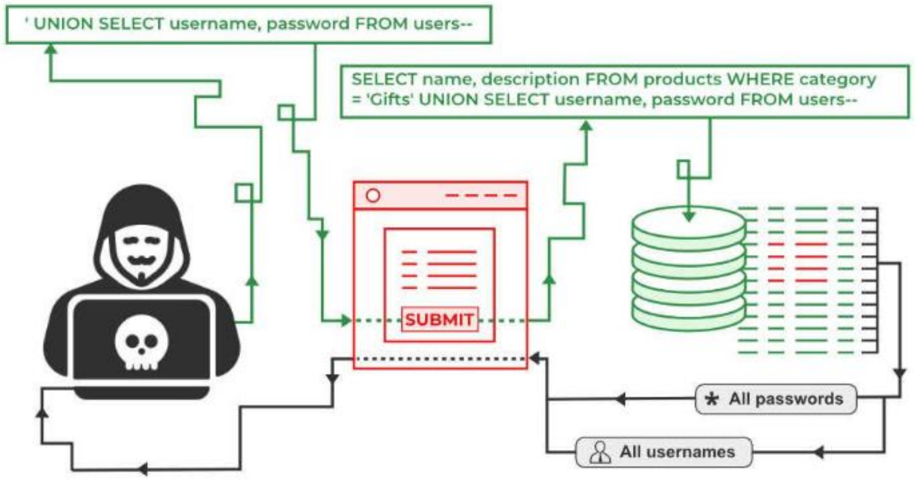
Web server Attacks

Week 2 Task 2

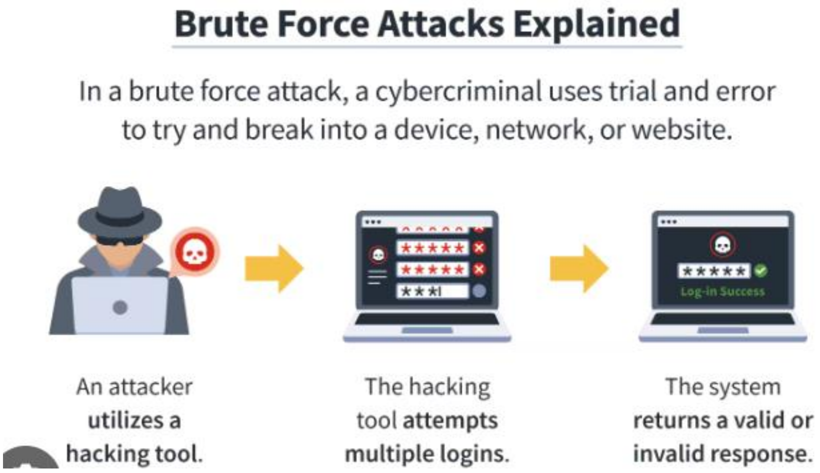
1. **SQL Injection**



' UNION SELECT username, password FROM users--
SELECT name, description FROM products WHERE category = 'Gifts' UNION SELECT username, password FROM users--
SUBMIT
All passwords
All usernames

SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.

2. **Brute force attack**



Brute Force Attacks Explained

In a brute force attack, a cybercriminal uses trial and error to try and break into a device, network, or website.

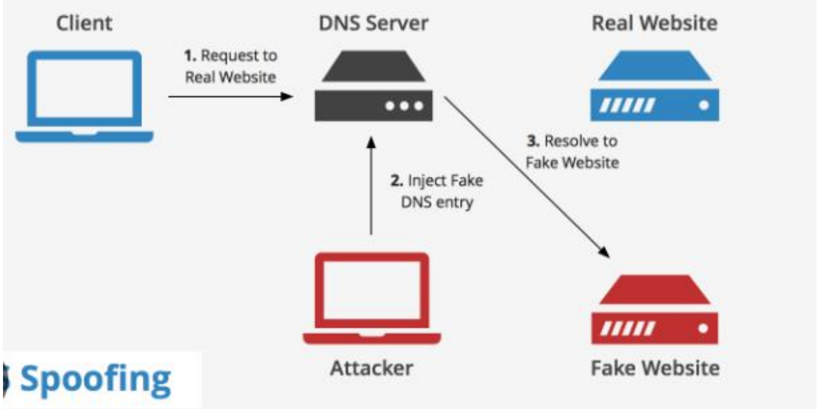
An attacker utilizes a hacking tool.

