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://www.jaydensecurityresume.com]
```

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

Blog Post 1 The Power of Unique Passwords: Your Shield Against Hacking

Defense against the dark arts of hacking

Hackers are persistent and resourceful, constantly seeking vulnerabilities to exploit. One of their most common techniques is trying to crack or guess passwords. If you reuse the same password across multiple accounts, you're essentially handing cybercriminals a master key that unlocks your entire digital presence. Once they gain access to one compromised account, they can potentially infiltrate others, resulting in identity theft, financial loss, or even reputational damage. By using unique passwords, you minimize the impact of a single compromised account. Each account becomes an isolated fortress, fortified by a password that is not reused elsewhere. This simple practice can significantly reduce the risk of unauthorized access and mitigate the potential damage caused by a security breach.

Blog Post 2 Beware of Phishing Emails: Safeguarding Yourself in the Digital World

The dangers of phishing emails

Phishing emails typically mimic legitimate communications from trustworthy sources, such as banks, social media platforms, or even colleagues. They often employ tactics like urgent requests, enticing offers, or alarming warnings to create a sense of urgency or curiosity, compelling recipients to respond without thinking twice. However, falling victim to a phishing scam can have severe consequences. First and foremost, phishing attacks can lead to identity theft. By tricking you into divulging your login credentials, financial information, or social security numbers, cybercriminals gain access to your personal data. With this information, they can impersonate you, commit fraudulent activities, or even sell your data on the dark web, putting your financial stability and reputation at risk. Furthermore, phishing emails are often gateways to malware infections. Clicking on suspicious links or downloading attachments from such emails can introduce harmful software onto your devices. This malware can compromise your system's security, steal sensitive information, or grant unauthorized access to hackers.

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?

[jaydensecurityresume.com]

Networking Questions

1. What is the IP address of your webpage?

[20.119.8.46]

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

[Canyon Lake,Texas,United States]

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

[]

```
jayden [ ~ ]$ nslookup jaydensecurityresume.com
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
Name:   jaydensecurityresume.com
Address: 20.119.8.46

jayden [ ~ ]$
```

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, often referred to as a technology stack, is a combination of programming languages, frameworks, libraries, and software components used to build and run web applications. It consists of two main components: the front end and the back end.The specific runtime stack you choose depends on your project's requirements, technology preferences, and the nature of

```
the web application you are building. Different stacks offer different
capabilities, performance characteristics, and development paradigms.]
```

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

```
[Assets contains a list of CSS: It may contain CSS (Cascading Style Sheets)
files that define the styles, layout, and visual appearance of the web pages
& images containing Background.jpg  Image1.jpg  Image2.jpg
LinkedIn-logo.png  RobertSmith-profile.jpg  readme]
```

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

```
 [The front-end stack, consisting of HTML, CSS, and JavaScript, handles the
user interface and client-side functionality. CSS files and image files play
a significant role in enhancing the visual experience and interactivity of
the front-end components.While the back end deals with server-side
operations, data processing, and business logic, the "assets" directory with
CSS and image files is primarily utilized on the front end to control the
presentation and aesthetics of the web application or website.]
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
[A cloud tenant is a dedicated virtual environment within the cloud
infrastructure, often referred to as a tenant space.This isolated space
allows the cloud tenant to deploy,manage and configure their application
services & data within the cloud environment.]
```

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

```
An access policy is crucial for a key vault because it helps enforce secure
```

```
and controlled access to the sensitive cryptographic keys, secrets, and
certificates stored within the key vault
```

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

```
[Within a key vault, keys, secrets, and certificates serve distinct purposes
and have different functionalities.]
```

Cryptography Questions

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

```
[Cost: Self-signed certificates are free to generate and use. Unlike
certificates issued by trusted third-party certificate authorities (CAs),
there are no associated costs or recurring fees.

