Understanding Cyber Attacks

Name : Syed Azharuddin Ali Khan
Role : Cybersecurity Analyst Intern
Date : 01/23/2026

Objective

To build **threat awareness** by understanding common cyber attacks, how they work, why they are dangerous, and how organizations and individuals can recognize and mitigate them.

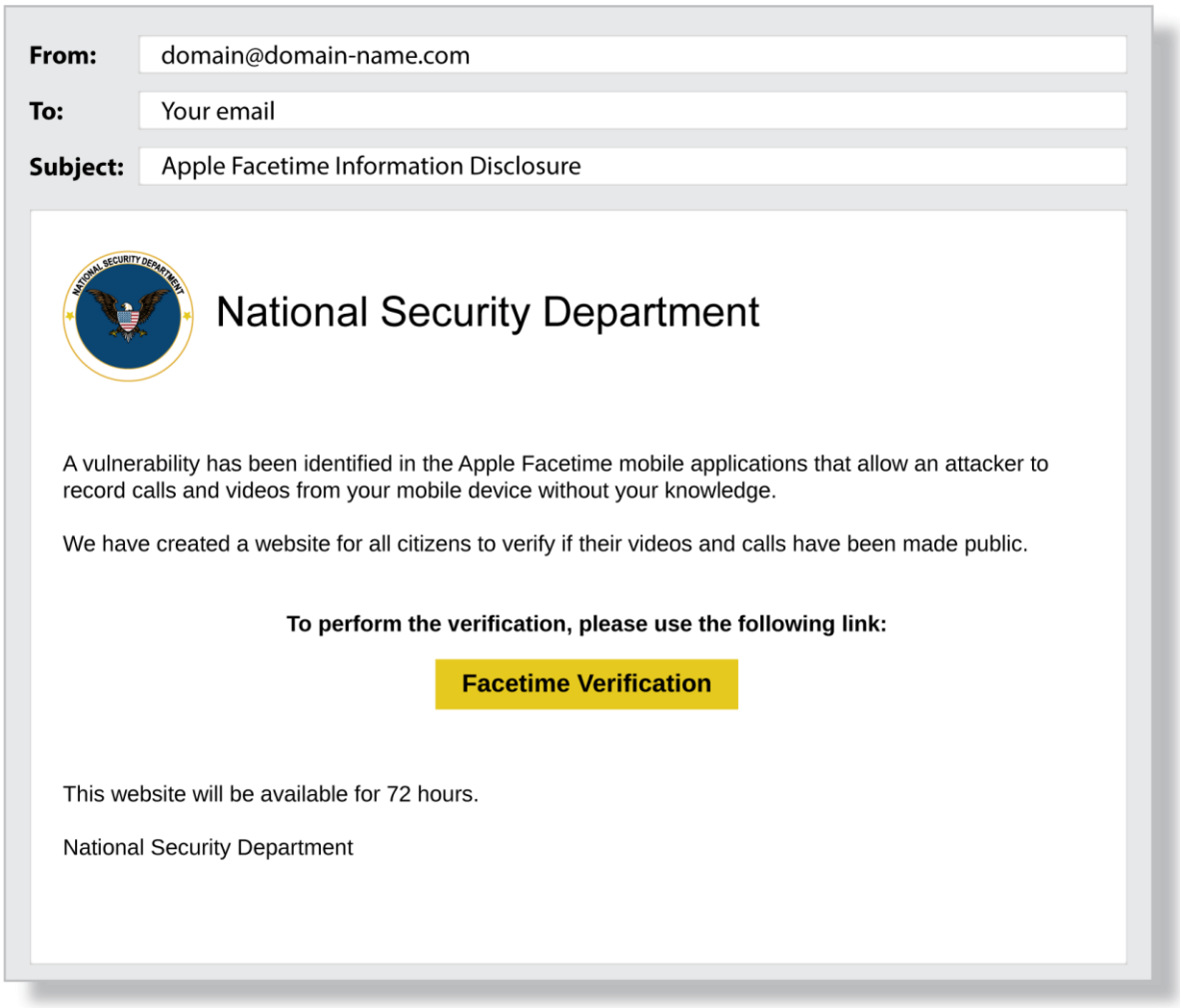
Introduction to Cyber Attacks

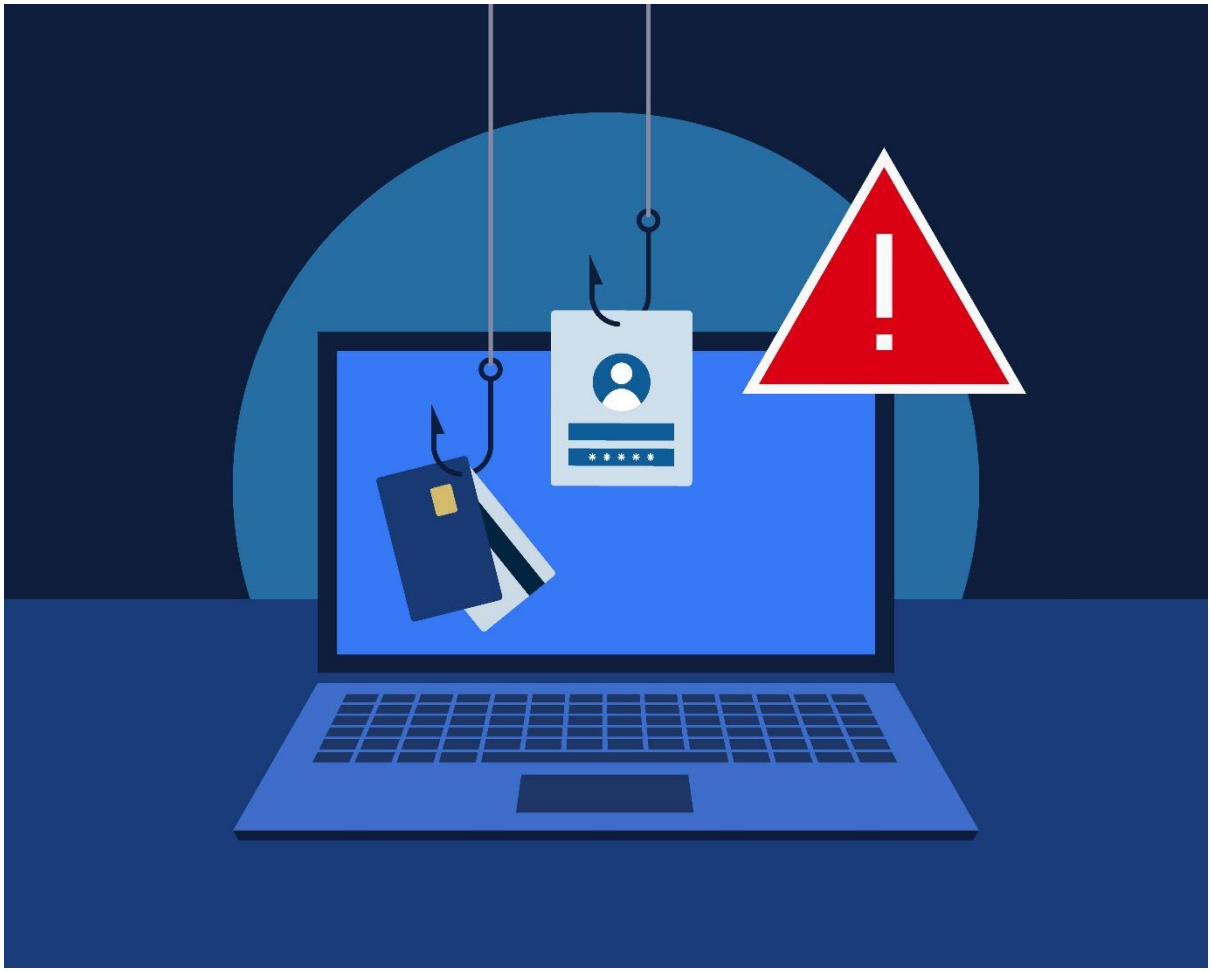
A **cyber attack** is a deliberate attempt by an attacker to compromise the **confidentiality, integrity, or availability (CIA Triad)** of information systems, networks, or users. Attackers exploit **human behavior**, **software vulnerabilities**, and **weak security controls** to gain unauthorized access, steal data, disrupt services, or cause financial and reputational damage.