The hacking tool attempts multiple logins.

The system returns a valid or invalid response.

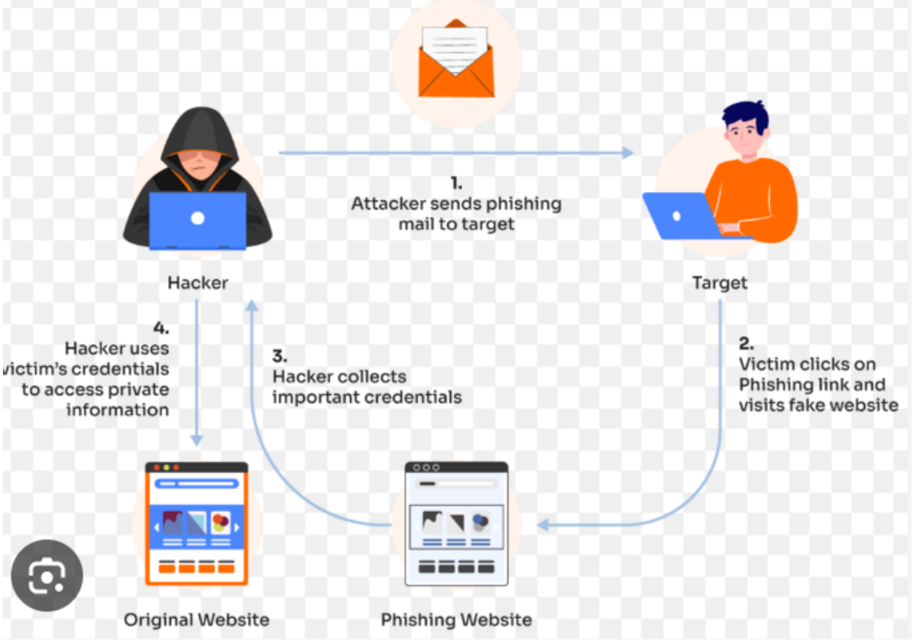
A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

3. **DNS Spoofing**



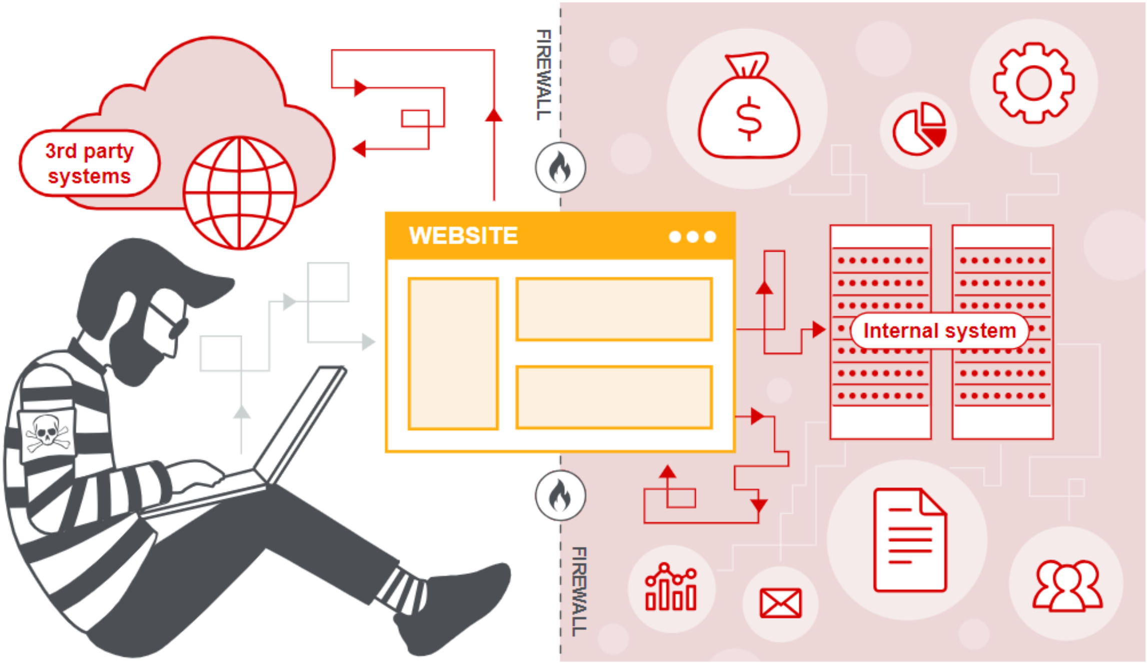
Domain Name Server (DNS) spoofing, or DNS cache poisoning, is an attack involving manipulating DNS records to redirect users toward a fraudulent, malicious website that may resemble the user's intended destination.