2.  Internal Use: Self-signed certificates are commonly used for internal or
private network communications. They are suitable for scenarios where the
primary concern is encryption and authentication within a controlled
environment.

3.  Rapid Deployment: Self-signed certificates can be quickly generated and
deployed without relying on external entities or waiting for certificate
issuance. This can be beneficial in situations that require immediate
implementation or testing.

4.  Encryption: Self-signed certificates provide the same level of
encryption as certificates issued by trusted CAs. They allow for secure
communications over HTTPS or other encrypted protocols, protecting data in
transit.]
```

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

```
[. 1.  Lack of Trust: Self-signed certificates are not issued or verified by
a trusted third-party CA. As a result, web browsers and client systems do
not inherently trust self-signed certificates. When a user encounters a
website with a self-signed certificate, they may receive security warnings
or errors, which can create doubt and hinder user trust.
```

```
2.  Vulnerable to Man-in-the-Middle Attacks: Since self-signed certificates
lack the validation from a trusted CA, they are more susceptible to
man-in-the-middle (MITM) attacks. Attackers can intercept communications,
present their own self-signed certificate, and impersonate the legitimate
website. Users may unknowingly trust the attacker's certificate and share
sensitive information, assuming it is secure.

3.  Difficult for Users to Verify: Validating the authenticity of a
self-signed certificate can be challenging for end-users. Unlike CA-issued
certificates, which have a chain of trust and can be verified through
well-established certificate authorities, self-signed certificates require
manual verification steps that may not be familiar to all users.]
```

3. What is a wildcard certificate?

```
[ wildcard certificate is a type of SSL/TLS certificate that is designed to
secure multiple subdomains under a single domain with a common base name. It
is denoted by an asterisk (\*) as a wildcard character in the leftmost part
of 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 as an option when binding a certificate to a
website in Azure because SSL 3.0 is considered outdated and insecure. It has
known vulnerabilities and weaknesses that make it susceptible to various
attacks, including the well-known "POODLE" attack (Padding Oracle On
Downgraded Legacy Encryption).]
```

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?

```
[Yes ,it was at first stated that rbd was not allowing validation at that
time.]
```

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

```
[Expiration Date:2024-01-06T23:59:59+00:00 Issued Date:2023-07-06T00:00:00+00:00]
```

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

```
[Red-Team-EastUSwebspace-Linux-230706002444]
```

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

```
jaydensecurityresume.com-Jaydensecurityresume /issuer:GeoTrust Global TLS
RSA4096 SHA256 2022 CA1]
```

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

```
Browsers typically come pre-installed with a set of trusted root
certificates from well-known Certificate Authorities (CAs). These root
certificates are used to establish trust and validate the authenticity of
SSL/TLS certificates presented by websites.

The root certificate store in a browser is periodically updated by the
browser vendors to add new trusted root certificates and remove any
compromised or outdated certificates. The specific set of root certificates
included in a browser's root store can vary depending on the browser vendor,
version, and geographical region.

To determine if a particular root certificate is present in your browser's
root store, you can review the list of trusted root certificates maintained
by the browser or consult the documentation provided by the browser vendor.
Most browsers offer settings or options to view and manage the trusted root
certificates within their configuration menus.

It's worth noting that root certificate stores can differ between different
browsers and platforms (e.g., Windows, macOS, Linux, mobile devices).
Additionally, users can manually import or remove root certificates in some
cases, allowing customization of the trusted root certificate list.
```

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

```
[ The set of trusted root CAs can vary based on the browser software, its
version, and the specific configuration. Browsers typically include a
```

```
collection of well-known and globally recognized CAs in their root
certificate store to establish trust for SSL/TLS certificate validation.To
obtain an up-to-date list of trusted root CAs in your browser's root store,
you can refer to the documentation or support resources provided by your
specific browser vendor. The browser's settings or preferences menu may also
provide an option to view the trusted root certificates.]
```

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 Azure services
designed to improve the performance, scalability, and security of web
applications. While they have some similarities, there are also key
differences in their functionalities and use cases. Let's explore their
similarities and differences:]
```

