



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://andreasecurityresume.azurewebsites.net/`

Inbox (5) - andreaszerbe@gmail.com | My Online Resume | PROJECT 1 - Google Drive | Day 1 Notes - Google Docs | Copy of Cyber Security resu... | Resume HTML - Google Docs | Project 1 Technical Brief - Go... | AndreaSecurityResume - Mo... | ash_769.254.130.2 | +


andreasecurityresume.azurewebsites.net

Gmail | CU - Outlook | DRIVE | TrueCoach | Netflix | PRIME | Discord | ChatGPT | Outdoor Profile | U of M CYBER BO... | networking | CSCS | Other Bookmarks

Andrea Zerbe

Minneapolis, MN
Phone: (652) 451-2301 | Email: andreaszerbe@gmail.com

[in](#)



Summary

Diligent, smart, and resourceful team player with a cyber security certification from the University of Minnesota and a bachelor's degree from the University of Colorado Boulder. 6 months of trouble shooting experience and excited to continue my learning through tackling daunting challenges in the immense cybersecurity industry. A natural leader with experience in military, business ownership, health sciences, professional athletics and customer service. Driven to learn and grow in a fast paced organization.

Certifications

Certified Strength and Conditioning Specialist (CSCS): National Strength and Conditioning Association (NSCA)
Level 1 USA Climbing Routesetter: USA Climbing
Lifeguard/First Aid/CPR/AED: American Red Cross

Technical Skills

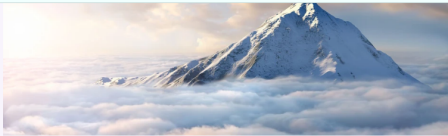
Programming Languages and Technologies: Terminal/bash, JavaScript, HTML, SQL, ChatGPT, AI prompt engineering, Windows OS, Mac OS, Linux OS, Screaming Frog SEO Spider, SEMRUSH, Wreshark, Kali Linux, John the Ripper, Aircrack-ng, Splunk, Snort
Cybersecurity and Networking: Network Security, Vulnerability Management, Information Assurance, Security information and Event Management (SIEM), Threat & Vulnerability Management, Linux, Malware Analysis, Penetration Testing, Cloud Security, Cryptography, Web Development, Digital Forensics

Experience

Sports Performance Coach • Andrea Zerbe Performance Coaching (AZPC) • Feb 2021 – Current
A small business that I founded based on a modern and more accessible approach to helping athletes achieve their performance goals and lower the risk of injury. Using organization skills, PaaS web development, management, research, and marketing I have created a profitable and fully online training business.

Sports Performance Coach • North South Consulting Group • September 2021 - December 2021
Strength coach working with the United States Military managing physical training and physical education of entire brigades. Wrote programs, tested soldiers, implemented and organized training, analyzed large cohorts of data and while working with a full sports medicine team. Through the use of empathetic leadership I received an honor award within 3 weeks for soldier and brigade leadership compliance.

Sports Performance Coach • USA Curling/Training HAUS • September 2020 - December 2020



Summary

Diligent, smart, and resourceful team player with a cyber security certification from the University of Minnesota and a bachelor's degree from the University of Colorado Boulder. 6 months of trouble shooting experience and excited to continue my learning through tackling daunting challenges in the immense cybersecurity industry. A natural leader with experience in military, business ownership, health sciences, professional athletics and customer service. Driven to learn and grow in a fast paced organization.

Certifications

Certified Strength and Conditioning Specialist (CSCS): National Strength and Conditioning Association (NSCA)
Level 1 USA Climbing Routesetter: USA Climbing
Lifeguard/First Aid/CPR/AED: American Red Cross

Technical Skills

Programming Languages and Technologies: Terminal/bash, JavaScript, HTML, SQL, ChatGPT, AI prompt engineering, Windows OS, Mac OS, Linux OS, Screaming Frog SEO Spider, SEMRUSH, Wreshark, Kali Linux, John the Ripper, Aircrack-ng, Splunk, Snort
Cybersecurity and Networking: Network Security, Vulnerability Management, Information Assurance, Security information and Event Management (SIEM), Threat & Vulnerability Management, Linux, Malware Analysis, Penetration Testing, Cloud Security, Cryptography, Web Development, Digital Forensics

Experience

Sports Performance Coach • Andrea Zerbe Performance Coaching (AZPC) • Feb 2021 – Current
A small business that I founded based on a modern and more accessible approach to helping athletes achieve their performance goals and lower the risk of injury. Using organization skills, PaaS web development, management, research, and marketing I have created a profitable and fully online training business.