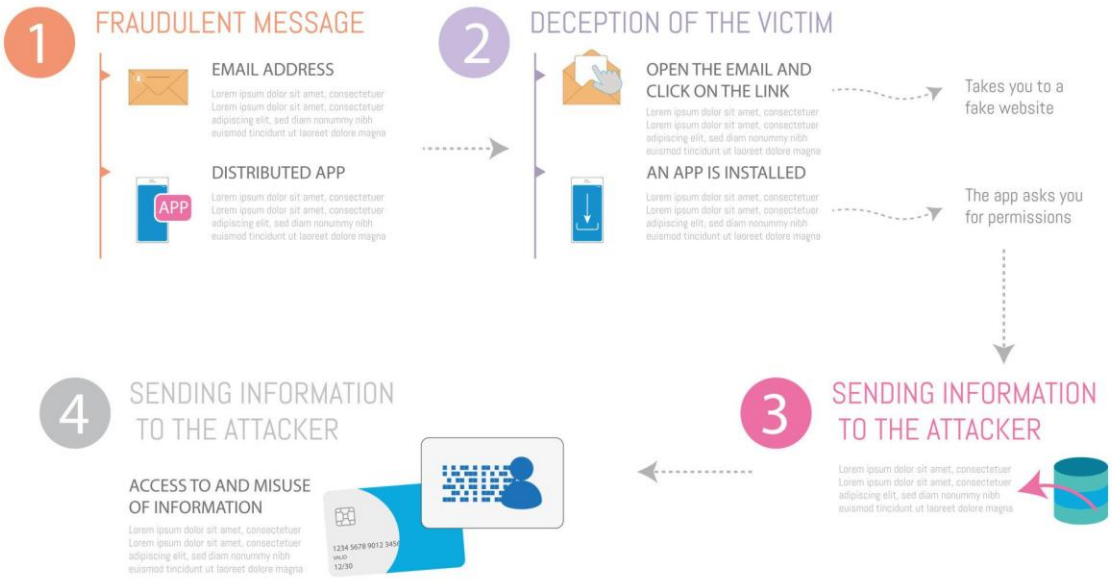
Understanding common cyber attacks is a **core skill for a cybersecurity analyst**, as early detection and awareness significantly reduce organizational risk.

---

1. Phishing Attack







4

What is Phishing?

Phishing is a **social engineering attack** where attackers impersonate a trusted entity to trick victims into revealing sensitive information such as:

- Usernames
- Passwords
- Credit/debit card details
- OTPs
- Banking information

The attack typically occurs via **email**, **SMS (smishing)**, **phone calls (vishing)**, or **fake websites**.

How Phishing Works

1. Attacker creates a **fake message or website** resembling a legitimate organization (bank, company, government).
2. Victim receives a message containing:

    - Urgent language (“Account will be suspended”)
    - A malicious link or attachment
3. Victim clicks the link and enters credentials on a **fake login page**
4. Attacker captures the information and misuses it

Common Types of Phishing

- **Email Phishing** – Generic mass emails
- **Spear Phishing** – Targeted at a specific person or company
- **Whaling** – Targets senior executives
- **Smishing** – Phishing via SMS
- **Vishing** – Voice-based phishing calls

