



Cybersecurity

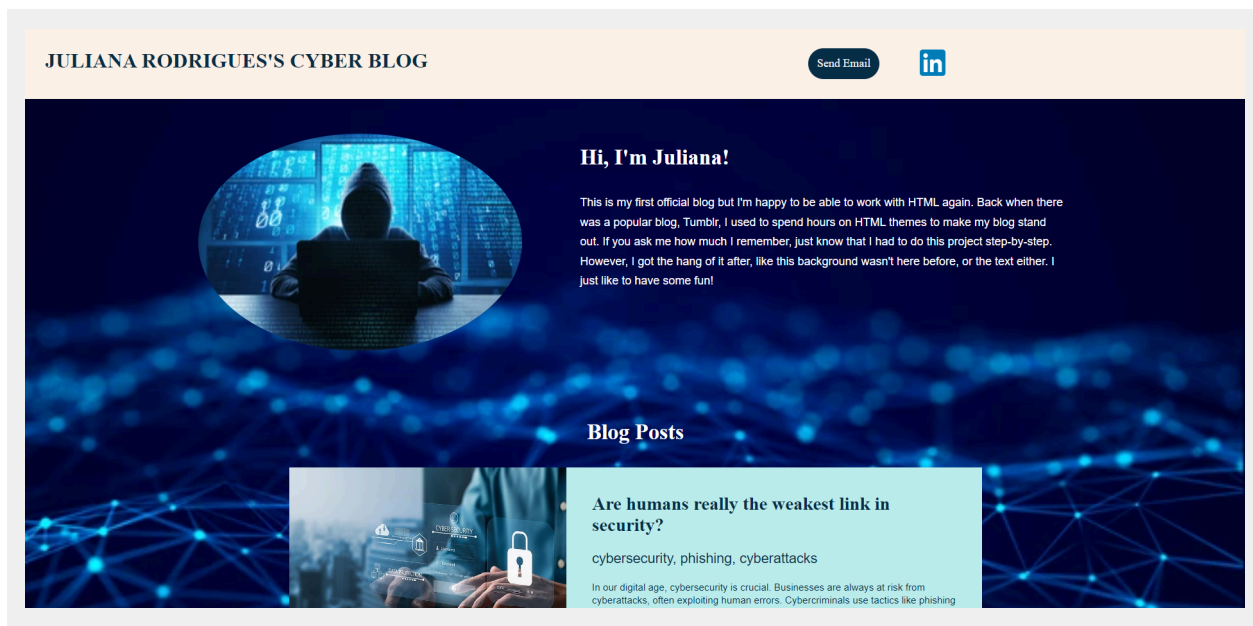
Project 1 Technical Brief

Your Web Application

Enter the URL for the web application that you created:

<https://julianawebapps.azurewebsites.net>

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



just like to have some fun!

Blog Posts



Are humans really the weakest link in security?

cybersecurity, phishing, cyberattacks

In our digital age, cybersecurity is crucial. Businesses are always at risk from cyberattacks, often exploiting human errors. Cybercriminals use tactics like phishing and social engineering to access data. The human factor is both a weakness and a priority in cybersecurity. By promoting awareness and best practices, businesses can empower employees to protect the organization's security. Social engineering attacks can be hard to detect because they target human vulnerabilities rather than technical weaknesses. This makes them especially dangerous, as even the most secure systems can be compromised if users are deceived into taking actions that give attackers access. Due to our natural inclination to trust and see the best in others, humans are vulnerable to scams and social engineering attacks. Exploiting this trust, scammers and attackers manipulate us to obtain what they desire. Our habitual nature makes it easy for attackers to exploit our known weak points. For instance, if an attacker knows your morning routine includes checking email first, they might send a phishing email at that time, counting on you to click on a link or attachment without much thought.



Your Password Is Too Simple

cyberattacks, often exploiting human errors. Cybercriminals use tactics like phishing and social engineering to access data. The human factor is both a weakness and a priority in cybersecurity. By promoting awareness and best practices, businesses can empower employees to protect the organization's security. Social engineering attacks can be hard to detect because they target human vulnerabilities rather than technical weaknesses. This makes them especially dangerous, as even the most secure systems can be compromised if users are deceived into taking actions that give attackers access. Due to our natural inclination to trust and see the best in others, humans are vulnerable to scams and social engineering attacks. Exploiting this trust, scammers and attackers manipulate us to obtain what they desire. Our habitual nature makes it easy for attackers to exploit our known weak points. For instance, if an attacker knows your morning routine includes checking email first, they might send a phishing email at that time, counting on you to click on a link or attachment without much thought.



