Cybersecurity

Project 1 Technical Brief

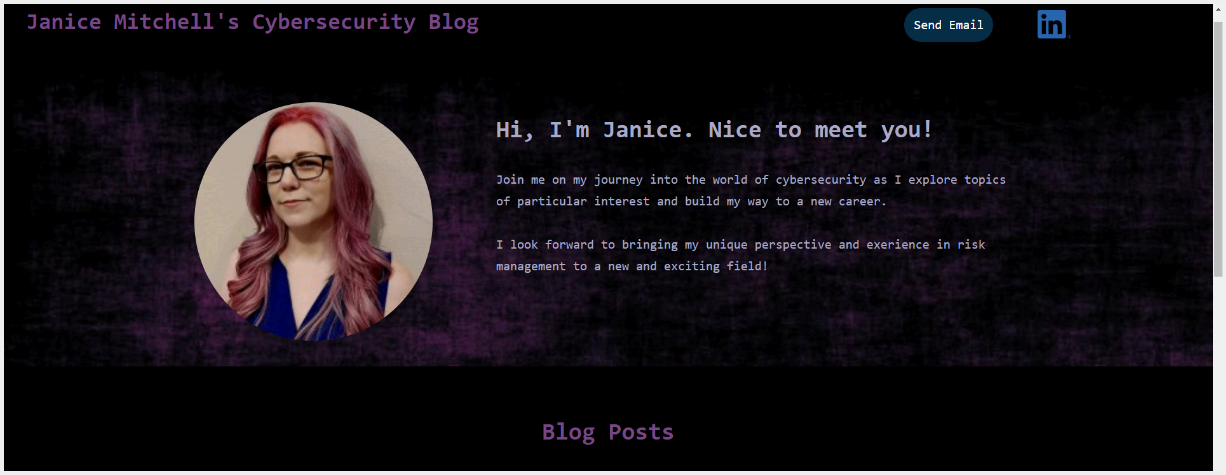
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
janicemitchellblog.azurewebsites.net
```

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



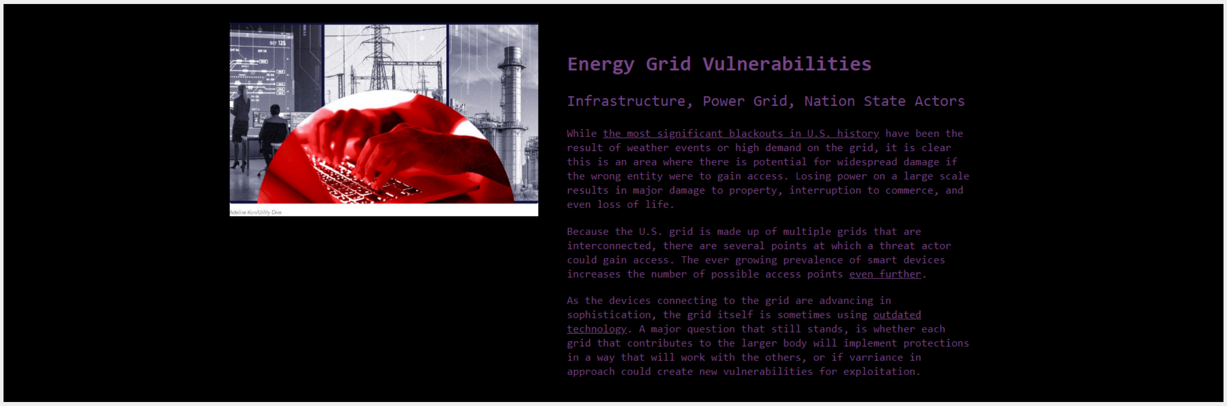
Janice Mitchell's Cybersecurity Blog

Hi, I'm Janice. Nice to meet you!

Join me on my journey into the world of cybersecurity as I explore topics of particular interest and build my way to a new career.

I look forward to bringing my unique perspective and exerience in risk management to a new and exciting field!

Blog Posts



Adeline Kon/Utility Dive

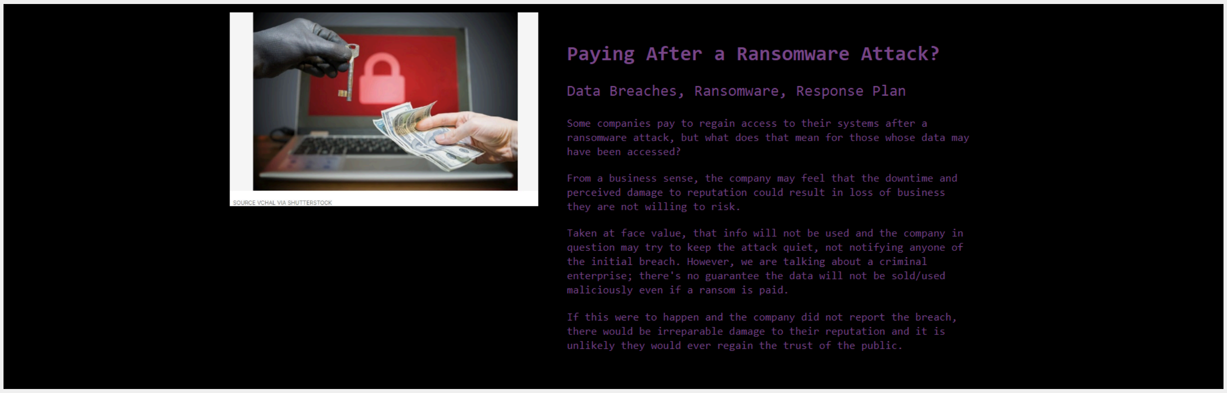
Energy Grid Vulnerabilities

Infrastructure, Power Grid, Nation State Actors

While the most significant blackouts in U.S. history have been the result of weather events or high demand on the grid, it is clear this is an area where there is potential for widespread damage if the wrong entity were to gain access. Losing power on a large scale results in major damage to property, interruption to commerce, and even loss of life.

Because the U.S. grid is made up of multiple grids that are interconnected, there are several points at which a threat actor could gain access. The ever growing prevalence of smart devices increases the number of possible access points even further.

As the devices connecting to the grid are advancing in sophistication, the grid itself is sometimes using outdated technology. A major question that still stands, is whether each grid that contributes to the larger body will implement protections in a way that will work with the others, or if varriance in approach could create new vulnerabilities for exploitation.



SOURCE VCHAL VIA SHUTTERSTOCK

Paying After a Ransomware Attack?

Data Breaches, Ransomware, Response Plan

Some companies pay to regain access to their systems after a ransomware attack, but what does that mean for those whose data may have been accessed?

From a business sense, the company may feel that the downtime and perceived damage to reputation could result in loss of business they are not willing to risk.

Taken at face value, that info will not be used and the company in question may try to keep the attack quiet, not notifying anyone of the initial breach. However, we are talking about a criminal enterprise; there's no guarantee the data will not be sold/used maliciously even if a ransom is paid.

If this were to happen and the company did not report the breach, there would be irreparable damage to their reputation and it is unlikely they would ever regain the trust of the public.

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?

