Cybersecurity

Project 1 Review Questions

Day 1 Questions

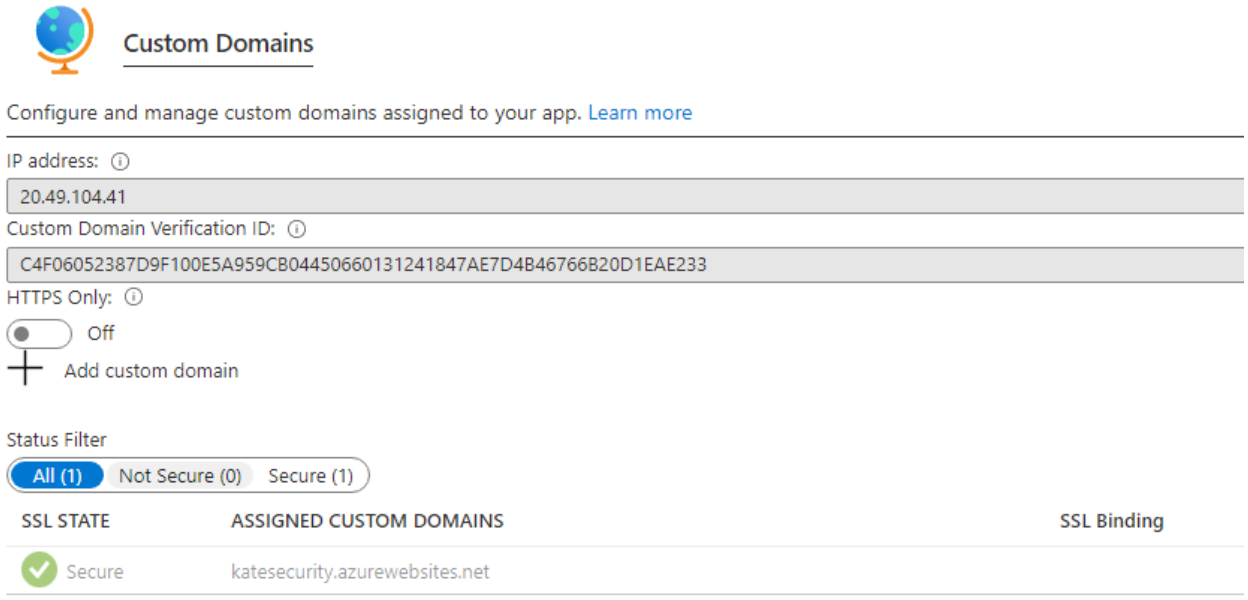
General Questions

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

2. What is your domain name?
   katesecurity.azurewebsites.net

Networking Questions

1 What is the IP address of your webpage?



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

IP Address	Country	Region	City
20.49.104.41	United States of America	Virginia	Washington

ISP	Organization	Latitude	Longitude
Microsoft Corporation	Not Available	38.7135	-78.1594

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

```
katerina@Azure:~$ nslookup katesecurity.azurewebsites.net
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
katesecurity.azurewebsites.net  canonical name = waws-prod-blu-263.sip.azurewebsites.windows.net.
waws-prod-blu-263.sip.azurewebsites.windows.net canonical name = waws-prod-blu-263-71e9.eastus.cloudapp.azure.com.
Name:   waws-prod-blu-263-71e9.eastus.cloudapp.azure.com
Address: 20.49.104.41

katerina@Azure:~$
```

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?
Run times tack PHP7.4. It works on the front end. Front-end development focuses on the client-facing aspects of a website or web application. This includes designing and optimizing the user interface, working on important visual aspects of web pages, and taking care of any website debugging issues

