**GENERAL CONFEDERATION OF LABOR OF VIETNAM**

**TON DUC THANG UNIVERSITY**

**FACULTY OF INFORMATION TECHNOLOGY**


# MIDTERM ESSAY

# WEB AND APPLICATION PROGRAMMING

## *Topic name:*

# WEBSITE SECURITY

**Instructing Lecturer: MR. BHAGAWAN NATH**

**Student's name: MAI THẾ GIA BẢO – 520H0513**

**HUỲNH VĂN ĐỆ – 520H0036**

**NGUYỄN CHÁNH TÍN – 520H0587**

**NGUYỄN TRUNG TÍN – 520H0589**

**Course : 24**

**HO CHI MINH CITY, 2022**

# ACKNOWLEDGEMENT

In order to get a complete and good report like this, our team has received enthusiastic help from lectures and classmates.

My team would also like to thank for the helpful knowledge and enthusiastic help from lecturer Mr. Bhagawan Nath. Thank you, Mr. Nath, for being so enthusiastic in teaching, educating, equipping us with the necessary knowledge and creating the most favorable conditions for us to complete this report.

And also thank Ton Duc Thang University for giving us a modern and developed educational environment.

With hard work and effort we have successfully completed this report. But surely, this report cannot avoid mistakes. We are looking forward to receiving from teacher so that we can improve it better.

We sincerely thank you!

# THE PROJECT WAS COMPLETED
# AT TON DUC THANG UNIVERSITY

We pledge that this is a product of our own project and is under the guidance of Mr. Bhagawan Nath. The content of research, results in this subject is honest and not published in any form before. The data in the tables used for the analysis, comment, and evaluation were collected by the authors themselves from various sources indicated in the reference section.

In addition, many comments and assessments as well as data from other authors and organizations have been used in the project, with references and annotations.

**If any fraud is found, we are fully responsible for the content of our project.** Ton Duc Thang University is not involved in any copyright infringement or copyright infringement in the course of implementation (if any).

Ho Chi Minh, May 25th 2022

Author

Mai Thế Gia Bảo

Huỳnh Văn Đệ

Nguyễn Chánh Tín

Nguyễn Trung Tín

# EVALUATION OF INSTRUCTING LECTURER

**Confirmation of the instructor**

_____

_____

_____

_____

_____

_____

_____

Ho Chi Minh City, 2022

(sign and write full name)

**The assessment of the teacher marked**

_____

_____

_____

_____

_____

_____

_____

Ho Chi Minh City, 2022

(sign and write full name)

# SUMMARY

The report includes chapters giving an overview of common security holes for a website, how "hackers" attack websites or steal user information through these vulnerabilities as well as remedial and preventive measures. Recommendations on what to do and what to avoid when developing and deploying a website.

The report introduces an overview of common security vulnerabilities such as SQL

Injection, XSS Scripting, CRFS, Clickjacking, DDOS.

# TABLE OF CONTENTS

# LIST OF FIGURES

# CHAPTER 1 – TOPIC OVERVIEW

## 1.1 Introduction

### *1.1.1 Reality:*

When web applications developing very quickly in all aspects, widely applicable, security issues for web applications are also more focused. Despite the undeniably advanced enhancements available today, the issue of security in web applications continues to grow. The cause may stem from inappropriate code snippets. Many serious weaknesses or vulnerabilities allow hackers to directly penetrate and access the database to extract sensitive data. Many databases contain valuable information (such as personal details, financial information) making them a frequent target for most hackers because of the huge profits from data acquisitions.

