



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:

`esalinascyberblog.info`

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

My Blog

esalinas cyberblog.info

Gmail

YouTube

Maps

News

The Linux comma...

The Linux comma...

The Linux comma...

Command Challen...

Newest Questions...

Krebs on Security...

Unsupervised Lear...

News | WCY5 - W...

35 of the Best Info...

Free Online Netwo...

report2021gr.pdf

Finish update

ESTEBAN SALINAS'S CYBER BLOG

Send Email

in



Hi, I'm Esteban!

Welcome to my blog, where I talk about cybersecurity. I invite you to join me on a new journey. Through this blog, I aim to share my experiences and knowledge of threats and how to defend against them.

Blog Posts



Ransomware: Steps to stay protected

ransomware, money, patch Tuesday

While the threat of ransomware is daunting there are steps you can take to protect yourself and your organization from falling victim. Educating your team brings awareness, which is key to preventing these attacks. You must train yourself and your employees to recognize phishing attacks, suspicious links, and email attachments. Updating software with the latest patches enhances your safety by mitigating vulnerabilities that can be exploited. Regularly backup all important data. If your hit with an attack, you can avoid paying a ransom and continue operation. Implementing security measures such as firewalls and IDS to detect ransomware attacks before it happens. And of course, you must have a response plan. This plan must have all the steps that must be taken in the event of a

My Blog

esalinas cyberblog.info

Gmail

YouTube

Maps

News

The Linux comma...

The Linux comma...

The Linux comma...

Command Challen...

Newest Questions...

Krebs on Security...

Unsupervised Lear...

News | WCY5 - W...

35 of the Best Info...

Free Online Netwo...

report2021gr.pdf

Finish update

Blog Posts



Ransomware: Steps to stay protected

ransomware, money, patch Tuesday

While the threat of ransomware is daunting there are steps you can take to protect yourself and your organization from falling victim. Educating your team brings awareness, which is key to preventing these attacks. You must train yourself and your employees to recognize phishing attacks, suspicious links, and email attachments. Updating software with the latest patches enhances your safety by mitigating vulnerabilities that can be exploited. Regularly backup all important data. If your hit with an attack, you can avoid paying a ransom and continue operation. Implementing security measures such as firewalls and IDS to detect ransomware attacks before it happens. And of course, you must have a response plan. This plan must have all the steps that must be taken in the event of a ransomware attack. This must include isolating infected systems, notifying authorities, and who to contact to mitigate the impact. Following these tips can help your organization stay safe and be prepared.



Breaking the Habit: The Importance of Avoiding Password Reuse

passwords, cybersecurity, lower risk

In today's landscape, passwords serve as the primary line of defense against unauthorized access to our sensitive data. Despite this critical role, many fall into the habit of reusing passwords across multiple accounts. This exposes them to security risks. So, we must first understand the risk. The use of a single passwords seems convenient but poses great risk. If a hacker gains access to the one account, that same hacker can exploit all the other accounts with the same password. This can lead to a much larger impact on the victim. We can begin to harden your password security by using stronger passwords. Use a unique password, enable two-factor authentication, and regularly update the passwords. Also, the use of a password manager can simplify better protection. In a time when threats are ever-more present, safeguarding your accounts with good password management is essential. By avoiding password reuse, you can lower your risk of attack.

Day 1 Questions

General Questions

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

GoDaddy domain

2. What is your domain name?

esalinascyberblog.info

Networking Questions

1. What is the IP address of your webpage?

20.119.0.38

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

Washington, Virginia, United States

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

Non-authoritative answer:
Name: esalinascyberblog.info
Address: 20.119.0.38

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?

5 seconds

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

There was a css and image directory. CSS has the style.css file which is used to style the webpage, and the images directory has the images used on the webpage.

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 the customer paying a provider for cloud services.

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

An access policy is important from a security standpoint because you can control who accesses keys, secrets, and certificates stored in the key vault.

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

Keys are used for encryption and decryption. Secrets are data such as passwords or credentials. Certificates are used for authentication, as in validating identity.

Cryptography Questions

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

Cost-effective, appropriate for a testing environment, and they are quick to deploy.

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

It is not signed by a CA, so certificates can be considered unsafe. Use is limited to internal environments due to lack of trust.

3. What is a wildcard certificate?

A wildcard certificate is a certificate issued to secure a domain, including its 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 has security vulnerabilities in its protocol, so Azure does not provide it for safety concerns.

