



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://chasehancocksecurityresume.azurewebsites.net/>

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

[Paste screenshots here]

Chase Hancock's CYBER BLOG

[Send Email](#)



Hi, I'm Chase!

Hello, and welcome to my page.
My name is Chase Hancock. I am
21 years old. I am currently a
student at Arizona State
University pursuing my bachelor's
degree in Computer Science
(CyberSecurity). I would like to
use this page to express my
passion in cybersecurity with you.



Blog Posts



Cyber Security 101: How to avoid being hacked.

Hacking, Phising

With the evolution of technology almost everything is done online. This makes things a lot more convenient and efficient; however, this also makes the population at more of a risk of being victims to cyber attacks. Is the basic cyber security offered on site you use enough to make you feel comfortable and safe while browsing and using the web?

This is a very controversial and complex topic among the general population. It is true that sites will provide enough security depending on the importance of what their site. For instance, the security provided ones personal blog (such as this one) may not have as complex security as a bank or any other site that may maintain your personal identifiable information or PII. This is simply due to the fact that your whole life is essentially in their hands. However, even with the security provided it still is not enough protection due to one simple factor, humans.

Hackers use methods such as, brute force attacks, man in the middle attacks, and



Ransomware: Should compainies pay or not?

Ransomware

Ransomware is a form of malicious malware that will infiltrate a system or network restricting access to critical data until a ransom is paid. Ransomware is not a new trend to the cyber security industry, in fact, the first usage of ransomware dates back to 1989. However, since then ransomware has only been on the rise; within the last five years ransomware attacks have increased by 148% due to pandemic causing more remote work. With the increase in ransomware attacks and the current trend leading to rise in future years, the \$1.5 million question is; should compainies pay these ransomware fees or not.

Although the price of the ransom fees has nearly doubled since last year, the best thing a company can do is pay the ransom and take the necessary steps to prevent being held by another ransomware attack in the future. Of course the company will take an immediate financial hit, but in the long run it is less financially punishing.

Lets take the recent ransomware attack on MGM that occurred earlier in September. A group known as Scattered Spider, were able to successfully break into MGM's system force many slot machines and hotel keys to stop working.

Day 1 Questions

General Questions

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

Azure

2. What is your domain name?

```
https://chasehancocksecurityresume.azurewebsites.net/
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.15
```

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

```
Sydney, New South Wales, Australia
```

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

```
chase@BOOK-E093N9HUK1 MINGW64 ~
$ nslookup chasehancocksecurityresume.azurewebsites.net
Server:  cdns1.cox.net
Address: 68.105.28.11

Non-authoritative answer:
Name:    waws-prod-sy3-097-ef32.australiaeast.cloudapp.azure.com
Address: 20.211.64.15
Aliases: chasehancocksecurityresume.azurewebsites.net
          waws-prod-sy3-097.sip.azurewebsites.windows.net
```

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; Back End
```

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

The CSS file; the style of the web page images and links

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 is someone or a company who uses the services and resources of a cloud computing provider.

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

If everyone had access to the key vault, anyone could make changes to the site which can lead to several negatives including breaches.

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

Keys: Used for encrypting/decrypting data or signing verifying messages

Secrets: Used for storing sensitive information such as, API keys or passwords

Certificates: Digital files to ensure a sites connection is secure SSL/TSL

Cryptography Questions

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

- Cost efficient
- Easy to Create

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

- Lack of trust
- Vulnerable to attacks
- Warning messages

3. What is a wildcard certificate?

- A single certificate to secure a single domain and 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 a known vulnerability

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?

- Using Azure's domain, they connected a secure SSL certificate

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

October 31, 2023 - June 27, 2024

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

No

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

DigiCert Global Root G2

- 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

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 types of load balancers. The difference between the two is Azure Front Door is a non-regional service where 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 in which the SSL encryption/decryption tasks are “offloaded” from a web server to a dedicated hardware or software program
 - Benefits: Better web performance, enhances security, scalability
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.

Directory Traversal: an HTTP exploit where a user can access folder or files outside of the server's root directory

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, without the Front Door a user can successfully use a directory traversal. This is due to the fact that the best defense against these attacks are user input restrictions and the current website does not contain that.

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?

- The custom WAF rule created blocks all traffic originating from Canada. Theoretically it should not allow any residents from Canada to access the site; however if the user were to use a VPN they would be able to access the site.

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

- a. Azure Front Door enabled

Azure Front Door

Microsoft Azure

Azure Front Door

Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. Use Front Door with Azure services including App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines—or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more](#)

✓ Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove web app from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
project1-FrontDoor	Azure Front Door Premium	project1-fzcbf5a9c4cxc8dn....	RedTeam

b. A WAF custom rule

Save Discard Refresh

There are pending changes, click 'Save' to apply.

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](#)

Add custom rule

Priority	Name	Rule type	Action	Status
100	Project1rule	Match	Block	Enabled

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.