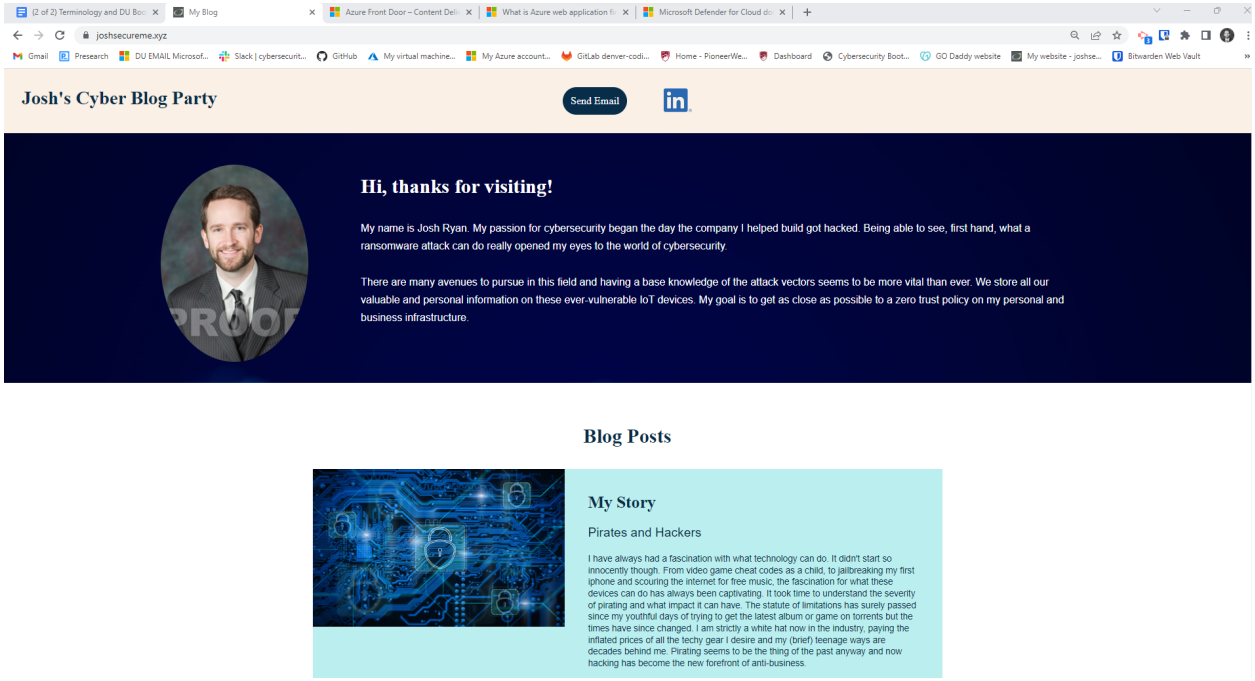
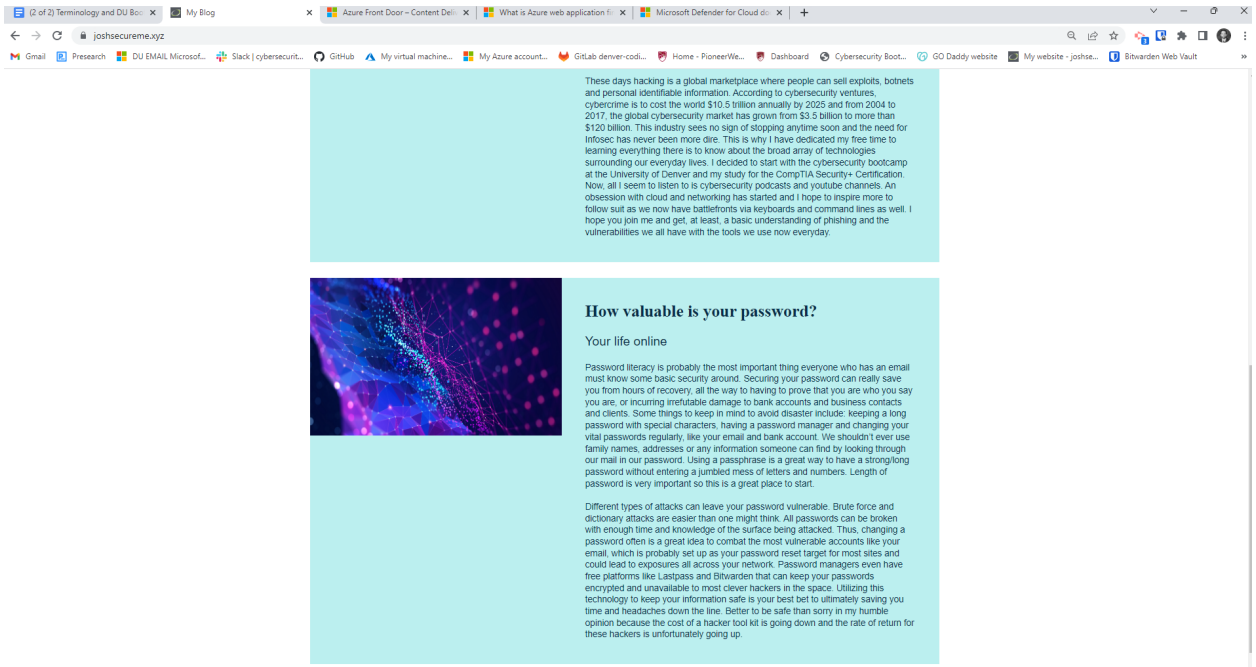
Cybersecurity