### *1.1.2 Website security situation 2021*

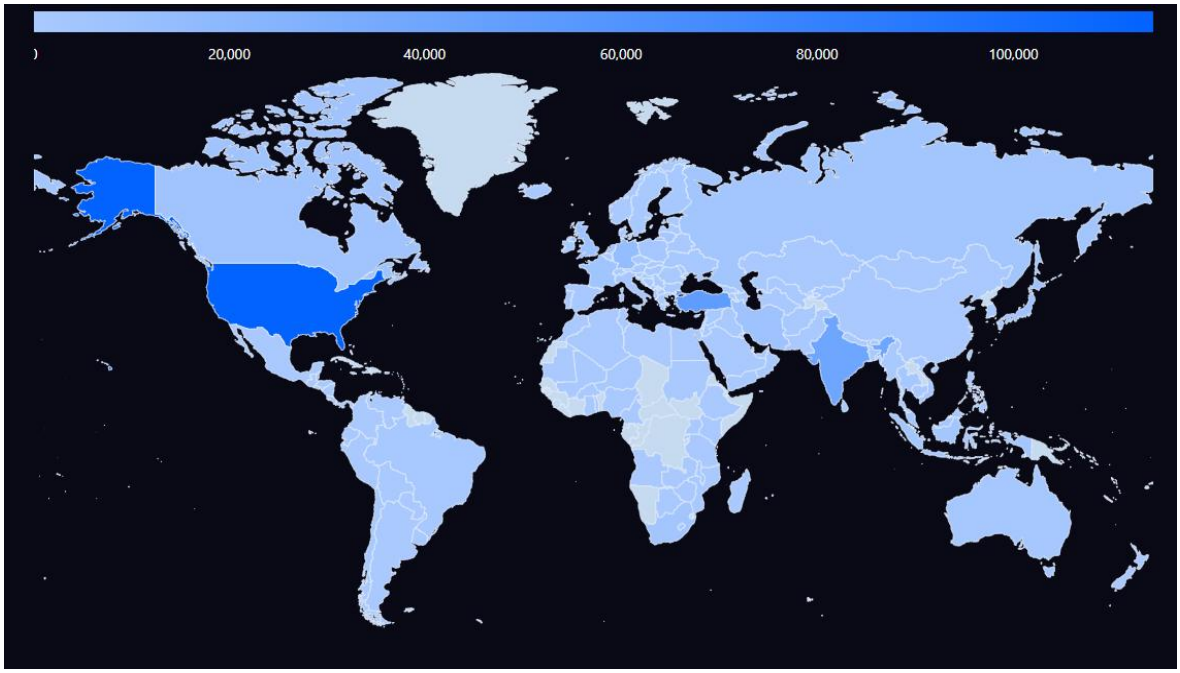


*Figure 1: Density map of hacked websites around the world*

According to the CyStack Attack Map (January 1st, 2021 - December 31th, 2021), there are more than 322,000 attacks on websites globally in 2021. In Vietnam, we have up to 2,852 hacked websites. On average, more than 200 websites are compromised every month - equivalent to 8 websites being hacked

every day. Previously, in 2020, Vietnam is ranked 14th in the country with the most cyberattacks with a total of 4,627 attacks.


*Figure 2: Top 15 countries with the most website attacks in the world (According to CyStack Attack Map)*

Compared to 2020, the number of attacks in 2021 has decreased, but the scale of attacks tends to increase. larger than the same period last year.

In Vietnam, more than 90% of hacked websites are commercial websites and websites of businesses and organizations (.com and . vn).