```
azurewebsites.net
```

Networking Questions

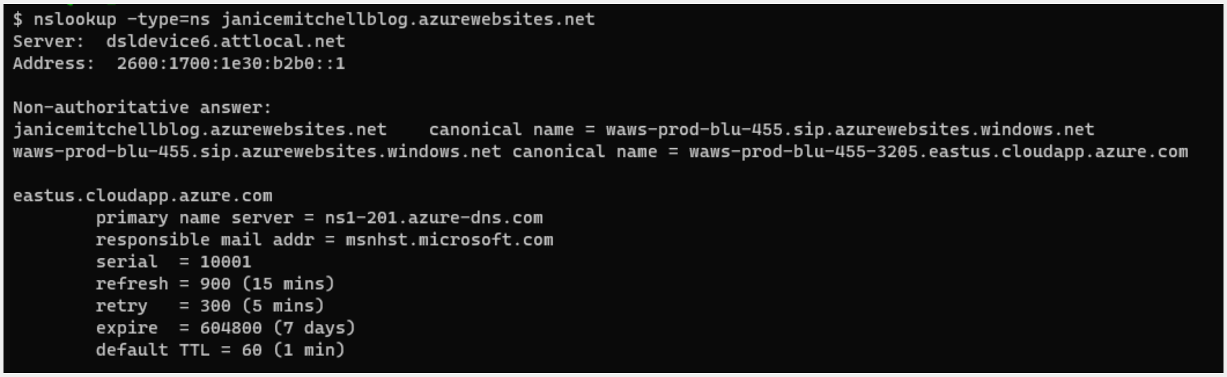
1. What is the IP address of your webpage?

```
20.119.16.39
```

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?



