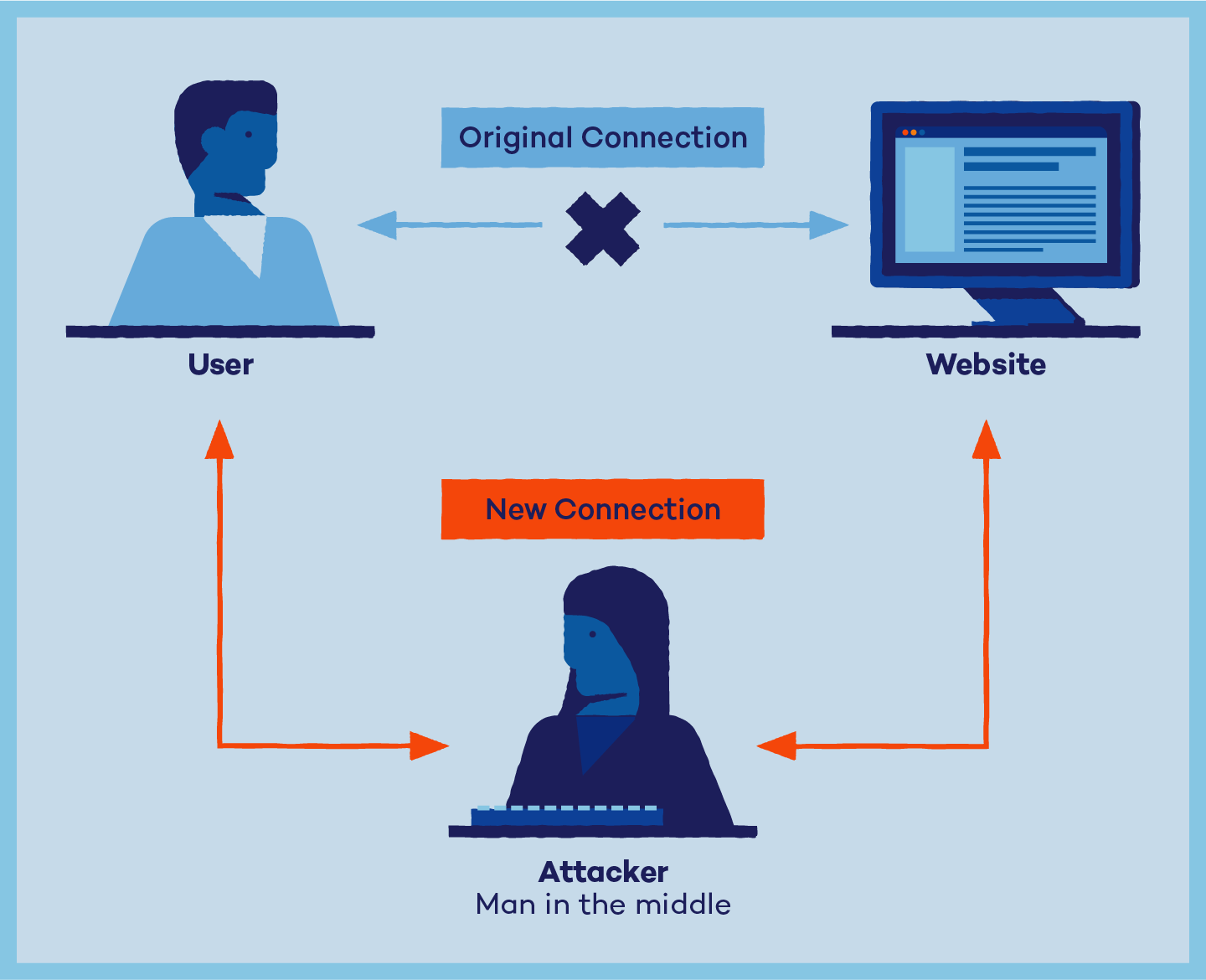
**TASK - 5**

[Bhumireddy Thanmaye 21BCI0013](mailto:bhumireddy.thanmaye2021@vitstudent.ac.in)