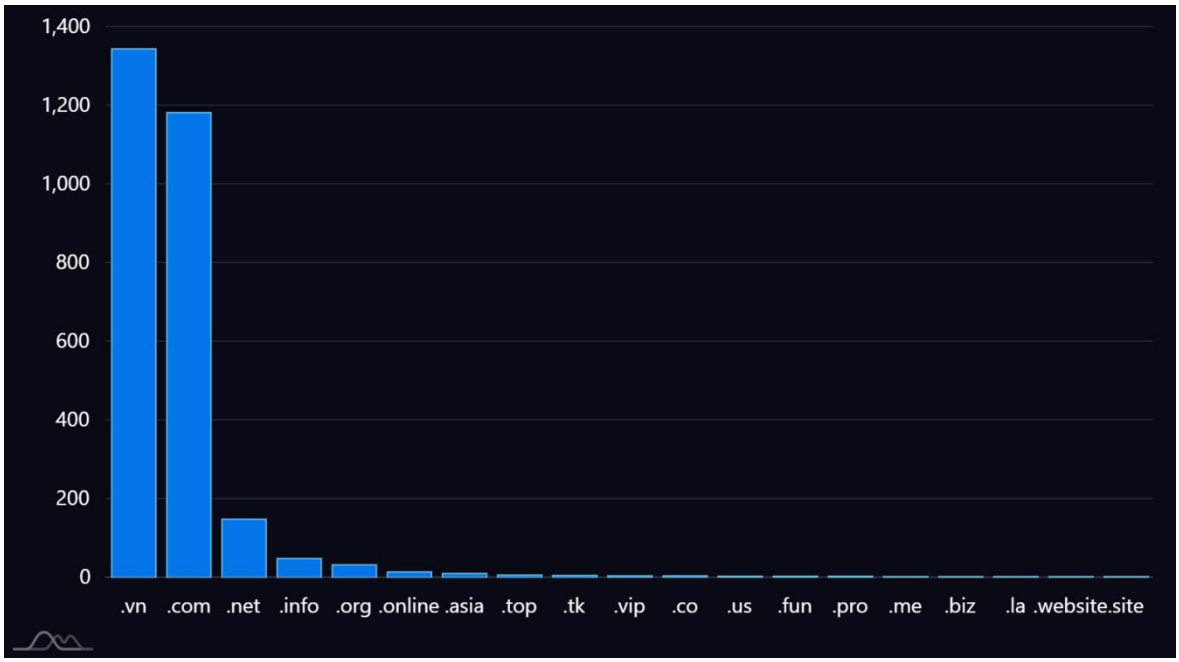


*Figure 3: Number of website attacks in Vietnam by Domains*

*(According to CyStack Attack Map)*

The data in the report shows that WordPress continues to be the most attacked content management platform (Content Management Systems) in Vietnam - accounted for 72,02%. Right after that is Elementor 13,22% and DNN 12%.

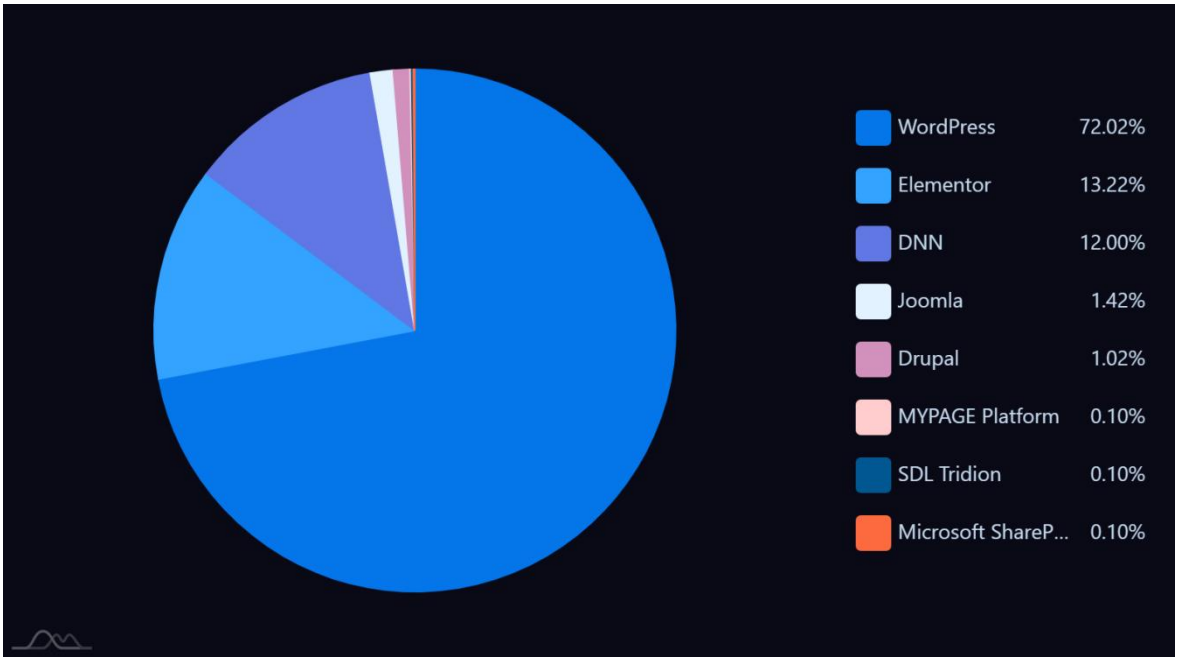


*Figure 4: Number of website attacks in Vietnam by Content Management Systems (According to CyStack Attack Map)*