4. **Phishing attack**


Hacker
1. Attacker sends phishing mail to target
Target
2. Victim clicks on Phishing link and visits fake website
3. Hacker collects important credentials
4. Hacker uses victim's credentials to access private information
Original Website
Phishing Website

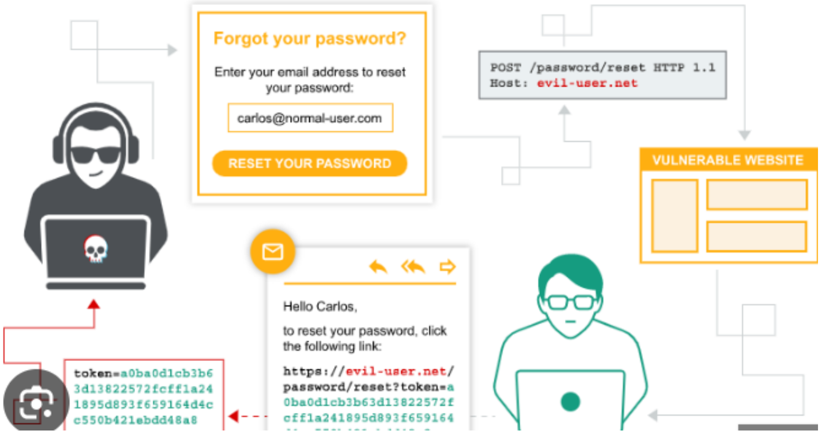
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

5. **Server - side request forgery attack**



Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location.

6. HTTP **Host header Attacks**



Forgot your password?

Enter your email address to reset your password:

carlos@normal-user.com

RESET YOUR PASSWORD

```
POST /password/reset HTTP 1.1
Host: evil-user.net
```

Hello Carlos,

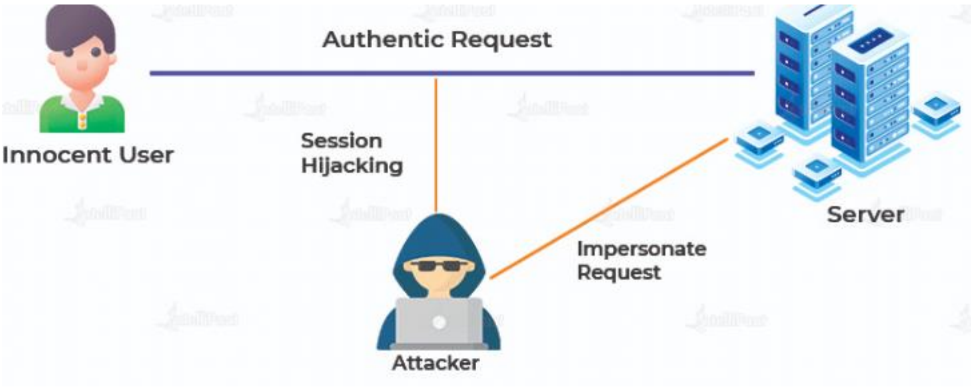
to reset your password, click the following link:

```
https://evil-user.net/
password/reset?token=a
0ba0d1cb3b63d13822572f
cffla241895d893f659164
```

```
token=a0ba0d1cb3b6
3d13822572fcffla24
1895d893f659164d4c
c550b421ebdd48a8
```

