Cybersecurity

Project 1 Technical Brief

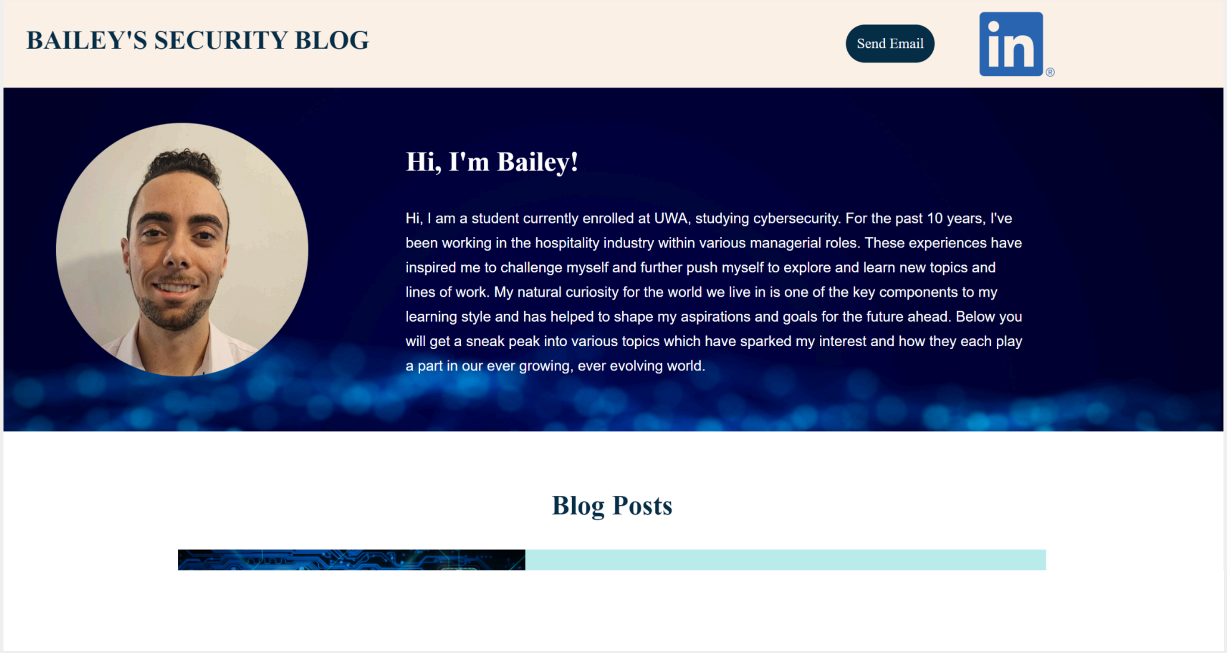
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://baileyssecurityblog.azurewebsites.net/
```

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

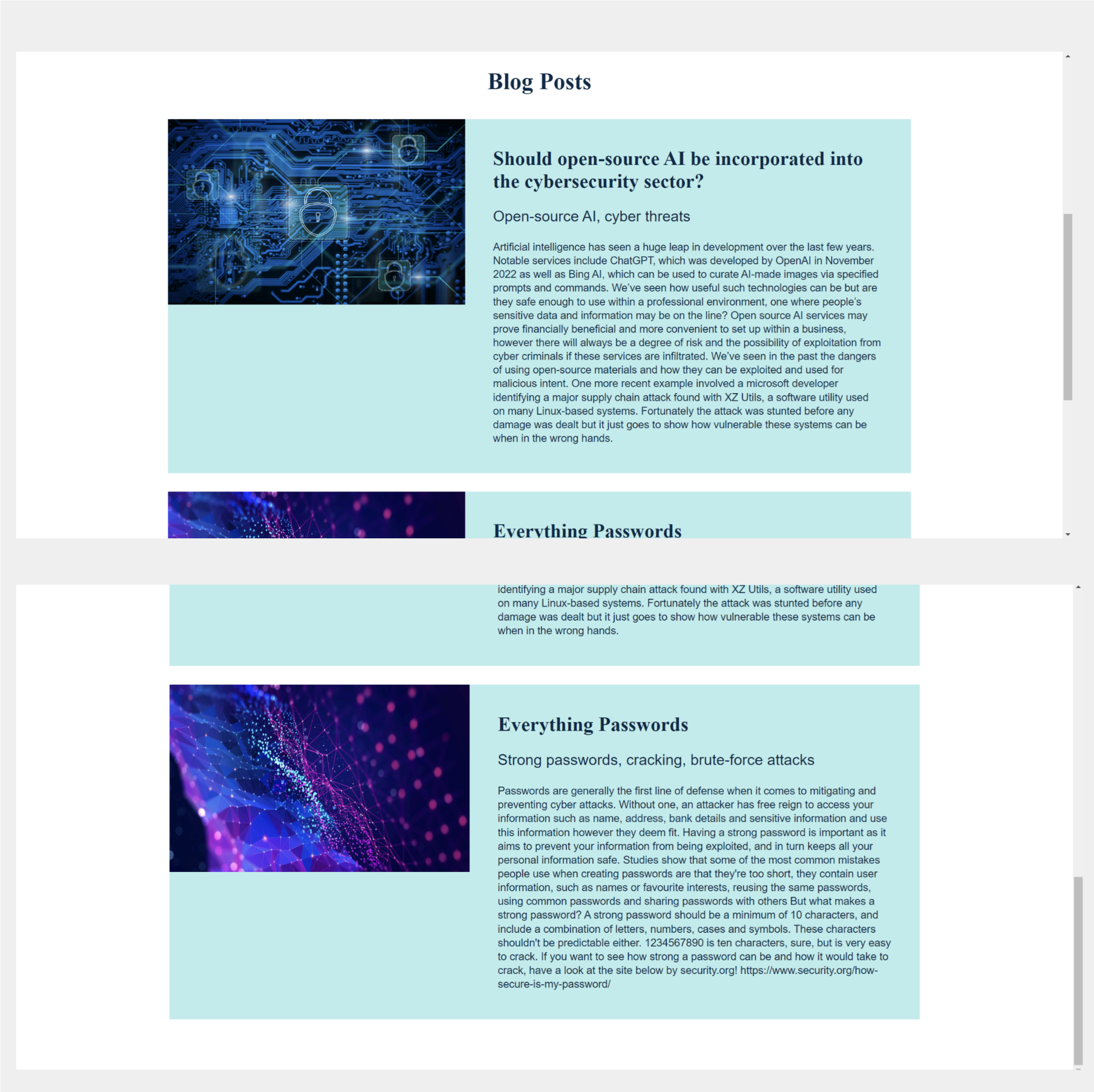


BAILEY'S SECURITY BLOG

Hi, I'm Bailey!

Hi, I am a student currently enrolled at UWA, studying cybersecurity. For the past 10 years, I've been working in the hospitality industry within various managerial roles. These experiences have inspired me to challenge myself and further push myself to explore and learn new topics and lines of work. My natural curiosity for the world we live in is one of the key components to my learning style and has helped to shape my aspirations and goals for the future ahead. Below you will get a sneak peak into various topics which have sparked my interest and how they each play a part in our ever growing, ever evolving world.

Blog Posts



Blog Posts

Should open-source AI be incorporated into the cybersecurity sector?

Open-source AI, cyber threats

Artificial intelligence has seen a huge leap in development over the last few years. Notable services include ChatGPT, which was developed by OpenAI in November 2022 as well as Bing AI, which can be used to curate AI-made images via specified prompts and commands. We've seen how useful such technologies can be but are they safe enough to use within a professional environment, one where people's sensitive data and information may be on the line? Open source AI services may prove financially beneficial and more convenient to set up within a business, however there will always be a degree of risk and the possibility of exploitation from cyber criminals if these services are infiltrated. We've seen in the past the dangers of using open-source materials and how they can be exploited and used for malicious