2. Inside the /var/www/html directory, there was another directory called assets. Explain what was inside that directory
Inside is directory css and document style.css how to design your website.

```
root@026894fc5ce3:~$ cd /var
root@026894fc5ce3:/var# ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  ssl  tmp  www
root@026894fc5ce3:/var# cd www
root@026894fc5ce3:/var/www# ls
html
root@026894fc5ce3:/var/www# cd hrml
-bash: cd: hrml: No such file or directory
root@026894fc5ce3:/var/www# cd html
root@026894fc5ce3:/var/www/html# ls
CHANGELOG.md  README.md  assets  docs  external     hackable     index.html  instructions.php  logo
COPYING.txt   about.php  config  dvwa  favicon.ico  ids_log.php  index.php   login.php         php.
root@026894fc5ce3:/var/www/html# cd assets/
root@026894fc5ce3:/var/www/html/assets# ls
css
root@026894fc5ce3:/var/www/html/assets# cd css
root@026894fc5ce3:/var/www/html/assets/css# ls
style.css
root@026894fc5ce3:/var/www/html/assets/css# head style.css
* {
  margin: 0;
  padding: 0;
  box-sizing: border-box;
}

body {
  font-family: Helvetica;
  color: #082D49
}
root@026894fc5ce3:/var/www/html/assets/css#
```

3. Consider your response to question #7. Does this work with the front end or back end?
It works with a frond end. Front-end development focuses on the client-facing aspects of a website or web application. This includes designing and optimizing the user interface, working on important visual aspects of web pages, and taking care of any website debugging issues

Day 2 Questions

Cloud Questions

1 What is a cloud tenant?
A tenant is essentially a customer who purchases cloud computing resources. This could be an individual user, a group of users, or an entire department or company.

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? When Azure Key Vault creates the certificate, it creates a related private key and password. The password is stored as an Azure Secret while the private key is stored as an Azure Key. Expired certificates can roll over with notifications before these operations happen.

Cryptography Questions

1 . What are the advantages of a self-signed certificate? Advantages: Self-signed certificates are free. They are suitable for internal network websites and development/testing environments. Encryption and 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? Self-signed SSL Certificates are risky because they have no validation from a third-party authority, which is usually a Trusted SSL Certificate Company. Developers and businesses try to save money by using or creating a free Self-Signed SSL Certificate. But there are several threats and possible consequences of the Self-Signed SSL certificates which you should know about

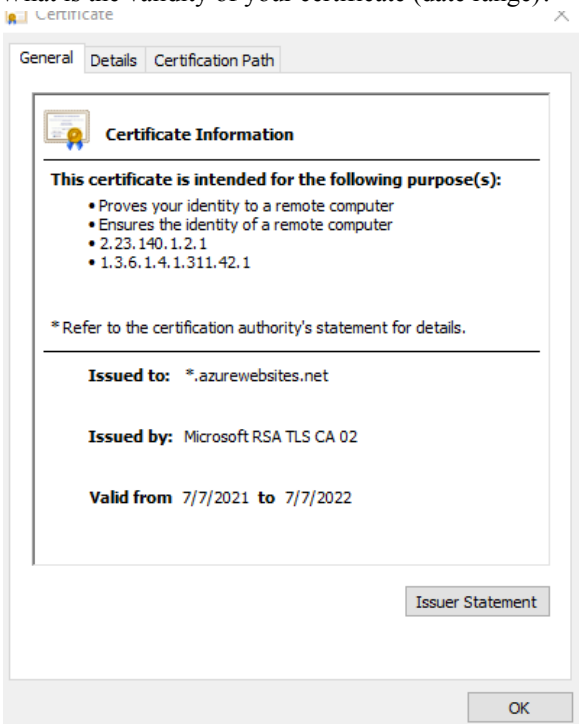
3. What is a wildcard certificate? A wildcard certificate is a public key certificate which can be used with multiple sub-domains of a domain. The principal use is for securing web sites with https, but there are also applications in many other fields. Compared with conventional certificates, a wildcard certificate can be cheaper and more convenient than a certificate for each sub-domain. Multi-domain wildcard certificates further simplify the complexity and reduce costs by securing multiple domains and their sub-domains.

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. Transport Layer Security (TLS), the successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network Azure Storage uses TLS 1.2 on public HTTPS endpoints, but TLS 1.0 and TLS 1.1 are still supported for backward compatibility. Azure Storage accounts permit clients to send and receive data with the oldest version of TLS, TLS 1.0, and above
SSL 3.0 is an encryption standard that's used to secure Web traffic using the HTTPS method. It has a flaw that could allow an attacker to decrypt information, such as authentication cookies, according to Microsoft.