Sports Performance Coach • North South Consulting Group • September 2021 - December 2021
Strength coach working with the United States Military managing physical training and physical education of entire brigades. Wrote programs, tested soldiers, implemented and organized training, analyzed large cohorts of data and while working with a full sports medicine team. Through the use of empathetic leadership I received an honor award within 3 weeks for soldier and brigade leadership compliance.

Sports Performance Coach • USA Curling/Training HAUS • September 2020 - December 2020
Strength and Conditioning Coach working with Head Sports Performance Coach for all teams under USA Curling and at Training HAUS. Teams include but are not limited to: USA Olympic curling, NHL, AHL, and NFL athletes. Runan training sessions, tested sport performance, improved programming skills, and transferred large amounts of data.

Swin Coach • Flatiron Swimming and YMCA - June 2018 - December 2019
Recruited assistant coach for YMCA summer league (2018) and Flatirons Swim Club. Certified USA Swim coach that mentored athletes ages 6-19 within a highly competitive swim club.

Education

Boot Camp Certificate: University of Minnesota, Minneapolis, MN
Intensive 24-week cybersecurity boot camp. Skills and troubleshooting experience in Kali Linux, Windows OS, Wreshark, Snort, Splunk, Aircrack-ng, John the Ripper. Training towards Security+, Network+, and CISSP certifications.

Bachelors of Science and Art: University of Colorado Boulder, Boulder, CO
Integrative Physiology major with extensive and comprehensive STEM skills and experience. Collegiate athlete representing the university in both swimming and rock climbing.

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?

andreasecurityresume.azurewebsites.net/

Networking Questions

1. What is the IP address of your webpage?

20.119.0.19

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

Tappahannock, Virginia, United States (US)

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

```
andreazerbe@Andrea-MBP ~ % nslookup andreasecurityresume.azurewebsites.net
Server:          192.168.1.1
Address:         192.168.1.1#53
Non-authoritative answer:
andreasecurityresume.azurewebsites.net    canonical name =
waws-prod-blu-351.sip.azurewebsites.windows.net.
waws-prod-blu-351.sip.azurewebsites.windows.net canonical name =
waws-prod-blu-351-4594.eastus.cloudapp.azure.com.
Name: waws-prod-blu-351-4594.eastus.cloudapp.azure.com
Address: 20.119.0.19
```

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 8.0, Back-end

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

CSS and Images. This contains all of the formatting configurations. Colors, fonts, layouts, ect.

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 cloud tenant is an entity (person, business, organization, etc.) that uses cloud computing resources provided by the cloud service provider to support its business operations.

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

Access policies are a set of rules/regulations set by the organization for a key vault. Access policies help organizations protect sensitive data, comply with regulations, and view/monitor/manage access to key vault resources efficiently.

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

1. Keys: A key is a cryptographic key that is used for encryption, decryption, or digital signatures.
2. Secrets: A secret is any type of sensitive information that needs to be protected, such as passwords and API keys.
3. Certificates: A certificate is a digital document that is used to verify the identity of a person, organization, or device. Certificates are commonly used for secure communication, authentication, and digital signatures.

Cryptography Questions

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

1. Cost: Self signed certificates are free to create and use. This would be useful if there were budgetary restraints.
2. Flexibility: Self signed certificates can be created quickly and easily, because you do not have to go through a third-party CA. This would be useful if you needed a certificate quickly.
3. Control: Because a self signed certificate is not from a trusted third-party CA, the creator of the certificate has control over the certificate and its properties. This would be useful if you have very specific needs.
4. Encryption: Self-signed certificates provide the same level of encryption as certificates from a trusted CA. This would be useful when security is not a main concern.