intent. One more recent example involved a microsoft developer identifying a major supply chain attack found with XZ Utils, a software utility used on many Linux-based systems. Fortunately the attack was stunted before any damage was dealt but it just goes to show how vulnerable these systems can be when in the wrong hands.

Everything Passwords

identifying a major supply chain attack found with XZ Utils, a software utility used on many Linux-based systems. Fortunately the attack was stunted before any damage was dealt but it just goes to show how vulnerable these systems can be when in the wrong hands.

Everything Passwords

Strong passwords, cracking, brute-force attacks

Passwords are generally the first line of defense when it comes to mitigating and preventing cyber attacks. Without one, an attacker has free reign to access your information such as name, address, bank details and sensitive information and use this information however they deem fit. Having a strong password is important as it aims to prevent your information from being exploited, and in turn keeps all your personal information safe. Studies show that some of the most common mistakes people use when creating passwords are that they're too short, they contain user information, such as names or favourite interests, reusing the same passwords, using common passwords and sharing passwords with others But what makes a strong password? A strong password should be a minimum of 10 characters, and include a combination of letters, numbers, cases and symbols. These characters shouldn't be predictable either. 1234567890 is ten characters, sure, but is very easy to crack. If you want to see how strong a password can be and how it would take to crack, have a look at the site below by security.org! https://www.security.org/how-secure-is-my-password/

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?