Impact of Phishing

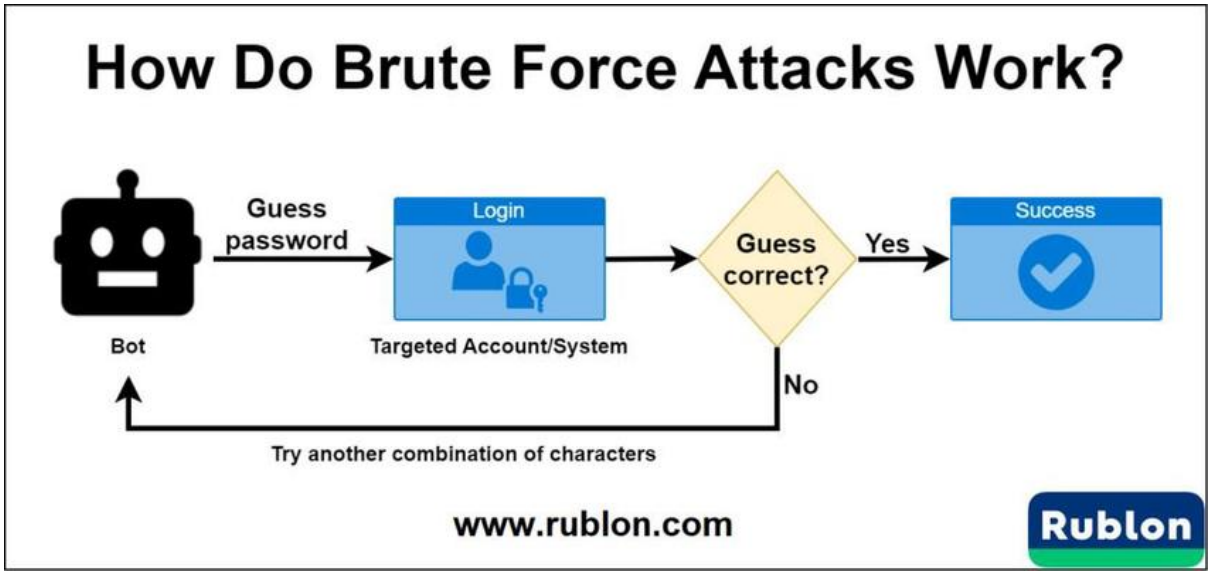
- Account takeover
- Financial fraud
- Identity theft
- Malware infection
- Corporate data breaches

Prevention Measures

- User awareness training
- Email filtering and anti-phishing tools
- Multi-factor authentication (MFA)
- Verifying URLs before clicking
- Never sharing OTPs or passwords

---

2. Brute Force Attack


How Do Brute Force Attacks Work?
Guess password
Login
Guess correct?
Yes
Success
Bot
Targeted Account/System
No
Try another combination of characters
www.rublon.com
Rublon


PASSW**
BRUTE FORCE ATTACK

What is a Brute Force Attack?

A **brute force attack** is an attack where the attacker **tries all possible combinations** of passwords or keys until the correct one is found.

This attack exploits:

- Weak passwords
- No login attempt limits
- Poor authentication mechanisms

How Brute Force Attacks Work

1. Attacker uses automated tools
2. Thousands or millions of password combinations are tried
3. Once the correct password is found, access is gained
4. Attacker may escalate privileges or steal data

Types of Brute Force Attacks

- **Simple Brute Force** – Tries all combinations
- **Dictionary Attack** – Uses common passwords
- **Credential Stuffing** – Uses leaked username/password pairs
- **Hybrid Attack** – Combination of dictionary + variations

