Cybersecurity

Project 1 Technical Brief

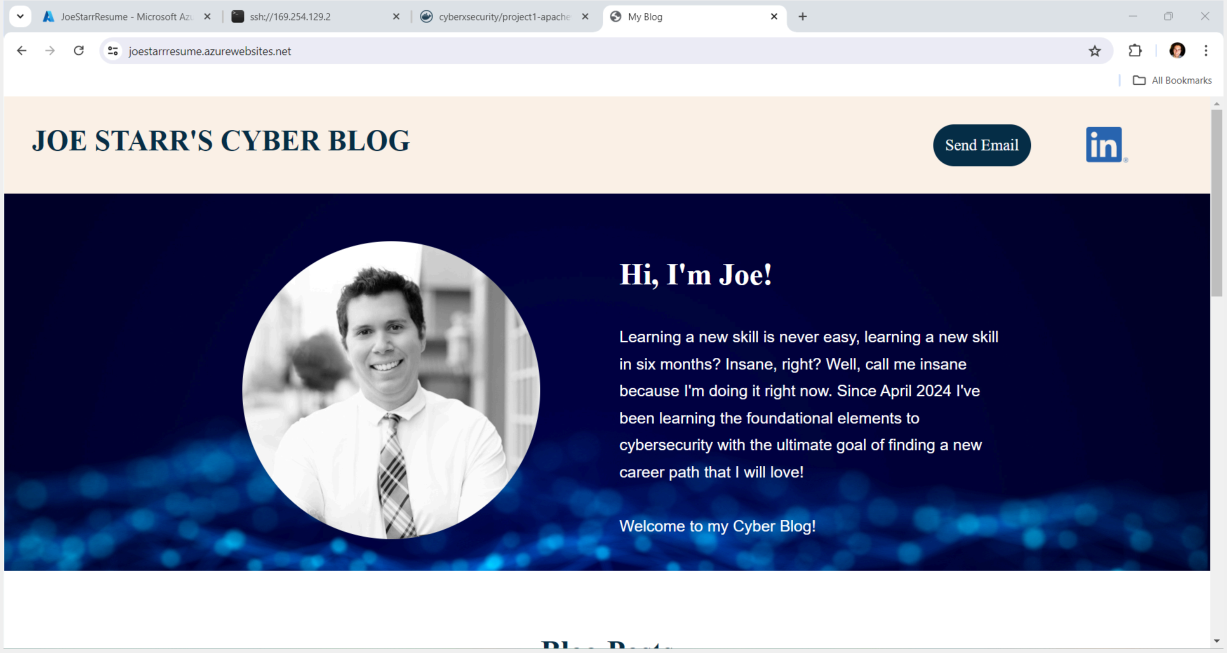
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://joestarrresume.azurewebsites.net/
```

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


JoeStarrResume - Microsoft Az
ssh://169.254.129.2
cyberxsecurity/project1-apache
My Blog
joestarrresume.azurewebsites.net
All Bookmarks
Send Email
in

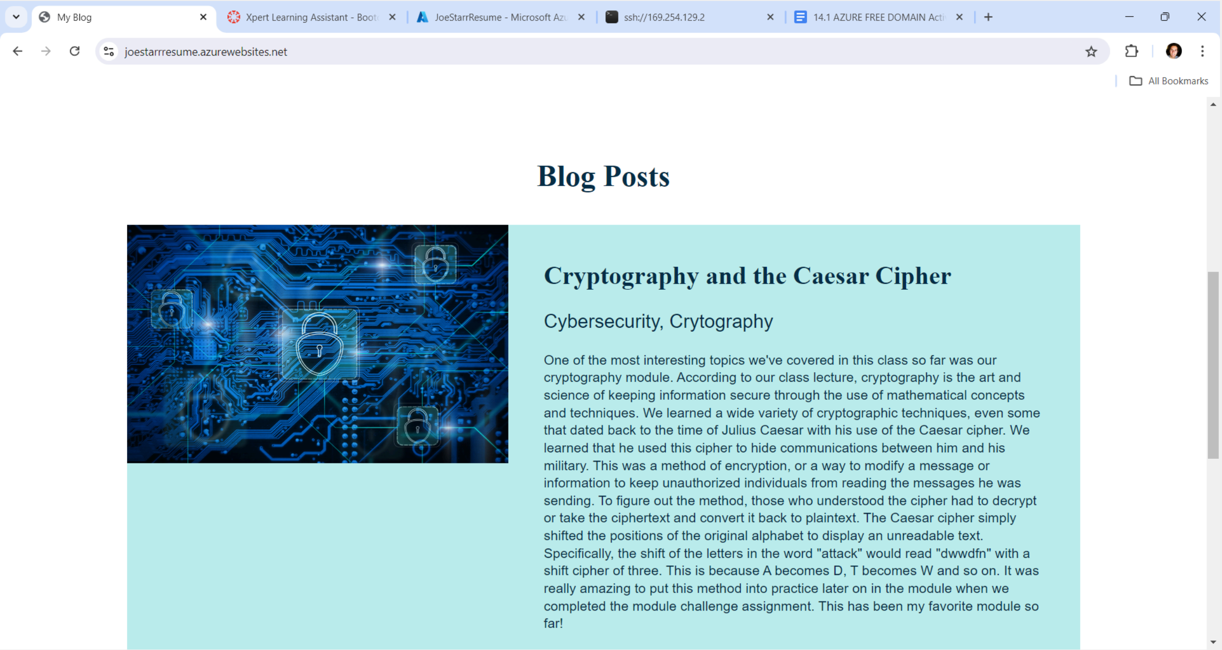
JOE STARR'S CYBER BLOG

Hi, I'm Joe!

