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://valcyberblog.azurewebsites.net/`

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

Discover The Unknown

Dive into the World of Cybersecurity

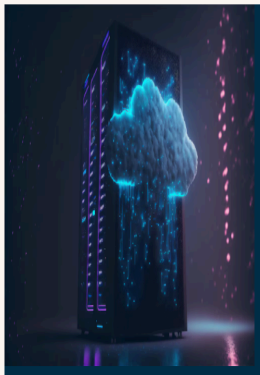
Send Email

Hi, I'm Valentina!

I'm a web developer with a passion for creating user-friendly and search-engine-optimized websites. I combine my web development expertise with SEO and online marketing strategies to craft websites that not only look great but also attract your target audience and drive results.

Dive Deeper: Explore Our Cybersecurity Blog!

Blog Posts



Azure Defense-in-Depth security

Azure, Cloud, Defence-in-Depth, Data Security

Azure Defense-in-Depth security is a layered approach that safeguards your cloud environment from various threats. By implementing multiple security controls, it minimizes the impact of a successful attack. Azure offers a wide range of built-in security features like identity and access management to fortify the first line of defense. Security Center provides centralized threat detection and vulnerability scanning, keeping your resources constantly monitored. Azure Sentinel acts as a cloud-native SIEM solution, offering advanced analytics and threat intelligence for proactive security.
Integration with endpoint protection services extends security beyond the cloud, safeguarding connected devices. Encryption at rest and in transit ensures data confidentiality throughout its lifecycle within Azure storage and services. Regular security best practices like role-based access control and strong password policies further strengthen the overall security posture.
Azure complies with a multitude of industry standards and regulations, demonstrating its commitment to data security. By adopting a Defense-in-Depth approach with Azure, you gain peace of mind knowing your cloud environment has multiple layers of protection.

Network Security Solutions for Today's Digital Infrastructure

Cyber Threats, Next-Generation Network Sercurity, Firewalls

Today's digital infrastructure demands robust network security solutions to combat ever-evolving cyber threats. Traditional security measures struggle to keep pace with the growing complexity and interconnectedness of modern networks. Next-generation network security solutions offer advanced features like intrusion detection and prevention systems (IDS/IPS) to proactively identify and block malicious traffic. Network segmentation isolates critical systems, minimizing the potential damage if a breach occurs in one segment.
Firewalls act as the first line of defense, filtering incoming and outgoing traffic based on predefined security policies. Zero-trust security principles eliminate implicit trust, requiring continuous authentication for all network access attempts. Encryption scrambles data in transit and at rest, ensuring confidentiality even if intercepted by unauthorized parties. Security Information and Event Management (SIEM) systems provide centralized visibility and analysis of security events across the network. Network security solutions should integrate seamlessly with cloud environments and mobile devices for comprehensive protection. By implementing a layered security approach with the right network security solutions, organizations can build a more resilient digital infrastructure.

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?

```
valcyberblog.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.119.16.45
```

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

```
Country:United States
State/Region:Virginia
City:Washington
```

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

```
Non-authoritative answer:
Server:  dsldevice6.attlocal.net
Address:  2600:1702:5287:600::1

valcyberblog.azurewebsites.net  canonical name =
waws-prod-blu-503.sip.azurewebsites.windows.net
waws-prod-blu-503.sip.azurewebsites.windows.net canonical name =
waws-prod-blu-503-45de.eastus.cloudapp.azure.com

eastus.cloudapp.azure.com
      primary name server = ns1-201.azure-dns.com
      responsible mail addr = msnhst.microsoft.com
```

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.
PHP works on the back-end of a website.
```

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

```
   Inside the assets directory we have 2 subdirectories:
 -  “css” subdirectory with the style.css file.
    CSS allows us to control the visual aesthetics of the website.
 -  Also we have “images” directory with images inside.
```

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

```
Front-end of a website.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant can be individuals, businesses, or organizations of any size
that utilizes resources (computer, software, networking resources) from a
cloud provider.
```

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

