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://tylercyberblog.azurewebsites.net/
```

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

```
[Paste screenshots here
```

TYLER CRAWFORD'S CYBER BLOG

Send Email

Hi, I'm Tyler!

Welcome to my cybersecurity blog. I am an independent security researcher based in Canada. I will be posting about a variety of cybersecurity and AI related topics such as ransomware incidents, data breaches, and other cyber crime news.

I will also be putting a spotlight on emerging AI technologies with a specific focus on their potential use in the field of cyber security. Please explore my blog posts below and get in touch if you have some thoughts to share.

Blog Posts

Ransomware: Should Organizations Pay or Not?

Ransomware, Cyber Crime

Since its early development in 1989, ransomware has quickly become one of the top cyber threats facing organizations today. If you follow any cybersecurity news sites, you will be well aware of the flood of ransomware attacks occurring worldwide everyday. Although many organizations would say they have a strong defensive cyber security strategy, we know that no one is truly 100% secure and that attackers are continuously improving their tactics, techniques and procedures. Many would say it's not a matter of "if" but "when" your organization will face a ransomware attack.

To pay or not to pay? The typical recommendation from industry professional and governments is to not pay, for the reasons highlighted in this quote from NextGov "Some cyber industry leaders say that paying ransoms should be banned because it emboldens cybercriminals and helps fund more illicit activities, and that, in some cases, paying a ransom does not necessarily guarantee that compromised data will be returned."

We can see this is sound advice with a solid reasoning, but there may be cases that do warrant payment. In the same report from NextGov we have noted the flip side is that "sometimes payments need to be made in order to recover vital systems, like those seen in hospitals and critical infrastructure." While there is merit to both sides of the argument, I think that it is ultimately up to the individual organization to weigh their losses against the price of the ransom and decide for themselves.

Sources:
1 - https://en.wikipedia.org/wiki/Ransomware
2 - https://www.nextgov.com/cybersecurity/2024/03/ransomware-payment-debate-resurfaces-amid-change-healthcare-incident/395026/

How Could Artificial Intelligence Affect Cybersecurity?

AI, ChatGPT, Cybersecurity

In 2023, artificial intelligence (AI) finally hit the mainstream with Microsoft among many others calling it "2023: The year of AI." ChatGPT put AI into the hands of millions of people, enabling the masses to use AI as a tool to improve their lives and help solve their problems. While AI has many of these types of upsides, it can also be used by hackers and cyber criminals to supercharge their illicit activities.

A recent report from DarkReading revealed this horrifying piece of news: "Threat actors have thus far used large language models (LLMs) to produce phishing emails, along with some basic malware, and to aid in the more ancillary aspects of their campaigns. Now, though, with only GPT-4 and an open source framework to package it, they can automate the exploitation of vulnerabilities as soon as they hit the presses." We know that threat actors are frequently developing new techniques and should not be surprised by this advancement. It is a great reminder that we need to be alert for new and innovative ways that hackers can exploit us.

I asked ChatGPT 4o for "cybersecurity tips for a normal person?" and was presented with some solid advice such as "Use Strong, Unique Passwords" and "enable Two-Factor Authentication (2FA)." This gives me a bit of hope to counter the mounting threat of AI enabled hackers. At least this new technology has good cyber hygiene!

Sources:
1 - https://en.wikipedia.org/wiki/Artificial_intelligence
