Cybersecurity

Project 1 Technical Brief

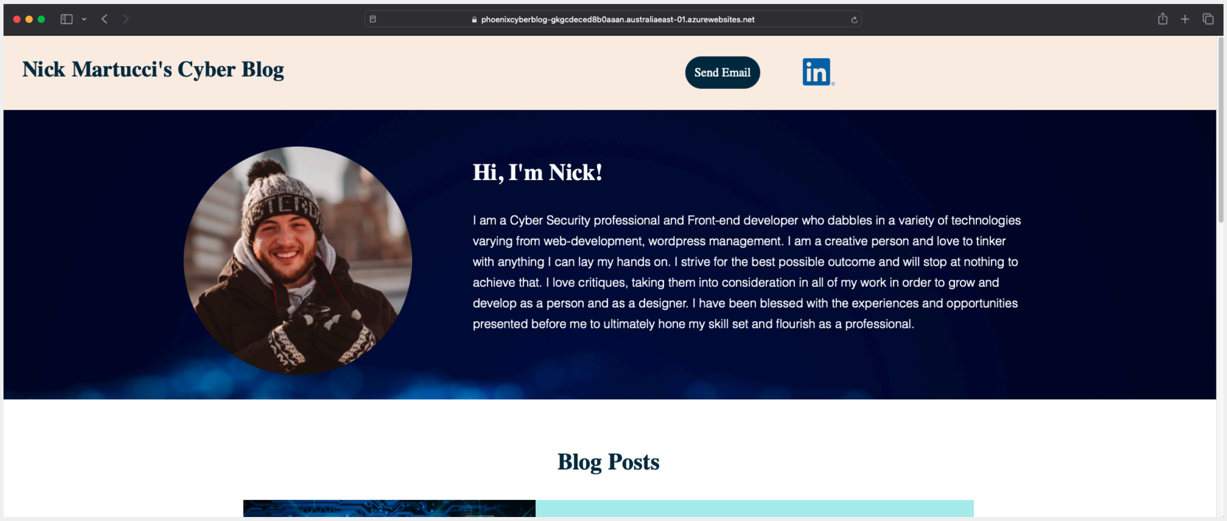
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://phoenixcyberblog-gkgcdeced8b0aaan.australiaeast-01.azurewebsites.net
/
```

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

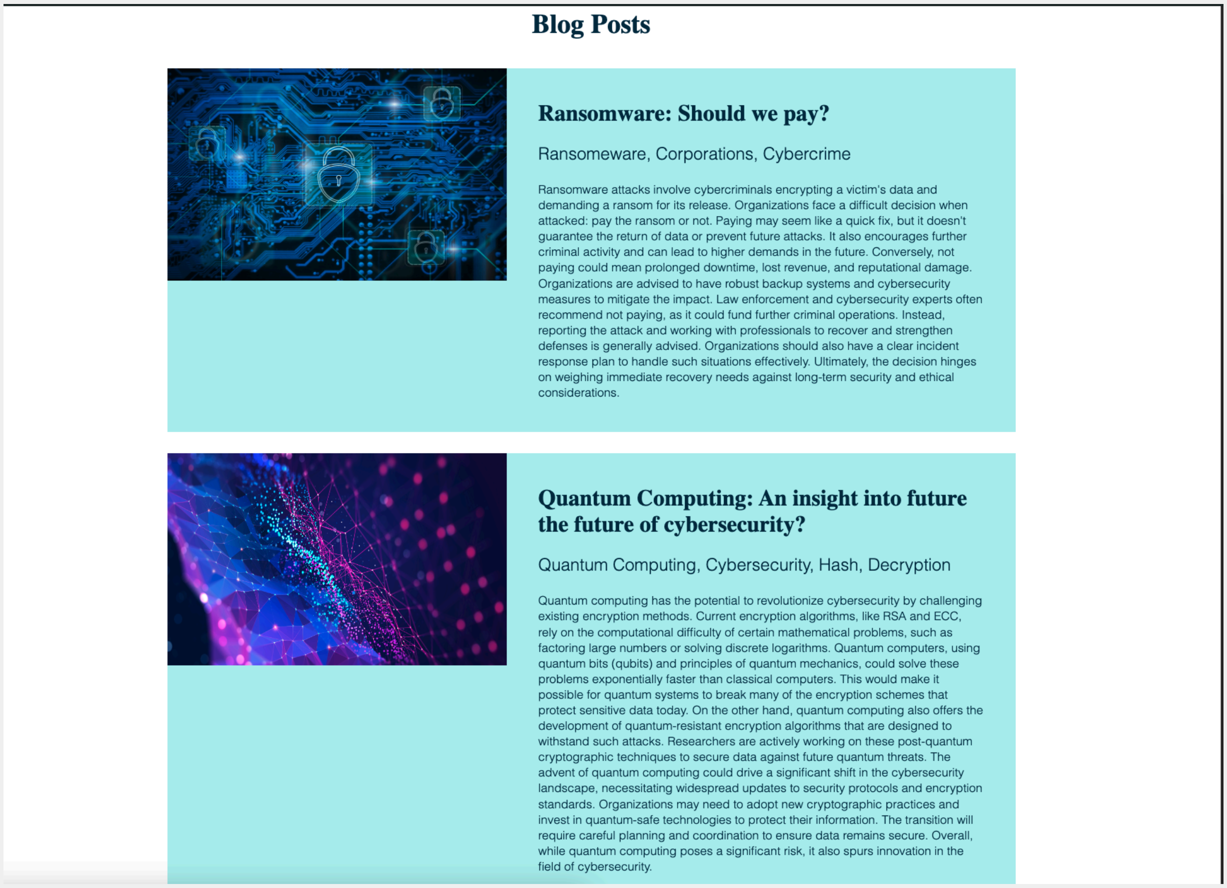

phoenixcyberblog-gkgcdeced8b0aaan.australiaeast-01.azurewebsites.net
Send Email
in

Nick Martucci's Cyber Blog

Hi, I'm Nick!

I am a Cyber Security professional and Front-end developer who dabbles in a variety of technologies varying from web-development, wordpress management. I am a creative person and love to tinker with anything I can lay my hands on. I strive for the best possible outcome and will stop at nothing to achieve that. I love critiques, taking them into consideration in all of my work in order to grow and develop as a person and as a designer. I have been blessed with the experiences and opportunities presented before me to ultimately hone my skill set and flourish as a professional.

Blog Posts



Blog Posts

Ransomware: Should we pay?

Ransomeware, Corporations, Cybercrime

Ransomware attacks involve cybercriminals encrypting a victim's data and demanding a ransom for its release. Organizations face a difficult decision when attacked: pay the ransom or not. Paying may seem like a quick fix, but it doesn't guarantee the return of data or prevent future attacks. It also encourages further criminal activity and can lead to higher demands in the future. Conversely, not paying could mean prolonged downtime, lost revenue, and reputational damage. Organizations are advised to have robust backup systems and cybersecurity measures to mitigate the impact. Law enforcement and cybersecurity experts often recommend not paying, as it could fund further criminal operations. Instead, reporting the attack and working with professionals to recover and strengthen defenses is generally advised. Organizations should also have a clear incident response plan to handle such situations effectively. Ultimately, the decision hinges on weighing immediate recovery needs against long-term security and ethical considerations.

