multiple sub-domains of a domain. The principal use is for securing web sites with HTTPS, but there are also applications in many other fields.

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 was found to have a major vulnerability, which has led to safety concerns. Microsoft has completely disabled SSL 3.0 in Azure.

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 now using a trusted and validated certificate so a warning message is not appearing.

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

03/01/2023 - 09/02/2023

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

GeoTrust GLoBal TLS RSA4096 SHA256 2022 CA1

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

DigiCert Global Root CA

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 2,O=Amazon,C=US

Day 3 Questions

Cloud Security Questions

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

Similarities:

- They both reside in front of your application.
- They work on Application Layer 7.
- PRimary solution is a load balancer.
- Can incorporate a web application firewall to protect against web vulnerability attacks.
- Have additional features such as URL path-based routing and SSL/TLS termination.

Differences:

- Web Application Gateway is more regional and is best suited to protect a web application in a single region in your cloud.
- The Azure Front Door is more global and is better suited 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?

SSL offloading takes care of the encryption/decryption process on a separate device so that it doesn't affect the web server's performance. The idea behind SSL offloading is to do encryption operations anywhere other than on the web server.

3. What OSI layer does a WAF work on?

Level 7, Application

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

SQL Injection - also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include a number of items, including sensitive company data, user lists or private customer details.

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?

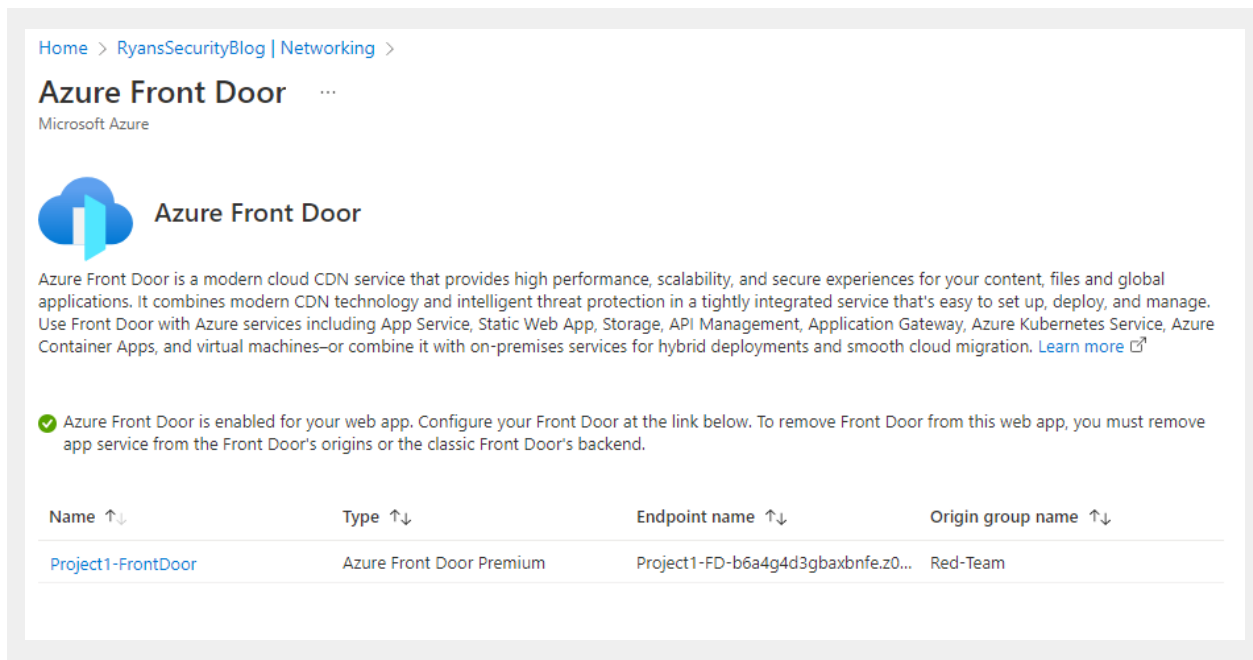
No, it would not be possible for somebody to use SQL injection to break into the site if the Front Door was not enabled. The reason for this would be simply because the website I am maintaining is not a database, and does not have a vulnerability for that specific type of attack and that sensitive information to be obtained.

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?

Not necessarily, it would mean that the user's IP address could not originate from Canada, which can be spoofed fairly simply with something like a VPN.

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


- a. Azure Front Door enabled



Home > RyansSecurityBlog | 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 ↑↓
Project1-FrontDoor	Azure Front Door Premium	Project1-FD-b6a4g4d3gbaxbnfe.z0...	Red-Team

- b. A WAF custom rule

DefaultWebAppWaf32d33e7f9cc2421c93f01958e48aa253 | Custom rules ☆ ⋮

Front Door WAF policy

Search

Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Policy settings

Managed rules

Custom rules

Associations

Properties

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. [Learn more](#)

+ Add custom rule

Priority	Name	Rule type	Action	Status
100	Project1Rule	Match	Block	Enabled

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.*