Project 1 Technical Brief





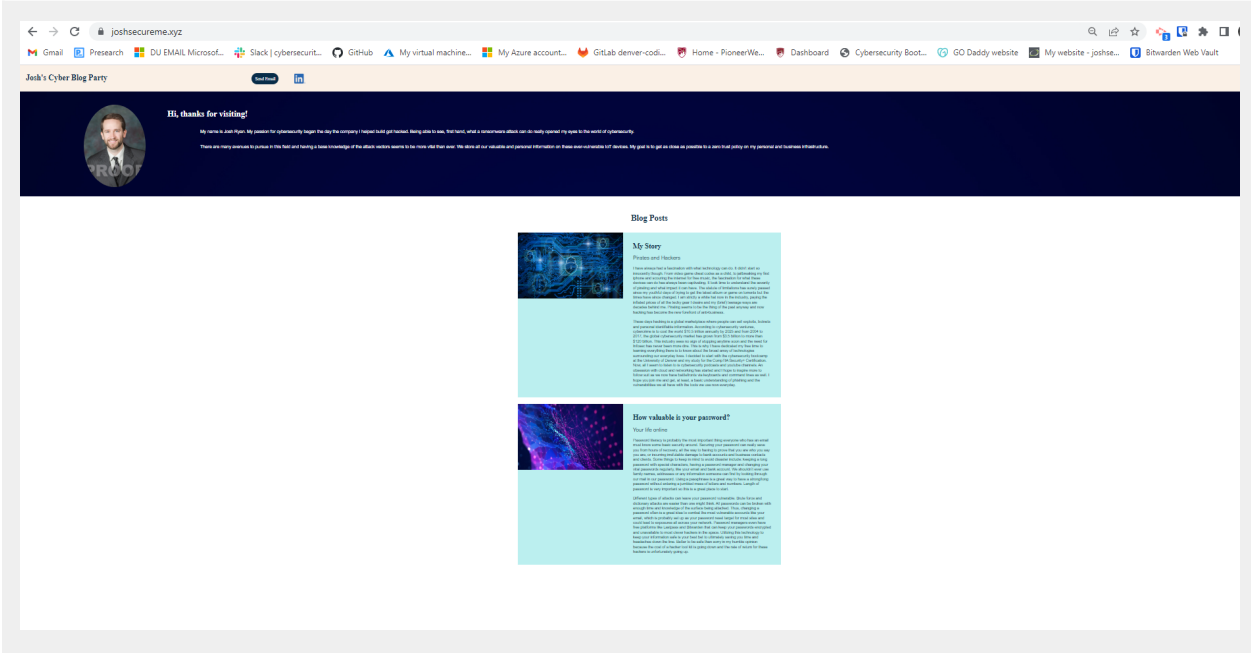
These days hacking is a global marketplace where people can sell exploits, botnets and personal identifiable information. According to cybersecurity ventures, cybercrime is to cost the world $10.5 trillion annually by 2025 and from 2004 to 2017, the global cybersecurity market has grown from $3.5 billion to more than $120 billion. This industry sees no sign of stopping anytime soon and the need for Infosec has never been more dire. This is why I have dedicated my free time to learning everything there is to know about the broad array of technologies surrounding our everyday lives. I decided to start with the cybersecurity bootcamp at the University of Denver and my study for the CompTIA Security+ Certification. Now, all I seem to listen to is cybersecurity podcasts and youtube channels. An obsession with cloud and networking has started and I hope to inspire more to follow suit as we now have battlefronts via keyboards and command lines as well. I hope you join me and get, at least, a basic understanding of phishing and the vulnerabilities we all have with the tools we use now everyday.