```
Access policies are essential for key vaults, securing sensitive data by
granting access only to authorized users, minimizing risks and ensuring data
integrity.
```

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

Keys: are used in cryptographic operations performing the encryption/decryption task.There are various types of keys used for different purposes: encryption keys, decryption key, signing keys (digital signatures).

Secrets: store sensitive data securely, this can include: database connection details like username, password, and server address, API keys, storage account keys etc

Certificates: establish trust and secure communication in digital interactions. They contain information about the certificate owner and a public key used for encryption.

Cryptography Questions

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

- Self-signed certificates are free to generate and use without involving a certificate authority (CA).
- Creating a self-signed certificate is a relatively simple process compared to obtaining one from a CA.
- Self-signed certificates are created instantly eliminating the wait for CA validation, which is beneficial for rapid deployment and testing.
- Self-signed certificates are ideal for learning environments, development, and testing scenarios where trust chains and extensive verification are not necessary.

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

- Self-signed certificates are not trusted by default by web browsers, leading to security warnings.
  ex: Web browsers can display warnings when encountering self-signed certificates because they haven't been verified by a trusted CA.
- Self-signed certificates are more susceptible to man-in-the-middle attacks where an attacker intercepts communication and impersonates a

```
trusted entity.
- For large deployments, self-signed certificates introduce significant management challenges. Updating and distributing them across many servers is far more complex than using trusted CAs.
- If a self-signed certificate is compromised, there's no central authority to revoke it. The owner must manually revoke (replace) the certificate on all connected systems.
- Self-signed certificates are best suited for controlled environments like internal testing where security risks are limited and user trust isn't a major concern. Public websites and applications should use trusted CA certificates for optimal security.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a type of SSL/TLS certificate that allows us to secure multiple subdomains under a single domain name with a single certificate. It achieves this by using an asterisk (*) as a wildcard character in the domain name.

Wildcard certificates are cost-effective and managing a single wildcard certificate is simpler than managing multiple certificates for each subdomain.
```

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 doesn't offer SSL 3.0 for website certificate binding due to several security vulnerabilities that have been identified and exploited in the past. In other words SSL 3.0 is no longer supported.

One of security vulnerabilities that have been identified was "Poodle Vulnerability" - this critical vulnerability allowed attackers to potentially decrypt communications using SSL 3.0, enabling them to steal sensitive information.
```

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, valcyberblog.azurewebsites.net is not returning an error because the connection is secure, we have a valid certificate (since I selected a free Azure domain - Azure provided a trusted certificate for my domain).

But the self-signed certificate (“**project1-cert.pfx**”) will return a “Your connection is not private” error.

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

For **Azure trusted certificate** validity period is:
Issued On Tuesday, March 12, 2024 at 8:26:53 PM
Expires On Friday, March 7, 2025 at 7:26:53 PM

For **Self-Signed Certificate**:
Activation date: 5/30/2024
Expiration date: 5/30/2025

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

Note: Since I selected a free Azure domain, I will answer this question for both: self-signed and trusted SSL certificates.

Self-Signed Certificate:
No, the Self-Signed Certificate “**project1-cert.pfx**” is a root certificate in this case.

Azure trusted SSL certificates:
The trusted SSL certificate provided by Azure is not an intermediate certificate but an ***end-entity certificate***.
Intermediate certificates are certificates that sit in the chain between the SSL certificate and the root certificate. They are used by CAs to create a chain of trust from the root certificate to the end-entity certificate.

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

Note: Since I selected a free Azure domain, I will answer this question for both: self-signed and trusted SSL certificates.

