Cybersecurity

Project 1 Technical Brief

Your Web Application

Enter the URL for the web application that you created:

```
https://stephanieortegablog.azurewebsites.net/
```

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

How To Be Tech Safe Without Being Tech Smart

Online Safety, Tech Knowledge, Tech Safe

In today's digital world, staying safe online is essential, even if you're not a tech expert. Fortunately, you don't have to be a guru to protect yourself and your personal information. Here are 10 simple tips to enhance your online security wihtout needing advanced tech skills. 1.Update, Update, Update! Keeping your devices and software up to date is crucial. Regularly install the latest updates and patches for your system, apps, and antivirus software. These updates often contain important security fixes that help safeguard your devices. 2.Strong Passwords: Choose strong, unique passwords for all your online accounts. Avoid using common phrases or personal information and instead go for a combination of letters, numbers, and symbols. Consider using a password manager to safely store your passwords. 3.Enable Two-Factor Authentication: Enable 2FA whenever possible. This adds an extra layer of security by requiring a second form of verification, such as a fingerprint scan or a unique code send to your phone to log in to your accounts. 4.Beware of Phishing: Phishing attempts are becoming increasingly complex. Exercise caution of suspicious emails, messages, or calls asking for personal information. Avoid clicking on suspicious links and double-check the sender's address before sharing anything. 5.Use Secure Networks: Avoid using public Wi-Fi networks for activities involving sensitive data. If you have to use a public network, using a VPN to encrypt your data and ensuring a secure connection is recommended. 6.Regular Backups: Back up your important files and data on the regular. This way, if you device is compromised or experiences some type of failure, you can restore your data and avoid losing valuable information. 7.Privacy Settings: Familiarize yourself with the privacy settings on your devices, social media accounts, and other online services. Adjust these settings to limit the amount of personal information that is shared publicly. 8.Be Cautious with Downloads: Download software, apps, and files only from reputable sources. Avoid pirated or suspicious websites that could potentially contain malware or other malicious programs that could harm your devices. 9.Educate yourself! Stay informed about common cybersecurity threats. Read up or listen to podcasts on the latest scams, malware trends, and best practices for safety to better protect yourself! 10.Trust Your Instincts: If something feels off or too good to be true it probably is! Trust your gut and be wary, when in doubt take a step back and research before proceeding. By following these 10 easy steps, you can learn how better protect yourself without an extensive tech knowledge! It's all about adopting good habits, staying vigilant, and always prioritizing your privacy and safety. Stay safe and enjoy your digital experience with peace of mind!

Cloudy with A Chance of Malware

Cloud vulnerabilities

In today's world mostlt everything is online. From personal use to business use, there is a need for immediate access to resources through the internet. It is no wonder that the cloud services continues to climb higher in popularity and along with it comes the need to address potential security vulnerabilities. Through Crowdstrike's article, "12 Cloud Security Issues: Risks, Threats, and Challenges" they discuss risks that come with using the cloud. For this blog we will be focusing on the threats that come with the cloud. 1.Zero-Day Exploits: This attack targets the vulnerabilities in popular software and systems that the vendor hasn't patched. Even if your configuration is strong, hackers can use zero-day attack to gain access. 2.Advanced Persistent Threats: This attack gains undetected access for the hacker to remain in the environment and be able to steal valuable information. 3.Insider Threats: This attack comes from someone from within the company such as an employee or someone who has access to the system that then sells information or intellectual property, business practices, and other information to help carry out an attack. 4.Cyberattacks: An attempt by a hacker to gain access to a network by using common attacks such as malware, phishing, DDoS, SQL injections or IoT. We can help protect against these threats by following secure code standards, double checking your configurations for any holes, and go on offensive threat hunting. Using the cloud gives us great advantages, being aware of the ongoing vulnerabilities will help protect the services from being compromised and help us to better protect data.

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?

```
stephanieortegablog
```

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
```

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

```
$ nslookup 20.211.64.16
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

*** cdns01.comcast.net can't find 20.211.64.16: Non-existent domain
```

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, frontend
```

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

```
Looking into the assets directory it had two other directories: css, and
images. Looking into both it seems like they contain the rest of the pieces
of the website such as style, color, images, etc.
```

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

```
The directory is the back end, the assets directory provides the code that
the user ultimately ends up seeing the results on the front end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
The user of cloud services
```

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

```
Because it limits who has access to keys
```

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

```
Keys are cryptographic keys used to encrypt, decrypt, sign, and verify which
create secure communication channels. Secrets are sensitive pieces of data
usually in the form of passwords, API key, or other confidential
information, usually used to authenticate to external sources. Certificates
are digitally signed by trusted CA, used to authenticate, encrypt, and
secure communication.
```

Cryptography Questions

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

```
1. They’re free to generate and use
2. Useful for internal purposes since they are not validated by the CA
   they can establish secure connections within a closed environment.
3. Can be generated quickly and easily
```