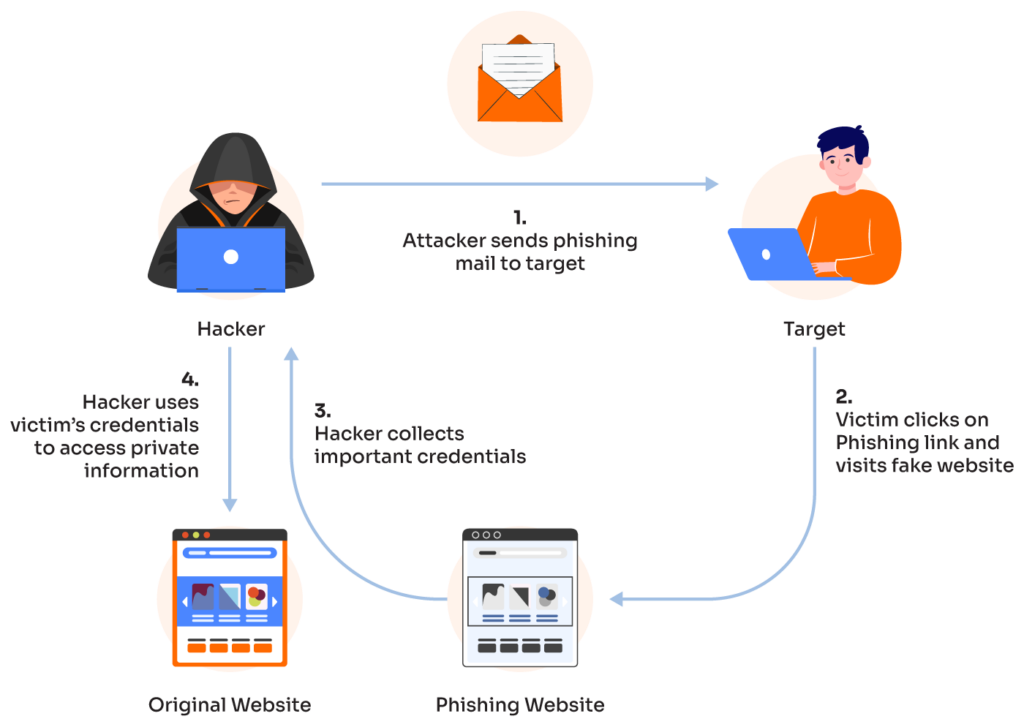
**Description of 10 Web Server Attacks**

**Explain about any 10 Web Server Attacks determine them with respective images if available**

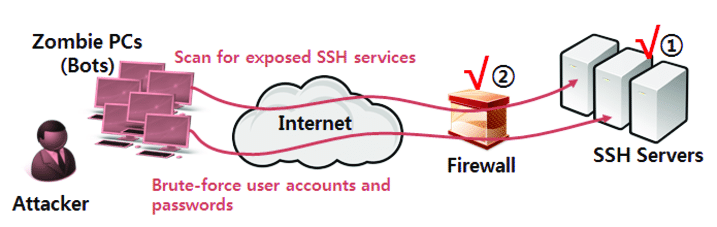
**1)MITM Attacks:** MITM attack allows an attacker to access sensitive information by intercepting and altering communications between an end user and web server.Attacker acts as a proxy such that all the communication between the user and the web server passes through the attacker