0. ***After*** **completing the Day 2 activities, view your SSL certificate and answer the following questions:**

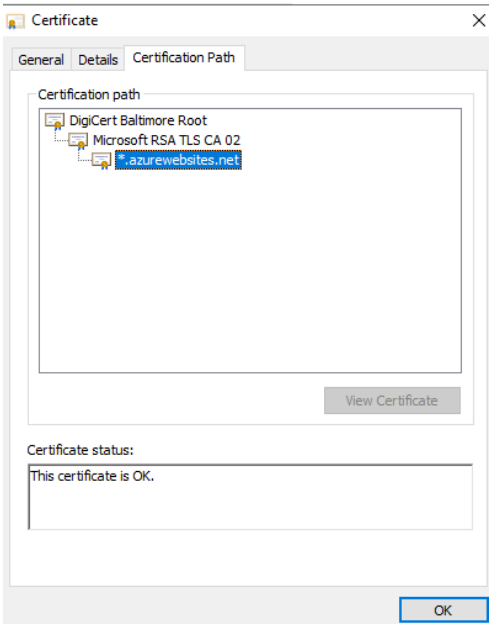
- Is your browser returning an error for your SSL certificate? Why or why not? No, my browser is not returning an error. Because my certificate is not expired and allow all traffic.

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



- Do you have an intermediate certificate? If so, what is it? Yes, I have intermediate certificate because its certificate issued by the trusted root certificate authority and provided to certificate providers to give them the authority to issue end-entity (SSL) server certificates.

- Do you have a root certificate? If so, what is it? DidiCert Baltimore Root is my root certificate



- Does your browser have the root certificate in its root store?

There are three parts to the chain of trust: Root Certificate. A root certificate is a digital certificate that belongs to the issuing Certificate Authority. It comes pre-downloaded in most browsers and is stored in what is called a "trust store." The root certificates are closely guarded by CAs.

- List one other root CA in your browser's root store.
  Microsoft RSA TLS CA 02

Day 3 Questions

Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?
While both Front Door and Application Gateway are layer 7 (HTTP/HTTPS) load balancers, the primary difference is that Front Door is a non-regional service whereas Application Gateway is a regional service

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. The processing is offloaded to a separate device designed specifically for SSL acceleration or SSL termination.
The device completes the handshaking of SSL quicker than the web server. This results in smooth loading of the website and faster processing of requests at the end of the web application.

1. What OSI layer does a WAF work on? A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors

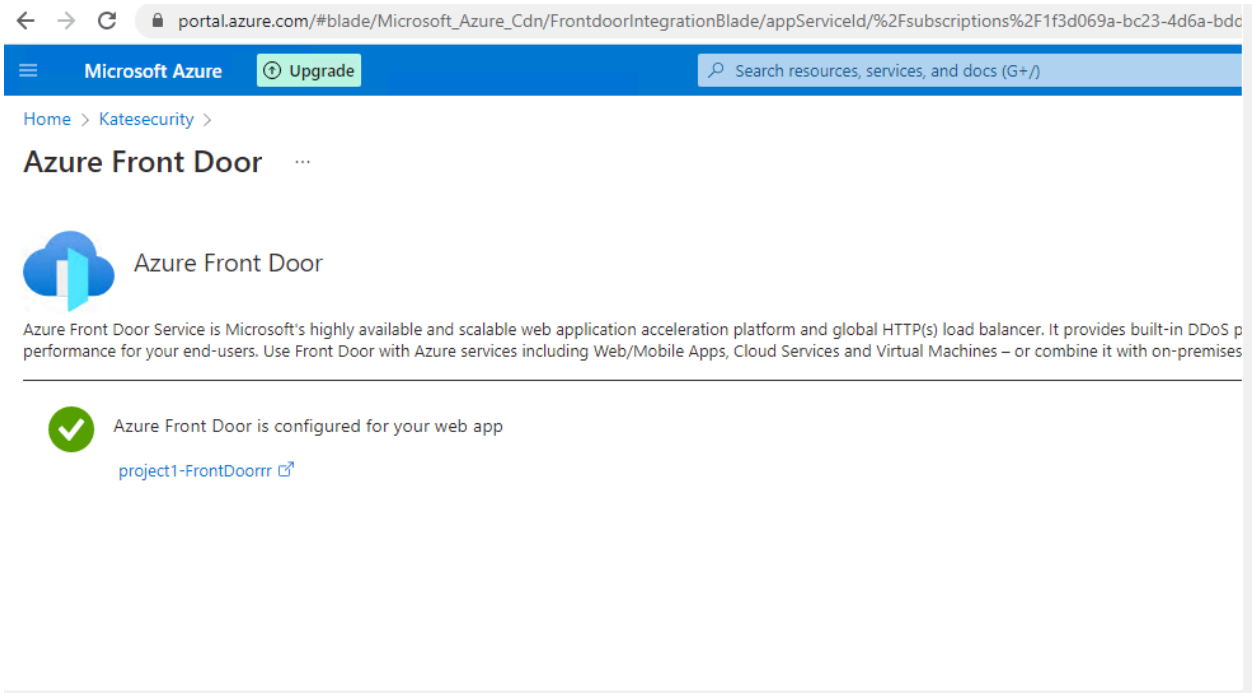
2. Select one of the WAF managed rules (e.g., directory traversal, SQL injection, etc.), and define it.
SQL injection
Attackers sometimes insert malicious SQL code into web requests to extract data from your database. To allow or block web requests that appear to contain malicious SQL code, create one or more SQL injection match conditions. An SQL injection match condition identifies the part of web requests, such as the URI or the query string, that you want AWS WAF to inspect. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious SQL code