Impact of Brute Force Attacks

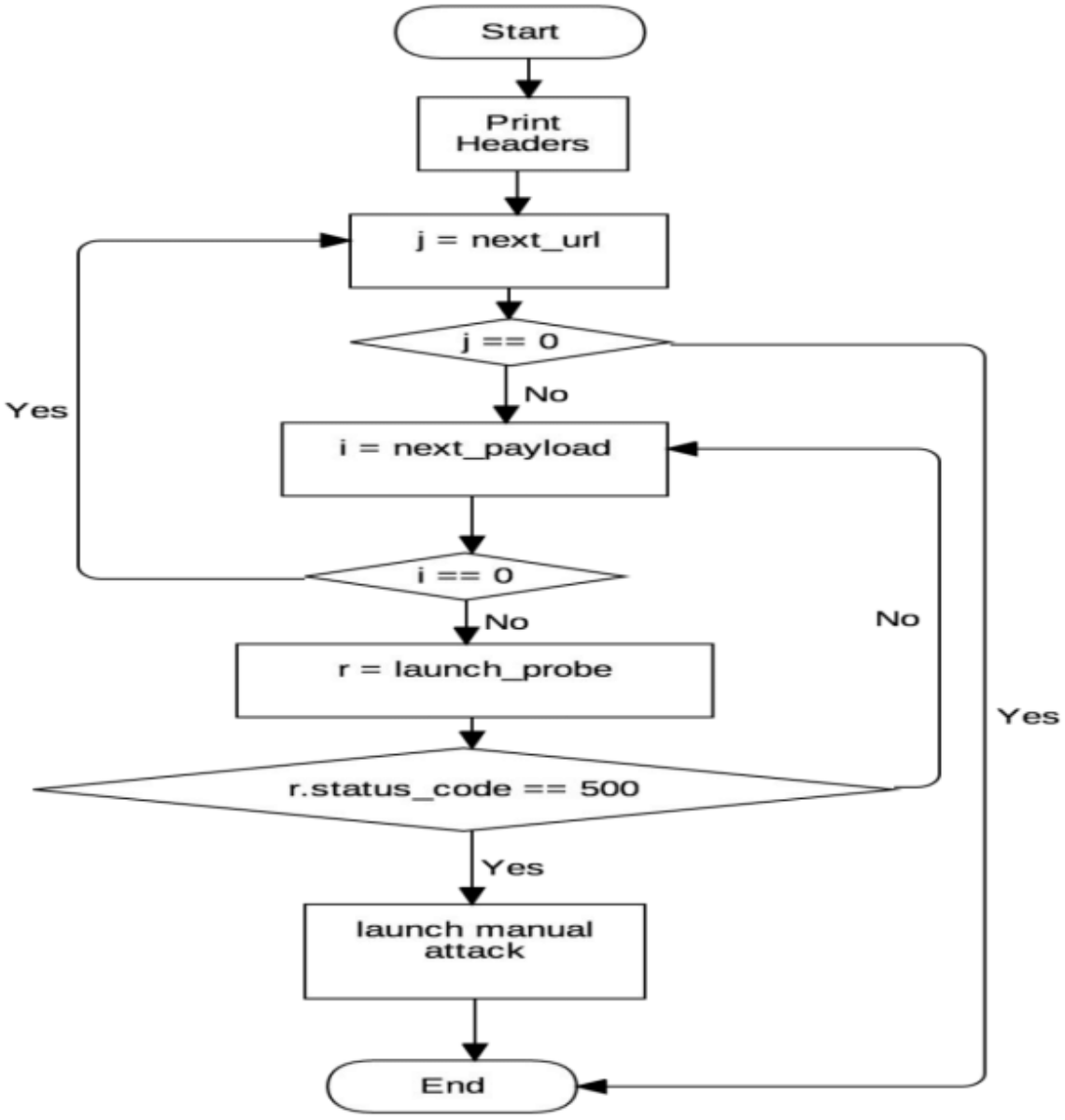
- Unauthorized account access
- Data theft
- Service disruption
- Reputational damage

Prevention Measures

- Strong password policies
- Account lockout after failed attempts
- CAPTCHA implementation
- Multi-factor authentication
- Monitoring failed login attempts

---

3. SQL Injection (SQLi)



4

What is SQL Injection?

SQL Injection is a **web application attack** where malicious SQL queries are injected into input fields to manipulate backend databases.

