



Cybersecurity

Project 1 Technical Brief

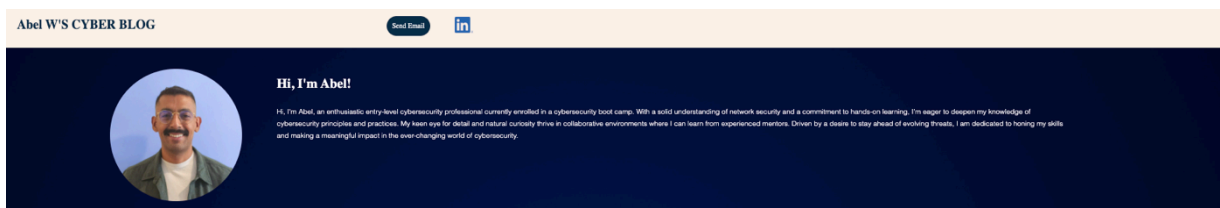
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

abelwcyberresume-crc4bgcnbxa3athm.japanwest-01.azurewebsites.net

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



Blog Posts





Embracing AI with a Human-Centric Approach: The Department of Labor's New Principles

AI in the Workforce

Artificial intelligence (AI) is quickly changing how we work and altering job roles across various industries. In response, the U.S. Department of Labor has created a new guide called Artificial Intelligence Best Practices. This guide aims to put worker wellbeing first as AI becomes more common. It is voluntary and focuses on ensuring that AI does not harm employee empowerment or job security. Acting Secretary of Labor Julia Su highlighted that innovation and worker well-being can go hand in hand. She said, "The false idea that we must choose between innovation and worker well-being is just that—a false idea." This reflects a major change in how we view AI: It is not here to replace human creativity but to help enhance it. The roadmap outlines principles that encourage workplaces and software developers to use AI in ethical, clear, and supportive ways for workers' rights. This framework aims to reduce the risks of AI while also creating new opportunities for workers. The roadmap outlines several core principles, each designed to protect and empower workers: 1. Ethically Deploying AI 2. Governance and Human Oversight* 3. Transparency 4. Protecting Labor Rights 5. Enabling Workers 6. Supporting Workers Impacted by AI 7. Responsible Use of Worker Data The Importance of Worker Involvement A key takeaway from the roadmap is the focus on gathering worker feedback and encouraging participation. By involving employees early in the AI adoption process, organizations can ensure that the implemented technologies genuinely enhance job quality and align with the workforce's needs.



North Korea Hackers Get Cash Fast in Linux Cyber Heists

Cyber Crime

North Korean hackers are using a type of Linux malware called "FASTCash" in a money-driven cyber campaign. FASTCash is malicious software that targets payment systems. The US government first identified it in October 2018 when these hackers used it in an ATM scheme aimed at banks in Africa and Asia. Since then, there have been two major updates. First, the malware can now also attack banks that use Windows Server for their payment systems. Second, it has expanded to target interbank payment processors. This malware changes transaction messages for debit and credit cards to make unauthorized withdrawals. It even tricks systems into processing declined transactions due to insufficient funds, allowing it to withdraw money in Turkish lira, between 12,000 and 30,000 lira (\$350 to \$875). Researchers note that any commercial or open-source Linux security tool should flag the method used to intercept these transaction messages. This method involves the ptrace system call. The researchers also mention recommendations from the Cybersecurity and Infrastructure Security Agency (CISA). These include using chip and PIN technology for debit cards, requiring message authentication codes for financial requests, and validating authorization responses in chip and PIN transactions to prevent exploitation.

Day 1 Questions

General Questions

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

Azure Free

2. What is your domain name?

Azurewebsites.net

Networking Questions

1. What is the IP address of your webpage?

40.74.100.142

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

Osaka, Osaka, Japan

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

No NS record found.
When I run a DNS for japanwest.01.azurewebsites.net records show servers:
ns1-34.azure-dns.com
ns2-34.azure-dns.net
ns3-34.azure-dns.org
ns4-34.azure-dns.info

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 and it works on the back end.

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

CSS directory and Images directory

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

CSS (cascading style sheets) works in the front-end. It's intended to style and layout web pages

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant is when a user or organization utilizes cloud services and resources within a cloud computing environment.

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

It's important because it determines whether a user, application, or group can perform operations on key vault secrets, keys, and certificates. This ensures that only authorized entities have access to sensitive information and enhancing security of the data stored in the key vault.

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

Keys: Supports multiple key types and algorithms and enables the use of software-protected and HSM-protected keys

Secrets: Provides secure storage of secrets, such as passwords and database connection strings

Certificates: Supports certificates, which are 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?

Self-signed certificates can be created for free and are easy to customize, allowing for larger key sizes or additional metadata. They also eliminate the need to trust third parties, reducing the complexity of certificate management and potentially presenting a smaller attack surface by avoiding complex validation and revocation checks.

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

Lack of trusted validation, which makes it difficult for users to differentiate between valid and forged certificates. This can lead to security risks such as man in the middle attacks as well as disruptions and errors since many modern services may refuse to connect over self-signed certificates.

3. What is a wildcard certificate?

A wildcard certificate is a single SSL/TLS certificate that includes a wildcard character in the domain name field. This allows it to secure multiple subdomains of the a primary domain. It simplifies the process by covering all subdomains under one certificate, providing cost savings and efficiency for businesses.

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 is not provided by Azure because it's outdated, insecure and have been replaced by more secure protocols like TLS 1.0, 1.1, 1.2

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, because Azure Free provides a SSL certificate

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

Validity Period	
Issued On	Tuesday, October 15, 2024 at 2:22:29 PM
Expires On	Friday, October 10, 2025 at 2:22:29 PM

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

No I do not, because I have a self-sign certificate

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

Microsoft Azure RSA TLS Issuing CA 07



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

No but it has a similar one.

Microsoft ECC Root Certificate Authority 2017	358DF39D764AF9E1B766E9C972D...		
Microsoft RSA Root Certificate Authority 2017	C741F70F4B2A8D88BF2E71C14122...		

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

Amazon Root CA 3

Amazon Root CA 3	18CE6CFE7BF14E60B2E347B8DFE...		
-------------------------	--------------------------------	---	---

Day 3 Questions

Cloud Security Questions

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

Azure application gateway is a traffic manager and load balancer that helps route your application traffic to suitable destination, this enhances the availability and scalability of the application

Azure Front Door is a content delivery network that helps provide static and dynamic web content to users with a higher availability, lower latency, greater scale and more secure manner across the globe

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

SSL offloading is a technique used in network management where the task of SSL encryption and decryption is moved from the backend servers to a dedicated device such as a load balancer,

Benefits are improved server performance, enhanced security, simplified SSL management, and better scalability.

3. What OSI layer does a WAF work on?

WAF operates in layer 7 Application Layer.

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

WAF defends against cross-site request forgery by filtering and monitoring HTTP traffic between a web application and the internet. It blocks malicious requests that exploit a user's browser trust.

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, if Front Door was removed malicious users can forge my authentication session and send unauthorized requests.

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, someone from Canada can use a VPN outside of Canada to access your website.

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

- a. A WAF custom rule