Learning a new skill is never easy, learning a new skill in six months? Insane, right? Well, call me insane because I'm doing it right now. Since April 2024 I've been learning the foundational elements to cybersecurity with the ultimate goal of finding a new career path that I will love!

Welcome to my Cyber Blog!

Blog Posts

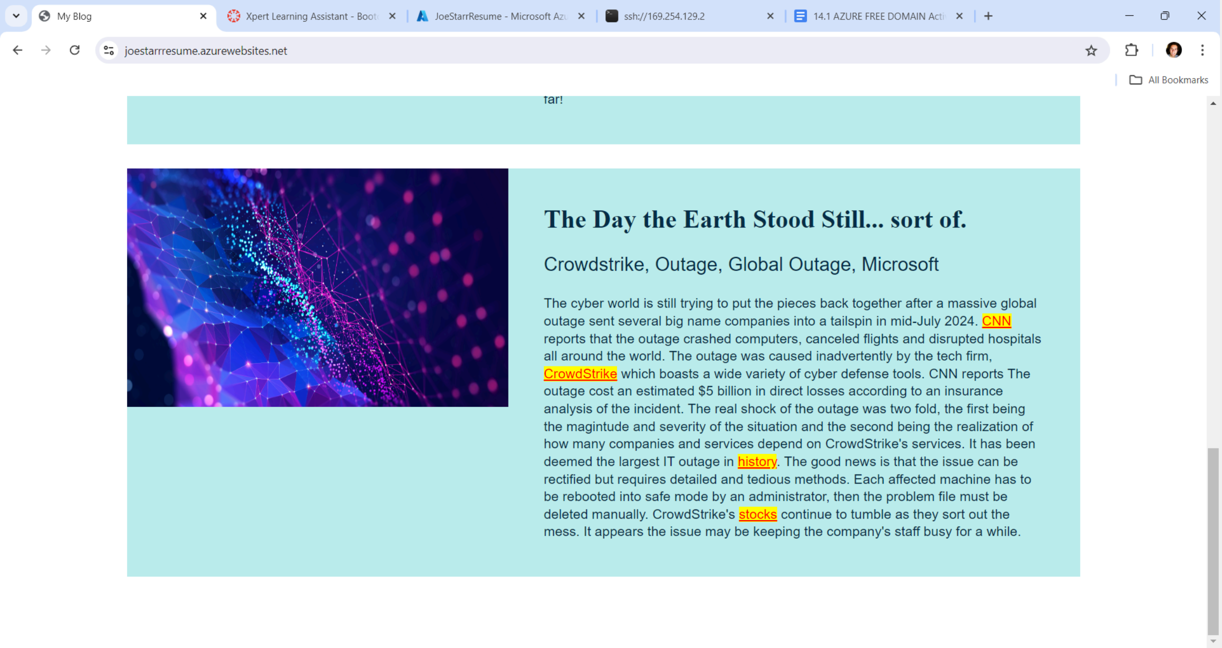

My Blog
Xpert Learning Assistant - Boot
JoeStarrResume - Microsoft Az
ssh://169.254.129.2
14.1 AZURE FREE DOMAIN Acti
joestarrresume.azurewebsites.net
All Bookmarks

Blog Posts

Cryptography and the Caesar Cipher

Cybersecurity, Crytography

One of the most interesting topics we've covered in this class so far was our cryptography module. According to our class lecture, cryptography is the art and science of keeping information secure through the use of mathematical concepts and techniques. We learned a wide variety of cryptographic techniques, even some that dated back to the time of Julius Caesar with his use of the Caesar cipher. We learned that he used this cipher to hide communications between him and his military. This was a method of encryption, or a way to modify a message or information to keep unauthorized individuals from reading the messages he was sending. To figure out the method, those who understood the cipher had to decrypt or take the ciphertext and convert it back to plaintext. The Caesar cipher simply shifted the positions of the original alphabet to display an unreadable text. Specifically, the shift of the letters in the word "attack" would read "dwwdfn" with a shift cipher of three. This is because A becomes D, T becomes W and so on. It was really amazing to put this method into practice later on in the module when we completed the module challenge assignment. This has been my favorite module so far!