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 it has a valid certificate.

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

02/22/24 to 08/23/24

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

Yes. GeoTrust Global TLS RSA4096 SHA256 2022 CA1

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

No. A root certificate is a self-signed certificate issued by the root CA that is typically installed on the web browser and used to verify other

certificates.

- 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 Global 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 are load balancers used for managing HTTP/HTTPS traffic. Azure Web Application Gateway differs by its use for distributing within a region, while Azure Front Door is used to distribute across regions.

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 from processing decrypted or encrypted traffic. This can improve the server's performance and reduce server load, and improve security.

3. What OSI layer does a WAF work on?

Layer 7

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

SQL injection is when an attacker inserts malicious SQL code into input fields of a web application in order to manipulate the SQL queries to gain access to data or execute unauthorized actions. The WAF managed rule will block or log the suspicious request.

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. The Front Door's built-in WAF protection would not inspect incoming traffic for malicious patterns.

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. If someone living in Canada is using a VPN to mask their IP address and make it appear as if the traffic comes from another country, they will have access.

7. Include screenshots below to demonstrate that your web app has the following:
 - a. Azure Front Door enabled

Microsoft Azure

Upgrade

Search resources, services, and docs (G+I)


esteban.d.salinas@gmail.com

DEFAULT DIRECTORY

Home > App Services > EstebanSecurityResume | 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](#)

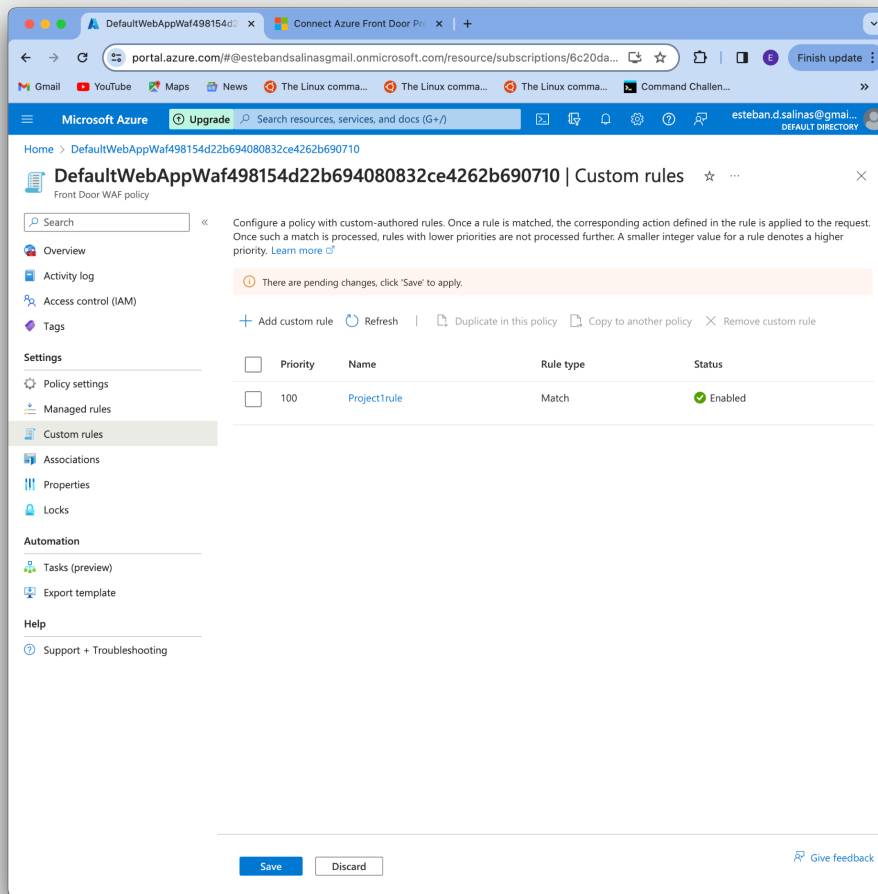
✔ Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove web app from the Front Door's origins or the classic Front Door's backend.

| Name ↑↓ | Type ↑↓ | Endpoint name ↑↓ | Origin group name ↑↓ |
|------------------------------------|--------------------------|-----------------------------------|----------------------|
| project1-FrontDoor | Azure Front Door Premium | project1-h3dcbnfcwc7daeyz02.az... | RedTeam |

Add

Close

b. A WAF custom rule



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*