2 - https://news.microsoft.com/year-of-ai/#:~:text=The%20pace%20of%20AI%20innovation,their%20careers%2C%20communit
3 - https://www.darkreading.com/threat-intelligence/gpt-4-can-exploit-most-vulns-just-by-reading-threat-advisories
4- OpenAI. (2023). ChatGPT (Mar 14 version) [GTP-4o]. https://chat.openai.com/chat

Blog Posts

Ransomware: Should Organizations Pay or Not?

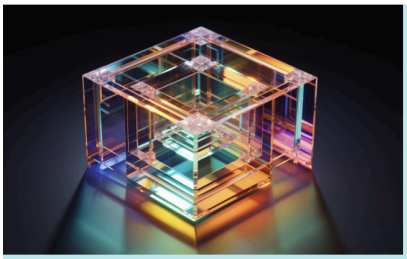
Ransomware, Cyber Crime

Since its early development in 1989, ransomware has quickly become one of the top cyber threats facing organizations today. If you follow any cybersecurity news sites, you will be well aware of the flood of ransomware attacks occurring worldwide everyday. Although many organizations would say they have a strong defensive cyber security strategy, we know that no one is truly 100% secure and that attackers are continuously improving their tactics, techniques and procedures. Many would say it's not a matter of "if" but "when" your organization will face a ransomware attack.

To pay or not to pay? The typical recommendation from industry professional and governments is to not pay, for the reasons highlighted in this quote from NextGov: "Some cyber industry leaders say that paying ransoms should be banned because it emboldens cybercriminals and helps fund more illicit activities, and that, in some cases, paying a ransom does not necessarily guarantee that compromised data will be returned."

We can see this is sound advice with a solid reasoning, but there may be cases that do warrant payment. In the same report from NextGov we have noted the flip side is that "sometimes payments need to be made in order to recover vital systems, like those seen in hospitals and critical infrastructure." While there is merit to both sides of the argument, I think that it is ultimately up to the individual organization to weigh their losses against the price of the ransom and decide for themselves.

Sources:
1 - https://en.wikipedia.org/wiki/Ransomware
2 - https://www.nextgov.com/cybersecurity/2024/03/ransomware-payment-debate-resurfaces-amid-change-healthcare-incident/395026/



How Could Artificial Intelligence Affect Cybersecurity?

AI, ChatGPT, Cybersecurity

In 2023, artificial intelligence (AI) finally hit the mainstream with Microsoft among many others calling it "2023: The year of AI." ChatGPT put AI into the hands of millions of people, enabling the masses to use AI as a tool to improve their lives and help solve their problems. While AI has many of these types of upsides, it can also be used by hackers and cyber criminals to supercharge their illicit activities.

A recent report from DarkReading revealed this horrifying piece of news: "Threat actors have thus far used large language models (LLMs) to produce phishing emails, along with some basic malware, and to aid in the more ancillary aspects of their campaigns. Now, though, with only GPT-4 and an open source framework to package it, they can automate the exploitation of vulnerabilities as soon as they hit the presses." We know that threat actors are frequently developing new techniques and should not be surprised by this advancement. It is a great reminder that we need to be alert for new and innovative ways that hackers can exploit us.

I asked ChatGPT 4o for "cybersecurity tips for a normal person?" and was presented with some solid advice such as "Use Strong, Unique Passwords" and "enable Two-Factor Authentication (2FA)." This gives me a bit of hope to counter the mounting threat of AI enabled hackers. At least this new technology has good cyber hygiene!

Sources:
1 - https://en.wikipedia.org/wiki/Artificial_intelligence
2 - https://news.microsoft.com/year-of-ai/#:~:text=The%20pace%20of%20AI%20innovation,their%20careers%2C%20communiti
3 - https://www.darkreading.com/threat-intelligence/gpt-4-can-exploit-most-vulns-just-by-reading-threat-advisories
4- OpenAI. (2023). ChatGPT (Mar 14 version) [GTP-4o]. https://chat.openai.com/chat

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?

