CYBERSECURITY BOOTCAMP

GDG Algiers

Women Techmakers
Algiers

Client-side Security

Table of contents

1. What is client side?
2. Client side V Server side
3. Client side vulnerabilities
   a. XSS
   b. CSRF
   c. Other vulnerabilities
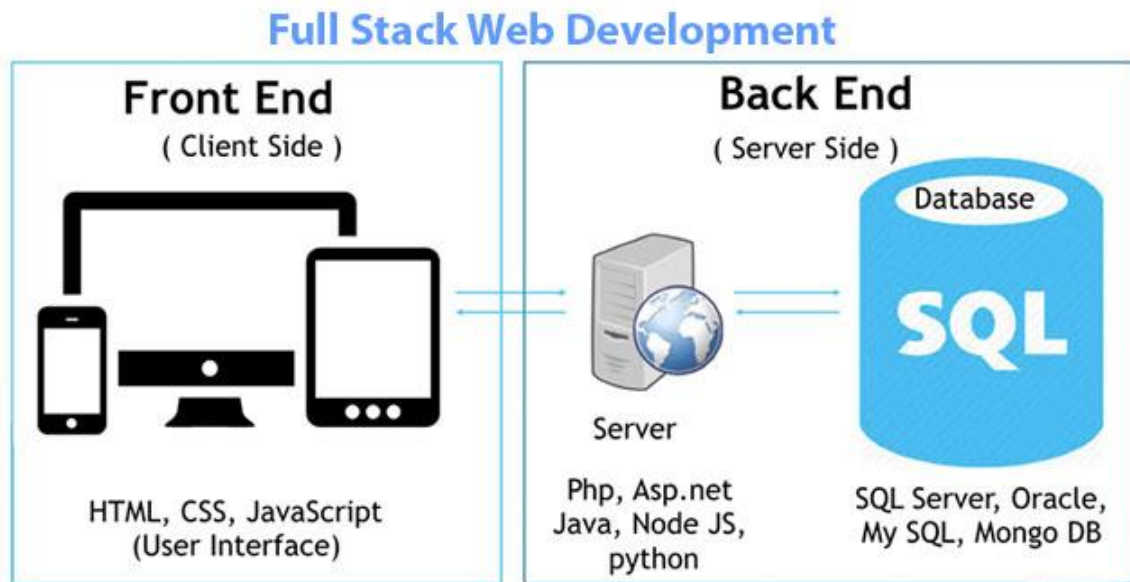4. SOP/CORS
5. Mitigations

What is client side?

Client-side architecture is a network topology that distinguishes clients or workstations requesting information from servers, as well as the hardware elements that provide that information and execute requests.

Client side V Server side

Full Stack Web Development

Front End
(Client Side)

HTML, CSS, JavaScript
(User Interface)

Back End
(Server Side)

Database

SQL

Server

Php, Asp.net
Java, Node JS,
python

SQL Server, Oracle,
My SQL, Mongo DB

Client-side vulnerabilities

1- Cross Site Scripting (XSS)

