Built, Secured and Protected Web Application

Summary:


```
I employed Azure Websites in collaboration with Git Bash and Terminal to
create an Azure web app, deploying it with a container on the web app.
Additionally, I designed a customized web application to meet specific
project needs. Notably, I established a secure environment by creating a Key
Vault and generating self-signed certificates for encryption. I effectively
analyzed both self-signed and trusted certificates. Moreover, I implemented
a Front Door instance, optimized WAF rule sets, configured custom WAF rules,
and addressed Security Center recommendations to ensure a robust and secure
application environment. My accomplishments demonstrate my proficiency in
Azure, web app deployment, security analysis, and proactive maintenance.
```


URL for the web application created (no longer in use):

```
williamcruickshanksecurityresume.azurewebsites.net
```

IP address of webpage (no longer in use):

```
20.119.16.24
```

IP address location:

```
Washington, Virginia, United States
```

DNS lookup on website:

```
Server:  dns.cp.net.rogers.com
Address:  2607:f798:18:10:0:640:7125:5204

Non-authoritative answer:
Name:    waws-prod-blu-379-f4e5.eastus.cloudapp.azure.com
Address:  20.119.16.24
Aliases:  williamcruickshanksecurityresume.azurewebsites.net
          waws-prod-blu-379.sip.azurewebsites.windows.net
```

The runtime stack selected:

```
PHP 8.2. This runtime stack was used on the back end of the server.
```

Validity of web application certificate:

```
Issued On: Thursday, March 9, 2023 at 10:05:55 PM
Expires On: Sunday, March 3, 2024 at 10:05:55 PM
```

Intermediate certificate of web application:

```
Microsoft Azure TLS Issuing CA 02
```

Root certificate of web application:

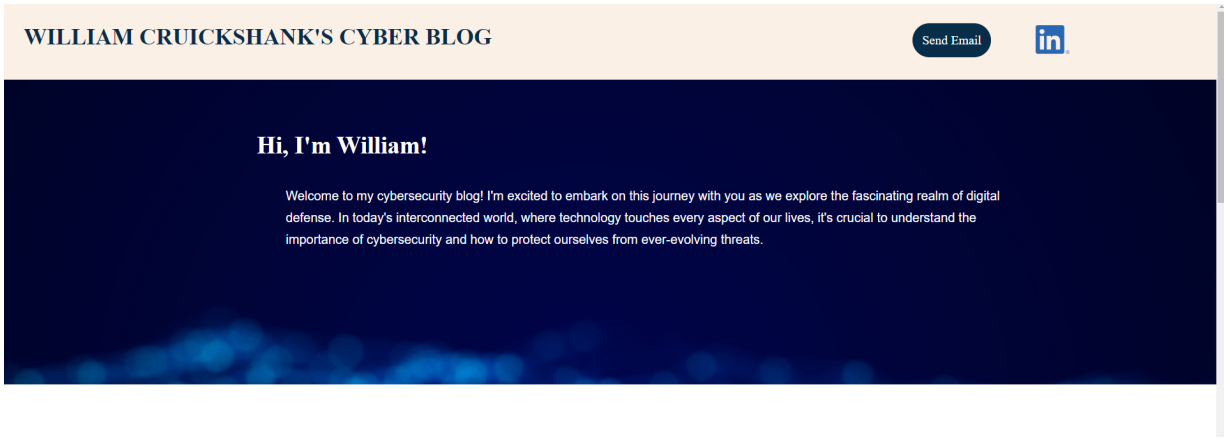
```
DigiCert Global Root G2
```

Example of WAF rule on web application:

```
Rule: Bot100100 - Malicious bots detected by threat intelligence
This rule is blocking any traffic that threat intelligence has detected to
make sure no Malicious bots are compromising the integrity of the system.
```

Screenshots:

Screenshots of website created:



Protecting Your Digital Identity: Essential Tips for Online Privacy

#Ransomware #CybersecurityThreats #Malware #DataProtection #CyberDefense #SecurityMeasures #BackupStrategies #EmployeeEducation #NetworkSecurity #IncidentResponse

