Cybersecurity

Project 1 Technical Brief

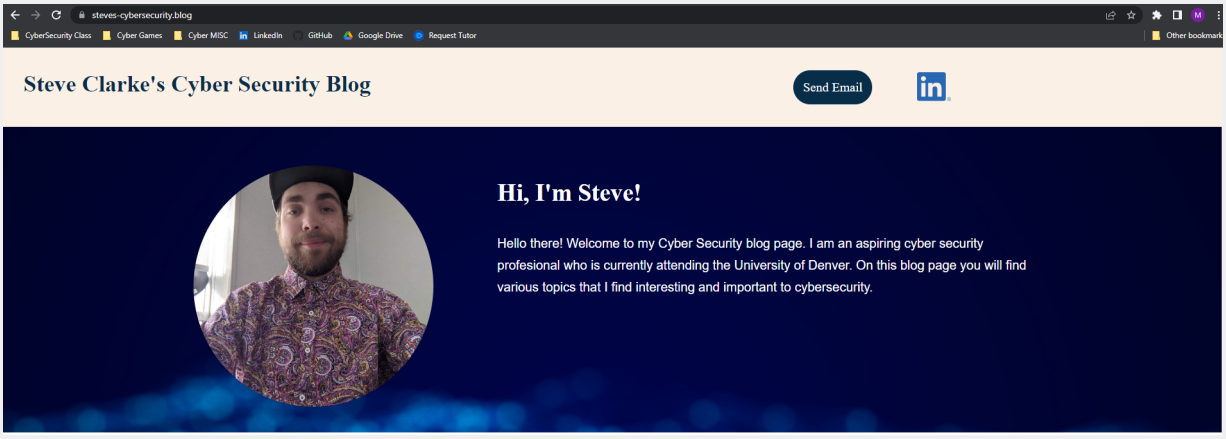
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
http://steves-cybersecurity.blog/
```

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



Blog Posts

Deep Insert ATM Skimmers

ATM, Card Skimming, Fraud

Numerous financial instituions around New York have been encountering a super thin skimming device that fits inside of an ATMs card slot. These skimming devices have been disguised to look as if it's part of the ATM cash machine. The skimmers that are being used are only .68 milimeters tall. To put that into perspective, a U.S dime is only 1.35 millimeters tall so this skimmer device is about half the size. Due to the skimming devices small size, there is plenty of room for a person to be able to insert their debit card normally without inhibiting the ATMs ability to take and return the customers card.
The skimmers are after the cardholders data that is stored on the magnetic strip on the back of the customers issued debit card. This information is still stored in plain text which is super insecure. On top of the cardholders personal information, the theives using the card skimmer are also able to get the customers 4 digit pin number. With this informatation, they are able to produce clone copies of the customers debit card. They will then use these 'cloned' debit cards to siphon money at other ATMs.

1-time Passcodes Are a Corporate Liability

Phishing, Web Fraud

Phishers have been extremely succesful using fradulent text messages to steal access credentials and 1-time passcodes from employees. These phishing attacks have been targetting some of the largest tech companies and customer support firms. One cybercriminal group that is conducting these attacks has been able to cause data breaches from the affected companies. These companies that have experienced the data breaches are still struggling to combat the threat of the scammers being able to interact with employees through mobile devices. The phishers typically create a fraudulent website domain with a similar name to the targetted company. Thry will then send the phishing text messages with a link to the fraudlent website to the companies employees. These text messages will usually tell the employee that they need to login to view a schedule change or something similar. These fraudulent phishing websites utilized a Telegram messaging bot to forward the employees credentials in real time. Since these credentials were being forwarded to the phisher in real time, they were able to steal the 1-time passcode and login as if they were the employee. During the course of two months, the telegram bot received close to 10,000 replies. That means 10,000 people from various companies have fallen victim to a phishing attack.

Day 1 Questions

General Questions

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

GoDaddy

2. What is your domain name?

```
http://steves-cybersecurity.blog/
```

Networking Questions

1. What is the IP address of your webpage?

```
20.118.40.5
```

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

```
Redmond, Washington - United States
```

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

```
steves-cybersecurity.blog     nameserver = ns05.domaincontrol.com.
steves-cybersecurity.blog     nameserver = ns06.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 and it works on the backend
```

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

```
CSS stylesheets
```

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?

```
An organization that owns and manages specific instances of the cloud services Microsoft offers.
```

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

```
It would be important because you can use it to grant permissions on who and who can not access the key vault to view secrets, keys and certificates which increases the security.
```

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

```
Keys are encryption keys that you use to encrypt your data, secrets are things like tokens and passwords and certificates deals with TLS/SSL certificates to use within azure
```

Cryptography Questions

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

```
They are free, well suited for intranet setups or testing environments and they encrypt incoming and outgoing data with the same ciphers as paid SSL certificates do.
```

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

```
They aren’t trusted by any browser or operating system,
```

3. What is a wildcard certificate?