```
$ nslookup -type=ns janicemitchellblog.azurewebsites.net
Server:  dsldevice6.attlocal.net
Address:  2600:1700:1e30:b2b0::1

Non-authoritative answer:
janicemitchellblog.azurewebsites.net    canonical name = waws-prod-blu-455.sip.azurewebsites.windows.net
waws-prod-blu-455.sip.azurewebsites.windows.net canonical name = waws-prod-blu-455-3205.eastus.cloudapp.azure.com

eastus.cloudapp.azure.com
        primary name server = ns1-201.azure-dns.com
        responsible mail addr = msnhst.microsoft.com
        serial  = 10001
        refresh = 900 (15 mins)
        retry   = 300 (5 mins)
        expire  = 604800 (7 days)
        default TTL = 60 (1 min)
```

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 8.2. It is a programming language that converts data to HTML websites.
It works on the backend b/c it is the language which is converted to what is
ultimately displayed on the front end on the website itself.
```

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

```
The CSS folder which contains: (style.css) Style data for the web page,
including font color/size, cursor type, background colors/images, alignment,
etc. for the header, body, buttons, and each section. As well as the backup
```

```
style options (style.css.bak).
The images folder, which contains: linked in logo (for the link to linked in
profile), the default RobertSmith profile image, background image and 2 blog
post images.
```

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

```
The front end, because this is the info for what is ultimately displayed on
the website.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A customer who pays for cloud services from a cloud provider.
```

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

```
To limit access to who is able to view/make changes to the details.
```

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

```
Keys are asymmetric algorithms for encryption. Certificates are SSL
Certificates, associated w/ a key, that verify the site can be trusted.
Secrets are any other sensitive info such as symmetric keys, tokens,
passwords, etc.
```

Cryptography Questions

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

```
Faster than obtaining a 3rd party certificate, free, easily
```

issued/modified/customized. Ideal for sites on an internal network or test sites.

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

Not widely trusted as secure, so the site may not be prioritized by search engines & can possibly generate error/warning messages which can have an impact on public trust and perception. Management can be complex.

3. What is a wildcard certificate?

Instead of a specified domain name, the certificate has a wildcard (*) which allows it to apply to subdomains.

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 is not as secure as 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?

No. The site has a valid/trusted certificate.

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

Issued on: 10/30/2023 5:48:44 PM
Expires on: 6/27/2023 6:59:59 PM

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

Yes. Microsoft Azure TLS Issuing CA 01

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.
```

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

```
Entrust Root Certification Authority
```

Day 3 Questions

Cloud Security Questions

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

```
Both are load balancers in front of a web app for protection. Front Door
distributes requests across different regions and works with scale units.
Gateway distributes requests w/in one region and works w/ containers,
virtual machines, etc..
```

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

```
Encryption/decription is done on a device separate from the web server so
performance will not be affected. The handshake can be done faster and the
other processes are not slowed when kept separate.
```

3. What OSI layer does a WAF work on?