My Blog
Xpert Learning Assistant - Boot
JoeStarrResume - Microsoft Az
ssh://169.254.129.2
14.1 AZURE FREE DOMAIN Acti
joestarrresume.azurewebsites.net
All Bookmarks
far!

The Day the Earth Stood Still... sort of.

Crowdstrike, Outage, Global Outage, Microsoft

The cyber world is still trying to put the pieces back together after a massive global outage sent several big name companies into a tailspin in mid-July 2024. CNN reports that the outage crashed computers, canceled flights and disrupted hospitals all around the world. The outage was caused inadvertently by the tech firm, CrowdStrike which boasts a wide variety of cyber defense tools. CNN reports The outage cost an estimated $5 billion in direct losses according to an insurance analysis of the incident. The real shock of the outage was two fold, the first being the magnitude and severity of the situation and the second being the realization of how many companies and services depend on CrowdStrike's services. It has been deemed the largest IT outage in history. The good news is that the issue can be rectified but requires detailed and tedious methods. Each affected machine has to be rebooted into safe mode by an administrator, then the problem file must be deleted manually. CrowdStrike's stocks continue to tumble as they sort out the mess. It appears the issue may be keeping the company's staff busy for a while.

Please note that the highlighted and underlined text are hyperlinks to redirect the reader to articles on the topics referenced in the blog post.

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?

```
joestarrresume.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 (www.iplocation.net/ip-lookup)
```

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

```
In GitBash, I ran “nslookup -type=NS joestarrresume.azurewebsites.net” and
it returned:

Server:  dynamic-75-76-160-3.knology.net
Address:  75.76.160.3

Non-authoritative answer:
joestarrresume.azurewebsites.net
canonical name = waws-prod-sy3-097.sip.azurewebsites.windows.net
waws-prod-sy3-097.sip.azurewebsites.windows.net canonical name =
waws-prod-sy3-097-ef32.australiaeast.cloudapp.azure.com
australiaeast.cloudapp.azure.com
        primary name server = ns1-06.azure-dns.com
        responsible mail addr = msnhst.microsoft.com
        serial  = 10001
        refresh = 900 (15 mins)
        retry   = 300 (5 mins)
        expire  = 604800 (7 days)
        default TTL = 60 (1 min)
```

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?

According to the Xpert Assistant, PHP is a type of scripting language used for web development. PHP is a popular scripting language among web developers and can be used to interact with databases. In this case we are using version 8.2. A runtime stack is the environment where the PHP code is being utilized.

The Xpert goes on to describe that the Front end of a web application is the part of the application that users can directly interact with in the browser. This includes the user interface, design elements and code like HTML and JavaScript.

Back End technologies are more “behind-the-scenes.” These include the server itself, databases and server-side scripts like PHP.

Therefore, in this particular context, PHP is working on the back end of the application.

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

It appears that in the assets directory, it contains two separate subdirectories labeled “CSS” and “Images.” According to the Xpert Assistant CSS stands for Cascading Style Sheets. It is a type of language that is used to describe the presentation of a document written in HTML or XML. The Images directory contains the images that are displayed on the website, like the LinkedIn logo, background imagery and the images associated with the blog posts.

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

Since these are design elements that the user can directly interact with, these files associated in the “assets” directory work with the front end of the web application.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

According to the Xpert Assistant, a cloud tenant is any person or organization that utilizes cloud services provided by a cloud service provider. Cloud tenants use the resources this provider has like virtual machines and applications to run in the cloud. Each tenant operates individually in their own environment hosted by the provider to ensure security and privacy.