Your Password Is Too Simple

password, cracking, cryptography

Security researchers generally agree on two indicators of a bad password: when it's easily guessable by a computer or human, and when it's difficult for a person to remember. One common mistake that aids password cracking is using a common word in your password. Most professional cracking tools rely on a word list or default password list, for what is known as a dictionary attack, which often brings successful results. Let's admit it, we've all used passwords with our home address, pet, or a relative. These are extremely unsafe choices, as someone with a bit of knowledge about us could easily guess them without any tools. But wait, there's more! If you find yourself needing to write your password on a piece of paper or in a notebook because it's too complex to remember, it becomes ineffective so you might as well get rid of it. Replacing characters with numbers is a common way to add complexity to passwords. Many of our passwords are based on things we remember, such as dates or favorite shows, making them easy to guess. What if we approached it differently? Cybercriminals are always finding new ways to breach our devices, but at the core of the passwords. If a hacker gets the keys, its game over.

Day 1 Questions

General Questions

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

Azure

2. What is your domain name?

julianawebapps.azurewebsites.net

Networking Questions

1. What is the IP address of your webpage?

20.211.64.19

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?

Server: G3100.mynetworksettings.com

Address: 192.168.1.1

Non-authoritative answer:

Name: waws-prod-sy3-103-e6e5.australiaeast.cloudapp.azure.com

Address: 20.211.64.19

Aliases: julianawebapps.azurewebsites.net

waws-prod-sy3-103.sip.azurewebsites.windows.net

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, back end

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

There is a `css` folder and `images` folder in which contains images and links for the website created.

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 refers to the sharing of computing resources in a private or public environment that is isolated from other users and kept secret.

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

It's important because an access policy on a key vault determines what operations users can perform on KV secrets, certificates, and keys.

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

Keys encrypt and decrypt data, certificates establish trust in communication, and secrets need secure storage.

Cryptography Questions

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

You have control over the software and can modify it to suit your specific needs and you can audit the source code to ensure there are no vulnerabilities or backdoors.

Bhattacharya, A. (2023, October 16). [What is a Self-Signed Certificate? Advantages, Disadvantages & Risks | Encryption Consulting. Encryption Consulting.](#)

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

The major drawback of self-signed certificates is the absence of trust validation, since users must manually verify and trust self-signed certificates by adding them to their trust stores.

Venafi. (n.d.). [What are Self-Signed Certificates? Risks and benefits | Venafi. Venafi.](#)

3. What is a wildcard certificate?

A SSL/TLS Wildcard certificate is a single certificate with a wildcard character (*) in the domain name field. This allows the certificate to secure multiple sub domain names (hosts) pertaining to the same base domain.

Home. What is a Wildcard Certificate? (2023, November 1). <https://knowledge.digicert.com/general-information/what-is-a-wildcard-certificate>

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 isn't provided because it's a known 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?

No because Azure provides the secure SSL certificate.

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

Issued On Tuesday, October 31, 2023 at 7:15:02 PM
Expires On Thursday, June 27, 2024 at 7:59:59 PM

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

No

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?

Yes

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

DigiCert Assured ID Root G3

Day 3 Questions

Cloud Security Questions

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

Azure Front Door and Azure Application Gateway are both load balancers for HTTP/HTTPS traffic, but they have different scopes. Front Door is a global service that can distribute requests across regions, while Application Gateway is a regional service that can balance requests within a region.

Duongau. (n.d.). Azure Front Door - Frequently asked questions. Microsoft Learn.
<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq>

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 to relieve a web server of the processing burden of decrypting and/or encrypting traffic sent via SSL. Some benefits include when this is used with clusters of SSL VPNs, because it greatly increases the number of connections a cluster can handle.

What is SSL offloading?. F5, Inc. (n.d.).
<https://www.f5.com/glossary/ssl-offloading>

3. What OSI layer does a WAF work on?

Layer 7 Defense

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

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements.

[*What is SQL Injection \(SQLi\) and How to Prevent Attacks. \(2024, January 9\). Acunetix.*](#)

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?