It occurs when:

- User input is not properly validated
- Dynamic SQL queries are used insecurely

How SQL Injection Works

1. Application accepts user input (login form, search box)
2. Input is directly added to an SQL query
3. Attacker inserts malicious SQL code
4. Database executes the injected query

Example:

' OR '1'='1

This can bypass authentication.

Types of SQL Injection

- **In-band SQLi** – Data retrieved using same channel
- **Blind SQLi** – No direct error output
- **Out-of-band SQLi** – Data exfiltration via external channels

---

Impact of SQL Injection

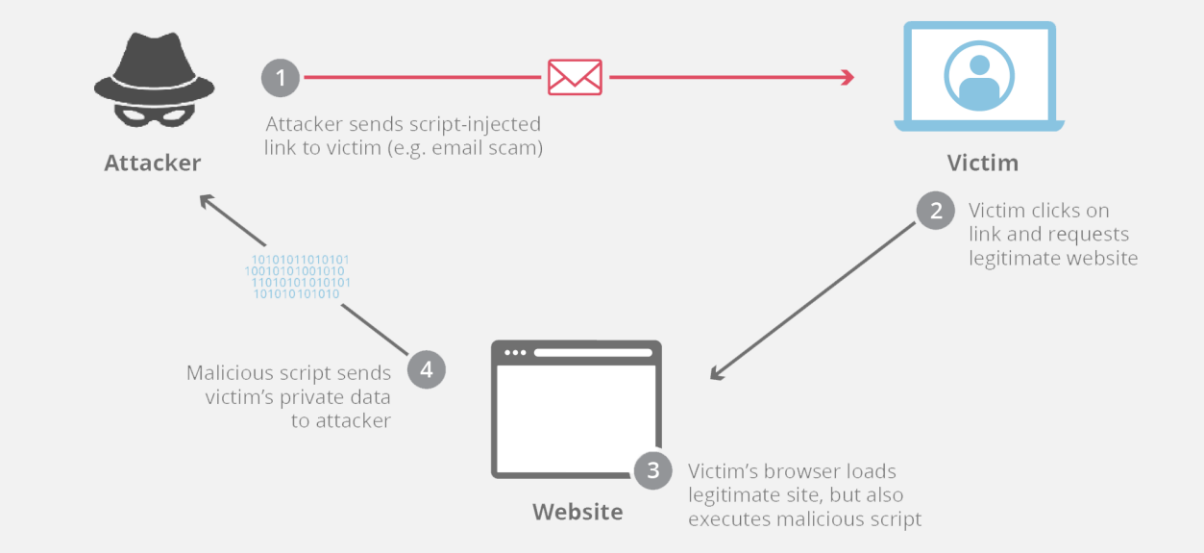
- Database compromise
- Unauthorized data access
- Data deletion or modification
- Full server takeover