```
https://tylercyberblog.azurewebsites.net/
```

Networking Questions

1. What is the IP address of your webpage?

```
20.48.202.167
```

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

```
Toronto, ON, Canada
```

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

```
No record found
```

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?

```
The runtime stack selected for the web application is the LEMP stack: Linux, nginx, MariaDB, and PHP.

Linux and nginx work on the front end dealing with HTTP requests.

MariaDB and PHP work on the backend managing data storage and processing data.
```

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

```
Inside the assets directory there is a folder (images) for all of the images on the website and a folder (css) for the style.css (Cascading Style Sheet) CSS is a style sheet language used to describe the presentation of a document written in HTML or XML, this contains the information about the visual appearance of our web application.
```

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

```
CSS and images both work on the front end of the web application, the user interacts with these when accessing the application and it determines the appearance they see in their web browser.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
In cloud computing, a cloud tenant is a user or organization that utilizes the services and resources offered by a cloud provider such as Azure, Google Cloud or AWS. These tenants rent or subscribe to virtual resources such as virtual machines, storage, and applications. Each tenant is operating in a secure, isolated environment within the cloud infrastructure. This ensures their data and applications are kept separate from other tenants on the same platform/physical server.
```

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

```
The key vault contains highly important and confidential items that can be maliciously altered or misused by potential attackers. The key vault should only be available to those who absolutely need them (IT / Security Team). We should apply the least privilege principle and also monitor the vault to setup notifications if there are any changes / anyone has accessed it.
```

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

```
In a key vault, keys are used for cryptographic operations like encryption, decryption, signing, and verification. There are two types of keys and they can be symmetric or asymmetric.

Secrets store sensitive information such as passwords and API keys securely, used by applications without exposing them in plain text format. These are not certificates or keys but they are secret information that is treated with the same level of security.

Certificates are digital certificates used for secure communication, authentication and encryption, such as SSL/TLS and code signing certificates. Keys, secrets, and certificates all play a crucial role in securing and managing sensitive data and resources for web applications.
```

Cryptography Questions

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

```
Self-signed certificates are a cost-effective and fast way to provide
encryption. They most are suitable for internal use, testing environments,
or personal projects. The can be used on projects where the trust of a
third-party CA is not necessary and if the project needs to be developed
quickly.
```

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

```
Self-signed certificates have several disadvantages compared to those issued
by trusted Certificate Authorities (CAs). They are not trusted by default in
web browsers, which can lead to warning messages that can deter users.
Self-signed certificates are more vulnerable to MITM attacks as they lack
third-party verification and they have a limited validity period, requiring
frequent renewals. They are not suitable for public-facing websites due to
limited browser support, some browsers may block the user from visiting what
it perceives as an untrusted website. One other issue that can occur with
self-signed certificates is that they do not have a revocation mechanism in
case of key compromise.
```

3. What is a wildcard certificate?

```
A wildcard certificate secures a domain and all its subdomains with one
single SSL certificate, using the wildcard character (*) to represent any
subdomain. This simplifies certificate management and reduces administrative
overhead while offering flexibility to create and easily manage 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 not supported for binding certificates to websites in Azure due
to its security vulnerabilities and deprecated status. It is susceptible to
attacks like POODLE, lacks support for modern cryptographic algorithms and
as a result, is not compatible with current cybersecurity standards and best
practices. Regulatory compliance frameworks also prohibit its use, favoring
more secure protocols like TLS instead.
```

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?

```
It is not returning an error, because the certificate is valid.
```

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

```
Wed, 13 Mar 2024 01:35:53 GMT to Sat, 08 Mar 2025 01:35:53 GMT
```

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

```
Yes, my site has an intermediate certificate. The server certificate is
issued by Microsoft Azure RSA TLS Issuing CA 07 - I have used online tools
and information from the certificate in the browser to determine that this
is an intermediate certificate. This certificate it is in between the server
and the root certificate.
```

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

```
My site does not have a root certificate directly itself but the
intermediate certificate links it to a root certificate from DigiCert
through a chain of trust.
```

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