Quantum Computing: An insight into future the future of cybersecurity?

Quantum Computing, Cybersecurity, Hash, Decryption

Quantum computing has the potential to revolutionize cybersecurity by challenging existing encryption methods. Current encryption algorithms, like RSA and ECC, rely on the computational difficulty of certain mathematical problems, such as factoring large numbers or solving discrete logarithms. Quantum computers, using quantum bits (qubits) and principles of quantum mechanics, could solve these problems exponentially faster than classical computers. This would make it possible for quantum systems to break many of the encryption schemes that protect sensitive data today. On the other hand, quantum computing also offers the development of quantum-resistant encryption algorithms that are designed to withstand such attacks. Researchers are actively working on these post-quantum cryptographic techniques to secure data against future quantum threats. The advent of quantum computing could drive a significant shift in the cybersecurity landscape, necessitating widespread updates to security protocols and encryption standards. Organizations may need to adopt new cryptographic practices and invest in quantum-safe technologies to protect their information. The transition will require careful planning and coordination to ensure data remains secure. Overall, while quantum computing poses a significant risk, it also spurs innovation in the field of cybersecurity.

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?

phoenixcyberblog-gkgcdeced8b0aaan.australiaeast-01.azurewebsites.net

Networking Questions

1. What is the IP address of your webpage?