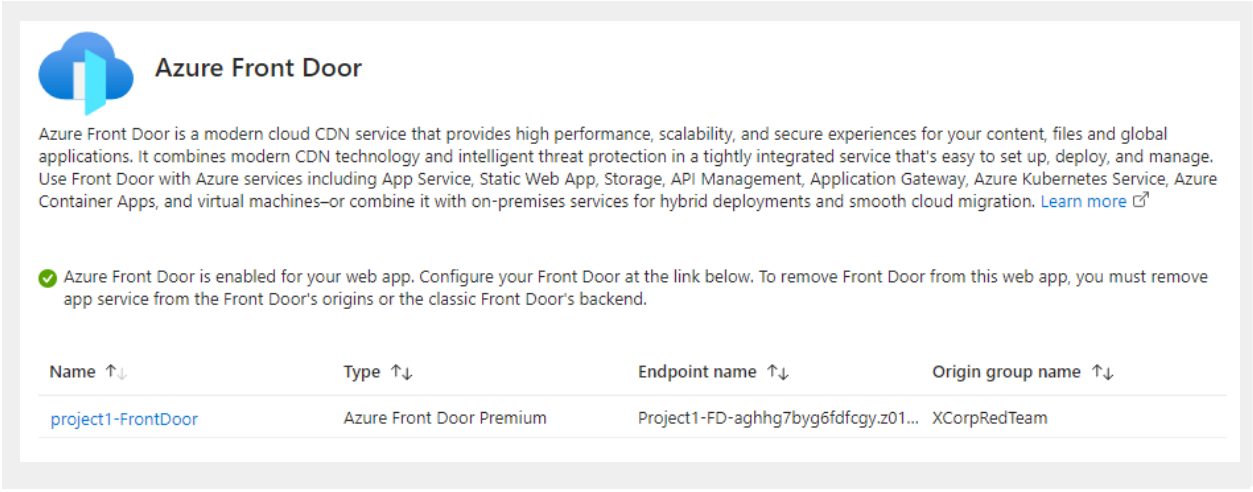
In today's digital age, safeguarding your personal information and preserving your online privacy has become more critical than ever. Here are some essential tips to help you protect your digital identity: Strong Passwords: Use unique and complex passwords for each of your online accounts. Avoid using common words or predictable patterns. Consider using a password manager to securely store and generate passwords. Two-Factor Authentication (2FA): Enable 2FA whenever possible. This adds an extra layer of security by requiring a second verification step, such as a code sent to your mobile device, in addition to your password. Keep Software Updated: Regularly update your operating system, web browsers, and other software to ensure you have the latest security patches. This helps protect against known vulnerabilities. Secure Wi-Fi Connections: When connecting to public Wi-Fi networks, be cautious. Avoid accessing sensitive information unless you're using a secure connection, such as a virtual private network (VPN). Be Wary of Phishing Attempts: Be cautious of suspicious emails, messages, or links that may try to trick you into revealing personal information. Verify the source before providing any sensitive data. Limit Personal Information Sharing: Be mindful of the information you share online. Minimize the details you provide on social media platforms, and adjust privacy settings to control who can access your information. Regularly Review Privacy Settings: Take the time to review and customize privacy settings on social media platforms, apps, and online services. Opt for stricter privacy controls to limit access to your personal data. Use Encryption: Whenever possible, choose encrypted communication channels. Look for websites that have HTTPS in their URL and consider using encrypted messaging apps to protect your conversations. Be Cautious of Third-Party Apps: Be selective when granting permissions to third-party applications. Review the data they collect and ensure they have reputable privacy practices. Stay Informed: Stay updated on the latest cybersecurity threats and best practices. Follow trusted sources, participate in cybersecurity awareness campaigns, and educate yourself to stay one step ahead of potential risks. Remember, protecting your digital identity is an ongoing effort. By implementing these tips and staying vigilant, you can significantly reduce the risk of falling victim to online privacy breaches.

Securing Your Home Network: Steps to Protect Your Connected Devices

#DigitalPrivacy #OnlineSafety #DigitalFootprint #SocialMediaPrivacy #MobileAppSecurity #TwoFactorAuthentication #PasswordSecurity #DataProtection #OnlinePrivacyTips #EmailSecurity

As our homes become more interconnected with smart devices, securing our home networks has become essential. Here are some steps you can take to protect your connected devices: Change Default Passwords: When setting up a new device, always change the default username and password. Default credentials are often known to hackers, making it easier for them to gain unauthorized access. Update Firmware: Regularly update the firmware or software of your devices. Manufacturers release updates to patch security vulnerabilities and improve device performance. Enable Network Encryption: Secure your Wi-Fi network with strong encryption, such as WPA2 or WPA3. Use a strong, unique password for your Wi-Fi network to prevent unauthorized access. Guest Network: Set up a separate guest network for visitors. This keeps your primary network and connected devices isolated from potential security risks. Firewall Protection: Enable the built-in firewall on your router to block unauthorized incoming connections. Additionally, consider using a network security solution that provides advanced firewall features. Disable Remote Management: Unless necessary, disable remote management features on your router. This prevents attackers from accessing and controlling your network remotely. Device Segmentation: Segment your devices into different network zones. For example, separate your smart home devices from your computers and personal devices. This adds an extra layer of protection. Strong Passwords for IoT Devices

Azure Front Door enabled:



WAF custom rule: