Cybersecurity

Project 1 Technical Brief

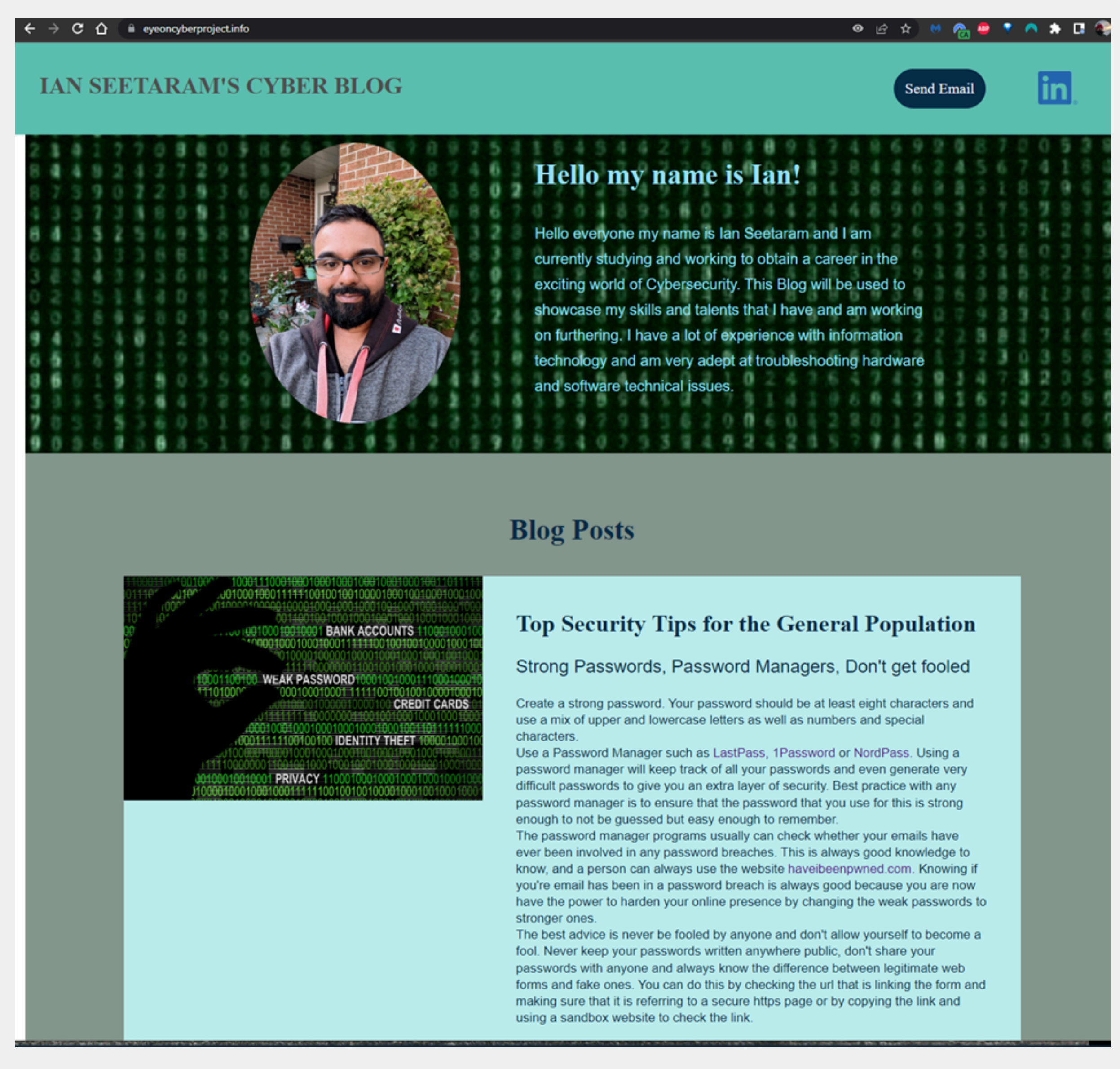
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://ianproject1custom.azurewebsites.net/
```

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



IAN SEETARAM'S CYBER BLOG

Hello my name is Ian!

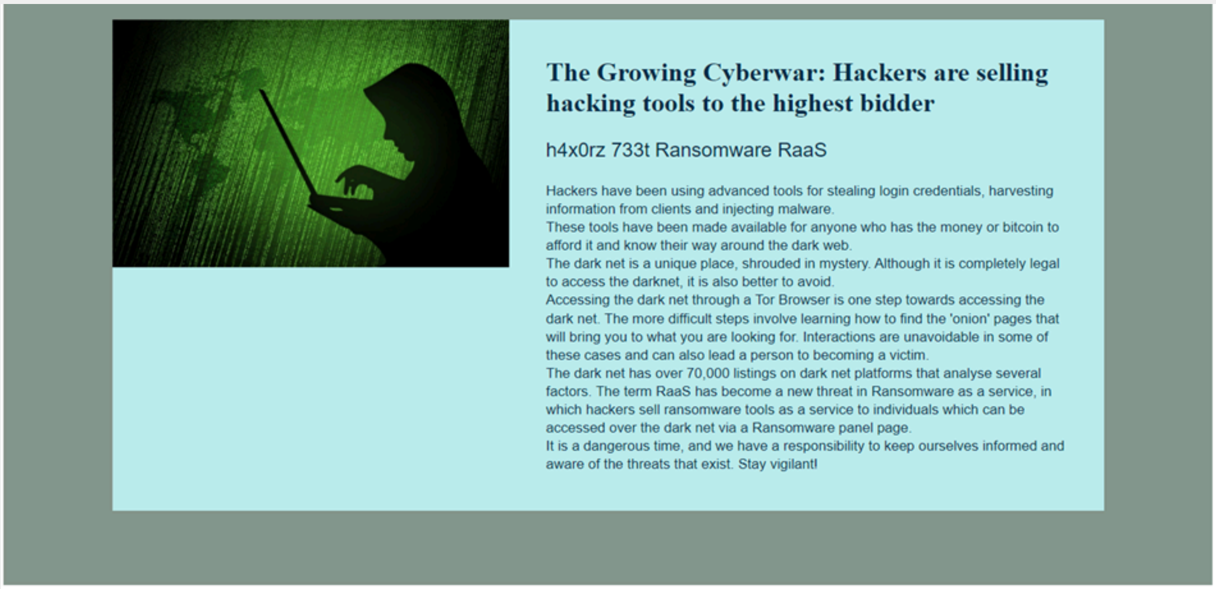
Hello everyone my name is Ian Seetaram and I am currently studying and working to obtain a career in the exciting world of Cybersecurity. This Blog will be used to showcase my skills and talents that I have and am working on furthering. I have a lot of experience with information technology and am very adept at troubleshooting hardware and software technical issues.

Blog Posts

Top Security Tips for the General Population

Strong Passwords, Password Managers, Don't get fooled

Create a strong password. Your password should be at least eight characters and use a mix of upper and lowercase letters as well as numbers and special characters.
Use a Password Manager such as LastPass, 1Password or NordPass. Using a password manager will keep track of all your passwords and even generate very difficult passwords to give you an extra layer of security. Best practice with any password manager is to ensure that the password that you use for this is strong enough to not be guessed but easy enough to remember.
The password manager programs usually can check whether your emails have ever been involved in any password breaches. This is always good knowledge to know, and a person can always use the website haveibeenpwned.com. Knowing if you're email has been in a password breach is always good because you are now have the power to harden your online presence by changing the weak passwords to stronger ones.
