



Cybersecurity

Project 1 Technical Brief

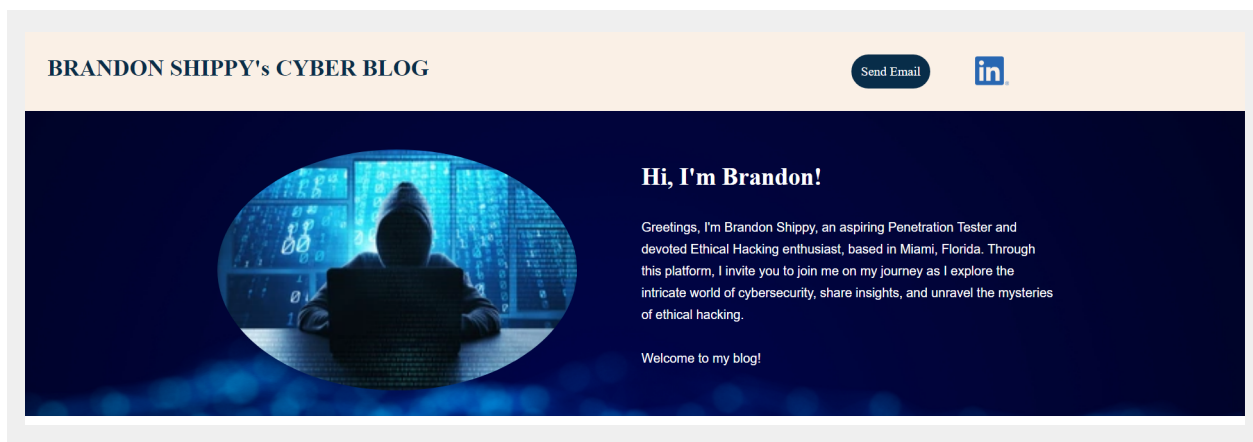
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

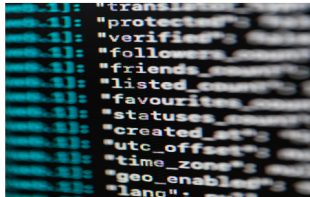
Enter the URL for the web application that you created:

`https://brandoncyber.live/`

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



Blog Posts



Ransomware: To Pay or Not to Pay?

Ransomware, Paying the Ransom, Cybercriminals, Business Disruption.

Ransomware attacks have become a pervasive threat in today's digital landscape, leaving organizations grappling with a daunting decision: should they pay the ransom or stand firm? The dilemma revolves around balancing financial losses against the ethical and strategic implications. Paying the ransom may offer a quick solution to regain access to critical data and systems. However, this choice emboldens cybercriminals and fuels their illicit activities. It also offers no guarantee that attackers will honor their end of the deal, potentially leading to repeated attacks. On the other hand, refusing to pay sends a strong message that organizations do not negotiate with cybercriminals. This stance can discourage future attacks and contribute to the collective fight against ransomware. Nonetheless, the cost of recovery, reputational damage, and potential business disruption must be carefully weighed. Ultimately, the decision to pay or not depends on the organization's risk appetite, backup capabilities, and the extent of the attack's impact. While it's tempting to seek a swift solution, organizations must consider the long-term consequences of their actions on the broader cybersecurity landscape.



Harnessing Open Source Security Software in Organizations

OSINT, Open Source, Software

In the dynamic realm of cybersecurity, the utilization of open source security software has sparked intriguing discussions. Embracing open source tools offers organizations the advantages of transparency, community collaboration, and rapid innovation. However, it also raises concerns about potential vulnerabilities and a lack of official support. Open source software allows experts worldwide to review the code for flaws and vulnerabilities, enhancing its overall security. The collaborative nature of open source projects facilitates quick bug fixes and continuous improvement. Moreover, open source solutions often come at a lower cost, making them an attractive option for resource-conscious organizations. However, the reliance on open source software demands a rigorous risk assessment. Organizations must diligently monitor the software's security updates, as delays in patching vulnerabilities can expose systems to exploitation. Additionally, the absence of dedicated support teams can lead to challenges in troubleshooting and rapid issue resolution. Striking a balance between leveraging open source security tools and maintaining a robust security posture requires a well-informed approach. Organizations should consider factors such as the software's track record, community engagement, and alignment with their security goals. By embracing open source selectively and with a keen focus on risk management, organizations can harness the power of collaborative innovation while safeguarding their digital assets.

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?

brandoncyber.live

Networking Questions

1. What is the IP address of your webpage?

20.90.134.25

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

London, England, United Kingdom of Great Britain and Northern Ireland

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

Server: 172.18.192.1
Address: 172.18.192.1#53

Non-authoritative answer:

brandoncyber.live nameserver = ns55.domaincontrol.com.

brandoncyber.live nameserver = ns56.domaincontrol.com.

Name: ns55.domaincontrol.com

Address: 97.74.107.28

Name: ns56.domaincontrol.com

Address: 173.201.75.28

Name: ns55.domaincontrol.com

Address: 2603:5:21b2::1c

Name: ns56.domaincontrol.com

Address: 2603:5:22b2::1c

Authoritative answers can be found from:

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 was PHP 8.2, it works on the backend

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

inside of assets were the different images and styles used on the website

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

This works with both the frontend and the backend.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant is an individual or organization that uses cloud computing resources and services from a cloud service provider while maintaining logical isolation from other users.

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

An access policy on a key vault is important to control and manage who has permissions to access and interact with sensitive information.

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

Within a key vault, keys are cryptographic objects for encryption, secrets store sensitive data like passwords, and certificates verify identities and enable secure communications.

Cryptography Questions

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

There's No cost, it's easy to generate, & self-validated

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

they have no validation from a third-party authority

3. What is a wildcard certificate?

A wildcard certificate is a type of SSL/TLS certificate that secures multiple subdomains of a single domain using a wildcard character in the domain name.

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 for binding certificates to websites because it has known security vulnerabilities, including the POODLE attack

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 isn't returning an error because the certificate is a trusted CA.

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

8/16/23, 8:00:00 PM EDT - 2/17/24, 6:59:59 PM EST

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

yes, GeoTrust Global TLS RSA 4096 SHA256 2022 CA1

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

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.

CN=D-TRUST Root Class 3 CA 2 EV 2009,O=D-Trust GmbH,C=DE

Day 3 Questions

Cloud Security Questions

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

The Web Application Gateway is more regional and is best suited to protect a web application in a single region in your cloud.
The Azure Front Door is more global and is better suited when you have a variety of regions in a cloud environment.

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 of decrypting SSL/TLS-encrypted traffic at a load balancer or gateway before forwarding it to backend servers, providing benefits such as improved performance, centralized certificate management, and enhanced security features.

3. What OSI layer does a WAF work on?

Application layer

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

SQL Injection (SQLi) is a web security vulnerability where attackers exploit poorly sanitized user inputs to inject malicious SQL queries into a web application's database, potentially leading to unauthorized access, data manipulation, or disclosure of sensitive information.

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?

Even if Front Door was on/off it wouldn't matter, as my website doesn't accept user input

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, that does not mean anyone in Canada can't access my website, as they can use a vpn to work around this.

7. Include screenshots below to demonstrate that your web app has the following:
 - a. Azure Front Door enabled



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 app service 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-FD-ggd3abbcgtg4brg4.z0...	Red-Team

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.