3. 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, it would be impact, because currently I am using a rule for 3 countries (US, CANADA, AUSTRALIA). Without WAF custom rule anybody would have access to the website. Custom rules allow you to create tailored rules to suit the exact needs of your applications and security policies. I can restrict access to my web applications by country/region

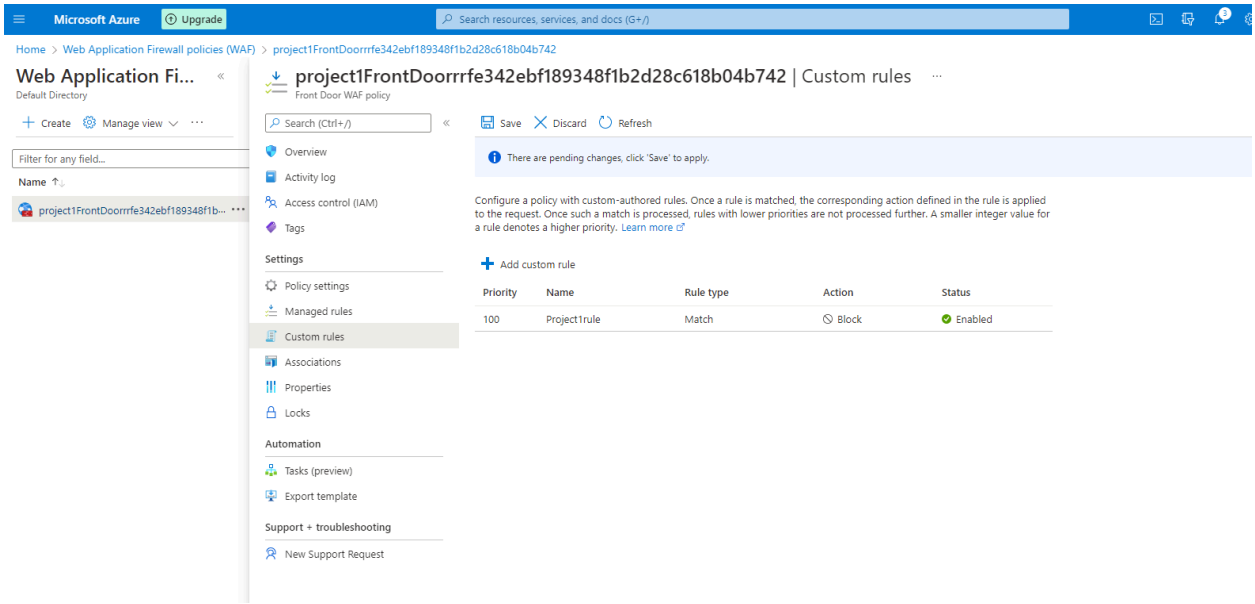
4. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not? Yes since I created a WAF custom rule people who resides in Canada wouldn't be able to access my website.
Yes, if I will block Canada, anyone who resides there wouldn't be able to access my website.

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

a. Azure Front Door enabled



a. 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 .Yes*

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*