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

An access policy is important on a key vault because it controls who has access to the information stored in the key vaults. By restricting access to this sensitive information, it ensures only authorized individuals can have access to its contents.

An access policy on a key vault can also help organizations with regulatory compliance and security best practices.

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

Within the context of a key vault using Azure, a key is used to encrypt, decrypt, sign and verify a set of data. It is mostly used to secure data.

A secret within a key vault in Azure can be any sensitive information a user would like protected like passwords or API Keys.

A certificate within a key vault is used to secure communication over HTTPS, authenticate users or encrypting data.

Cryptography Questions

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

Some of the advantages of a self-signed certificate include being able to be set up and executed quickly, they are cheaper than going through a Certification Authority which is ideal for smaller companies.

Source:
https://www.encryptionconsulting.com/education-center/self-signed-certificates/#h-benefits-of-using-self-signed-ssl-certificates

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

Some disadvantages of a self-signed certificate include not being signed by a trusted 3rd party Certification Authority. This can cause users to see a warning displayed on “untrusted” sites. This lack of validation can also be a potential vulnerability for attackers to exploit.
Furthermore, the Xpert assistant states that some CA-signed certificates come with warranties that protect a user in the event of a security breach. Self-signed certificates do not provide that level of protection.

3. What is a wildcard certificate?

A wildcard certificate secures a domain and all of its subdomains in one certificate. After examining the certificate for my Azure Web App, it appears that “*.azurewebsites.net” is denoted. This means my joestarrresume.azurewebsites.net and all associated subdomains are secured as well because of the wildcard certificate.

Source:
https://knowledge.digicert.com/general-information/what-is-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 isn’t provided because it is vulnerable to attacks such as the POODLE attack (Padding Oracle on Downgraded Legacy Encryption). cisa.gov states that the POODLE attack takes advantage of the built-in protocol version negotiation feature to decrypt information within the SSL session. It can be done on any system or application that supports SSL 3.0.

Source: https://www.cisa.gov/news-events/alerts/2014/10/17/ssl-30-protocol-vulnerability-and-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?

My browser is not returning an error for my SSL certificate because it is verified by a trusted Certificate Authority. The Xpert assistant explains that the web server presents its certificate to the browser.
The browser checks the SSL certificate to ensure it is valid and signed by a trusted CA. If it is signed by a trusted CA recognized by my browser, meaning the root certificate is in my browser’s root store, then the certificate is valid and the connection is secure.

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

The certificate was issued on Tuesday March 12, 2024 at 9:36:42 PM and it expires on Friday, March 7, 2025 at 8:36:42 PM

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

Yes, it is Microsoft Azure RSA TLS Issuing CA 07 and the organization is the Microsoft Corporation.

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

Yes, it is DigiCert Global Root G2.

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

Yes, it is stored in my browser’s root store under the Trusted Root

Certification Authorities Tab in Google Chrome.

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

Another root CA in my browser’s root store is COMODO RSA Certification Authority. My root store states the certificate’s intended purposes are client authentication, code signing, encrypting file system, secure email and IP security tunnel termination to name a few.

Day 3 Questions

Cloud Security Questions

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

According to the Xpert assistant, some similarities between the Azure Web Application Gateway and Azure Front Door is that both provide security at the Application Layer (Layer 7) of the OSI model. They both act as load balancers that distribute incoming traffic and they both can integrate a Web Application Firewall to protect against common web vulnerabilities.

Some differences between the two are: The Azure Web Application Gateway protects a web application within a specific region, while an Azure Front Door is global and can be deployed across several regions.
The Xpert assistant claims that the Azure Front Door is simpler and easier to manage while the Web Application Gateway is more complex to configure.
Finally, Azure Web Application gateway is more suitable for applications hosted in a single region that call for more advanced routing features. The Azure Front Door is ideal for global applications that require a high level of availability and scalability across several regions.

2. What is SSL offloading? What are its benefits?

SSL offloading is a method that sends the SSL encryption and decryption traffic to a separate dedicated server. The encryption and decryption processes of SSL can be demanding on a server. Offloading sends those processes to a dedicated server to encrypt and decrypt SSL traffic. This frees up CPU resources on the web server so it can handle other requests.