```
7
```

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

930130 Restricted File Access Attempt
Identifies anomalies in requests for restricted files and blocks suspect traffic.

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?

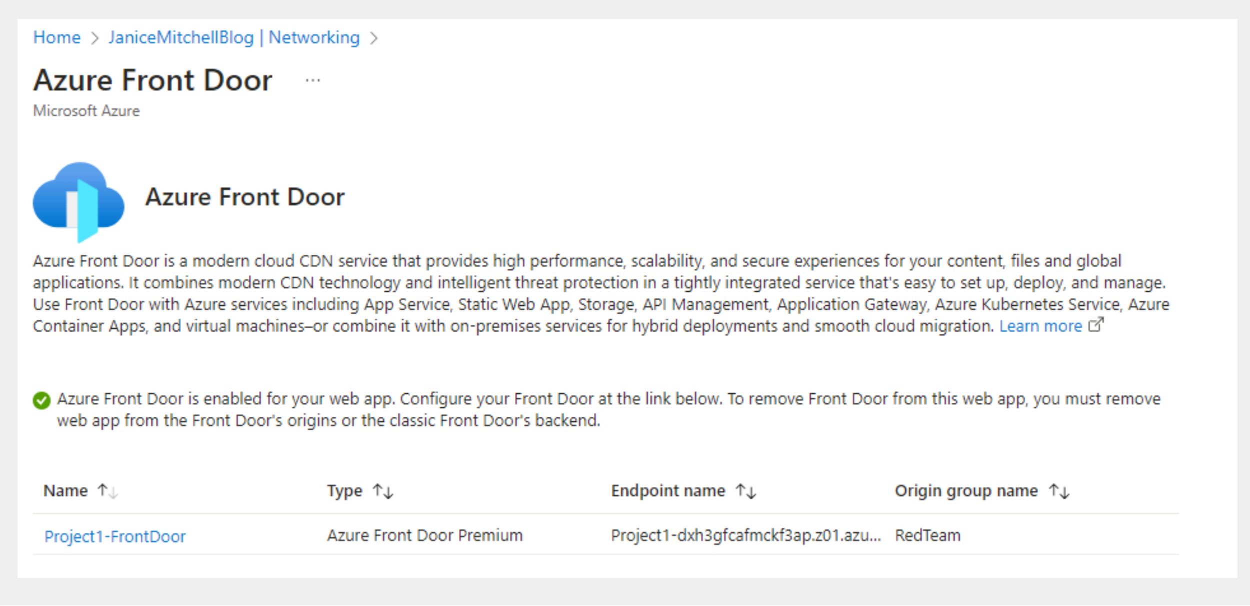
Yes. While the app in question doesn't currently store files with contact/financial info that would need to be protected, any updates/changes that included this type of submission would be in danger. Furthermore, it could be possible for an attacker to make changes to the site if any of the scripting files were to be accessed.

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. It would block Canada based IP addresses, but someone in Canada could use a VPN that portrayed their location as somewhere else and still gain access.

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

    a. Azure Front Door enabled



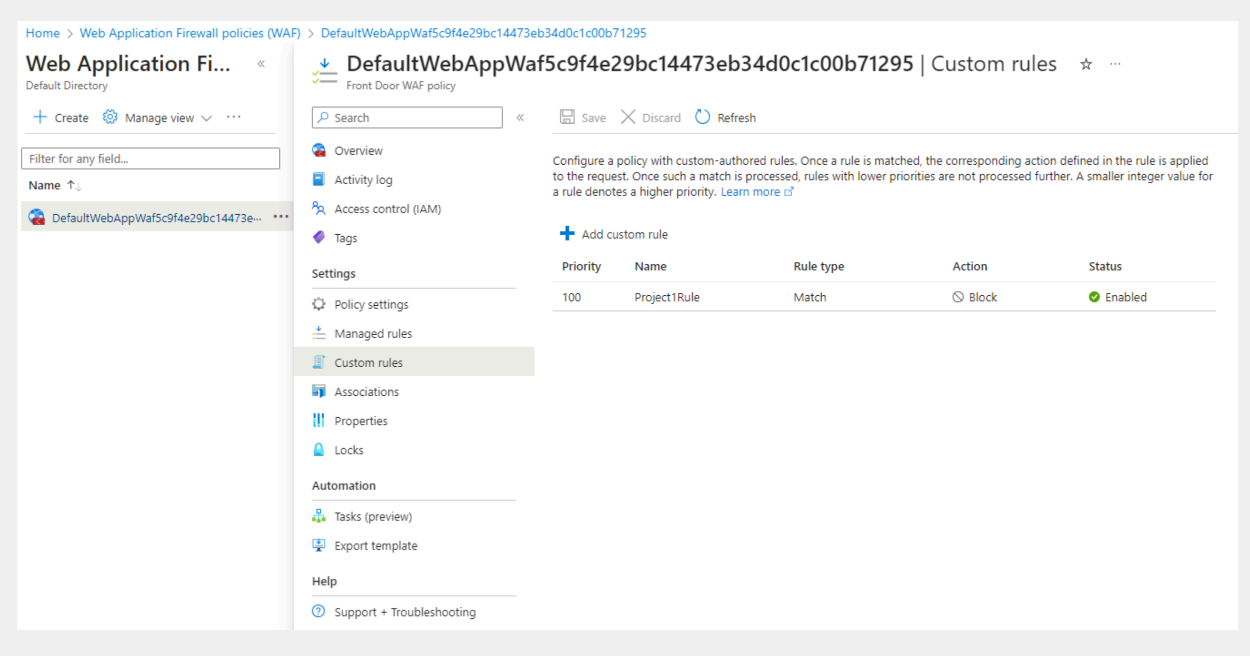
Azure Front Door

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 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-dxh3gfcafmckf3ap.z01.azu...	RedTeam

b. A WAF custom rule



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

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**

Sources:

https://www.dreamhost.com/blog/php-8-2/
https://www.redswitches.com/blog/tenant-in-cloud-computing/
https://learn.microsoft.com/en-us/azure/key-vault/general/about-keys-secrets-certificates
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq#:~:text=Azure%20Front%20Door%20and%20Azure%20Application%20Gateway%20are%20both%20load,balance%20requests%20within%20a%20region.
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq
https://www.indusface.com/blog/the-benefits-limitations-of-ssl-certificates/
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,than%20on%20the%20web%20server.
https://www.encryptionconsulting.com/education-center/self-signed-certificates/