The best advice is never be fooled by anyone and don't allow yourself to become a fool. Never keep your passwords written anywhere public, don't share your passwords with anyone and always know the difference between legitimate web forms and fake ones. You can do this by checking the url that is linking the form and making sure that it is referring to a secure https page or by copying the link and using a sandbox website to check the link.



The Growing Cyberwar: Hackers are selling hacking tools to the highest bidder

h4x0rz 733t Ransomware RaaS

Hackers have been using advanced tools for stealing login credentials, harvesting information from clients and injecting malware.
These tools have been made available for anyone who has the money or bitcoin to afford it and know their way around the dark web.
The dark net is a unique place, shrouded in mystery. Although it is completely legal to access the darknet, it is also better to avoid.
Accessing the dark net through a Tor Browser is one step towards accessing the dark net. The more difficult steps involve learning how to find the 'onion' pages that will bring you to what you are looking for. Interactions are unavoidable in some of these cases and can also lead a person to becoming a victim.
The dark net has over 70,000 listings on dark net platforms that analyse several factors. The term RaaS has become a new threat in Ransomware as a service, in which hackers sell ransomware tools as a service to individuals which can be accessed over the dark net via a Ransomware panel page.
It is a dangerous time, and we have a responsibility to keep ourselves informed and aware of the threats that exist. Stay vigilant!

Day 1 Questions

General Questions

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

```
Google Domains and Azure Web App
```

2. What is your domain name?