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

```
[SSL offloading, also known as SSL termination or SSL acceleration, is a
feature provided by both Azure Web Application Gateway and Azure Front Door.
It involves the process of handling SSL/TLS encryption and decryption at the
gateway or load balancer level, rather than on the backend servers hosting
the web application.]
```

3. What OSI layer does a WAF work on?

```
[A Web Application Firewall (WAF) typically operates at the application
layer, which is Layer 7 of the OSI (Open Systems Interconnection) model. The
OSI model is a conceptual framework that defines how network protocols and
communication occur within a computer network.The application layer is the
highest layer of the OSI model and is responsible for managing the
interaction between applications and end-users. It deals with protocols and
services that support tasks such as data formatting, encryption,
```

```
authentication, and application-specific functions.A WAF is designed to
protect web applications from various types of attacks, including those
targeting application-layer vulnerabilities. It analyzes HTTP and HTTPS
traffic at the application layer, inspecting the contents of the requests
and responses exchanged between clients and web servers. By examining the
application-layer data, a WAF can detect and mitigate common web-based
attacks, such as SQL injection, cross-site scripting (XSS), and cross-site
request forgery (CSRF).]
```

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

```
[SQL Injection: SQL Injection is a type of attack where an attacker
maliciously injects SQL (Structured Query Language) code into a web
application's input fields or parameters that interact with a backend
database. The goal of an SQL Injection attack is to manipulate the
application's database queries and gain unauthorized access to data, modify
data, or execute unintended actions on the database.]
```

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?

```
[SQL Injection vulnerabilities typically arise when user-supplied input is
not properly validated, sanitized, or parameterized before being used in SQL
queries. If your website handles user input and interacts with a backend
database without implementing adequate input validation and parameterization
techniques, it could be susceptible to SQL Injection attacks.]
```

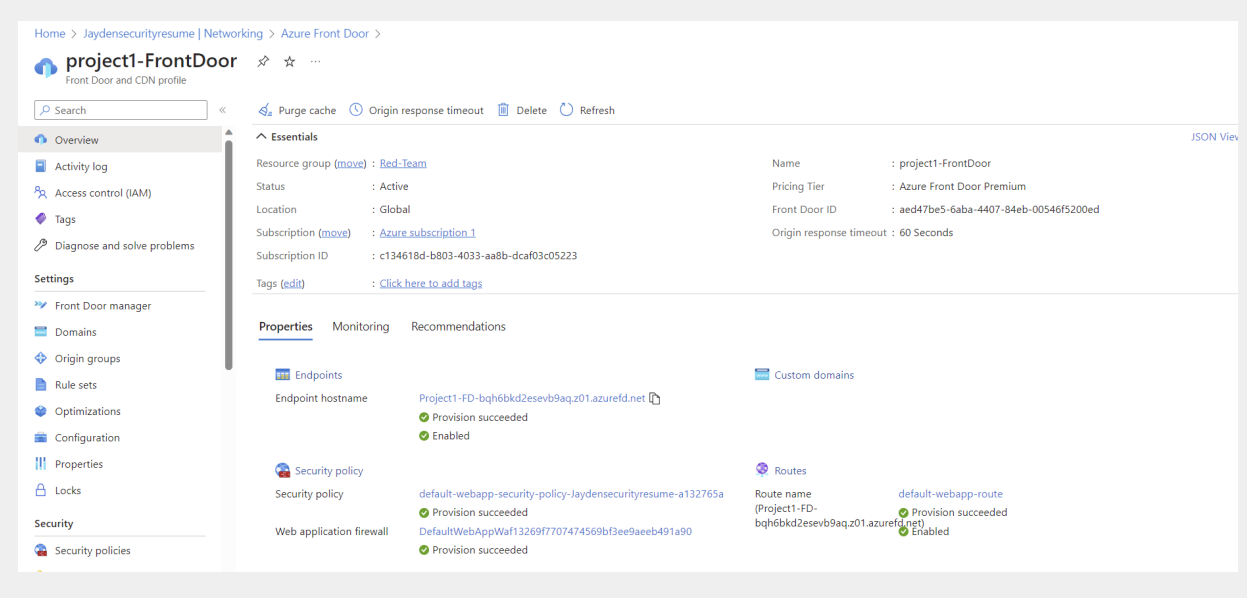
6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

```
[ Yes, if you create a custom WAF rule to block all traffic from Canada, it
would mean that anyone residing in Canada would not be able to access your
website. The reason is that the custom rule specifically targets traffic
originating from IP addresses associated with Canada and blocks it.WAF rules
are based on various criteria such as IP addresses, geographic location,
user agents, or specific patterns in request payloads. By creating a rule
that blocks traffic from a particular country, such as Canada, the WAF will
```