****

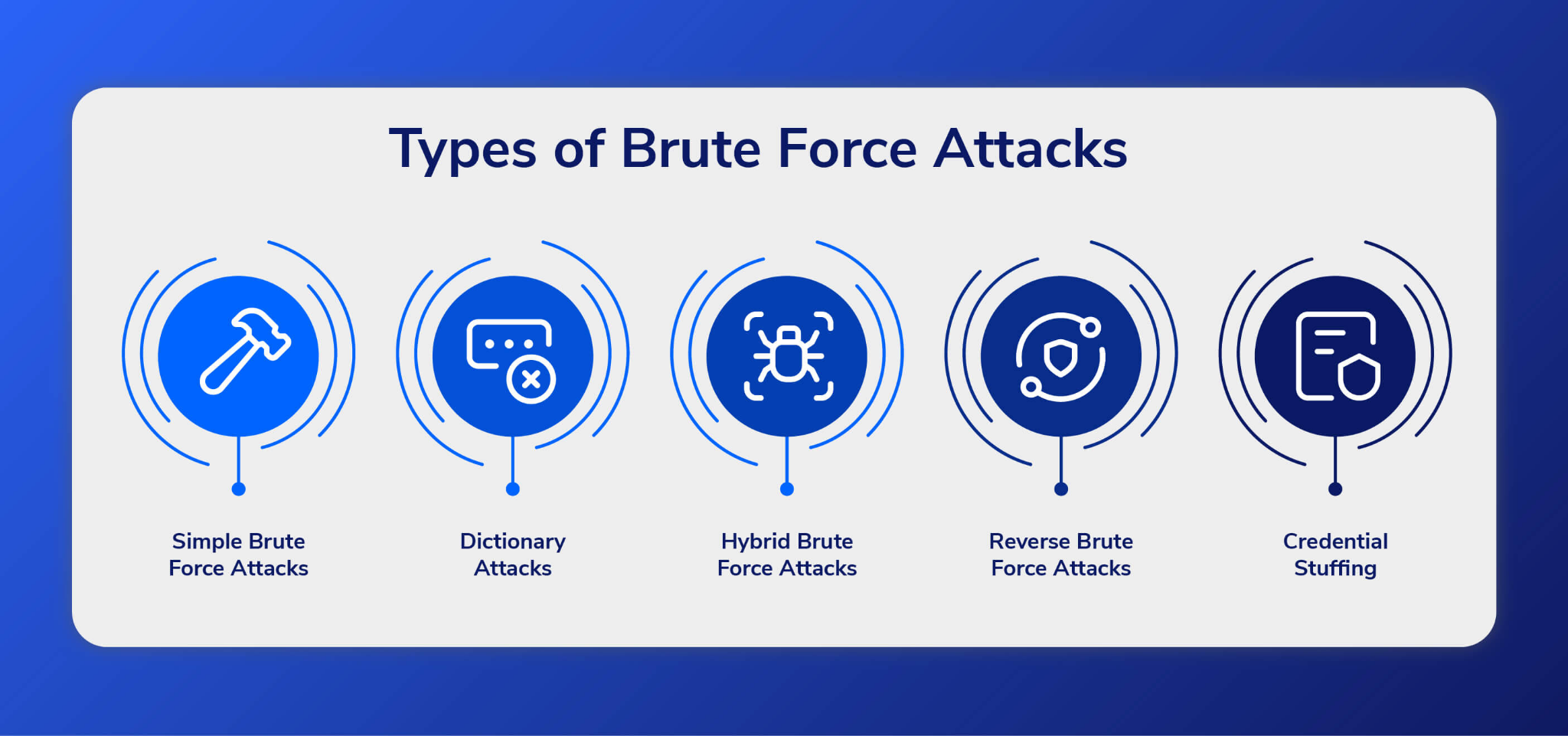
**2)Phishing Attacks:** Attackers tricks user to submit login details for website that looks legitimate but it redirect to the malicious website hosted on the attacker web server.Attacker steals credentials and uses them to impersonate the user.Attack can then perform malicious operations