```
Yes it does.
```

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

```
Entrust.net
```

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 both technologies for securing and protecting web applications. They operate on the Application Layer (Layer 7). They can act as load balancers, include Web Application Firewall (WAF) capabilities and they offer features such as URL path-based routing and SSL/TLS termination.

Their differences are mainly in their scope and complexity: Azure Web Application Gateway is regionally focused and more appropriate for single-region protection. It has advanced configuration options, but is also more complicated to configure. Azure Front Door is globally focused and is ideal for multi-region deployments while also being more simple to implement. The choice depends on your app's geographical distribution and desired implementation complexity.
```

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

```
SSL offloading, which can also be known as SSL termination, handles encryption and decryption before the web traffic reaches the server, improving server performance by reducing the amount of processing resources used  by the server.

This process enhances security by providing protection from SSL-based attacks. It also aids in scalability by offloading tasks from the web server and offers centralized certificate management for easier updates. SSL offloading allows for content inspection of decrypted traffic to view threats before they reach the server. It often includes load balancing as well as optimizing the performance and security of web applications.
```

3. What OSI layer does a WAF work on?

```
It operates at Layer 7 - the Application layer
```

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

```
942150 - SQL Injection Attack - This type of cyber attack involves a
malicious actor inserting harmful SQL code into an input field on a web
application. This exploit takes advantage of vulnerabilities in the
application's code, allowing the attacker to execute unauthorized SQL
commands. As a result, the attacker can access, modify, or delete data
within the application's database. These attacks are particularly dangerous
because they can lead to significant data breaches and compromise the
integrity and security of the affected web application.
```

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?

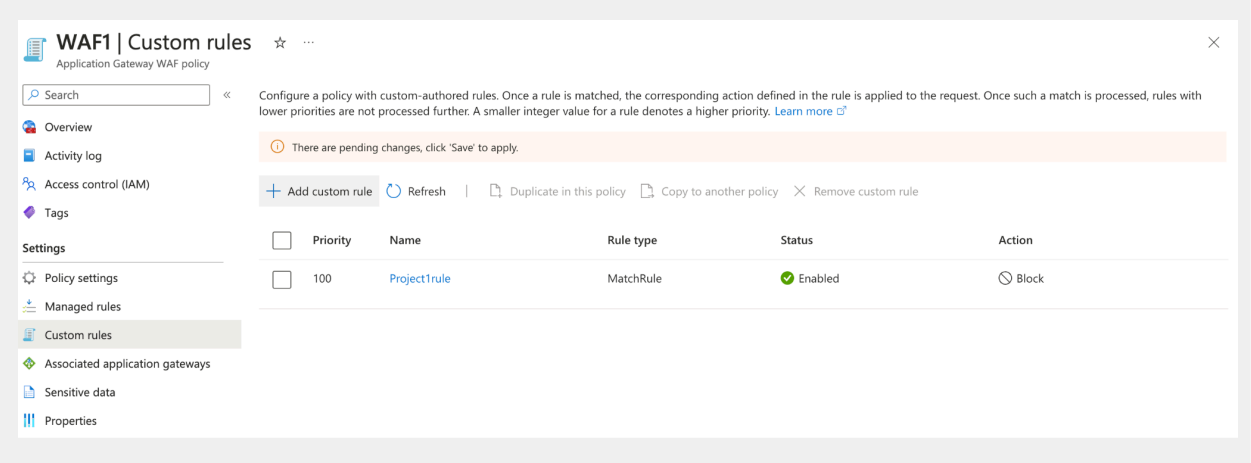
```
I do not have any input fields on my website right now and am not currently
susceptible to the SQL Injection attack. That being said, we are using
MariaDB, which is a SQL based database and it could be an issue in the
future if we add input fields to the website. With FrontDoor disabled, it
could be possible for an attacker to exploit the database through an SQL
injection attack.
```

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?

```
Someone from Canada would not be able to access your website. WAF uses the
IP address to determine the geo location of those requesting access to your
website. IP addresses identified as Canadian would be blocked from the site.
Those located in Canada would need to use a VPN to circumvent your WAF rule.
```

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.*
- *YES*

- ***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.*