How valuable is your password?

Your life online

Password literacy is probably the most important thing everyone who has an email must know some basic security around. Securing your password can really save you from hours of recovery, all the way to having to prove that you are who you say you are, or incurring irrefutable damage to bank accounts and business contacts and clients. Some things to keep in mind to avoid disaster include: keeping a long password with special characters, having a password manager and changing your vital passwords regularly, like your email and bank account. We shouldn't ever use family names, addresses or any information someone can find by looking through our mail in our password. Using a passphrase is a great way to have a strong/long password without entering a jumbled mess of letters and numbers. Length of password is very important so this is a great place to start.

Different types of attacks can leave your password vulnerable. Brute force and dictionary attacks are easier than one might think. All passwords can be broken with enough time and knowledge of the surface being attacked. Thus, changing a password often is a great idea to combat the most vulnerable accounts like your email, which is probably set up as your password reset target for most sites and could lead to exposures all across your network. Password managers even have free platforms like Lastpass and Bitwarden that can keep your passwords encrypted and unavailable to most clever hackers in the space. Utilizing this technology to keep your information safe is your best bet to ultimately saving you time and headaches down the line. Better to be safe than sorry in my humble opinion because the cost of a hacker tool kit is going down and the rate of return for these hackers is unfortunately going up.



Day 1 Questions

General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

```
GoDaddy domain
```

2. What is your domain name?

```
joshsecureme.xyz
```

Networking Questions

1. What is the IP address of your webpage?

address **20.118.56.8** as per azure too (and server being 168.63.129.16 per nslookup)

```
joshua [ ~ ]$ nslookup -type=any joshsecureme.xyz
Server:         168.63.129.16
Address:        168.63.129.16#53

Non-authoritative answer:
Name:   joshsecureme.xyz
Address: 20.118.56.8
joshsecureme.xyz        nameserver = ns65.domaincontrol.com.
joshsecureme.xyz        nameserver = ns66.domaincontrol.com.
joshsecureme.xyz
        origin = ns65.domaincontrol.com
        mail addr = dns.jomax.net
        serial = 2022091203
        refresh = 28800
        retry = 7200
        expire = 604800
        minimum = 600

Authoritative answers can be found from:
ns65.domaincontrol.com  internet address = 97.74.102.43
ns65.domaincontrol.com  has AAAA address 2603:5:2164::2b
ns66.domaincontrol.com  internet address = 173.201.70.43
ns66.domaincontrol.com  has AAAA address 2603:5:2264::2b
```