```
https://eyeoncyberproject.info
```

Networking Questions

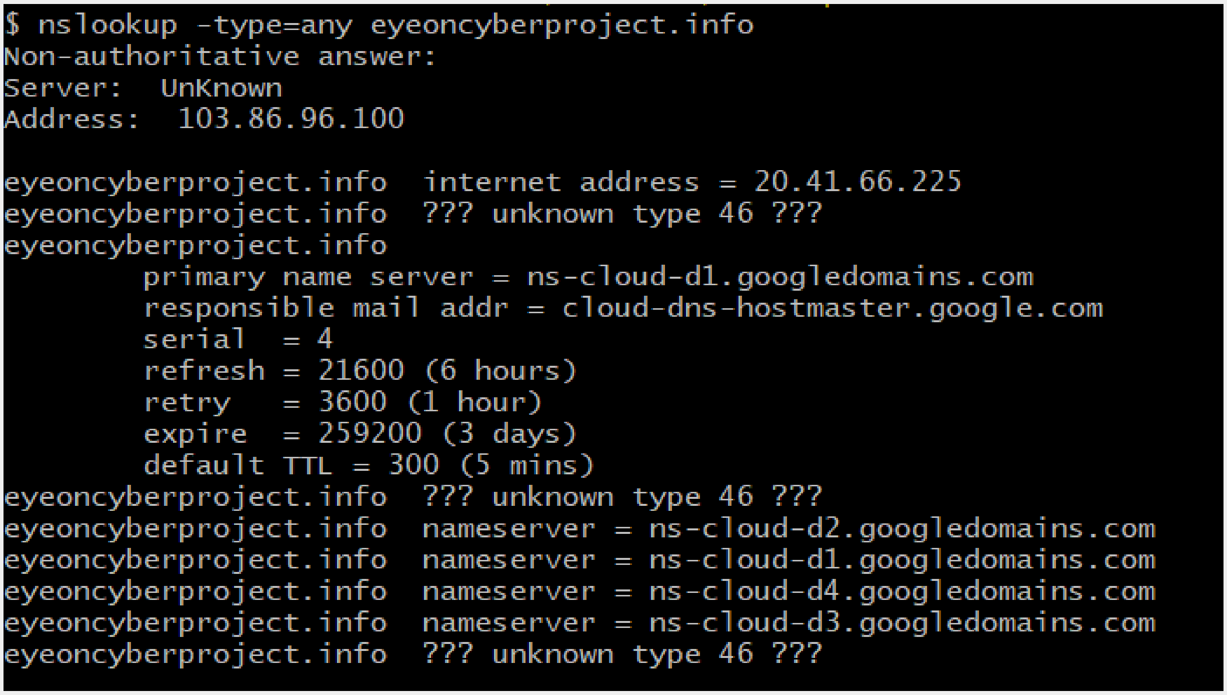
1. What is the IP address of your webpage?

```
20.41.66.225
```

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

```
Seoul-teukbyeolsi, Seoul, Korea
```

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



```
$ nslookup -type=any eyeoncyberproject.info
Non-authoritative answer:
Server:  UnKnown
Address:  103.86.96.100

eyeoncyberproject.info  internet address = 20.41.66.225
eyeoncyberproject.info  ??? unknown type 46 ???
eyeoncyberproject.info
        primary name server = ns-cloud-d1.googledomains.com
        responsible mail addr = cloud-dns-hostmaster.google.com
        serial  = 4
        refresh = 21600 (6 hours)
        retry   = 3600 (1 hour)
        expire  = 259200 (3 days)
        default TTL = 300 (5 mins)
eyeoncyberproject.info  ??? unknown type 46 ???
eyeoncyberproject.info  nameserver = ns-cloud-d2.googledomains.com
eyeoncyberproject.info  nameserver = ns-cloud-d1.googledomains.com
eyeoncyberproject.info  nameserver = ns-cloud-d4.googledomains.com
eyeoncyberproject.info  nameserver = ns-cloud-d3.googledomains.com
eyeoncyberproject.info  ??? unknown type 46 ???
```

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?