Source: https://avinetworks.com/glossary/ssl-offload/

3. What OSI layer does a WAF work on?

The WAF works on the OSI Layer 7 - Application

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

921120 - HTTP Response Splitting Attack

According to owasp.org, an HTTP Response Splitting Attack occurs when data enters a web application through an untrusted source— commonly an HTTP request. Data is included in an HTTP response header sent to a web user without being analyzed for malicious information. The attackers can gain control of remaining headers and body of the response the application intends to send and allow them to create more responses as well.
Source: https://owasp.org/www-community/attacks/HTTP_Response_Splitting

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?

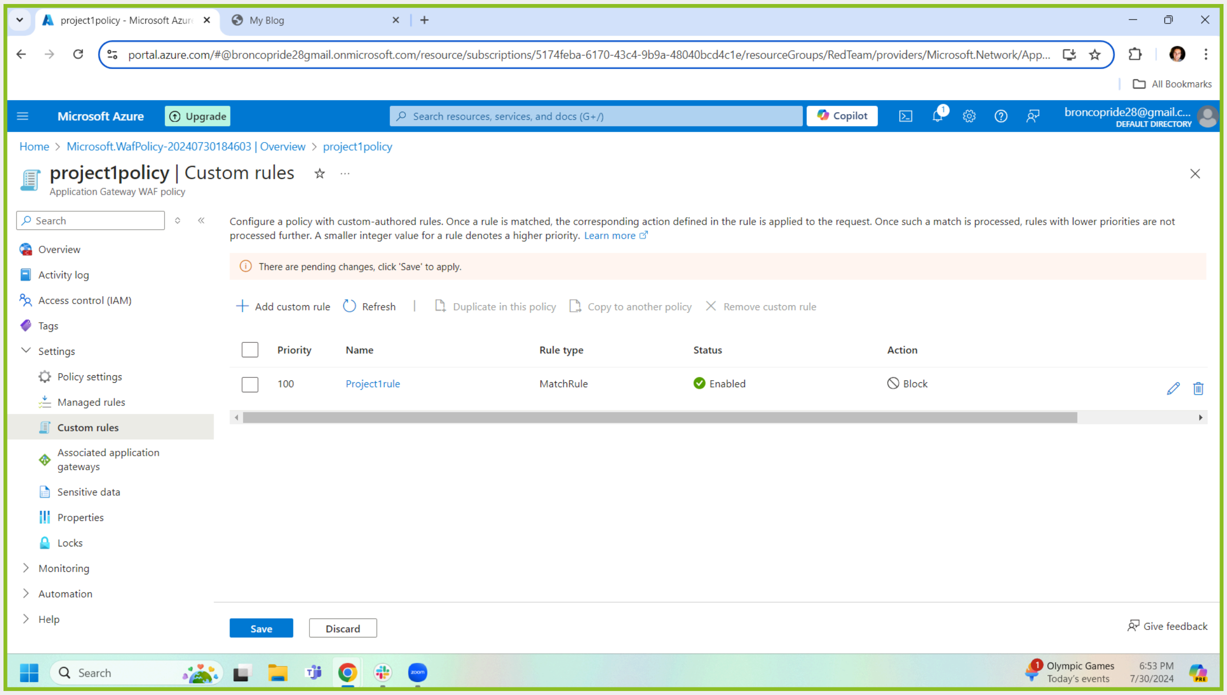
I do not think my website as it is currently designed could be impacted by this vulnerability if Front Door wasn't enabled. The same OWASP.org article further explains that the vulnerability has been fixed in most modern application servers, regardless of what language the code has been written in. However, the Xpert Assistant states that in order to ensure if my web application is vulnerable to a HTTP response splitting attack, I would need to perform code analysis and penetration testing to be certain if any potential weaknesses exist.

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 to block all traffic from Canada will NOT guarantee that anyone residing in Canada will not be able to access my website. The hypothetical rule would only block users with Canadian IP addresses from the site. Users residing in Canada utilizing a proxy server or a virtual private network (VPN) may still be able to access the site. Therefore, simply having a rule blocking Canadian IP traffic may not be 100% effective.

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

    a. A WAF custom rule



portal.azure.com/#@broncopride28gmail.onmicrosoft.com/resource/subscriptions/5174feba-6170-43c4-9b9a-48040bcd4c1e/resourceGroups/RedTeam/providers/Microsoft.Network/App...

Home > Microsoft.WafPolicy-20240730184603 | Overview > project1policy

project1policy | Custom rules

Application Gateway WAF policy

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

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

	Priority	Name	Rule type	Status	Action
□	100	Project1rule	MatchRule	✓ Enabled	Block

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