Cybersecurity

Project 1 Technical Brief

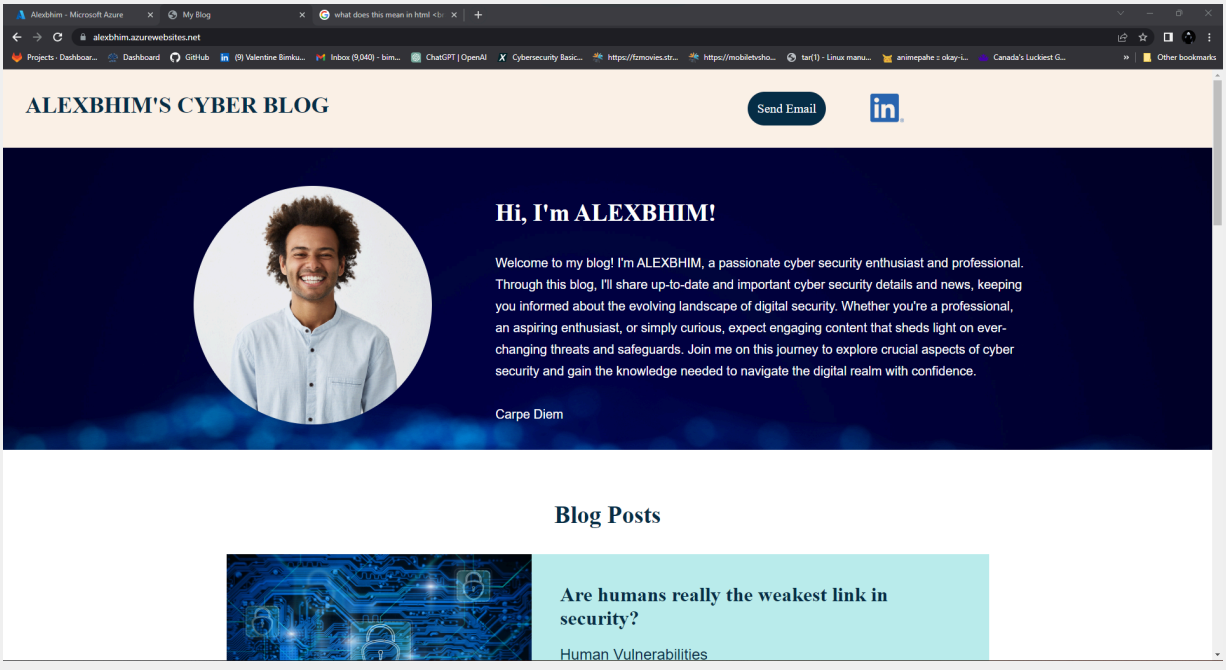
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://alexbhim.azurewebsites.net/
```

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

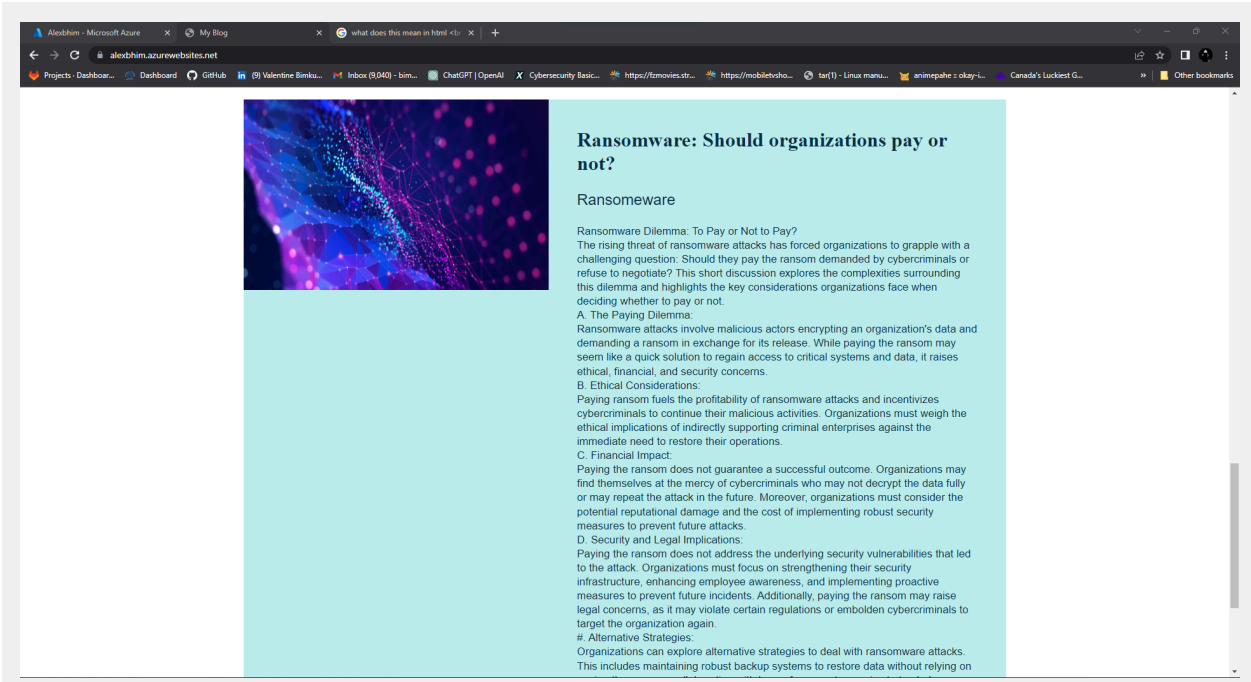


Are humans really the weakest link in security?

Human Vulnerabilities

Title: Humans:
The Vulnerable Link in Security
Introduction:
In an age dominated by technological advancements and sophisticated security systems, it's ironic that humans remain the weakest link in the realm of security. Despite the implementation of state-of-the-art software and hardware solutions, the fallibility of human behavior and decision-making processes continues to create vulnerabilities that malicious actors can exploit. This short blog post delves into why humans are the weakest link in security and highlights the importance of addressing this critical issue.
The Human Factor:
Human beings possess an array of unique qualities, but their susceptibility to manipulation, error, and oversight makes them a prime target for security breaches. While technology can assist in protecting sensitive data and systems, it is humans who ultimately wield the power to determine the efficacy of security measures. Whether it's falling victim to social engineering attacks or inadvertently clicking on malicious links, human actions often lead to successful breaches that compromise security.
Factors Influencing Human Weaknesses:
Several factors contribute to the vulnerabilities exhibited by humans in the realm of security:
1. Lack of Awareness:
Many individuals are unaware of the evolving tactics used by cybercriminals. They may overlook warning signs, such as phishing emails, or unknowingly disclose sensitive information, leaving organizations exposed to potential threats.
2. Negligence:
Even with knowledge of security best practices, human negligence can undermine efforts to maintain a secure environment. This includes practices like weak passwords, failure to update software, or careless sharing of confidential information.
3. Insider Threats:

efforts to maintain a secure environment. This includes practices like weak passwords, failure to update software, or careless sharing of confidential information.
3. Insider Threats:
While most employees are trustworthy, disgruntled or malicious insiders can pose a significant risk. These individuals have access to sensitive data and may deliberately compromise security measures or leak information.
Addressing the Issue:
To mitigate the risks associated with human vulnerabilities in security, organizations must take proactive steps:
1. Education and Training:
By fostering a culture of security awareness, organizations can empower individuals to make informed decisions and recognize potential threats. Regular training programs can educate employees about the latest cyber threats, emphasizing the importance of vigilance and adherence to security protocols.
2. Robust Policies and Procedures:
Establishing comprehensive security policies and procedures can provide guidelines for employees to follow. This includes implementing strong password requirements, enforcing regular software updates, and defining protocols for handling sensitive information.
3. Technology and Automation: Leveraging technology to automate security processes can reduce human error and minimize the impact of human vulnerabilities. Employing advanced intrusion detection systems, multi-factor authentication, and artificial intelligence-powered threat monitoring can enhance overall security posture.
Conclusion:
While technology continues to advance, humans remain the weakest link in security. Recognizing and addressing this vulnerability is crucial to safeguarding sensitive data and systems. Through education, robust policies, and leveraging technology, organizations can reduce the risks associated with human fallibility and strengthen their overall security posture. By actively involving individuals in the pursuit of a secure environment, we can collectively bolster our defenses against ever-evolving cyber threats.



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?