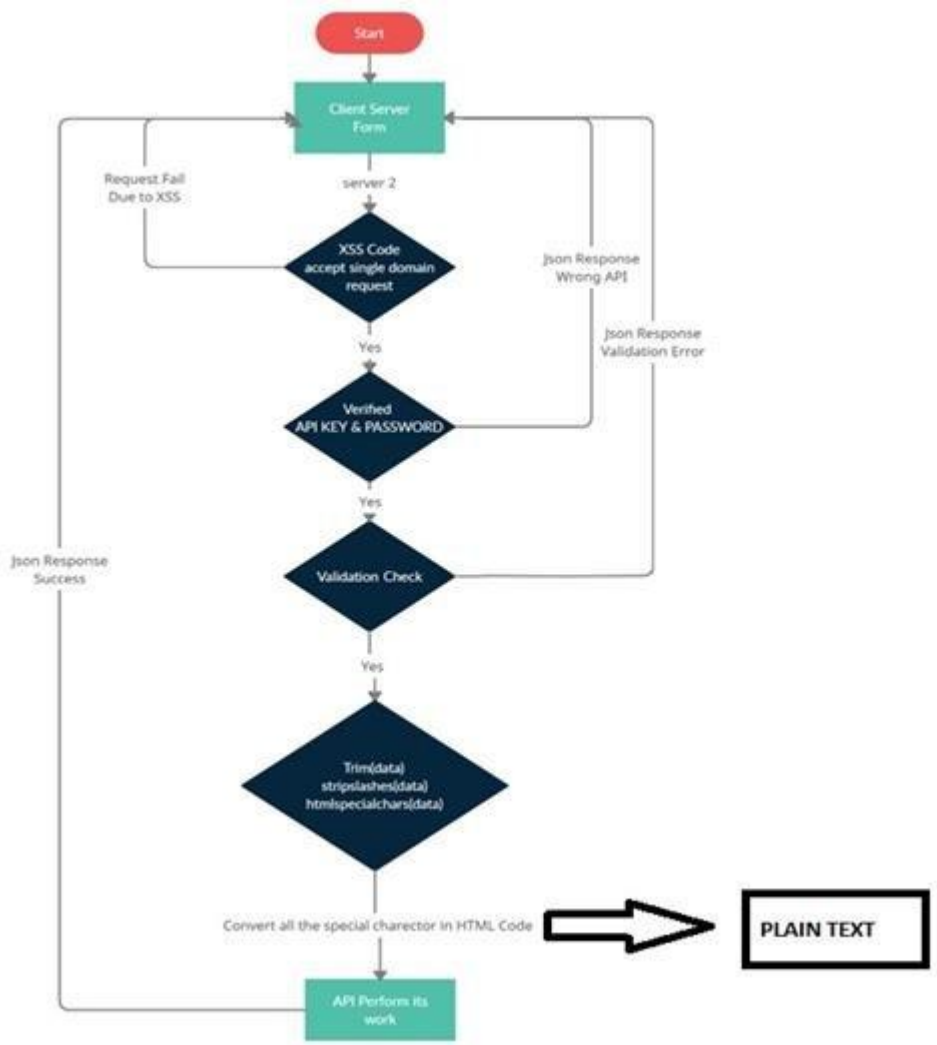
Prevention Measures

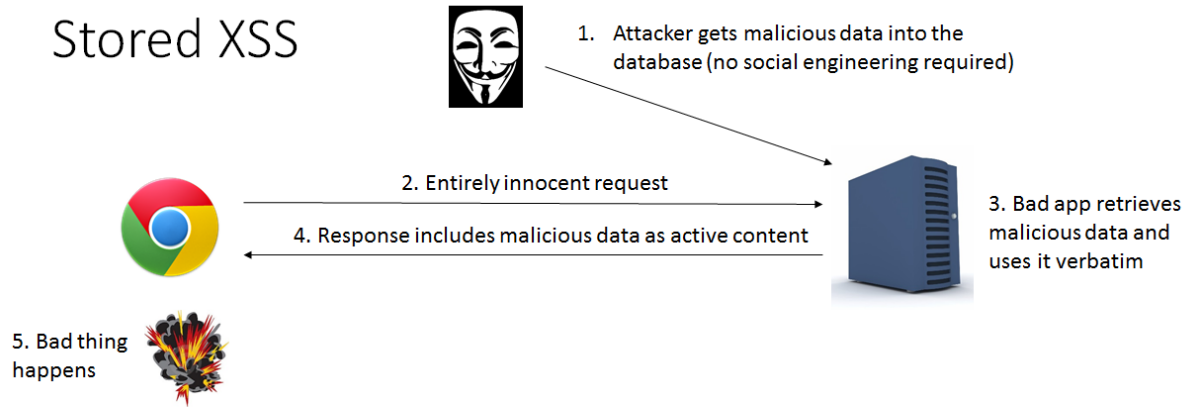
- Prepared statements / parameterized queries
- Input validation and sanitization
- Web Application Firewalls (WAF)
- Least privilege database access
- Secure coding practices

---

4. Cross-Site Scripting (XSS)







4

What is XSS?