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

```
1. Lack of trust since they are not validated by the CA
2. Vulnerable to Man-in-the-Middle Attacks
3. Not suitable for public facing websites or services since they do not
   have user trust and compatibility
4. Have shorter lifetimes and require manual renewal and distribution
```

3. What is a wildcard certificate?

```
It’s a certificate that is designed to cover and secure multiple subdomains
of a domain with just one certificate. For a example a domain like
example.com can have sub domains such as mail.example.com and a wildcard
certificate would cover all of them that way they don’t need individual
certificates for each one.
```

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.

```
3.0 isn’t provided because it is considered insecure due to multiple
vulnerabilities and security flaws.
```

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?

```
Yes because it is not trusted since it wasn’t created by a trusted CA
```

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

```
Not before 3/9/23 not after 3/3/24
```

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?

```
Microsoft Azure TLS Issuing CA 02
```

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.

```
*azurewebsites.net
```

Day 3 Questions

Cloud Security Questions

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

```
Similarities:
   1. Traffic Routing: both offer traffic routing capabilities to distribute
      incoming requests to various backend servers based off rules
   2. Load Balancing
   3. SSL/TLS Termination: both have this to allow better handle of HTTPS
      requests
Differences
   1. Primary Use: Azure Gateway used primarily for hosting and managing web
      apps while Azure Front Door improves performance and reach of web
      apps.
```

```
2. Caching: Gateway does not have built-in caching while Front door does.
3. Global Load Balancing: Gateway focuses on load balancing on a single
   virtual network while Front Door offers global load balancing
4. Backend Service Support: Gateway can route traffic to backend servers
   in Azure while Front Door can route traffic to that and external
   services as well.
```

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 where SSL/TLS encryption and decryption take
place by a load balancer or proxy server such as Azure Web Application
Gateway or Azure Front Door instead of the backend servers. The benefits to
this is that it improves performance by relieving the backend servers of
encryption/decryption which in turn reduces processing times, it also
centralizes certificate management and allows for extra security functions
such as SSL inspection and content filtering.
```

3. What OSI layer does a WAF work on?

```
Usually occurs at the Application Layer, Layer 7
```

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

```
Blocks SQL injection attacks
```

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?

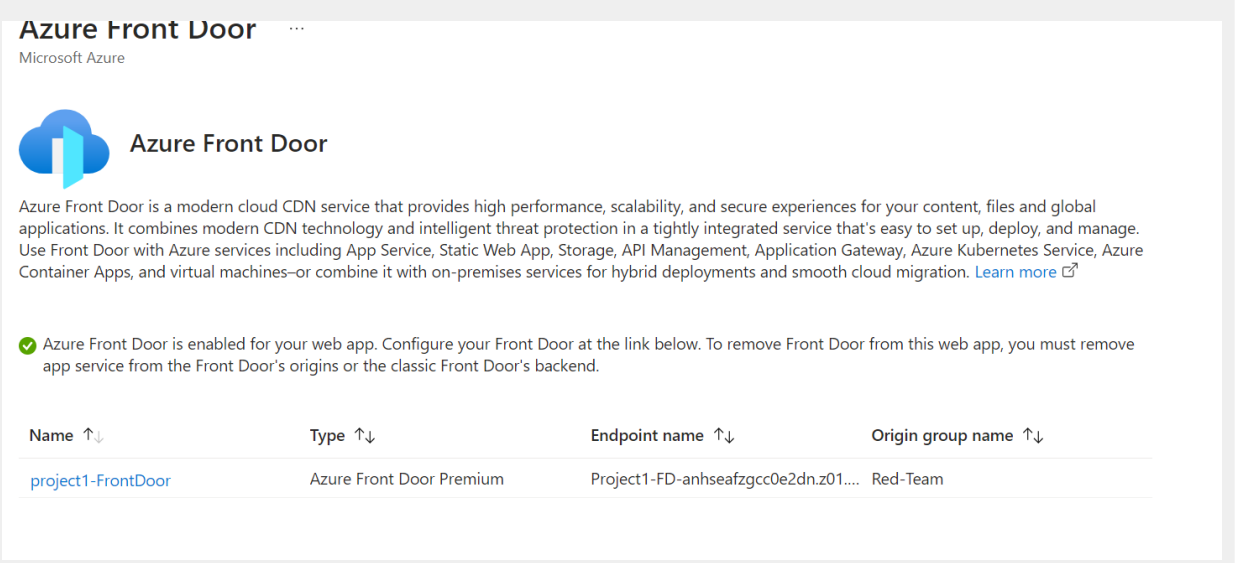
```
I personally don’t have a comment section but if my website did it could be
vulnerable to SQL injection.
```

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?

```
Not necessarily because someone could be using a VPN that shows them as a
different location other than Canada.
```

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

    a. Azure Front Door enabled



    b. A WAF custom rule