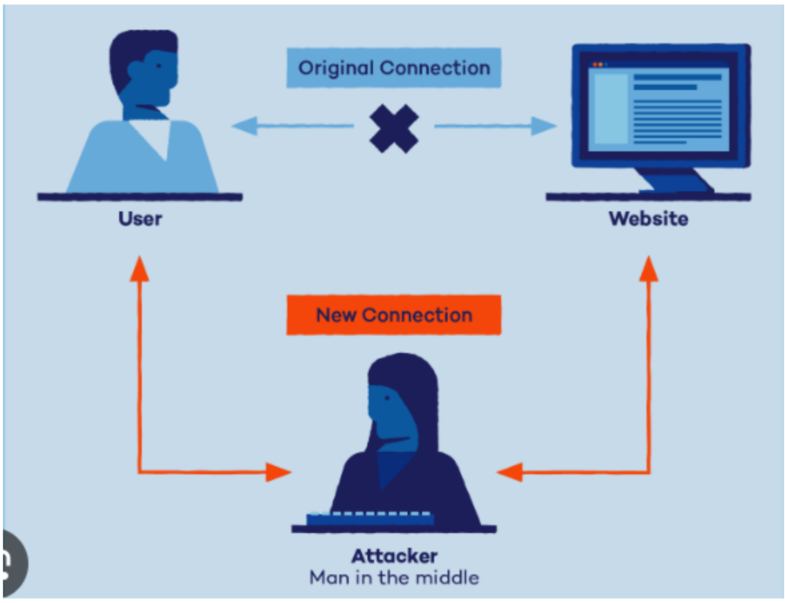
HTTP Host header attacks exploit vulnerable websites that handle the value of the Host header in an unsafe way. If the server implicitly trusts the Host header, and fails to validate or escape it properly, an attacker may be able to use this input to inject harmful payloads that manipulate server-side behavior.

7. Session Hijacking



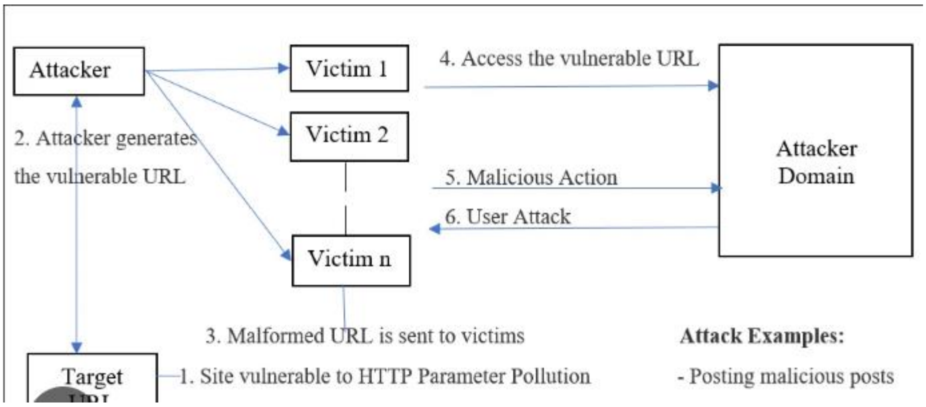
When the tracking of these states is based on poor mechanism, session hijacking becomes easy for the hackers. It is also called cookie hijacking because a web server determines the session with a user based on the cookie.

8. Man in the middle attack



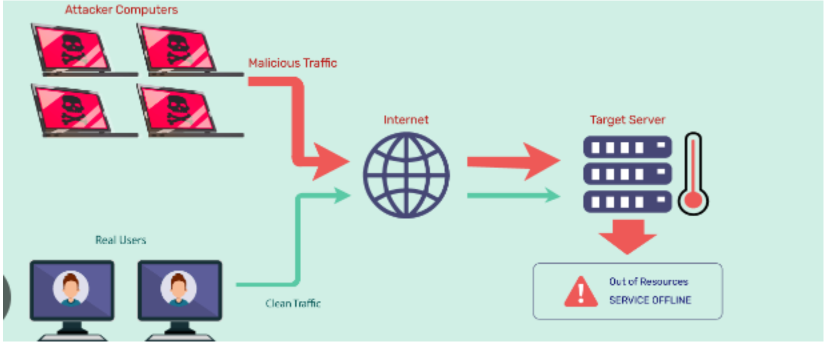
A man-in-the-middle (MiTM) attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

9. Http parameter pollution


Attacker
Victim 1
4. Access the vulnerable URL
Victim 2
2. Attacker generates the vulnerable URL
Attacker Domain
5. Malicious Action
6. User Attack
Victim n
3. Malformed URL is sent to victims
Attack Examples:
Target URL
1. Site vulnerable to HTTP Parameter Pollution
- Posting malicious posts

HTTP Parameter Pollution (HPP) is an attack evasion technique that allows an attacker to craft an HTTP request to manipulate or retrieve hidden information. This technique is based on splitting an attack vector between multiple instances of a parameter with the same name.

10.DDoS Attack



DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.