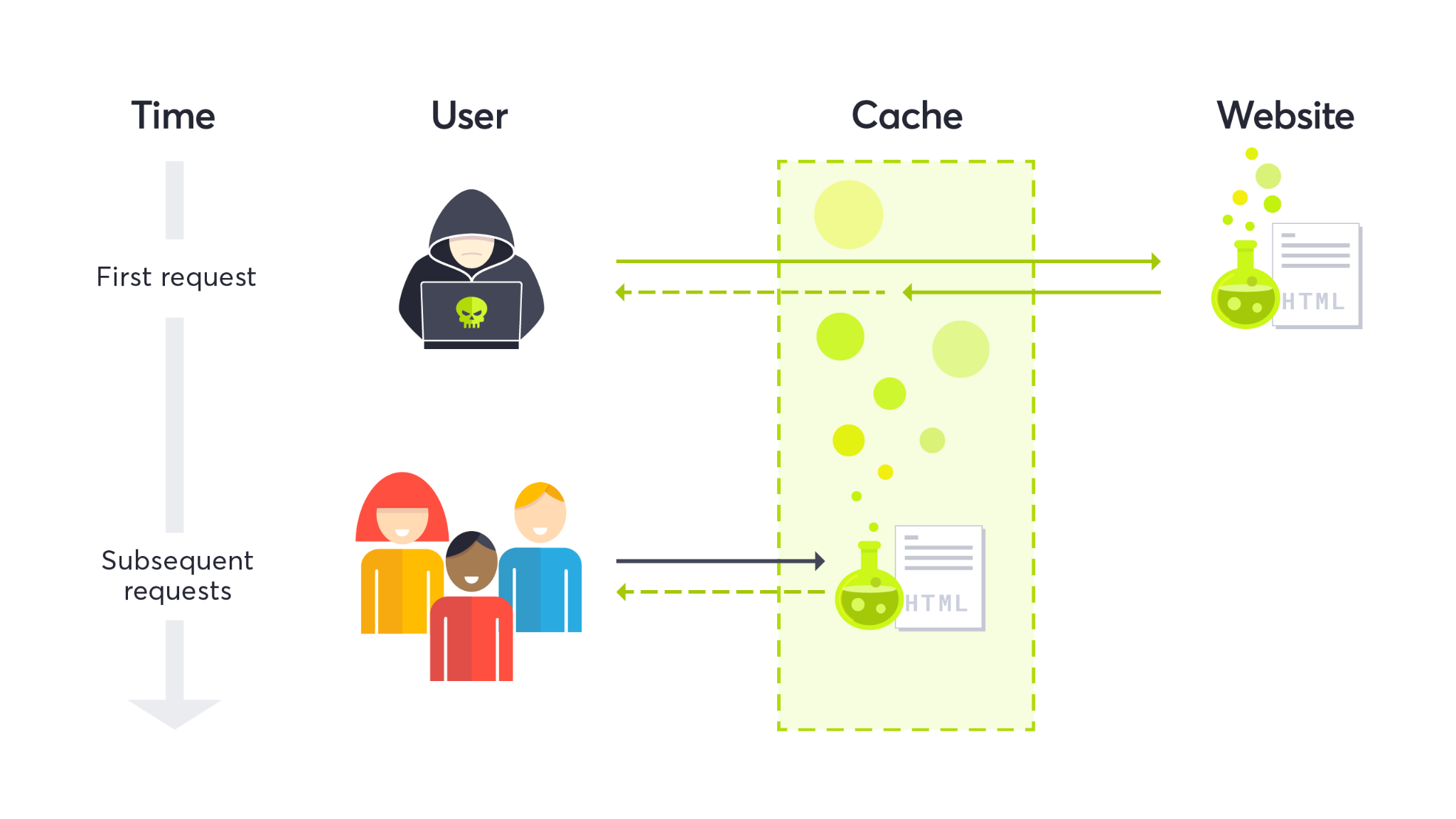
**3)SSH Brute Force Attacks:** SSH protocols are used to create an encrypted SSH tunnel between two hosts in order to transfer un-encrypted data over and insecure network.Attackers brute force the SSH login.SSH tunnels are used to transmit malware and other exploits to victims without being detected.



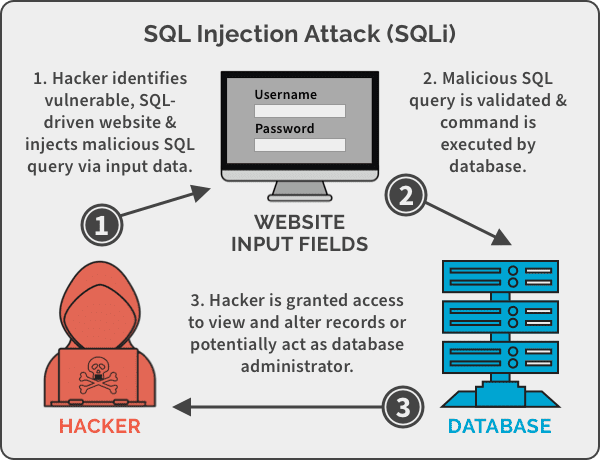
**4)Web Server Password Cracking Attacks:** Attacker tries to exploit weakness to hack well chosen passwords.Many hacking attempts start with password cracking to prove to the web server that you are a trusted user.Password can be cracked manually or by using automated tools