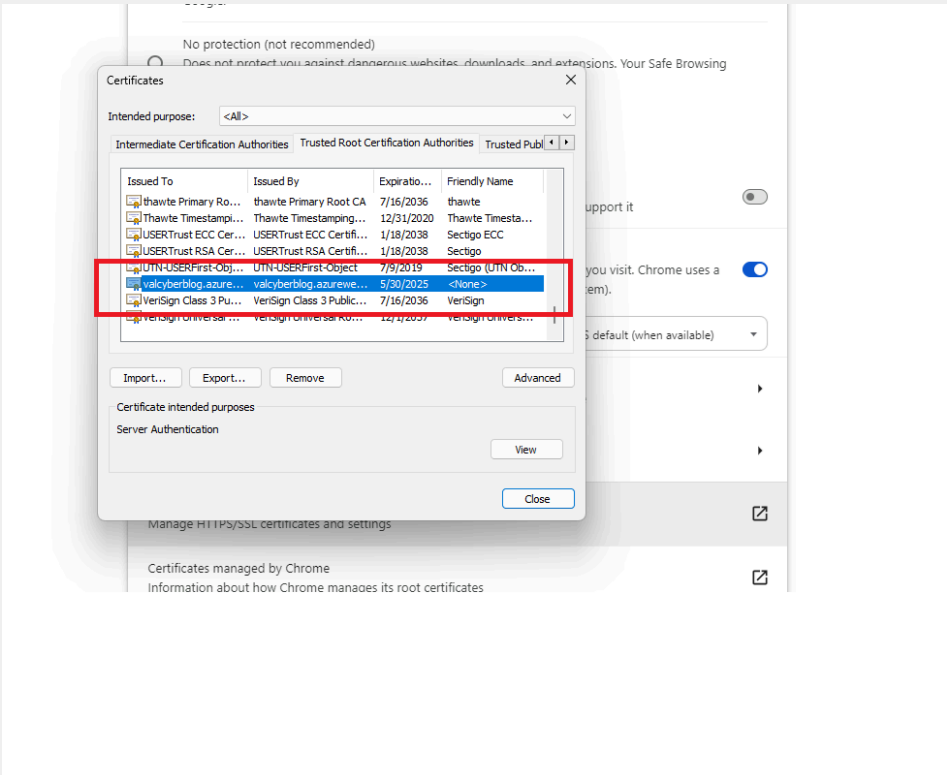
Self-Signed Certificate:
Yes, **project1-cert.pfx** is a root certificate.

Azure trusted SSL certificates:
Root certificates are the top-most certificates in the certificate hierarchy and are used to sign intermediate certificates, which in turn sign end-entity certificates.
"Azure trusted SSL certificates" - it's signed by an intermediate certificate (Microsoft Azure RSA TLS Issuing CA 08) which in turn is signed by the root certificate (DigiCert Global Root G2). This chain of trust establishes the legitimacy of the certificate and allows browsers to verify a secure connection.