```
The runtime stack was PHP 7.4
The runtime stack works on the back end
```

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

```
There is a folder called css and a folder called images
The css holds stylesheets which change visually how the elements on the page are displayed.
The images folder has a backup of the images that are used on the page.
```

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

```
This works with the front end since it is part of the presentation
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is an architecture where a single software instance and its supporting infrastructure/database.  Provides a single place to manage users, groups, and the permissions they hold in relation to applications published.
```

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

A Key Vault access policy determines whether a given security principal, namely a user, application, or user group, can perform different operations on Key Vault secrets, keys, and certificates.

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

Keys are cryptographic keys that enable use of software-protected and HSM-protected keys

Secrets provide secure storage of passwords and database connection strings

Certificates can help encrypt communications over the internet and establish the identity of websites making the entry point and mode of communication secure.

Cryptography Questions

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

Self-signed certificates are free, suitable for internal network websites and development/testing environments and encryption/decryption of the data is done with the same ciphers used by paid SSL certificates.

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

Browsers and Operating Systems do not trust self-signed certificates since a Publicly trusted CA does not sign them.

Attackers can generate self-signed certificates, which can be used for man-in-the-middle attacks, leaving users vulnerable to data theft and other forms of cyber-attacks.

3. What is a wildcard certificate?

An SSL/TLS wildcard certificate is a single certificate with a wildcard character (*) in the domain field. Allowing the certificate to secure multiple sub domain names (hosts) pertaining to the same base domain.

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 in Azure because of an industry-wide vulnerability in SSL 3.0, commonly known as POODLE. Microsoft completely disabled SSL 3.0 in Azure websites by default to protect customers from the vulnerability.

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?