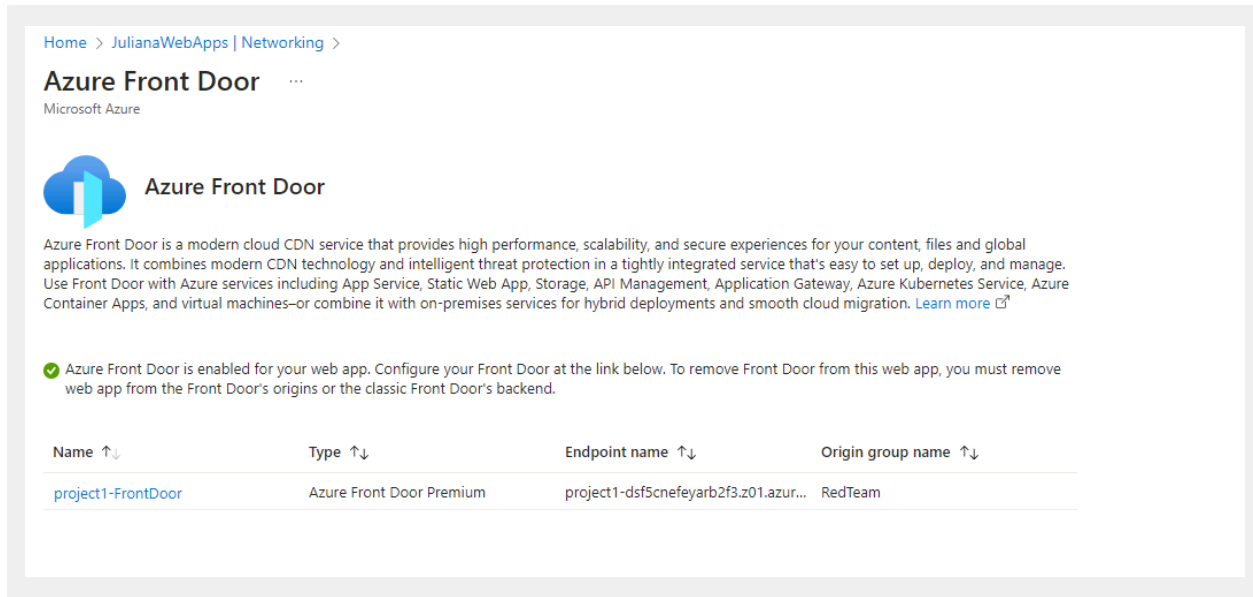
No, because with Front Door Enabled, my WAF rules will block malicious SQL code and inspect query strings.

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?

The WAF is blocking IPs from Canada, but we can't confirm if the user is truly in Canada. For instance, a person in Canada could use a VPN to hide their IP and bypass the WAF rule.

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

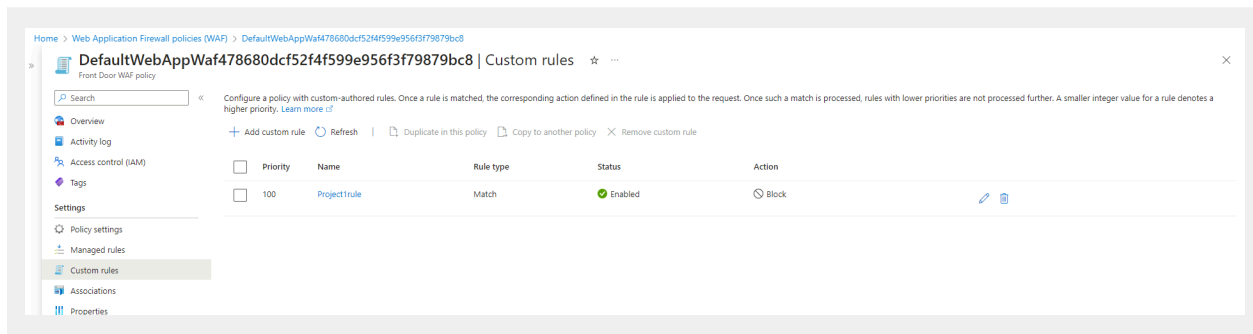
a. Azure Front Door enabled



The screenshot shows the 'Azure Front Door' configuration page in the Azure portal. The breadcrumb navigation at the top reads 'Home > JulianaWebApps | Networking >'. The page title is 'Azure Front Door' with a three-dot menu icon. Below the title is the Microsoft Azure logo and the text 'Azure Front Door'. A descriptive paragraph explains that Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for content, files, and global applications. It mentions integration with various Azure services like App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines. A green checkmark icon indicates that 'Azure Front Door is enabled for your web app'. Below this, a table lists the configured Front Door instance.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
project1-FrontDoor	Azure Front Door Premium	project1-dsf5cnefeyarb2f3.z01.azur...	RedTeam

b. A WAF custom rule



The screenshot shows the 'Custom rules' configuration page for a Web Application Firewall (WAF) policy. The breadcrumb navigation at the top reads 'Home > Web Application Firewall policies (WAF) > DefaultWebAppWaf478680dc52f4f599e956f3f79879bc8'. The page title is 'DefaultWebAppWaf478680dc52f4f599e956f3f79879bc8 | Custom rules'. A search bar is present at the top left. Below the search bar is a sidebar with navigation options: Overview, Activity log, Access control (IAM), Tags, Settings, Policy settings, Managed rules, Custom rules (selected), Associations, and Properties. The main content area shows a table of custom rules. A single rule is listed with a priority of 100, named 'Project1rule', with a 'Match' rule type, 'Enabled' status, and a 'Block' action.

Priority	Name	Rule type	Status	Action
100	Project1rule	Match	Enabled	Block