Cybersecurity

Project 1 Technical Brief

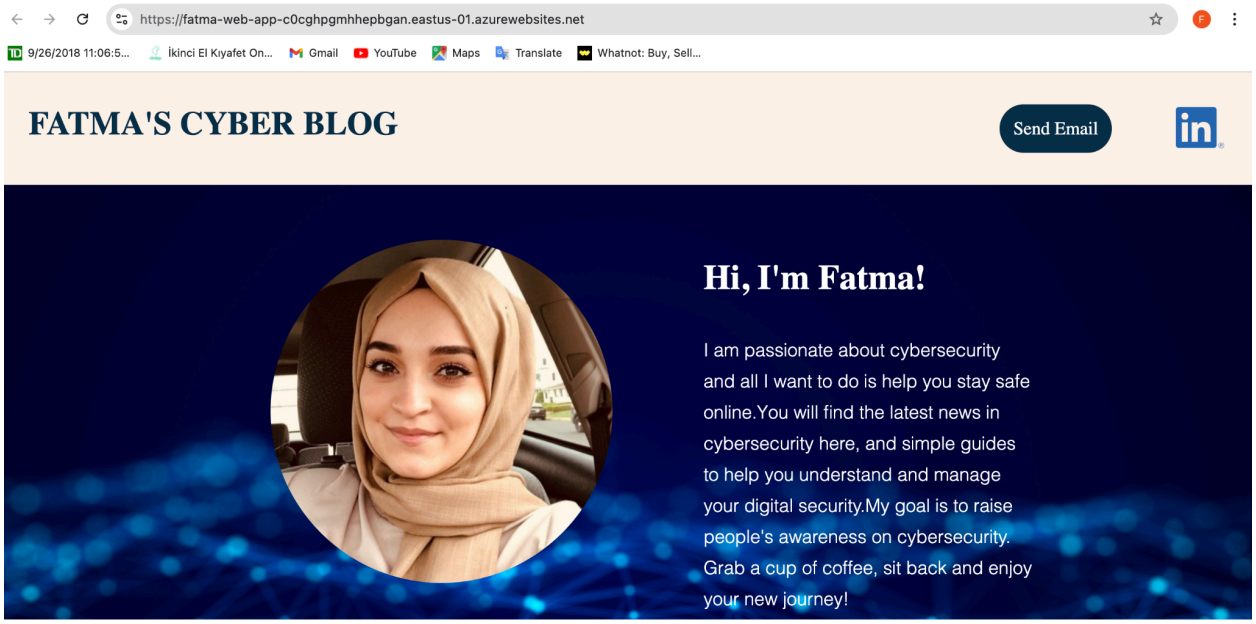
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://fatma-web-app-c0cghpgmhhepbgan.eastus-01.azurewebsites.net/
```

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



Ransomware: Should organizations pay or not?

Ransomware

Paying ransom has both advantages and disadvantages.The advantage of paying the ransom to provide you to receive a decryption key,which could be the fastest way to recover encrypted data.However,there is a disadvantage of this fastest way that we have to be careful is there is no guarantee that paying the ransom will result in the successful decryption of data because some attackers may not provide the key. As an another advantage is,sometimes,paying the ransom may be seen as a way to avoid further damage or loss of critical data.That makes the organizations feel comfortable but unfortunately to pay the ransoms can encourage further attacks,as it signals that the organization is willing to comply. Other than these,the organizations should have well-defined incident response plan which can help manage and contain the attack effectively.Or reporting the incident to law enforcement can sometimes provide assistance and help in tracking down the perpetrators.So,when it comes to my opinion,I prefer to focus on the future.Why?Because what the first thing that I need to think is,if I pay it now,it will make the organization a more attractive target for future attacks.That means it will not work by paying the ransom according to my opinion.Organizations must have a incident response plan, educated employees that can mitigate the risks before the attacks.So,they will not have to answer that question. Finally,the decision to pay or not to pay should be guided by the specific circumstances of the attack, including the organization's ability to recover from the incident,the potential for future attacks and the legal and ethical implications.

Why Using Strong/Unique Passwords

Passwords

Securing your online accounts is more critical than ever.One of the most straightforward yet effective ways to protect yourself is by using strong,unique passwords.But,why?A strong password is one that's difficult for hackers to guess.That's why,instead of using easily guessable passwords, aim for a combination of strong ones. For example, use at lest 12 characters.The longer,the better.Or,mix uppercase and lowercase letters,numbers, and special characters.Use a random combination of unrelated words and characters.After creating the passwords use different passwords for each websites.Because using the same password across multiple sites might seem convenient,but it is a huge security risk.If one account gets compromised, all your accounts with the same password are at risk.So,having different passwords will mitigate the risks,if a hacker gain access to one account they won't automatically have access to your other accounts.By investing a little time in creating and managing these passwords,you significantly enhance your protection against unauthorized access and cyber threats.Remember, how you do not let unknown people get in your house,and you use multiple keys on your door which will make it harder to unlock the door,likewise using strong and multiple password will protect your digital house.

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?