```
20.37.196.202
```

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

```
Sydney, New South Wales, Australia
```

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

```
The main recorded is associated with the parent domain:
ns1-33.azure-dns.com.   Validating in 48h
ns2-33.azure-dns.net.   Validating in 48h
ns3-33.azure-dns.org.   Validating in 48h
ns4-33.azure-dns.info.  Validating in 48h
```

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:5.3 - runs the Backend
```

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

```
imahes and CSS, images hosts all images where CSS hosts all css files for
formatting/styles
```

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 essentially a dedicated space within the a cloud ecosystem, encompassing identity management, resource organization, and access control.

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

You maintain tighter control over who can access your Key Vault and how they can interact with it

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

Keys: For cryptographic operations (encryption, decryption, signing).
Secrets: For storing sensitive data like passwords and API keys.
Certificates: For securing communications and validating identities with a combination of keys and metadata.

Cryptography Questions

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

[Enter answer here]

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

In production environments or public-facing services, certificates issued by a trusted CA are generally preferred to ensure proper validation and trust.

3. What is a wildcard certificate?

A wildcard certificate is a versatile and cost-effective solution for securing multiple subdomains under a single primary domain. It simplifies certificate management and provides broad coverage, but it’s important to consider its limitations and ensure proper security practices to protect all covered 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 3.0 is not provided by Azure due to its inherent security vulnerabilities, deprecated status, and the need to adhere to current security standards and best practices.

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?

It is not returning an error for the SSL certificate due to the inheritance from the parent certificate from azure.

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

Issued On Sunday, August 4, 2024 at 4:40:00 AM

Expires On Wednesday, July 30, 2025 at 4:40:00 AM

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

Yes, Microsoft Azure RSA TLS CA 08

   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?

GTS Root R1

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

AAA Certificate Sevices

Day 3 Questions

Cloud Security Questions

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

Azure Web Application Gateway is ideal for regional applications that require advanced routing within a region, integration with virtual networks, or internal application delivery.

Azure Front Door is suited for global applications requiring high availability, low latency, and intelligent routing across multiple regions, especially when combined with its CDN capabilities.

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

SSL offloading is the process of decrypting SSL/TLS traffic at the edge of a network, often on a load balancer or a dedicated device, rather than at the backend servers. This a technique that improves performance, simplifies management, and enhances security for web applications and services that rely on secure connections.

3. What OSI layer does a WAF work on?

Layer 7 - Application

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

[Directory Traversal (aka Path Traversal) is an attack where an attacker attempts to access files or directories stored outside the web root folder, potentially gaining access to sensitive information or configuration files. Managed rules detect patterns that try to exploit file paths, such as “../”, which indicates attempts to move up directories.

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?

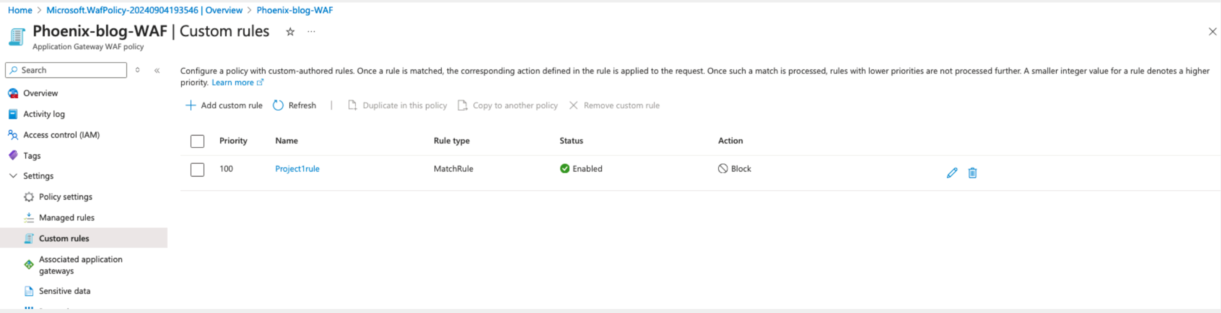
No, all data is stored in the root folder therefore not accessible via this attack

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?