```
BaileysSecurityBlog
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.22
```

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

```
Sydney, NSW, Australia
```

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

```
Ns record shows name server, in this case the name server is
ns1-06.azure-dns.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?

```
A runtime stack is a combination of software and technology that is used to
develop a web application. This works for the back end of the web
application.
```

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

```
The assets directory contains two directories; css and images. These are
responsible for the containing static images (images directory), font files
and additional controls for text and headers (css).
```

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

This works on the front-end.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

Is a user renting a subscription for cloud computing services from a provider.

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

Maintains and restricts sensitive data and information. Reduces the risk of unauthorized activity and also mitigates the risks of data breaches.

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

Keys are used for data encryption and decryption such as through OpenSSL. They are also used for signing and verifying data. Certificates are digital certificates stored on websites that validate the integrity and security of a site and also contain public keys as well as their corresponding information. Secrets store small pieces of data on a website such as usernames and passwords that are required to be kept confidential.

Cryptography Questions

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

They are free to create, therefore make them very convenient to use. They give the user full control and customization and there are no wait times for them to be deployed.

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

They aren’t validated by a third party and they are also vulnerable to man-in-the-middle attacks. Depending on the size of an organization, they can be hard to manage trust and distribute.

3. What is a wildcard certificate?

Is a certificate that can be used over multiple subdomains of a main domain.

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.

This is because there have been multiple security vulnerabilities found with version 3.0 and 3.0 has been deprecated. Here are also stronger certificates more readily available and accepted across applications and sites.

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 it’s not, because it is validated via Azure and their third parties.

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

13th March 2024 to 8th March 2025.

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

No, however they are issued by trusted root certificate authority.

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

Yes, it is a public key certificate issued from a trusted certificate authority. They can be used to issue additional certificates within a

```
system.
```

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.

```
AAA Certificate Services
```

Day 3 Questions

Cloud Security Questions

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

```
Both services can be used as load balancers and to manage network traffic.
Azure Web Application Gateway is a regional service, meaning it is only
accessible if the user is within the same region. Azure Front Door is a
global service, therefore can be used anywhere in the world, much like
accessing a VM.
```

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

```
The process of removing SSL based encryption from network traffic to a
website. As a result, this relieves the site from decrypting data and
instead decryption/encryption is done via a separate platform/site.
```

3. What OSI layer does a WAF work on?

```
It works on layer 7, which is the application layer.
```

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

HTTP Parameter Pollution: Involves an attacker hiding scripts in URLs to retrieve hidden information. The rule mitigates against this attack.

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?

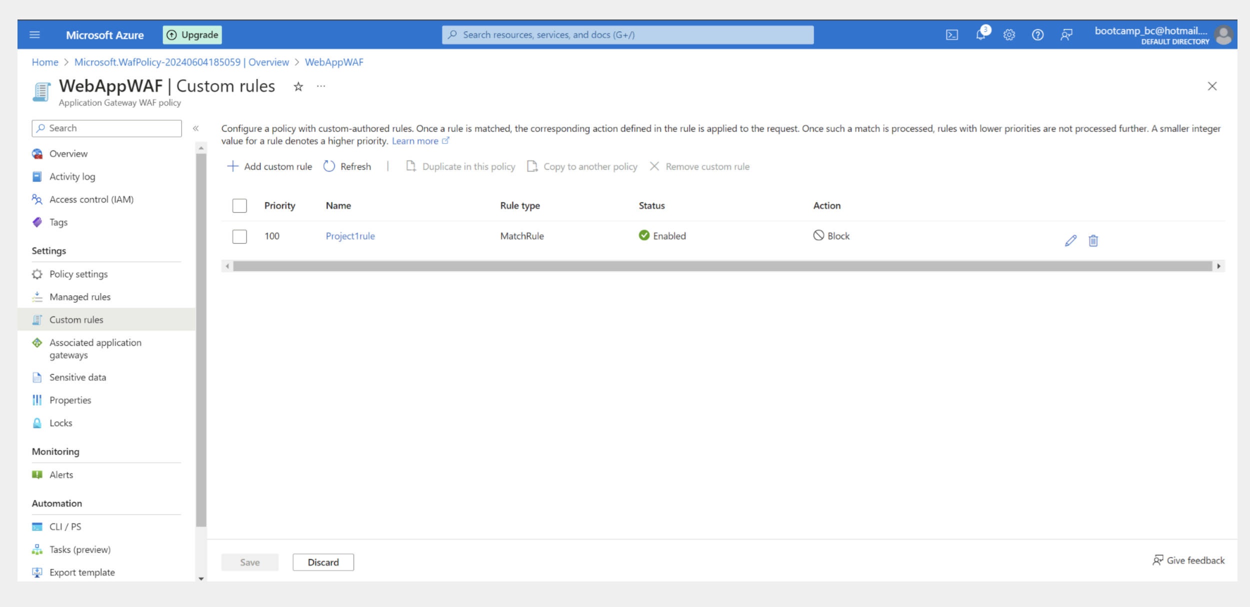
Yes it could, due to the fact that HPP can bypass WAF if executed correctly. Because HPP works by hiding scripts in URLs, it can go undetected and data could be retrieved for malicious intent. Fortunately personal credentials are not required to access the platform for web browsing and all other information is locked behind the main Azure website.

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, nobody in Canada would be able to access the site as their IP is based on their geo-location. Therefore the IP is registered in Canada and access to the website would be denied. The only exception would be if they used a VPN to mask their IP to make it look like they are accessing the site from outside of Canada.

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

    a. A WAF custom rule



WebAppWAF | Custom rules

Application Gateway WAF policy

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. Learn more

□	Priority	Name	Rule type	Status	Action
□	100	Project1rule	MatchRule	✓ Enabled	⦸ Block

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.*