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

1. **Lack of Trust:** Self signed certificates are not from a trusted third-party certificate authority (CA). This means that they are not automatically trusted by web browsers which will result in warning messages or other issues for users. This may discourage users from accessing your website or application.
2. **Security Risks:** Self signed certificates are vulnerable to spoofing and man-in-the-middle attacks. There is no third party validation of the certificate, so attackers can create their own self-signed certificates with the same name and use them to intercept communications.
3. **Management Challenges:** Self signed certificates require more upkeep than certificates from trusted CAs. For example, you must manually renew and update the certificate to make sure that it remains valid. This can take a lot of time, especially if you have many certificates to manage.
4. **Limited Use/Security:** Self signed certificates are not good for production/business environments, where security is critical. They are useful for testing, development, or other situations where security is not a primary concern.

3. What is a wildcard certificate?

A wildcard certificate is a digital certificate that allows one certificate to be used for multiple subdomains of a single domain. It is denoted with an '*' (*example.com). This would be useful for businesses/organizations that need to have their subdomains encrypted but do not want to manage numerous certificates.

For example;

*example.com

This certificate could be used for...

about-us.example.com

contact-us.example.com

shop.example.com

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.

Azure only provides TLS 1.0, 1.1, 1.2 and not SSL 3.0 because SSL has been found to have security vulnerabilities. Since 2018 the PCI Security Standards Council has mandated that SSL 3.0 should not be used after 06/30/2018.

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, my browser is not returning an error because my SSL certificate is valid and created by a third-party trusted certificate authority (CA).

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

Issued On- Thursday, March 9, 2023 at 9:05:55 PM

Expires On- Sunday, March 3, 2024 at 9:05:55 PM

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

Yes, Microsoft Azure TLS Issuing CA 02.

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

Yes, DigiCert Global Root G2

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

Yes,
[https://chromium.googlesource.com/chromium/src/+main/net/data/ssl/chrome_root_store/root_store.md](https://chromium.googlesource.com/chromium/src/+/main/net/data/ssl/chrome_root_store/root_store.md). I know it does because I do not get an error or warning when trying to access my domain.

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

COMODO Certification Authority

Day 3 Questions

Cloud Security Questions

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

Similarities:

1. Both are services used to increase the performance, availability, and security of web applications.
2. Both can do SSL/TLS termination and can offload SSL/TLS processing from the web server.
3. Both can route traffic to different backend servers (routing depends on service type).
4. It provides Layer 7 (application layer) load balancing.

Differences:

1. Azure Web Application Gateway is best for single region security.
2. Azure Front Door is simpler to use.
3. Azure Web Application Gateway uses URL-based routing.
4. Azure Front Door routes traffic to the closest backend server, based on the user's physical location.

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

SSL/TLS offloading is a feature that allows SSL/TLS processing (SSL/TLS encryption and decryption) to be handled by a gateway or load balancer rather than the backend servers.

Benefits include:

1. Improved performance in response time due to less load on the backend servers.
2. Enhanced security by using the gateway to perform SSL/TLS processing thereby shielding the backend servers from the internet.
3. Simplified management by only having to manage one set of certificate configurations on the gateway/load balancer instead of all the web servers.

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 protection: This rule looks for SQL injection attacks. SQL injection attacks are when malicious SQL code is injected into a web application to steal or manipulate data.

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?