```
alexbhim.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.19
```

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

```
Canada ontario Toronto
```

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

```
Server:           8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
alexbhim.azurewebsites.net    canonical name =
waws-prod-sy3-103.sip.azurewebsites.windows.net.
waws-prod-sy3-103.sip.azurewebsites.windows.net canonical name =
waws-prod-sy3-103-e6e5.australiaeast.cloudapp.azure.com.

Authoritative answers can be found from:
australiaeast.cloudapp.azure.com
      origin = ns1-06.azure-dns.com
      mail addr = msnhst.microsoft.com
      serial = 10001
      refresh = 900
      retry = 300
      expire = 604800
      minimum = 60
```

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 8.2 it works on the back end
```

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

```
The directory contains two files which include css and images ,these two
files determines how the web pages is displayed to the user or viewer
```

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

```
This works with the frontend
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is a logical unit of isolation within a cloud environment
that represents a specific user or organization's dedicated space,
resources, and services within a shared infrastructure.
```

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

By utilizing access policies on a key vault, you can enforce security, adhere to compliance requirements, implement least privilege, and maintain control over access to sensitive keys and secrets stored within the vault.

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

keys are used for cryptographic operations within the key vault, secrets are sensitive information that needs to be protected, and certificates are used for secure communication and authentication purposes. Key vaults provide a secure environment for generating, storing, and managing keys, secrets, and certificates, ensuring the confidentiality, integrity, and availability of these critical resources.

Cryptography Questions

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

```
1. **Quick and Easy Setup**: Self-signed certificates can be generated
quickly and easily without relying on external certificate authorities,
```

```
making them convenient for internal testing and development environments.

2. **Suitable for Offline or Isolated Environments**: Self-signed
certificates can be used in offline or isolated environments where obtaining
certificates from trusted authorities is not feasible, allowing for secure
connections within those environments. However, they lack the trust and
validation provided by certificates from trusted authorities.
```

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

```
Here are two disadvantages of using self-signed certificates:

1. **Lack of Trust**: Self-signed certificates are not issued by trusted
certificate authorities (CAs), which means they are not inherently trusted
by web browsers or external systems. This can lead to warnings or errors
being displayed to users, as they cannot validate the authenticity of the
certificate. It can undermine the trustworthiness of your application or
website in the eyes of users.

2. **Limited Validity**: Self-signed certificates have a limited validity
period, typically shorter than certificates issued by trusted CAs. This
means that they need to be regenerated and updated more frequently. Renewing
certificates and distributing them across multiple systems can be a manual
and time-consuming process, especially in larger or distributed
environments.
```

3. What is a wildcard certificate?

```
A wildcard certificate is an SSL/TLS certificate that secures a domain and
all its subdomains with a single certificate. It uses a wildcard character
(*) to represent any subdomain. This simplifies management and can save
costs. However, if the private key is compromised, it can be used to
impersonate any subdomain. Consider your specific needs and security
requirements when deciding to use a wildcard certificate.
```

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 when binding a certificate to a website in Azure
```

```
because it has significant security vulnerabilities, including the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack. To ensure stronger security and protect against known exploits, Azure only supports the more secure TLS versions 1.0, 1.1, and 1.2 for website certificate binding.
```

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 ,because i am using a free domain provided by azure
```

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

```
[Enter answer here]
```

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

```
[Enter answer here]
```

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

```
[Enter answer here]
```

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

```
[Enter answer here]
```

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

```
[Enter answer here]
```

Day 3 Questions

Cloud Security Questions

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

```
similarities and differences between Azure Web Application Gateway and Azure
Front Door:

Similarities:
1. Load Balancing: Both Web Application Gateway and Front Door help
distribute incoming traffic across multiple backend resources, like web
servers or application instances.

2. SSL/TLS Termination: Both services can handle the encryption and
decryption of traffic, reducing the workload on backend servers.

3. High Availability: Both services are designed to be reliable and handle
failures by automatically routing traffic to healthy resources.

Differences:
1. Layer of Operation: Web Application Gateway focuses on routing traffic at
the application level, while Front Door operates at a broader level,
including network-level routing.

2. Backend Resource Support: Web Application Gateway primarily supports web
applications hosted in Azure, while Front Door supports a wider range of
backend resources, including Azure services, storage accounts, and external
resources.

3. Global Load Balancing: Front Door offers built-in global load balancing,
routing users to the nearest available backend resource based on their
geographic location. Web Application Gateway doesn't have this capability.
```