Yes because it is blocking IPs originating from Canada. This however can be bypassed via a VPN that changes the appearance of the location of the host IP

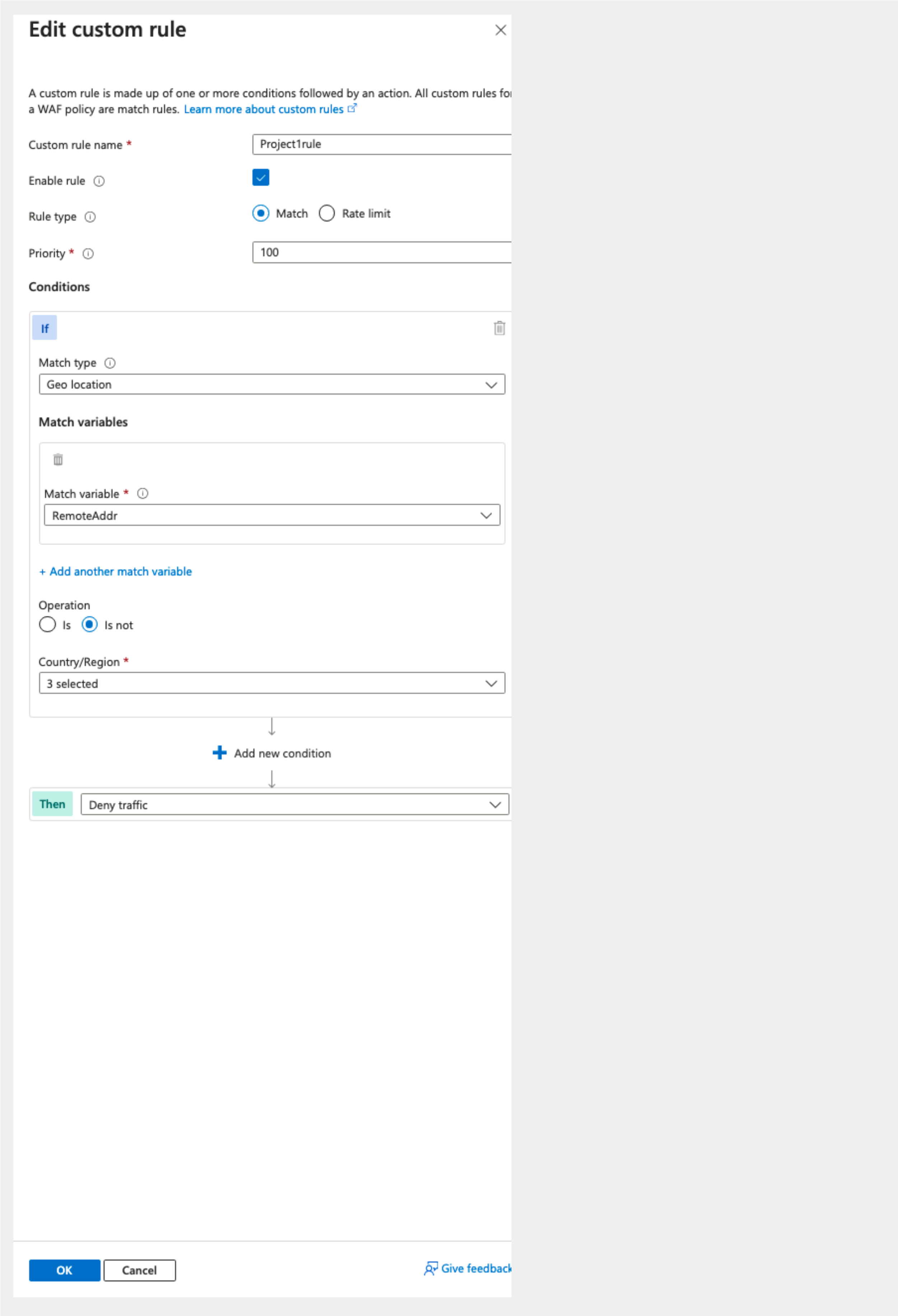
7. Include screenshots below to demonstrate that your web app has the following:

   a. 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	Status	Action
□	100	Project1rule	MatchRule	✓ Enabled	⃠ Block



Edit custom rule

A custom rule is made up of one or more conditions followed by an action. All custom rules fo
a WAF policy are match rules. Learn more about custom rules

Custom rule name * Project1rule

Enable rule ☑

Rule type ● Match ○ Rate limit

Priority * 100

Conditions

If

Match type: Geo location

Match variables

Match variable * RemoteAddr

+ Add another match variable

Operation ○ Is ● Is not

Country/Region * 3 selected

Add new condition

Then: Deny traffic

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