Cross-Site Scripting (XSS) is a vulnerability where attackers inject **malicious JavaScript** into trusted websites, which executes in the victim's browser.

How XSS Works

1. Website allows unfiltered user input
2. Attacker injects JavaScript code
3. Code is executed when another user visits the page
4. Attacker steals cookies, session tokens, or performs actions as the victim

---

Types of XSS

- **Stored XSS** – Malicious script stored in database
- **Reflected XSS** – Script reflected via URL/request
- **DOM-based XSS** – Client-side execution via JavaScript

Impact of XSS

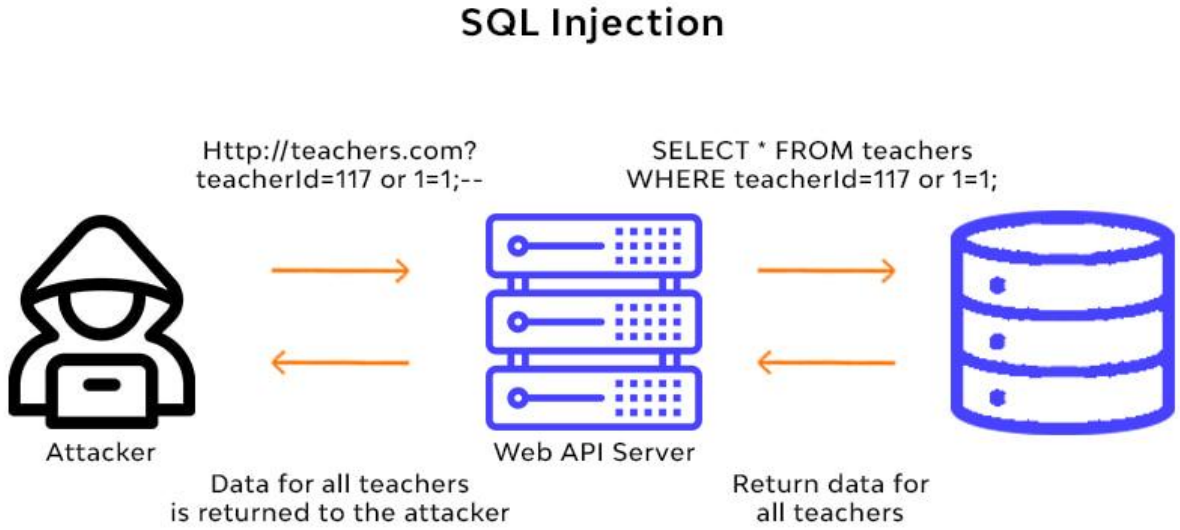
- Session hijacking
- Credential theft
- Website defacement
- Malware delivery

Prevention Measures

- Input validation and output encoding
- Content Security Policy (CSP)
- Escaping user-generated content
- Secure JavaScript handling

---

5. Real-World Breach Example (SQL Injection)



TalkTalk Data Breach (2015)

Attack Type: SQL Injection
Organization: TalkTalk (UK telecom company)

What Happened

- Attackers exploited a **SQL Injection vulnerability**
- Gained access to customer databases
- Exposed personal and financial data of ~157,000 customers

Data Compromised

- Names

- Addresses
- Dates of birth
- Bank account details

Impact

- Financial losses (~£60 million)
- Heavy regulatory fines
- Severe reputational damage
- Loss of customer trust

Key Lessons Learned

- Secure coding is critical
- Input validation cannot be ignored
- Regular security testing is mandatory
- Web applications are high-value targets

Conclusion

Understanding cyber attacks such as **Phishing, Brute Force, SQL Injection, and XSS** is essential for any cybersecurity professional.
Each attack exploits **different weaknesses**:

- **Humans** (phishing)
- **Authentication** (brute force)
- **Application logic** (SQLi, XSS)

A strong security posture combines:

- Technical controls
- Secure development
- User awareness
- Continuous monitoring