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

IP2Location

IP: 20.118.56.8

Country: United States of America

State: Iowa

City: Des Moines

Latitude: 41.6005

Longitude: -93.6091

IP2Location

IP: 168.63.129.16

Country: Hong Kong

State: Hong Kong

City: Hong Kong

Latitude: 22.2855

Longitude: 114.1576

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

```
It shows that the server is a comcast.net server as below
```

```
Josh@LAPTOP-N3DBMKUU MINGW64 ~
$ nslookup -type=NS joshsecureme.xyz
Server:  cdns01.comcast.net
Address:  2001:558:feed::1
Non-authoritative answer:
joshsecureme.xyz        nameserver = ns65.domaincontrol.com
joshsecureme.xyz        nameserver = ns66.domaincontrol.com
ns65.domaincontrol.com  internet address = 97.74.102.43
ns65.domaincontrol.com  AAAA IPv6 address = 2603:5:2164::2b
ns66.domaincontrol.com  internet address = 173.201.70.43
ns66.domaincontrol.com  AAAA IPv6 address = 2603:5:2264::2b
```

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 7.4, works on the back end
```

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

```
CSS color style sheet code and images for the site.
```

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

```
This would be part of the front end development of the site.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
Basically a client to the cloud environment. The customers of the cloud
provider are the tenants of the system.
```

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

```
It would lay out which users, application and user groups can perform
operations on Key Vault secrets, keys and certificates. Allowing only the
need to know admin access.
```

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

```
Keys are the asymmetric encryption keys you create. A Secret can be anything
you want kept secret that is not an asymmetric key or cert, like symmetric
keys, data strings or API tokens. Certificates are associated with the
private keys and the public key is in the certificate; its job is to bind
the name to a public key and must have a private key associated.
```

Cryptography Questions

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

```
They are simple to create and have no expense associated. Great for test
environments and development.
```

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

```
They are not vetted and can be revoked by a CA. They don't provide a padlock
indicating to the browser that the site is safe for your consumers. They can
be forged more easily and lack visibility to security teams.
```

3. What is a wildcard certificate?

```
It uses a single certificate with the wildcard (*) to allow the certificate
to secure multiple sub domain names. It is similar to the CNAME, in which a
wildcard certificate using * as the subdomain to use a shell expansion
procedure to match.
```

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 is outdated and more vulnerable to attack (one attack notably called
POODLE). TLS is a way for a web server to support older web browsers,
replacing SSL.
```

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, I am getting the padlock showing that the site is secure. The Cert
issued by DigiCert Global Root CA.
```

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

```
Issued on 9-13-2022 and expires on 3-14-2023.
```

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