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

```
[SSL offloading, found in Azure Web Application Gateway and Azure Front
Door, handles encryption and decryption, improving performance and
simplifying certificate management.

One benefit of SSL offloading is improved performance by reducing the
workload on backend servers, resulting in faster response times for users.
```

3. What OSI layer does a WAF work on?

```
A Web Application Firewall (WAF) typically operates at the application layer
(Layer 7) of the OSI model.
```

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

```
SQL injection is a type of cybersecurity attack where malicious actors
exploit vulnerabilities in a web application's database query system. By
inserting malicious SQL code into user input fields, they can manipulate the
application's database and potentially gain unauthorized access, extract
sensitive information, modify or delete data, or execute other malicious
actions.
```

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?

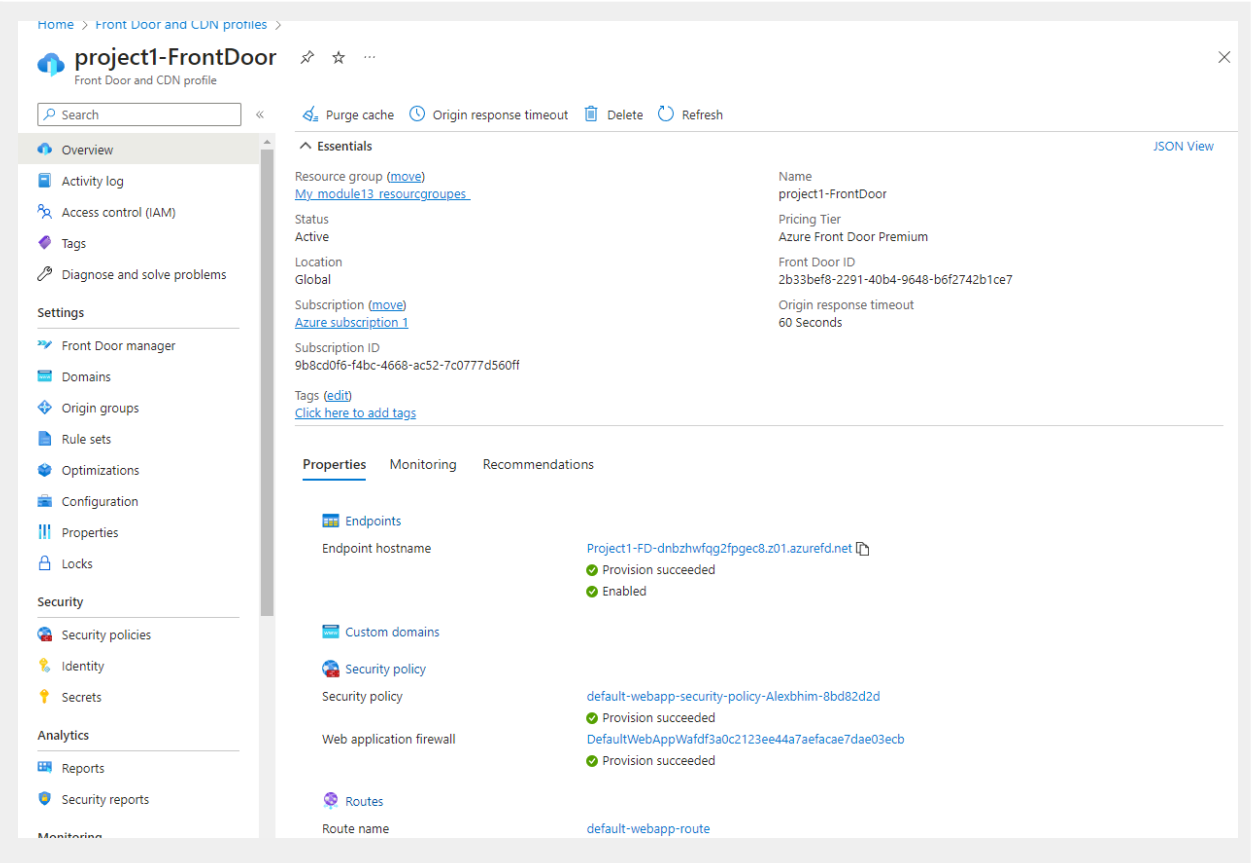
```
My web app can not be impacted by sql injections because it has no user
input fields
```

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?

