j)

**Distributed denial-of-service (DDoS) attack:** A distributed denial-of-service (DDoS) attack — or DDoS attack — is when a malicious user gets a network of zombie computers to sabotage a specific website or server. The attack happens when the malicious user tells all the zombie computers to contact a specific website or server over and over again. That increase in the volume of traffic overloads the website or server causing it to be slow for legitimate users, sometimes to the point that the website or server shuts down completely. The attacks are "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attacks.

**solution**

* Install and maintain anti-virus software.
* Install a firewall, and configure it to restrict traffic coming into and leaving your computer.

## Hacking

Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer, databases. The availability of information online on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities.

**Solution**

* Commit your passwords to memory and don't store them on your computer or in your mobile phone.
* If the browser asks to keep you signed in, unclick that option and take the time to re-enter your password each time.
* Clear your browsing history or cache after chatting.

## Spam The mass distribution of unsolicited messages, advertising or pornography to addresses which can be easily found on the Internet through things like social networking sites, company websites and personal blogs.

## Pharming

A means to point you to a malicious and illegitimate application by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website.

## Phishing

Fake text messages and websites created to look like they're from authentic companies. They're sent by criminals to steal personal and financial information from you. This is also known as “spoofing”.

k)

**SQL Injection**

SQL Injection is an attack where users can inject SQL commands via user input form and have them executed on the server. This SQL commands could do everything: read sensitive data, modify the database data, perform administrative tasks against the database server. Your application can be exposed to this attack when you dynamically create SQL statements (concatenating data based on user’s input).

This was implemented on lummox chat engine log in page application by entering the SQLite

commands as below.

**Cross-site request forgery**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application. XSS is amongst the most rampant of web application vulnerabilities and occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

By leveraging XSS, this implementation wasn’t intended target a victim directly. Instead, it will exploit a vulnerability within chat application that the victim will visit.

***Implementation***

**Cross-Site Request Forgery**

An XSRF attack is functionally the opposite of a cross-site scripting (XSS) attack, in which the hacker inserts malicious coding into a link on a Web site that appears to be from a trustworthy source. When an end user clicks on the link, the embedded programming is submitted as part of the client's Web request and can execute on the user's computer.

An XSRF attack also differs from cross-site tracing (XST), a sophisticated form of XSS that allows an intruder to obtain [cookie](https://searchsoftwarequality.techtarget.com/definition/cookie)s and other authentication data using simple client-side [script](https://whatis.techtarget.com/definition/script). In XSS and XST, the end user is the primary target of the attack. In XSRF, the Web server is the primary target although collateral harm is often done to individual end users.

***Implementattion***

i)

**Input Validation**

This checks if the data inputs meet a set of criteria such as a string containing no standalone single quotation marks. Since the web is used extensively, knowing what information you are putting into particular fields on a web page can make a big difference. Vigilance is the key here.

**Network segmentation and segregation**.

This is a highly effective strategy, it limits the impact of a network intrusion and significantly makes it more difficult for an adversary to locate and gain access to most sensitive information; and increase the likelihood of detecting an adversary’s activity in a timely manner.

**File Reputation**

This way verifies that files have not changed on your system without you knowing about it. Some anti-virus and anti-malware products do this Yes, there are other ways to get into your system that they don’t protect against, but they can stop a large portion of unwanted changes.

**Irreversible Encryption**

A cryptographic process that transforms data deterministically to a form from which the original data cannot be recovered, even by those who have full knowledge of the method of encryption. The process will be used to protect stored [passwords](https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/password#1O11password) in a system where the password offered is first encrypted before it is matched against the stored encrypted password. Illegal access to the stored password therefore does not permit access to the system.