Cybersecurity

Project 1 Technical Brief

Your Web Application

Enter the URL for the web application that you created:

https://www.robustsecurity.info/

Day 1 Questions

General Questions

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

GoDaddy lowcost domain

2. What is your domain name?

robustsecurity.info

Networking Questions

1. What is the IP address of your webpage?

20.40.202.3

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

```
Galve, Gavleborgs Ian, Sweden
```

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

```
ns39.domaincontrol.com & ns40.domaincontrol.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 7.4
```

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

```
The file inside is the CSS file. This file is used to present the information on the site in a specific format. This provides flexibility and improves content accessibility.
```

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

```
The CSS operates on the front end of the site.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant comes in two categories: single and multi -cloud tenant. Therefore, a cloud tenant is a computing architecture which allows individuals and or organizations to share resources in a public or private sphere.

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

The access policy for a specific key vault determines who or what has access to the resources and what can be done with this access.

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

The key vault supports keys, secrets and certificates. Keys are cryptographic data imported into Key Vault. While secrets are sequences of connecting strings, account keys or passwords for PFX. Finally, certificates are used to provide validity of the public key associated with the site.

Cryptography Questions

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

The main advantage of a self-signed certificate is that it's free and can be used internally without additional cost.

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

Self-signed certificates are not trusted outside of the organization that generated the certificates. As a result, visitors to the site will not feel confident interacting with the site.

3. What is a wildcard certificate?

The advantage of having a wildcard certificate is that it can be used to secure multiple sub-domains. However, if one of the domains covered by the certificate is compromised there's a possibility that all may be compromised.

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 a known vulnerability and as a result is deemed insecure, and no longer recommended. Using a Man-in-the Middle attack a threat actor can intercept and decrypt data using SSL 3.0.

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?

My browser is not returning an error because a certificate was generated wit hin Azure and binds to the website.

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

Valid From: 6/17/2022 to 12/18/2022

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

Yes, my root certificate is robustsecurity.info

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

The root certificate is GeoTrust Global

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

The browser does not have the root certificate in its store due to the site being stored on a remote server and not on the local machine.

    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?

Azure Web Application Gateway and Azure Front Door are similar, yet different services within the Microsoft ecosystem. While AWAG is a regional solution, AFD is global. You may be wondering what exactly this means. It means that AWAG allows an administrator to manage and tweak their solution at the VM and or container level. Whereas AFD tweaking can only be performed at the cluster level. Additionally, bot h solutions detect attacks and anomalies but only the AWAG stops the suspicious activity. Several white papers recommended using both options within a single solution to provide layered protection.

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 by which SSL traffic is diverted to an SSL Load Balancer for decryption and encryption. Since SSL enc ryption and decryption are resource intensive processes, delegating the encryption \ decryption to a separate dedicated web server allows the web server to focus on other service requests.

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: This is a security exploit targeting the back - end database of a web application. It’s specifically effective on web applications, where inp ut validation is non - existent. It allows an attacker to use malicious SQL code to access sensitive information.

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?

My website based on its current configuration is not susceptible to a SQL Injection attack because a database is not attached.

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?

All users with a Canadian IP address will not be able to access the website. As the Web Application Firewall (WAF) rule will be blocking all traffic from these addresses.

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

    a. Azure Front Door enabled

See FigA- Azure Front Door.jpg

    b. A WAF custom rule

See FigB- WAF Custom Rule.jpg

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 the project has been graded.*
    - ***Yes***

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.