A type of client side code injection attack. The attacker intends to run <script>alert(1)</script>harmful scripts in the victim's web browser by embedding malicious code in a web page.
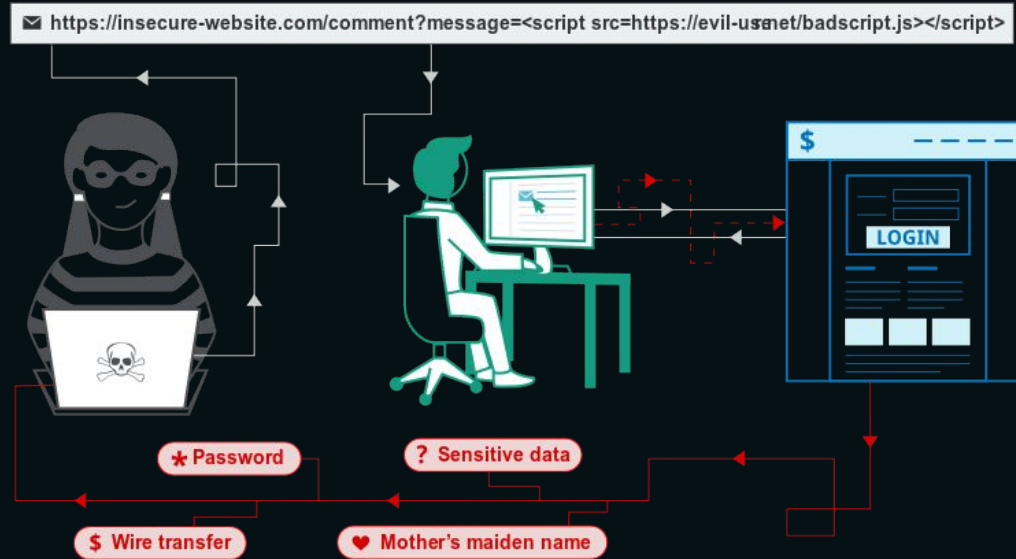
1- XSS impact

- Hijack a user's session
- Perform unauthorized activities
- phishing attacks
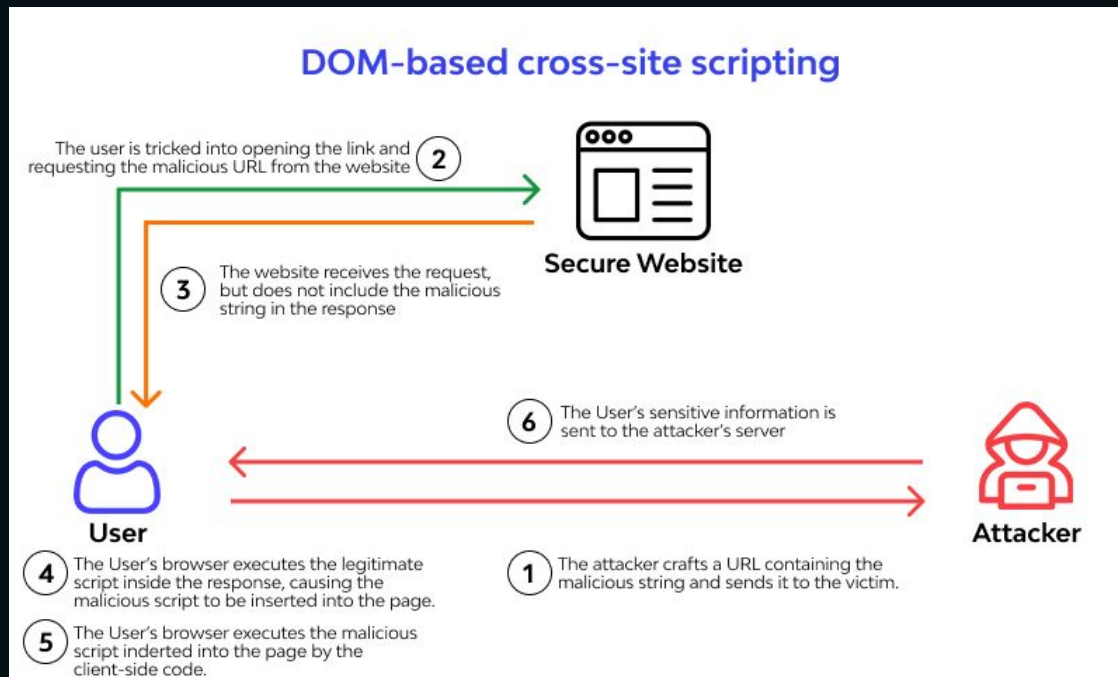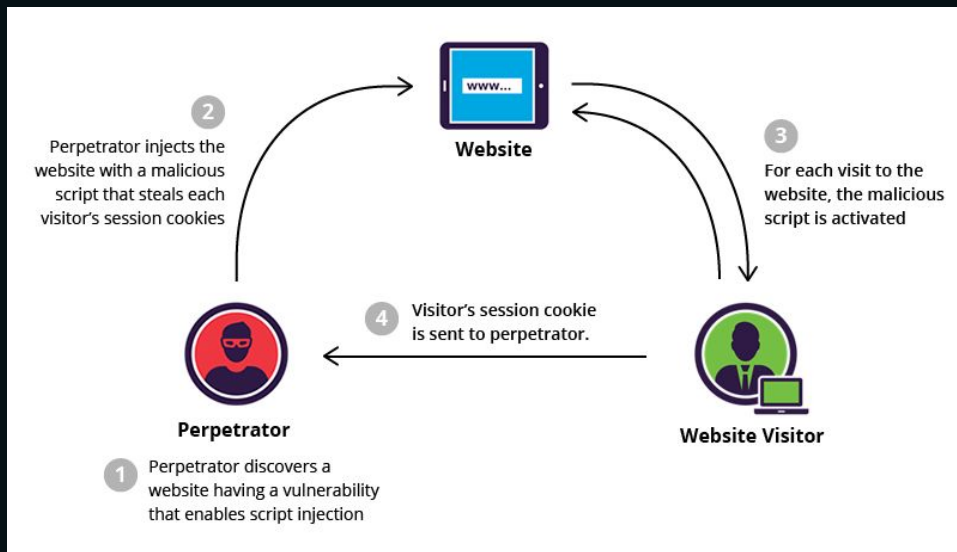- Steal sensitive information