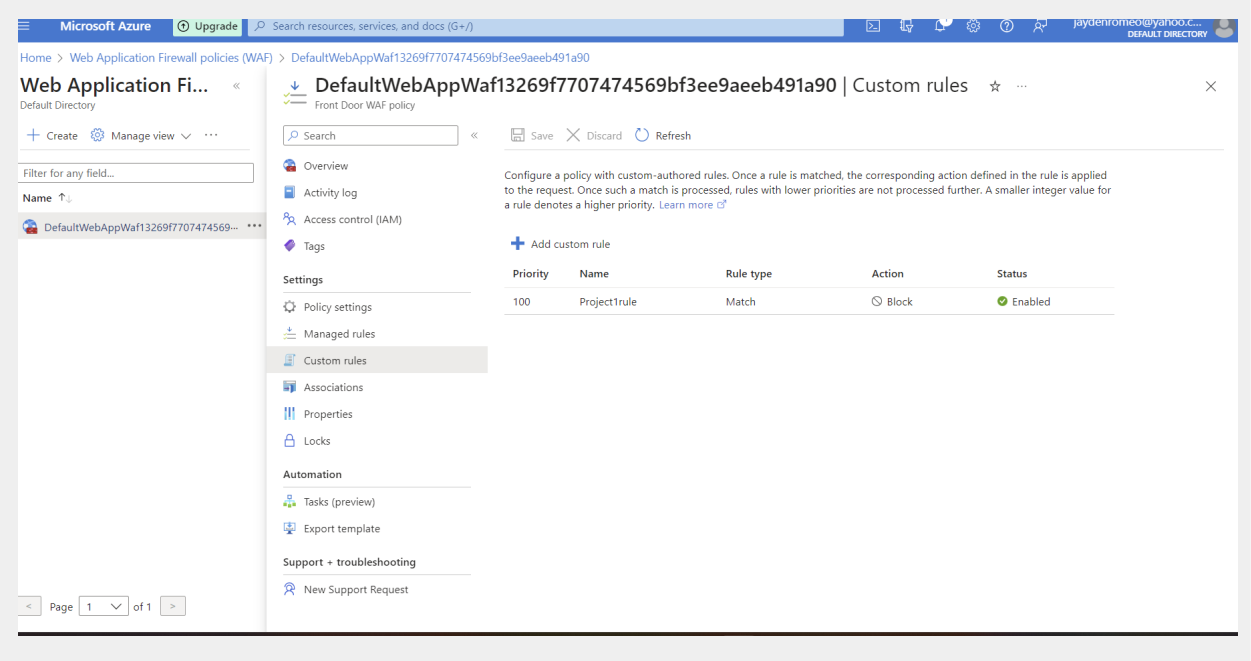
```
examine the source IP address of incoming requests and compare it against
the specified criteria. If the source IP address is identified as
originating from Canada, the WAF will block the request.]
```

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.* Yes