Cybersecurity

Project 1 Technical Brief

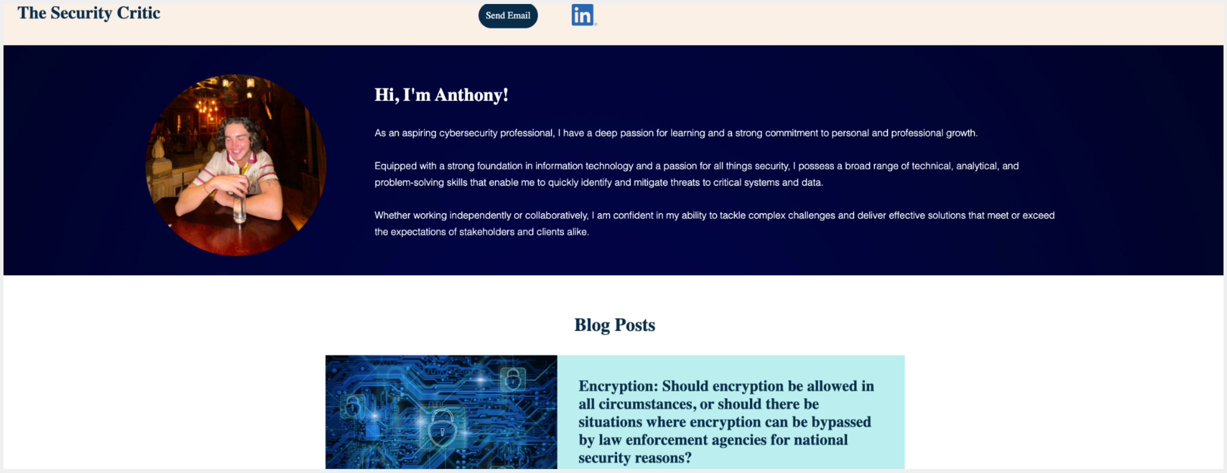
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
thesecuritycritic.azurewebsites.net
```

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



The Security Critic

Hi, I'm Anthony!

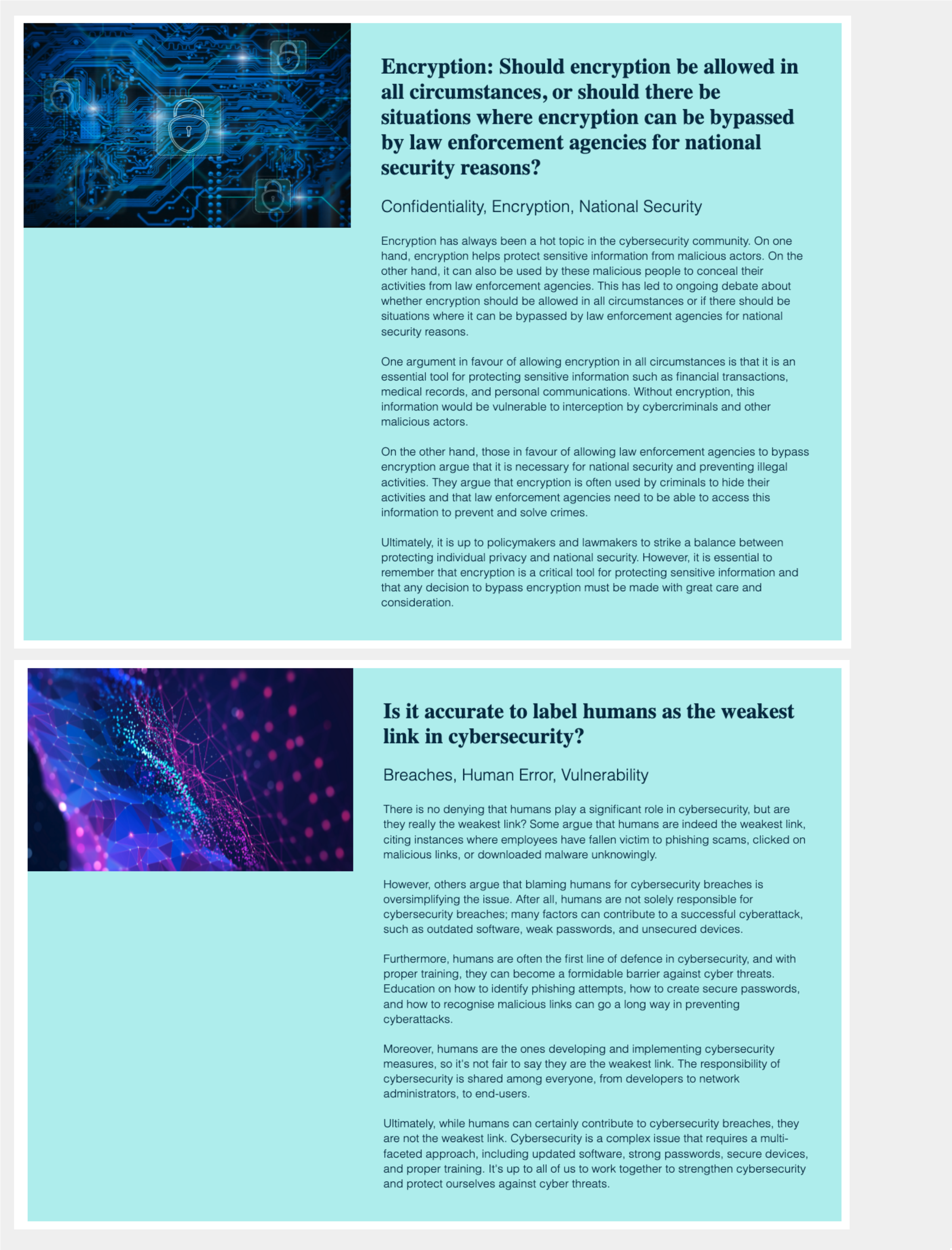
As an aspiring cybersecurity professional, I have a deep passion for learning and a strong commitment to personal and professional growth.

Equipped with a strong foundation in information technology and a passion for all things security, I possess a broad range of technical, analytical, and problem-solving skills that enable me to quickly identify and mitigate threats to critical systems and data.

Whether working independently or collaboratively, I am confident in my ability to tackle complex challenges and deliver effective solutions that meet or exceed the expectations of stakeholders and clients alike.

Blog Posts

Encryption: Should encryption be allowed in all circumstances, or should there be situations where encryption can be bypassed by law enforcement agencies for national security reasons?



Encryption: Should encryption be allowed in all circumstances, or should there be situations where encryption can be bypassed by law enforcement agencies for national security reasons?

Confidentiality, Encryption, National Security

Encryption has always been a hot topic in the cybersecurity community. On one hand, encryption helps protect sensitive information from malicious actors. On the other hand, it can also be used by these malicious people to conceal their activities from law enforcement agencies. This has led to ongoing debate about whether encryption should be allowed in all circumstances or if there should be situations where it can be bypassed by law enforcement agencies for national security reasons.

One argument in favour of allowing encryption in all circumstances is that it is an essential tool for protecting sensitive information such as financial transactions, medical records, and personal communications. Without encryption, this information would be vulnerable to interception by cybercriminals and other malicious actors.