****

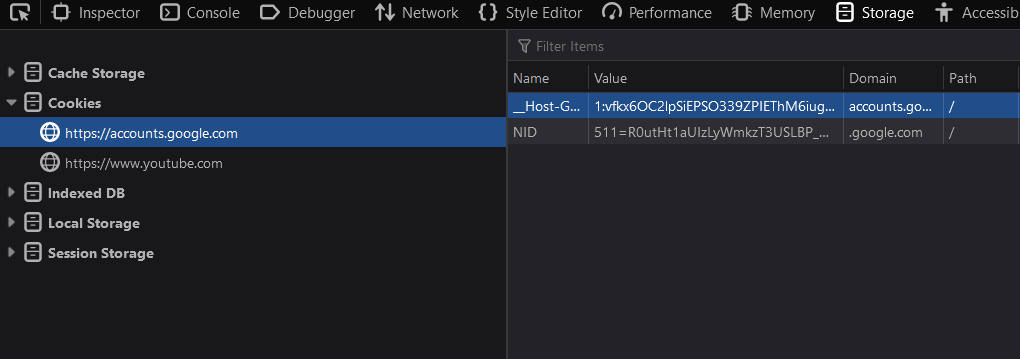
**5)Web Cache Poisoning Attack:** Attacks the reliability of an intermediate web cache source.Attacker swaps cached content for a random URL with infected content.Users of the web cache source and unknowingly use the poisoned content instead of the true content

****

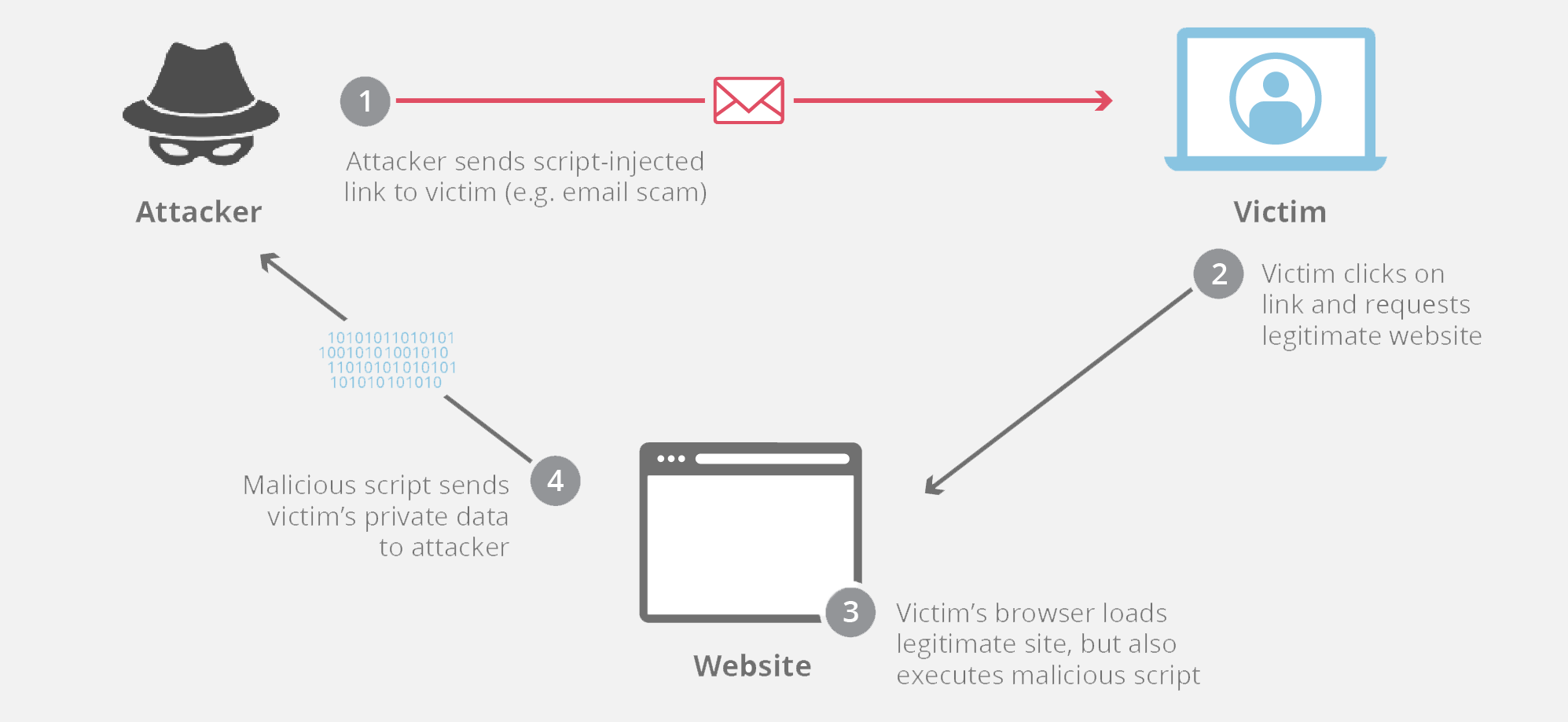
**6)SQL Injection Attacks:** SQL injection attacks exploits the security vulnerability of a database for attacks.Attacker injects malicious SQL code into a string that is later sent to the SQL server by the web server