```
Yes, GeoTrust Global TLS
```

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

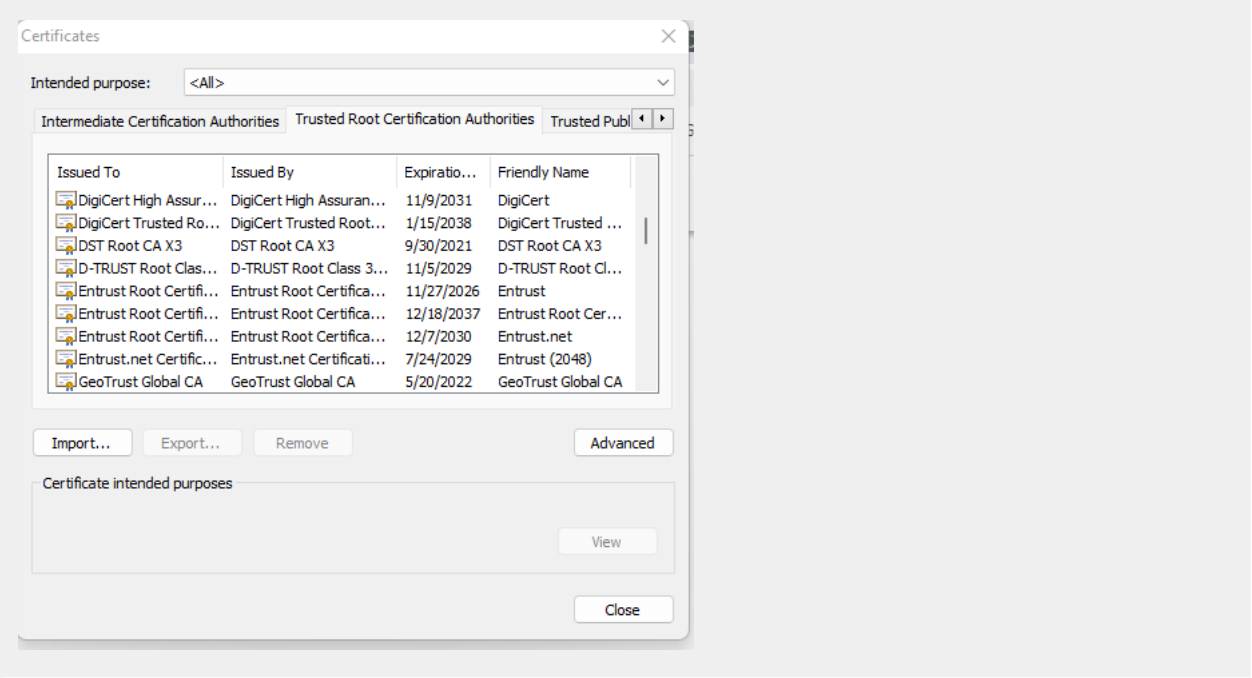
```
Yes, DigiCert Global Root CA
```

    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.

```
DST Root CA X3
```



Day 3 Questions

Cloud Security Questions

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

```
Azure front door applies the WAF filters at edge locations before it gets to
the data center. Azure Web App Gateway applies the filter when it enters
your VNET through the App Gateway. They are both part of the layer 7 model.
The Gateway should be deployed behind the front door. They both have very
similar functions being WAF firewalls to filter for the presence of malware
or viruses. They both are load balancers (their primary solution).
```

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 a solution that companies choose to reduce latency and
demand on their servers. Its device is known as an application-specific
integrated circuit processor, a proxy server or a load balancer. Designed to
use the secure SSL/TLS protocol to terminate or bridge to reduce operational
burden. One huge benefit is increasing up time and decreasing down time.
```

```
Another added layer of protection and availability.
```

3. What OSI layer does a WAF work on?

```
Layer 7
```

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

```
SQL Injection Attack: Common Injection Testing detected. It is a technique
that allows an attacker to insert SQL commands into the queries that an
Application makes into its database. Some common attacks include:
error-based SQL injection, union-based sql injection, blind sql injection
and out-of-band sql injection.
```

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?