On the other hand, those in favour of allowing law enforcement agencies to bypass encryption argue that it is necessary for national security and preventing illegal activities. They argue that encryption is often used by criminals to hide their activities and that law enforcement agencies need to be able to access this information to prevent and solve crimes.

Ultimately, it is up to policymakers and lawmakers to strike a balance between protecting individual privacy and national security. However, it is essential to remember that encryption is a critical tool for protecting sensitive information and that any decision to bypass encryption must be made with great care and consideration.

Is it accurate to label humans as the weakest link in cybersecurity?

Breaches, Human Error, Vulnerability

There is no denying that humans play a significant role in cybersecurity, but are they really the weakest link? Some argue that humans are indeed the weakest link, citing instances where employees have fallen victim to phishing scams, clicked on malicious links, or downloaded malware unknowingly.

However, others argue that blaming humans for cybersecurity breaches is oversimplifying the issue. After all, humans are not solely responsible for cybersecurity breaches; many factors can contribute to a successful cyberattack, such as outdated software, weak passwords, and unsecured devices.

Furthermore, humans are often the first line of defence in cybersecurity, and with proper training, they can become a formidable barrier against cyber threats. Education on how to identify phishing attempts, how to create secure passwords, and how to recognise malicious links can go a long way in preventing cyberattacks.

Moreover, humans are the ones developing and implementing cybersecurity measures, so it's not fair to say they are the weakest link. The responsibility of cybersecurity is shared among everyone, from developers to network administrators, to end-users.

Ultimately, while humans can certainly contribute to cybersecurity breaches, they are not the weakest link. Cybersecurity is a complex issue that requires a multi-faceted approach, including updated software, strong passwords, secure devices, and proper training. It's up to all of us to work together to strengthen cybersecurity and protect ourselves against cyber threats.

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?