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

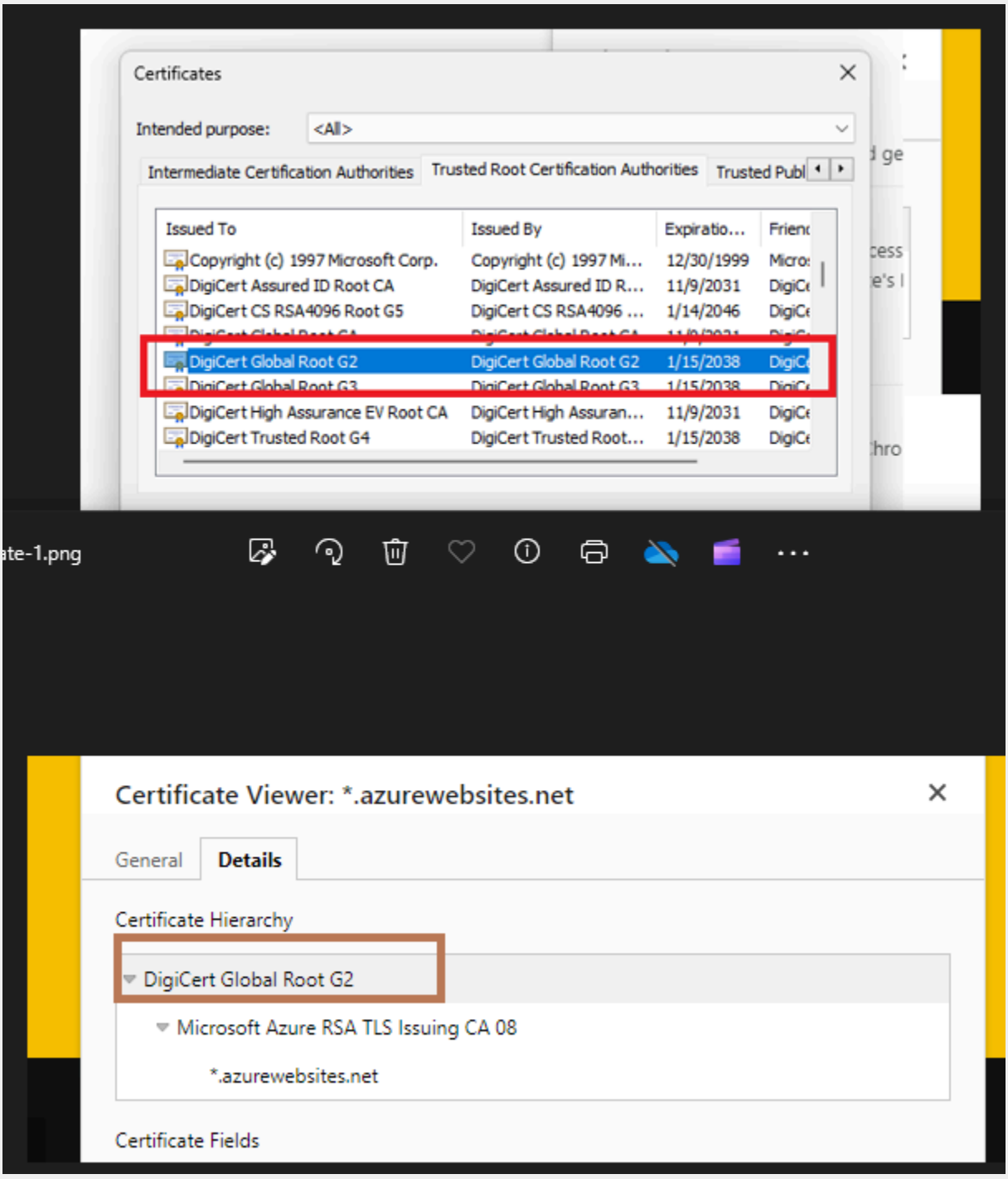
Note: Since I selected a free Azure domain, I will answer this question for both: self-signed and trusted SSL certificates.

Self-Signed Certificate:
Yes, the root certificate is in the root store if we import it.



Azure trusted SSL certificates:

Web browsers come pre-installed with a set of trusted root and intermediate certificates. Yes, “DigiCert Global Root G2” is in the browser root certificate store.



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

```
AAA Certificate Service
```

Day 3 Questions

Cloud Security Questions

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

Similarities:

Load Balancing: Both Azure Web Application Gateway and Azure Front Door provide load balancing features, and can distribute incoming traffic across multiple backend servers or resources in the Azure environment.

Health Monitoring: Both services offer health monitoring capabilities. They can check the health of backend resources and automatically route traffic away from unhealthy servers.

Application Layer Routing: Both services operate at the application layer (Layer 7)

URL Routing: We can configure both services to route traffic based on specific criteria.

DDoS Protection: Both services can be configured to leverage Azure's DDoS protection services.

Custom Rules and Policies: Both services allow the creation of custom security rules and policies to enforce specific access controls and traffic management requirements.

Differences:

Purpose:
Azure Web Application Gateway: primarily designed for regional traffic management and is best suited to protect a web application in a single region in a cloud.
Azure Front Door: designed for global traffic management and is better suited when you have a variety of regions in a cloud environment.

Primary Function:
Azure Web Application Gateway: Focuses on web application security,

filtering malicious traffic and protecting web applications from SQL injection and cross-site scripting and more.
Azure Front Door: Focuses on content delivery and traffic management. It acts as a global traffic router and optimizer.

Complexity:
Azure Web Application Gateway: It offers more advanced features and configurations, making it more complex to set up and manage.
Azure Front Door: It is simpler to implement and manage.

Content Delivery:
Azure Web Application Gateway: doesn't have content delivery functionalities.
Azure Front Door: have content delivery functionalities such as:

- Strategically placed servers around the world for optimized content delivery
- Caching capabilities for faster delivery from the closest network point

2. What is SSL offloading? What are its benefits?

SSL offloading, also known as TLS termination, is a technique that improves the performance and security of a web server by transferring the encryption and decryption tasks to a dedicated device or service, such as a load balancer.