1- XSS : Reflected

1- XSS : DOM based

DOM-based cross-site scripting

The user is tricked into opening the link and requesting the malicious URL from the website ②

③ The website receives the request, but does not include the malicious string in the response

Secure Website

⑥ The User's sensitive information is sent to the attacker's server

User

④ The User's browser executes the legitimate script inside the response, causing the malicious script to be inserted into the page.

⑤ The User's browser executes the malicious script inderted into the page by the client-side code.

① The attacker crafts a URL containing the malicious string and sends it to the victim.

Attacker

1- XSS : Stored

Website

2 Perpetrator injects the website with a malicious script that steals each visitor's session cookies

3 For each visit to the website, the malicious script is activated

4 Visitor's session cookie is sent to perpetrator.

Perpetrator

1 Perpetrator discovers a website having a vulnerability that enables script injection

Website Visitor

2- Cross Site Request Forgery (CSRF)

CSRF is an attack in which the attacker makes the target user unwittingly do an action while they are authenticated.
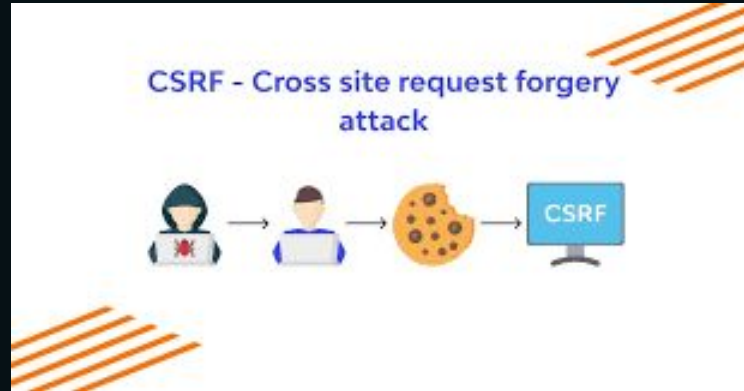
2- Cross Site Request Forgery (CSRF)