```
It is a digital certificate that can be used for a domain AND all of 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 is no longer secure and has lots of vulnerabilities.
```

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 trusted certificate binded to it
```

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

```
9/13/22 through 3/14/2023
```

    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?

```
Yes, DigiCert Global Root CA
```

    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 G2
```

Day 3 Questions

Cloud Security Questions

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

```
The similarities are that they both operate on layer 7 of OSI as load balancers while the differences is that Azure Front Door is a non-regional service that can load balance between different scale units/clusters/stamp units across various regions while Azure Application Gateway is a regional service that allows you to load balance between your VMs/containers within the same scale unit.
```

2. A feature of the Web Application Gateway and Front Door is “SSL Offloading.” What is SSL offloading? What are its benefits?

```
It is the process of removing SSL-based encryption from incoming web traffic to relieve the server of having to process the decrypting or encrypting traffic sent via SSL. A benefit of this is it results in a smoother loading website that’s faster at processing 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
```

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?

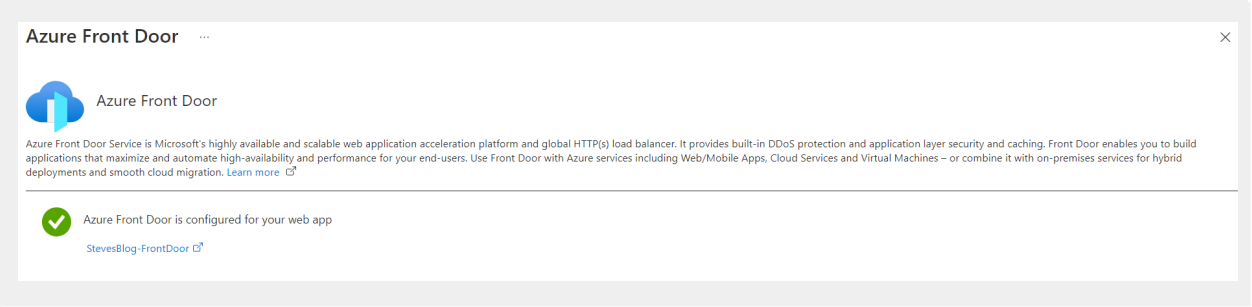
```
No because there are no user input fields that would communicate with a database to allow for a SQL injection to be successful.
```

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?

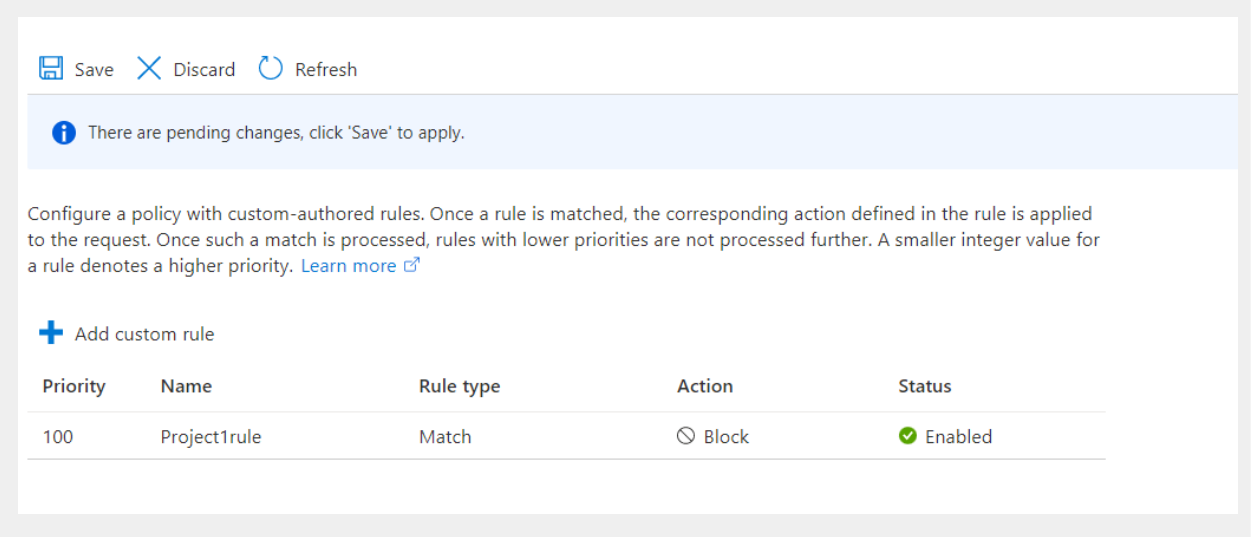
```
No because they could hypothetically use a VPN to change their IP address to a different region that isn't blocked
```

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

    a. Azure Front Door enabled



    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.*