

# Threat Modeling



## THREAT MODELING STRIDE

### SPOOFING

This is when a malicious actor pretends to be someone they're not by faking information. For instance, email spammers changing the sender's name to appear trustworthy. In applications, it's like someone using stolen login details to impersonate a user.

### TAMPERING

Tampering means intentionally altering data to compromise its integrity. It could involve changing data on a device, in memory, or during data transmission. Weak input validation can allow attackers to modify data, leading to issues.

### REPUDIATION

This is about denying responsibility for actions. It's like a user claiming they didn't make an online purchase when they did. To counter this, comprehensive logging, digital signatures, and multifactor authentication can be used.

### INFORMATION DISCLOSURE

This threat involves sharing information with unauthorized parties, like during data breaches or sending an email to the wrong recipient. Safeguarding against it includes data encryption and strong access controls.

### DENIAL OF SERVICE

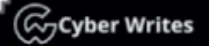
Denial of Service (DoS) attacks block legitimate users' access to resources. Monitoring for abnormal resource usage is crucial to detect these attacks, and applications should be designed with availability in mind.

### ELEVATION OF PRIVILEGE

Elevation of privilege happens when an unprivileged user gains access to higher-level privileges, potentially compromising sensitive data. Robust access controls, user identity validation, and multifactor authentication are needed to protect against this threat.

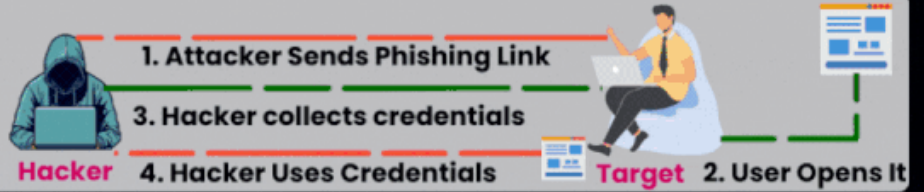
*Cybershield Insights – by Irudaya Praveen*

# Top 8 Cyber Attacks - 2024



## Phishing Attack

**1** The use of deceptive emails, texts, or websites to gain sensitive information.



## Ransomware

**2** Malware that can encrypt data and make you pay to get them back.



## Denial-of-Service (DoS)

**3** Loading excessive load on a machine or network so that it stops working normally.



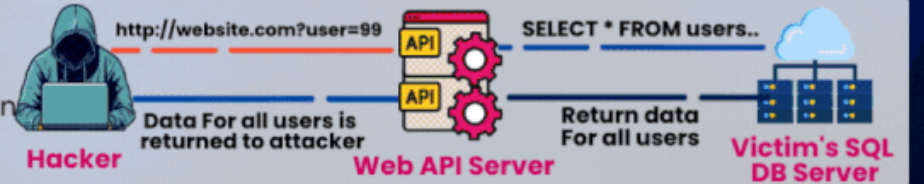
## Man-in-the-Middle (MitM)

**4** Engaging in covert interception and manipulation of communication between two parties without noticing it.



## SQL Injection

**5** To get the Access to the database, Vulnerabilities in Database queries can be exploited



## Cross-Site Scripting (XSS)

**6** Putting malicious code into websites that other people visit.



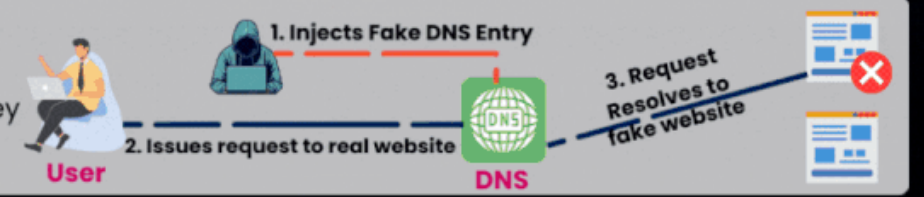
## Zero-Day Exploits

**7** Attacks take advantage of unknown vulnerabilities before programmers can fix them.



## DNS Spoofing

**8** Sending DNS queries to malicious sites so that they can be accessed without permission.



From:

<https://wiki.fortier-family.com/> - **Warnaud's Wiki**

Permanent link:

<https://wiki.fortier-family.com/cybersecurity/threats>

Last update: **2024/02/02 06:54**