With the self-signed certificate it returns an error because the certificate is not trusted by my computer’s operating system

With the App Service Managed Certificate there is no error because it is using a trusted CA and shows a lock to signify this

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

Self-signed certificate:

Issued On Monday, September 12, 2022 at 6:58:10 PM

Expires On Tuesday, September 12, 2023 at 6:58:10 PM

App Service Managed Certificate:

Issued On Sunday, September 11, 2022 at 8:00:00 PM

Expires On Sunday, March 12, 2023 at 7:59:59 PM

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

Not with the self-signed certificate

With the App Service Managed: GeoTrust Global TLS RSA4096 SHA256 2022 CA1

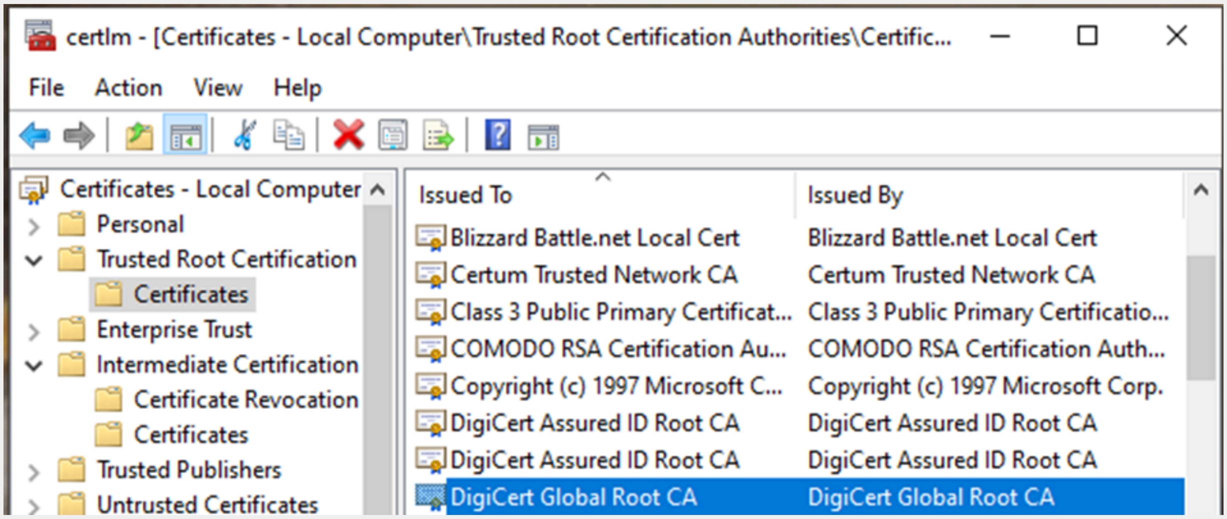
d. Do you have a root certificate? If so, what is it?

Not with the self-signed certificate

With the App Service Managed: DigiCert Global Root CA

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

Yes


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certific...
File
Action
View
Help

- Certificates - Local Computer
  - Personal
  - Trusted Root Certification
    - Certificates
  - Enterprise Trust
  - Intermediate Certification
    - Certificate Revocation
    - Certificates
  - Trusted Publishers
  - Untrusted Certificates

Issued To	Issued By
Blizzard Battle.net Local Cert	Blizzard Battle.net Local Cert
Certum Trusted Network CA	Certum Trusted Network CA
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...
COMODO RSA Certification Au...	COMODO RSA Certification Auth...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA
DigiCert Global Root CA	DigiCert Global Root CA

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

GlobalSign Root CA

Day 3 Questions

Cloud Security Questions

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

Both reside in front of your web application to protect it.

Both work on Application Layer (7) of the OSI model.

Their primary solution is a load balancer

They can incorporate a web application firewall (WAF) to protect against web vulnerability attacks.

They have additional features such as URL path-based routing and SSL/TLS termination.

The differences are.

The Web Application Gateway is more regional, to protect a web application in a single region in your cloud.

The Azure Front Door is more global and is better suited when you have a variety of regions in a cloud environment.

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 removing the SSL-based encryption from incoming traffic; the benefit is that it relieves a web server of the processing burden of decrypting and/or encrypting traffic sent via SSL.