### *1.1.3 The harms when the website is hacked*

- Interrupting the operation of the website

Your website is inaccessible will definitely lose the number large existing customers. This number of customers will gradually disappear into the hands of your competitors.

The inactivity of the web means that the web will not be able to run ads, affecting the effectiveness of promoting products of businesses, reducing sales, and losing revenue.

- Information leak

If the website is not well secured, an attacker can steal sensitive user data from our website. In the business sector it is possible to lose data on business strategy and will fall to rival businesses. In the political field, if you lose personal information, it will be difficult to manage information about people in a country.

- Loss of Google Search Rankings

If your website is infected with a virus or malware, Google will not list your page in the search engine. This directly affects the online marketing of the website.

- Negative effects on the brand

Websites that are constantly inaccessible or reported for viruses will lead to a decrease in customer trust. Damage to business reputation and brand is considered one of the huge consequences.

From being aware of the danger of security holes in websites and their consequences for individuals, business organizations, countries... our group chose the topic "Understanding website security" web".

**1.2 Objectives of choosing the topic**

The main objective of the main topic is to bring website security knowledge closer to everyone, to help readers have a better overview of the current situation of website attacks, to gain a deeper understanding of the situation. Some concepts of website attack, some common website vulnerabilities.

**1.3 The significance of the topic**

In today's economy, for many industries and services, a well-secured website has the potential to generate higher profits for the business, improve its reputation and help make the most of the resources available to the business.

Avoiding security holes helps countries better manage and access personal data, stabilize the economy as well as social security by reducing the amount of cybercrime.

Equipping with knowledge about website security to help individuals manage their information as well as important data, improving work performance.

**1.4 Scope of the topic The topic**

is done based on knowledge of web security, experimenting on the web platform with HTML, CSS, Javascript, PHP.

# CHAPTER 2: POPULAR WEB SECURITY VULNERABILITIES AND PREVENTION

## 2.1 Concept, classification and meaning of the website

With the strong and continuous development of the information technology industry at the present time, especially is the Internet has appeared many types of websites. Figuring out what a website is all about in the current era is probably not a difficult task. Normally, we just need to turn on the computer, open the web browser, and then type the website address to read information, buy goods ... but now to ask what the website is, many people may find it awkward to find the answer.

### *2.1.1 What is a Website?*

Website, also known as website, is a collection of information in text, digital, images, audio, video clips ... of an organization, individual or business located on a main domain name or subdomains on the World Wide Web of the Internet and hosted on a server system (web server).

### *2.1.2 What types of websites are there?*

Depending on the content and usage features of the website, people can divide the website into many different types.

- Classification by data:

1. Static web: is a web with data that does not change or change little. This website does not have a content management system and users cannot edit or change any data.
2. Dynamic Web: is a web with a content management system and users can easily edit or update data. This is the type of website that is recommended to be used to sell or PR products, ...

- Categorized by object:

1. Business Web: Enterprises use to promote, introduce information, advertise products, and at the same time update updates. Update information for the purpose of reaching customers.
2. Personal Web: Popular personal web is used by celebrities, artists, singers, graphic designers, this is where they interact with fans, PR for themselves.

- Classification by form of use:

1. Web news: developed on the basis of traditional newspapers but expanded on the Internet by high user interaction and faster time.
2. E-commerce Web: was established with the purpose of convenience for information reference and online purchase and sale, limiting time for buying and selling goods and can be purchased anytime, anywhere.
3. Forum: is the most powerful place to interact with users because everyone can comment and exchange on a certain issue.
4. Social network: this is the website with the largest number of users today because of its popularity and independence. Each person has their own account and can post personal information, interact, chat, call, make friends, post photos, etc.