```
fatma-web-app-c0cghpgmhhepbgan.eastus-01.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.119.8.29
```

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

```
United States, Virginia, Washington
```

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

```
nslookup -type=ns
fatma-web-app-cOcghpgmhhepbgan.eastus-01.azurewebsites.net
Server: 168.63.129.16
Address :168. 63.129.16#53

Non-authoritative answer:
fatma-web-app-cOcghpgmhhepbgan. eastus-01 azurewebsites.net
canonical name = waws-prod-blu-413.sip.azurewebsites.windows.net.
waws-prod-blu-413.sip.azurewebsites.windows.net
canonical name = waws-prod-blu-413-aaf1.eastus.cloudapp.azure.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 8.2 BACK END
```

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

```
There are two directories called CSS and IMAGES.
The CSS is used to define styles for the web pages, including the design,
layout and variations in display for different devices and screen sizes.
The IMAGES directory is storing images used by the website.
```

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 a distinct, separate entity within a cloud
computing environment that has its own resources, settings, and data,
isolated from other tenants. In a multi-tenant cloud environment, multiple
customers (tenants) share the same physical infrastructure but have their
own virtualized environments.
```

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

```
Because it allows/restricts access ‘permissions’ separately to keys, secrets
or certificates.
```

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

```
Keys support multiple key types and algorithms.
Secrets provide secure storage for passwords and database connection
strings.
Certificates are built on top of keys and secrets with an added auto renew
```

```
feature.
```

Cryptography Questions

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

```
They are free and suitable for internal network websites and testing and development environments.
```

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

```
They are risky because they do not have validation from any third party authority.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a type of SSL/TLS certificate that allows you to secure multiple subdomains of a domain with a single 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 is not provided by Azure due to its inherent security weaknesses and the fact that more secure, modern protocols like TLS offer better protection against a variety of threats.
```

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 I secured it with an app service managed certificate.
```

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

```
Issued On: Friday, May 24, 2024 at 2:15:06 AM
```

```
Expires On: Monday, May 19, 2025 at 2:15:06 AM
```

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

```
Yes. An intermediate certificate is part of a chain of trust used in digital
security, specifically in the context of SSL/TLS certificates.
Microsoft Azure RSA TLS Issuing CA 03
```

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

```
Yes. A root certificate is a critical component in the system of digital
certificates used for establishing secure communications over networks.
DigiCert Global Root G2
```

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

```
Yes, it does. DigiCert Inc
```

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

```
Certum Trusted Root CA
```

Day 3 Questions

Cloud Security Questions

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

```
SIMILARITIES:
1-Both services help manage and route traffic to web applications.
2-Both services support SSL/TLS termination, allowing secure communication
between clients and the service.
3-Both support Web Application Firewall (WAF) capabilities to protect
against common web vulnerabilities.
DIFFERENCES:
1-Front door is global, Application Gateway is regional.
```

```
2-Application Gateway provides load balancing based on application layer (Layer 7) routing and supports URL-based routing, path-based routing, and multiple site hosting.Front door Offers global load balancing, dynamic site acceleration, and can route traffic based on URL, geolocation, and other criteria. It also provides automatic failover and can route traffic to multiple regions based on performance or availability.
```

2. What is SSL offloading? What are its benefits?

```
SSL offloading helps streamline and optimize the handling of secure communications, enhancing both server performance and security while potentially reducing costs and improving the user experience.
BENEFITS:
1- Offloading SSL/TLS processing from web servers reduces their computational load, allowing them to focus on handling application logic and serving content.
2-SSL offloading devices can provide centralized management of SSL/TLS certificates and policies, simplifying updates and ensuring consistent security practices.
3-Offloading SSL/TLS processing can reduce the need for high-performance web servers, potentially lowering overall infrastructure costs.
```

3. What OSI layer does a WAF work on?

```
LAYER 7 - APPLICATION LAYER
```

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

```
SQL Injection
It is a type of web vulnerability where an attacker can execute malicious SQL statements in a web application's database query.This happens when an application improperly filters or sanitizes user input,allowing an attacker to inject or manipulate SQL queries.
```

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?

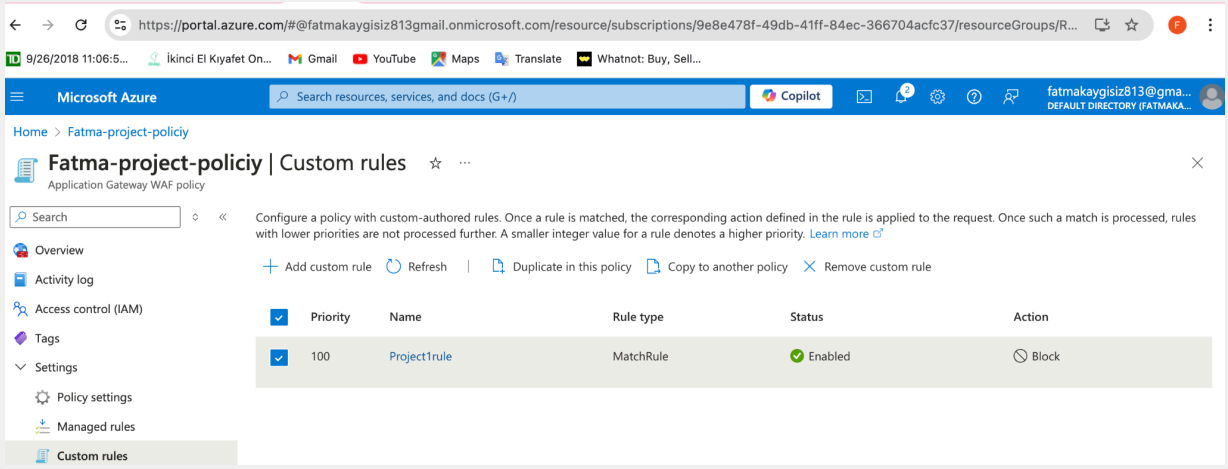
Ye, it could. Because without Front Door (or another WAF), the website is more vulnerable to SQL Injection attacks if there are weaknesses in how it handles user input and database queries. Implementing a WAF is a crucial step in defending against such attacks by providing an additional layer of security that can detect and block malicious traffic before it reaches the application.

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?

Yes it does with the exception of if the user attempting to access the site from Canada is using a VPN to gain access.

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

    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.*

- ***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.*