3. What OSI layer does a WAF work on?

WAF is a part of layer 7 defense protocol layer.

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

HTTP request smuggling attack - an HTTP request smuggling vulnerability occurs when an attacker sends both headers in a single request. This can cause either the front-end or the back-end server to incorrectly interpret the request, passing through a malicious HTTP query.

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?

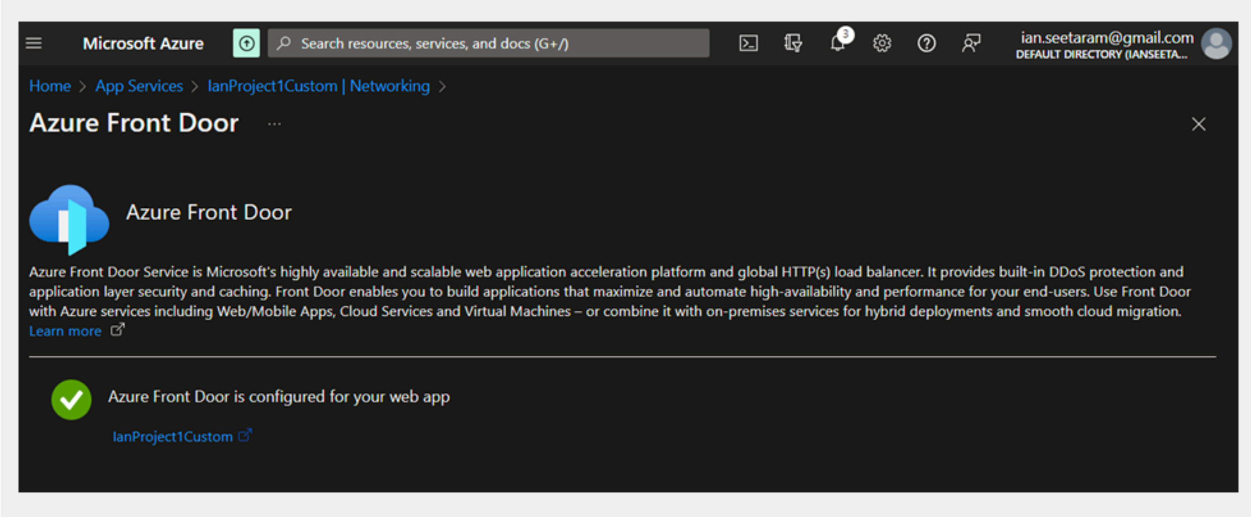
I believe that even though the front door is not enabled Microsoft Azure provides sufficient defenses to mitigate the risk. The blog page also does not have many susceptible resources and the attacker would not be able to manipulate enough to gain elevated credentials to make any changes through SSH.

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, nobody who resides from Canada would be able to access my website, although if they were to use a VPN that changes the region of their IP they still would be able to access it.

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

   a. Azure Front Door enabled


Microsoft Azure
Search resources, services, and docs (G+/)
ian.seetaram@gmail.com
DEFAULT DIRECTORY (IANSEETA...
Home > App Services > IanProject1Custom | Networking >

Azure Front Door

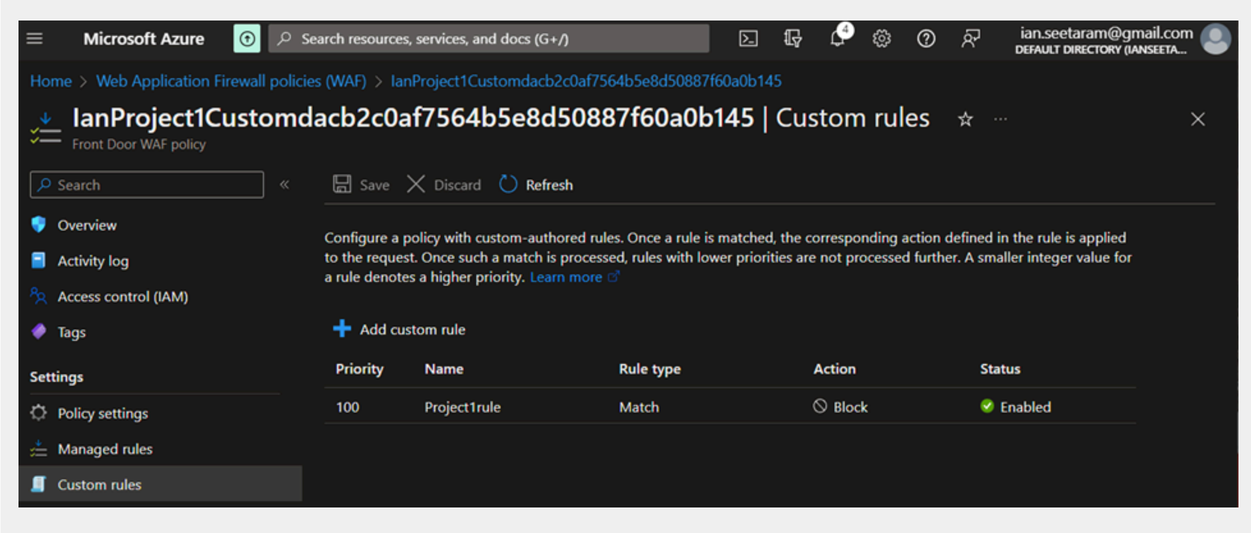
Azure Front Door

Azure Front Door Service is Microsoft's highly available and scalable web application acceleration platform and global HTTP(s) load balancer. It provides built-in DDoS protection and application layer security and caching. Front Door enables you to build applications that maximize and automate high-availability and performance for your end-users. Use Front Door with Azure services including Web/Mobile Apps, Cloud Services and Virtual Machines – or combine it with on-premises services for hybrid deployments and smooth cloud migration. Learn more

Azure Front Door is configured for your web app

IanProject1Custom

   b. A WAF custom rule


Microsoft Azure
Search resources, services, and docs (G+/)
ian.seetaram@gmail.com
DEFAULT DIRECTORY (IANSEETA...
Home > Web Application Firewall policies (WAF) > IanProject1Customdacb2c0af7564b5e8d50887f60a0b145
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Policy settings
Managed rules
Custom rules
Save
Discard
Refresh

IanProject1Customdacb2c0af7564b5e8d50887f60a0b145 | Custom rules

Front Door WAF policy

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

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**