```
thesecuritycritic.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.16
```

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

```
Australia East (Sydney, NSW)
```

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

```
Non-authoritative answer:
thesecuritycritic.azurewebsites.net canonical name =
waws-prod-sy3-101.sip.azurewebsites.windows.net
waws-prod-sy3-101.sip.azurewebsites.windows.net canonical name =
waws-prod-sy3-101-06a2.australiaeast.cloudapp.azure.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 8.0. Back end

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

Inside this directory were the following folders: ‘css’ + ‘images’. These folders are used to control the style of a web application.

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

While primarily associated with the front-end, they can also be used by the back-end for serving or generating content that is ultimately consumed by the front-end.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant is an individual or organisation that has subscribed to a cloud computing service to host and run their applications, services, or data. In cloud computing, a tenant is an isolated and independent entity that has access to a specific set of resources and services provided by a cloud provider.

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

A key vault is used to securely store cryptographic keys, secrets, and certificates, which are used to protect data and authenticate access to resources. If the key vault is not secured properly, it can lead to unauthorised access to sensitive data or resources, which can result in data breaches and other security incidents.An access policy is crucial on a key vault as it ensures that only authorised individuals or systems have the necessary permissions to access and manage the cryptographic assets stored within the vault.

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

Keys: A key is a piece of information that is used to encrypt or decrypt data. In a key vault, keys are used to protect data at rest or in transit.
Secrets: A secret is any piece of sensitive information that needs to be protected, such as passwords, connection strings, and API keys.
Certificates: A certificate is a digital document that is used to establish the identity of an entity, such as a person, organisation, or device.

Cryptography Questions

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

Advantages of self-signed certificates include: no cost, quick deployment, control over certificate creation, and usefulness for testing.

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

One disadvantage of self-signed certificates is that they are not trusted by most web browsers and operating systems by default, which can make users feel uncertain and increase security risks. Also, users may see security warnings when accessing websites or applications secured with self-signed certificates, which can decrease credibility.

3. What is a wildcard certificate?

A wildcard certificate is a type of digital certificate that is used to secure a domain and its subdomains with a single certificate. It allows you to secure multiple subdomains with a single certificate, rather than having to obtain a separate certificate 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.

```
SSL 3.0 is not provided by Azure for binding certificates to websites due to
its inherent vulnerability to security exploits. SSL 3.0 is an outdated
protocol that has been found to be susceptible to various security
vulnerabilities, including the widely known POODLE attack. This
vulnerability allows attackers to decrypt and tamper with encrypted data
transmitted over the SSL 3.0 connection.
```

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 it's not because it is a valid certificate by a trusted CA
```

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

```
28 DEC 2022 - 23 DEC 2023
```

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

```
Microsoft Azure TLS Issuing CA 05
```

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

```
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.

```
D-TRUST Root CA 3 2013
```

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 designed for application-level load
balancing and traffic routing, while Azure Front Door is designed for global
traffic management and CDN capabilities. Web Application Gateway supports
SSL/TLS offloading, while Front Door supports SSL/TLS pass-through. Both
services support WAF rules, health monitoring, and auto-scaling.
```

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

```
SSL offloading is the process of decrypting SSL/TLS traffic at the gateway
or front door and sending unencrypted traffic to the back-end servers.
Benefits include improved server performance, simplified server management,
centralised certificate management, and reduced attack surface.
```

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.