### *2.1.3 What does the website mean?*

Website is not only increasingly popular but also an indispensable tool for every business and individual doing business today. This is a quick and convenient way to advertise information to everyone. On the other hand, the website is an important step in the company's marketing strategy. For individuals, the use of the website is a simple and fast way to access news, information about products and services and collect information from important business partners and especially with entertainment anytime, anywhere.

## 2.2 Overview of Web Site

Vulnerability A vulnerability is a weakness in a system or contained in a service that the system provides that allows an attacker to exploit, damage, and hijack resources. illegal.

## 2.3 Common Vulnerabilities

### *2.3.1 XSS*

#### 2.3.1.1 Introduction to XSS

XSS (Cross site scripting) is a common vulnerability in web applications that allows hackers to embed malicious code (Javascript) into another web page. . . Hackers can take advantage of this malicious code to deface websites, install keylogs, bypass access controls and impersonate users.

XSS is one of the most common security mistakes on websites.

#### 2.3.1.2 Common types of XSS errors XSS

classification:

- Stored XSS (targeting more victims): Hackers take over sessions of mass users and submit content with malicious code.
- Reflected XSS (direct attack on the victim targeted by the hacker): The hacker takes over the user's session.
- DOM-based XSS: Exploiting an XSS vulnerability by changing the structure of the DOM.

Stored XSS

- This error occurs when the web application does not carefully check the input data before saving it in the database, for example: comment forms, comments, etc.
- Hackers do not need to exploit directly, but do it through two steps:
  - Step 1: Through the input points (form, input, textarea) do not check carefully to insert malicious code.
  - Step 2: The user accesses the website and performs operations related to this saved data, the hacker's malicious code will be executed on the user's browser.

  Victims will not know that the data they access has been infected.

The malicious code is stored in a web database, so whenever the user accesses it, the read code will be executed.

More dangerous than Reflected XSS

Reflected XSS

- Hacker inserts malicious code into the URL as a querystring.
- If the user clicks on this URL, the website will read the querystring, render the malicious code into the HTML, and the user will get the malicious code. The
- server responds to the victim, with the data contained in the request.
- The victim's browser receives the response and executes the Javascript.
- Hacker will capture the above request and consider the user's session to be occupied. Hackers can masquerade as the victim and exercise all the rights on the website that the victim has.

DOM-based XSS

- Based on changing the DOM structure of a document like HTML.
- First, the user logs in, then the hacker sends the exploit URL to the user. When the user accesses the URL, the server responds then the user's session is sent to the hacker and the hacker captures the user's session.