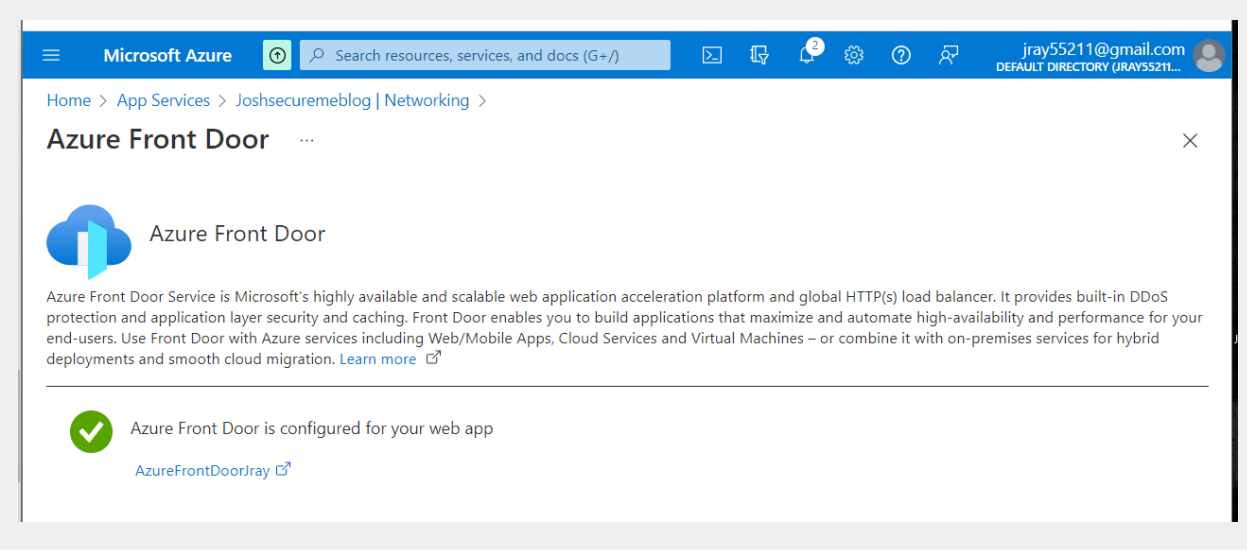
```
Yes, because that is the first layer of defense blocking the injection. This
is one of the core benefits of WAF protection.
```

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?

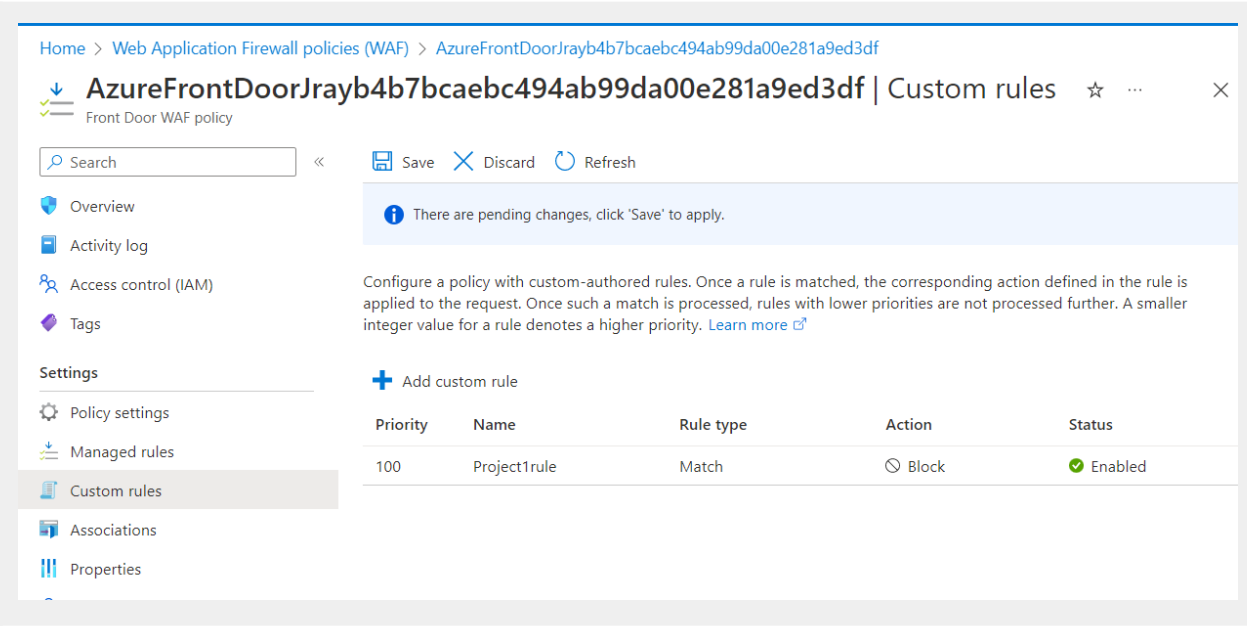
```
No, because people could still use a VPN or could ‘spoof’ their IP address.
```

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***