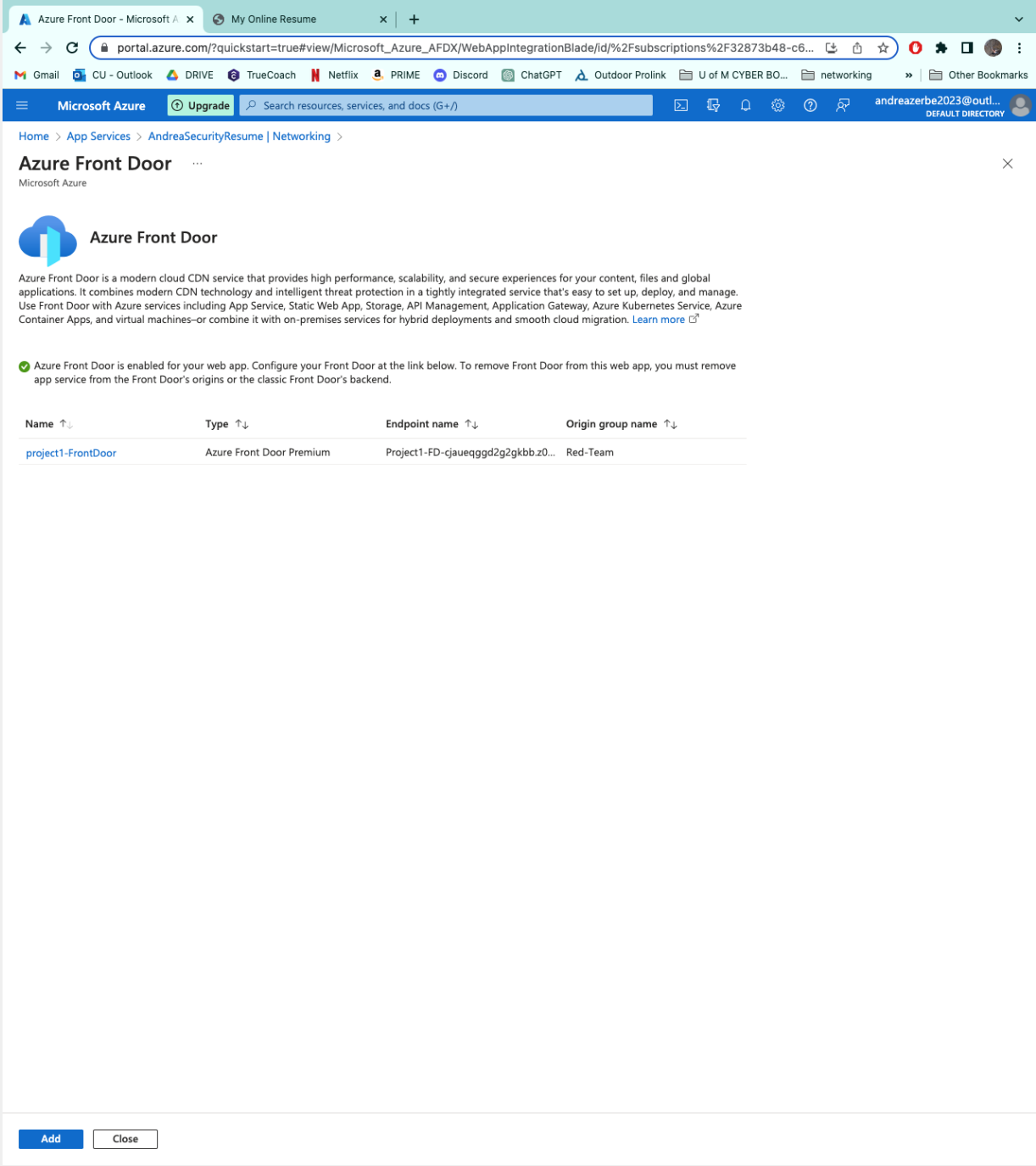
Yes, protecting against SQL injections is incredibly difficult and is often not mitigated even with the Front Door enabled. So, without Front Door, it is most certainly possible for my website to be compromised via a SQL injection attack.

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?

If you created a custom WAF rule that blocked all traffic from Canada you would only block all traffic coming from Canadian IP addresses, not whether or not the person is physically located in Canada. The user could also spoof their IP address to side step this rule.

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

a. Azure Front Door enabled



The screenshot shows the Azure Front Door configuration page in the Azure portal. The page is titled "Azure Front Door" and includes a description of the service. A table lists the configuration details for the Front Door instance.

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 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-cjaueggd2g2gkbb.z0...	Red-Team

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

b. A WAF custom rule

DefaultWebAppWaf4215d70a7 x My Online Resume x +

portal.azure.com/?quickstart=true#@andreazerbe2023outlook.onmicrosoft.com/resource/subscriptions/32873b48-c6ff-4cd9-b...

Gmail CU - Outlook DRIVE TrueCoach Netflix PRIME Discord ChatGPT Outdoor Prolink U of M CYBER BO... networking Other Bookmarks

Microsoft Azure Upgrade Search resources, services, and docs (G+/)

Home > Web Application Firewall policies (WAF) > DefaultWebAppWaf4215d70a790347adbda5806bfd98adfd

DefaultWebAppWaf4215d70a790347adbda5806bfd98adfd | 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. **YES***