Benefits:
Improved Performance: traffic can be more efficiently distributed across multiple backend servers.

Enhanced Scalability: Offloading devices can be powerful and handle encryption for multiple web servers.

Centralized Management: Security policies and certificates can be managed in one place on the offloading device, this way simplifying administration.

3. What OSI layer does a WAF work on?

WAF works on Layer 7 Application Layer of the OSI.

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

A SQL injection rule in a Web Application Firewall is a specific instruction designed to identify and block malicious attempts to inject unauthorized SQL code into a web application. These rules are typically created based on known patterns and behaviors associated with SQL injection attacks.

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?

Note: **The question is very confusing because we don't have a Front Door enabled in our Project. The question's wording seems a little off, it might be more accurate to ask about disabling Azure WAF's impact on the website.**

1) **Answering the question if WAF is disabled:**
Disabling WAF could impact website security because Azure Web Application Gateway sits in front of web applications and acts as a security gateway. It offers built-in WAF rules that can detect and block SQL injection attempts. The Azure-managed Default Rule Set includes rules against not only SQL Injection but: XSS, Java attacks, Local file inclusion, PHP injection attacks etc

2) **Answering the question if Front Door is disabled**
It's unlikely that the web application will be impacted by SQL injection if the Front Door is disabled.

Azure Front Door (AFD) itself cannot directly protect against SQL Injection attacks. AFD is primarily a Content Delivery Network service, its core function isn't web application security.

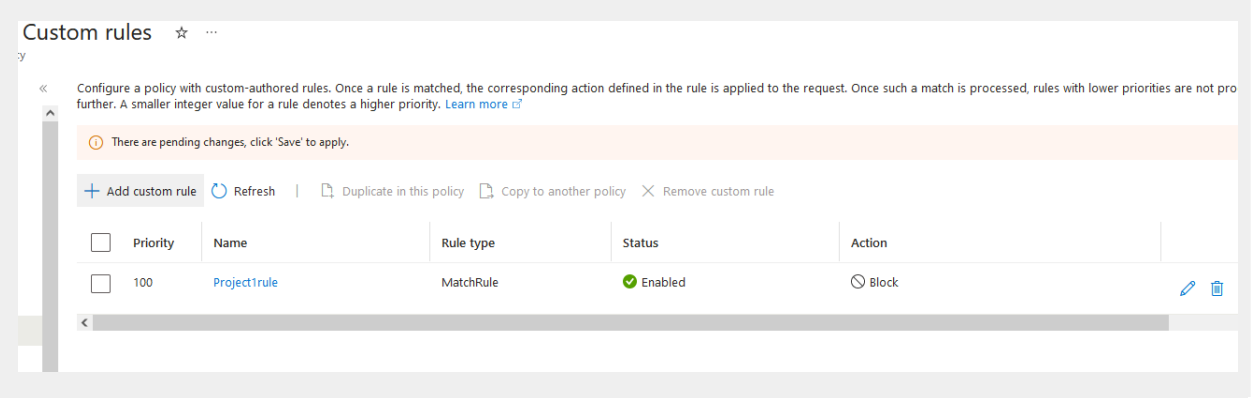
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

Blocking all Canadian traffic via a WAF rule may not be the most effective solution, some residents in Canada might still be able to access the website. Ex:
1. Canadian residents can use Virtual Private Networks (VPNs) to mask

```
   their true IP addresses.
2. Using proxy servers located outside of Canada can allow Canadian
   residents to access the website. In this case WAF will see the proxy
   server's IP address, masking the user's actual location.
3. The Tor network and other anonymity services can route traffic through
   various nodes globally, again masking the user's actual location.
4. Mobile network operators have a large pool of IP addresses they assign
   to their customers. When a Canadian resident connects to the internet
   through their mobile network, they are assigned an IP address from the
   provider's pool. This IP address might not necessarily be registered
   or associated with Canada.
```

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

    a. 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