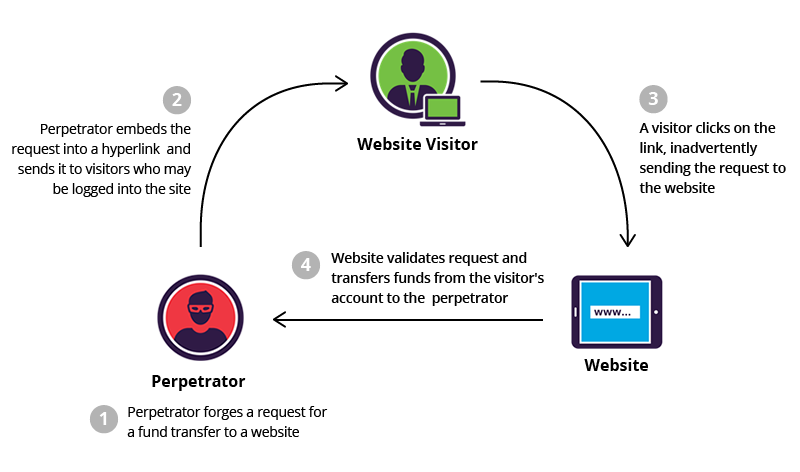
**7)Cookie Tampering:** Cookie tampering is a method in which the attacker manipulates or modifies the information of the stored data on a web browser. This includes all types of data like personal information (name, number, address), and credentials for certain websites, or it can be the settings for specific websites. It is intended to steal valuable information from users. Sends a modified cookie form the client side to the server



**8)Cross-Site Scripting (XSS) Attacks:** An exploit where the attacker attaches code onto a legitimate website that will execute when the victim loads the website. That malicious code can be inserted in several ways. Most popularly, it is either added to the end of a url or posted directly onto a page that displays user-generated content. In more technical terms, cross-site scripting is a client-side code injection attack.



**9)Cross-Site Request Forgery (CSRF) Attack:** Cross site request forgery (CSRF), also known as XSRF, Sea Surf or Session Riding, is an attack vector that tricks a web browser into executing an unwanted action in an application to which a user is logged in.A successful CSRF attack can be devastating for both the business and user. It can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft—including stolen session cookies..CSRFs are typically conducted using malicious social engineering, such as an email or link that tricks the victim into sending a forged request to a server. As the unsuspecting user is authenticated by their application at the time of the attack, it’s impossible to distinguish a legitimate request from a forged one.



**10)DoS/DDoS Attacks:**

Attackers may send numerous fake request to the web server which results in the web server crashing or becoming unavailable to the legitimate users.Attacker may target high profile web servers to steal user credentials