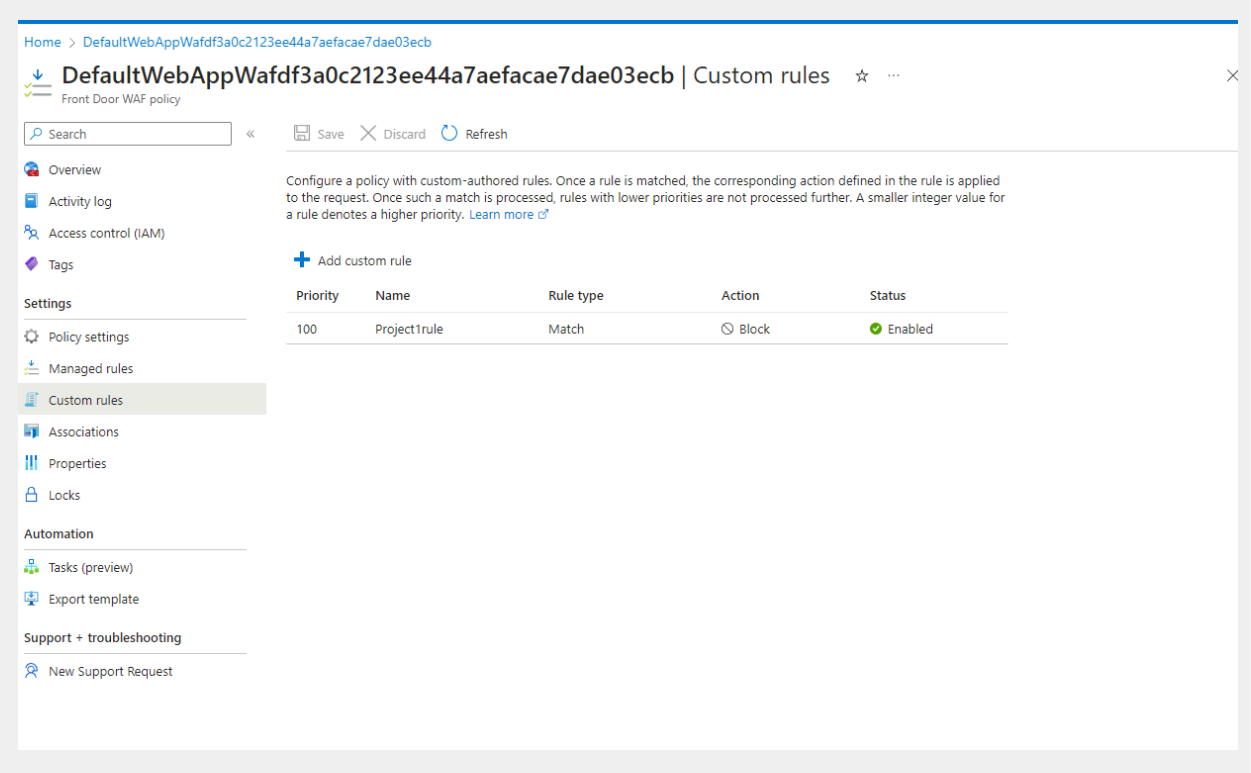
```
If you create a custom Web Application Firewall (WAF) rule to block all
traffic from Canada, anyone residing in Canada would not be able to access
your website. The WAF examines IP addresses, and if a user's IP is
identified as Canadian, the rule blocks their access. However, IP-based
blocking is not foolproof, and there can be inaccuracies in geolocation
databases. Additionally, users can bypass restrictions using proxies or
VPNs. Blocking Canadian traffic may unintentionally block legitimate users
and have business implications. Careful evaluation and additional safeguards
are recommended.
```

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