```
SQL injection is a type of cyber attack where an attacker tries to insert
malicious SQL code into a web application's input fields, such as a search
box or login form, in order to gain access to sensitive information or
perform unauthorised actions on the application's underlying database. The
goal of the attack is to exploit vulnerabilities in the application's code
that allow the attacker to bypass authentication, view or modify data, or
execute malicious commands on the database.
```

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?

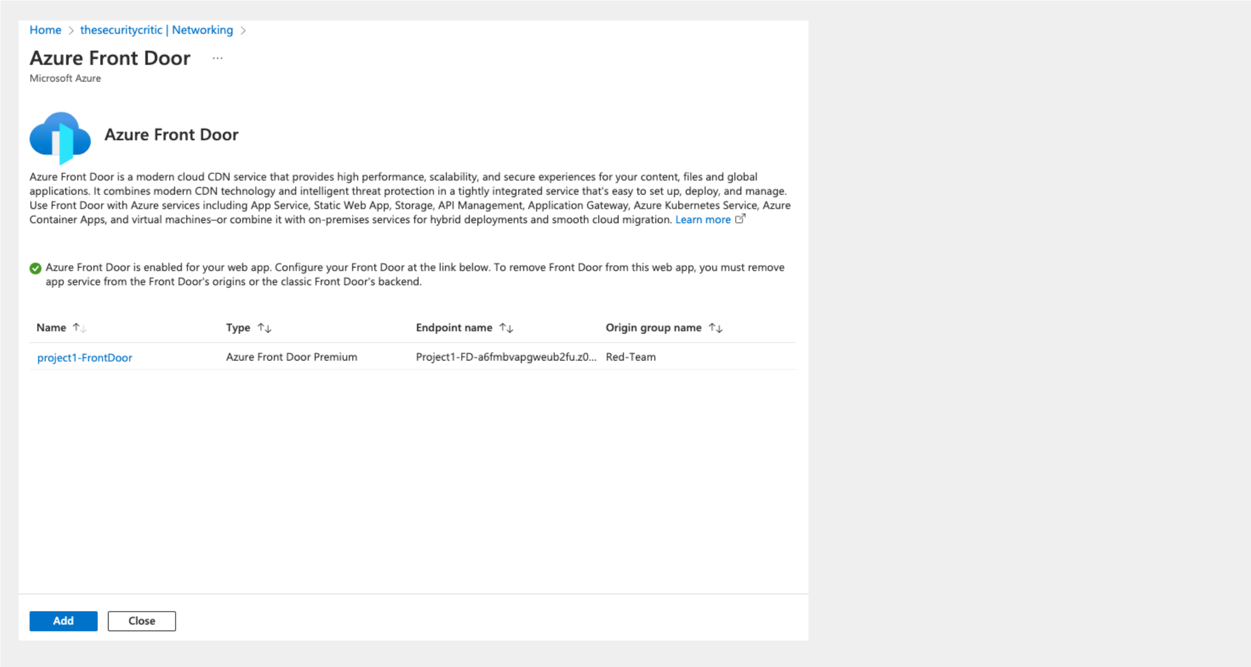
No, my website, as it is currently designed, would not be impacted by the SQL injection vulnerability, even if Front Door wasn't enabled. The reason is that my website is solely designed for viewing blog posts created by me, and it does not involve any interaction with a database or dynamic content that could be susceptible to SQL injection attacks.

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 create a custom Web Application Firewall (WAF) rule to block all traffic from Canada, then anyone who resides in Canada or who is attempting to access the website from a