2- CSRF impact

- Transform money
- change emails
- change roles
- perform privilieged actions

3- Other vulnerabilities

- Clickjacking
- XS-leaks
- DOM-clobbering
- Broken link hijacking
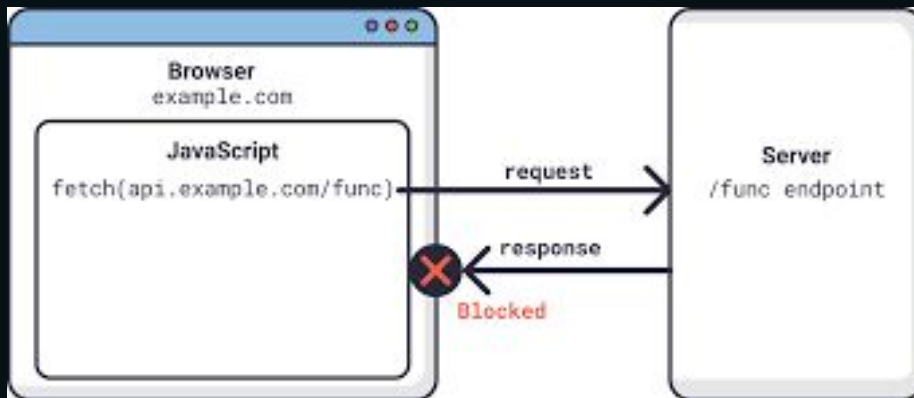- Client side : open redirection
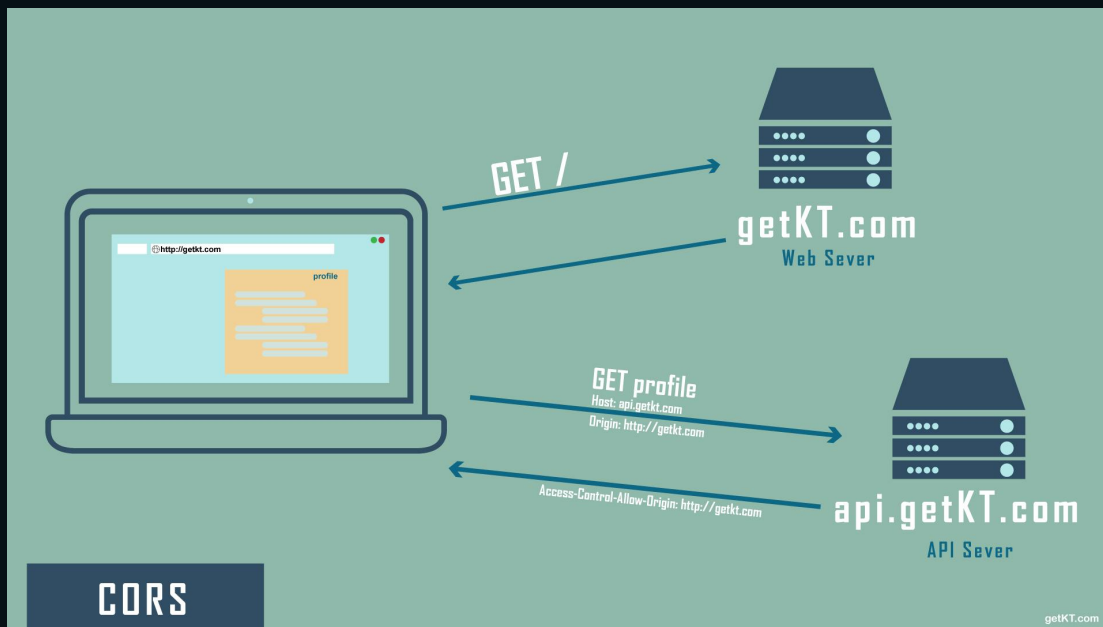
SOP/CORS

1- Same Origin Policy (SOP)

A security mechanism that restricts how a document or script loaded from one origin interacts with a resource from another.

2- Cross Origin Resource Sharing (CORS)

The mechanism that gives the possibility and regulates access to resources from another origin.

Mitigations

Mitigations

- Never trust user input
- XSS :
    - Sanitize user input
    - HTTPOnly cookies
    - Using CSP
- CSRF Token

Ressources

- CTF
  - Root-me
  - HTB
  - ringzer0
- PwnFunction
- LiveOverflow
- Bug Bounty Reports Explained
- The hacker playbook 3

Thank you