Canadian IP address would be blocked and unable to access your website. Even if a VPN was used, traffic still originates from the VPN server's IP address, which could be located in Canada. Therefore, traffic originating from a Canadian IP address, including those that are coming through a VPN server, will be blocked by the WAF.

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

    a. Azure Front Door enabled



Home > thesecuritycritic | Networking >

Azure Front Door ···

Microsoft Azure

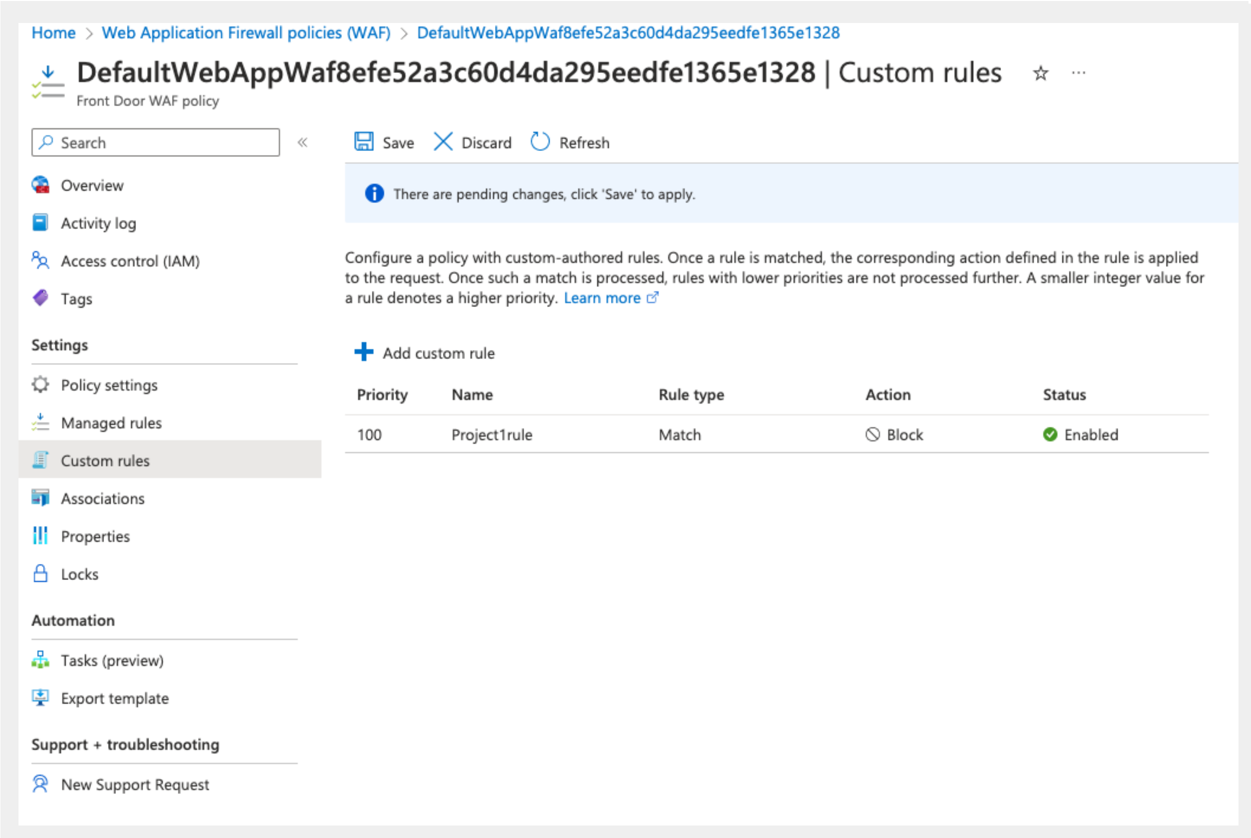
Azure Front Door

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 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-a6fmbvapgweub2fu.z0...	Red-Team

b. A WAF custom rule



Home > Web Application Firewall policies (WAF) > DefaultWebAppWaf8efe52a3c60d4da295eedfe1365e1328

DefaultWebAppWaf8efe52a3c60d4da295eedfe1365e1328 | Custom rules ☆ ···

Front Door WAF policy

There are pending changes, click 'Save' to apply.

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

Home > thesecuritycritic

thesecuritycritic | Microsoft Defender for Cloud ☆ ···

Web App

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**