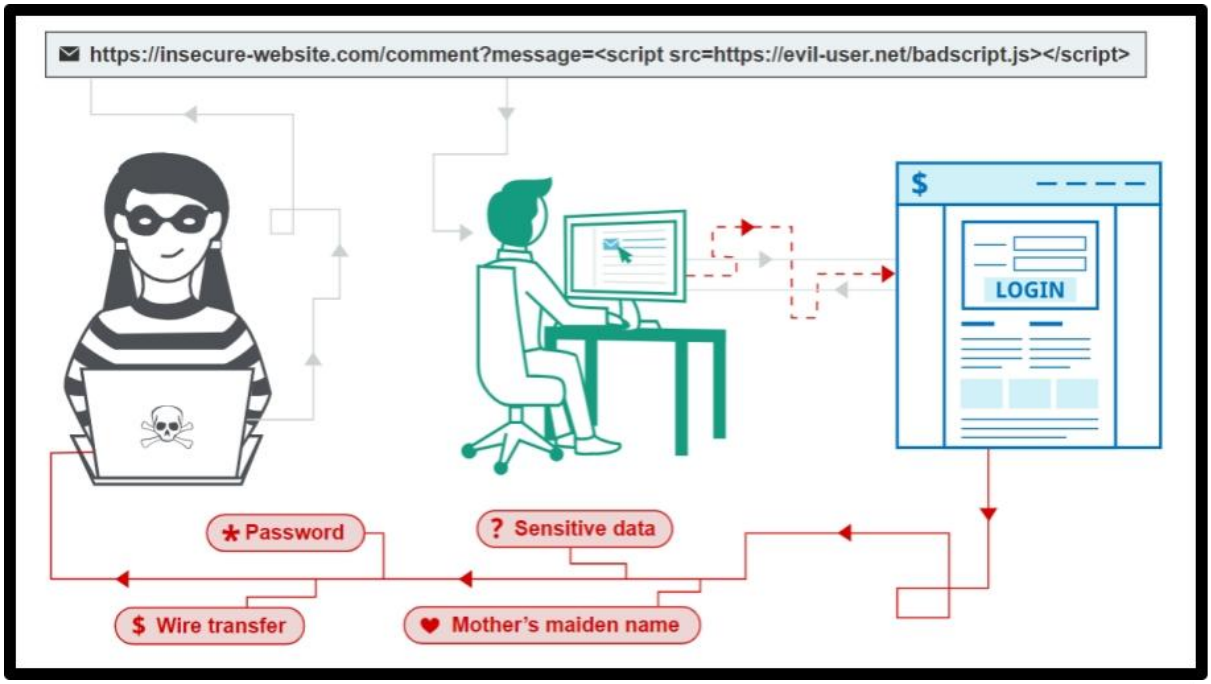


*Figure 5: Cross-Site Scripting (XSS)*

#### 2.3.1.3 Prevention

There are several ways to prevent XSS:

Filtering: there are two filtering processes, input filtering and output filtering. Each filtering process will have 2 different types of filtering: White-List Filtering and Black-List Filtering.

- White-List Filtering: allows pre-defined a valid list, only when entering the correct type of list will it be performed.
- Black-List Filtering: filter predefined definitions in a given list, when an invalid request is encountered, it will cancel, not perform the request.

Data encryption: converting data into different forms to increase data security. If the data is stolen, it will take a long time to decrypt the data.

Data usage: there are many libraries that help us to prevent XSS, but we need to learn these types of libraries to know more about their functions.

Instead of using innerHTML, outerHTML, document.write functions, use textContent instead.

Using a web application firewall (web application firewall)

```php
<?php
    $db=mysqli_connect('localhost','root','','xss',3306);
    if(!$db){
        die("h1 Can't connect to database!h1)");
    }
    $content="<script>alert('Hello World!')</script>";
    $content=htmlspecialchars($content);
    // change to:&lt;script&gt;alert('Hello World!')&lt;/script&gt;gt;
    $content=mysqli_real_escape_string($db,$content);
    // change to:&1t;script&gt;alert(\'Hello World!\')&lt;/script&gt;gt;
?>
```

*Figure 6: Fix XSS error*

### *2.3.2 SQL Injection*

#### 2.3.2.1 Introduction to SQL Injection

SQL Injection (Structured Query Language) is a technique that allows attackers to take advantage of a vulnerability of SQL injection. input checking in web applications and the error messages returned by the database administration system, done by inserting illegal SQL to falsify the original query , from which it is possible to exploit data from the database (to make the conditions in the SQL statement always true.

SQL Injection can allow attackers to perform webmaster-like operations on the web application whose data is managed by database management systems such as SQL Server, MySQL, Oracle, DB2, Sybase, ...

#### 2.3.2.2 Common SQL Injection error types

- Do not check query escape characters

Here is a type of SQL Injection error that occurs when the code that checks the input data in the SQL query is missing,

resulting in the end user c Some unexpected queries may be made against the application's database.

- Improper handling

This is a type of SQL Injection error that occurs when the programmer defines the input data incorrectly or lacks input data type checking and filtering to verify the type of the data entered by the user. Is it a number or not?

- Blind SQL Injection

This type of SQL injection error is a type of error that exists in a web application but whose consequences are not visually visible to attackers. It can cause errors when displaying the content of a page containing this security bug.

The result: making it take a lot of time for the programmer or user to recover every bit of data. Attackers can also use a number of tools to detect this type of error and attack with pre-configured information.

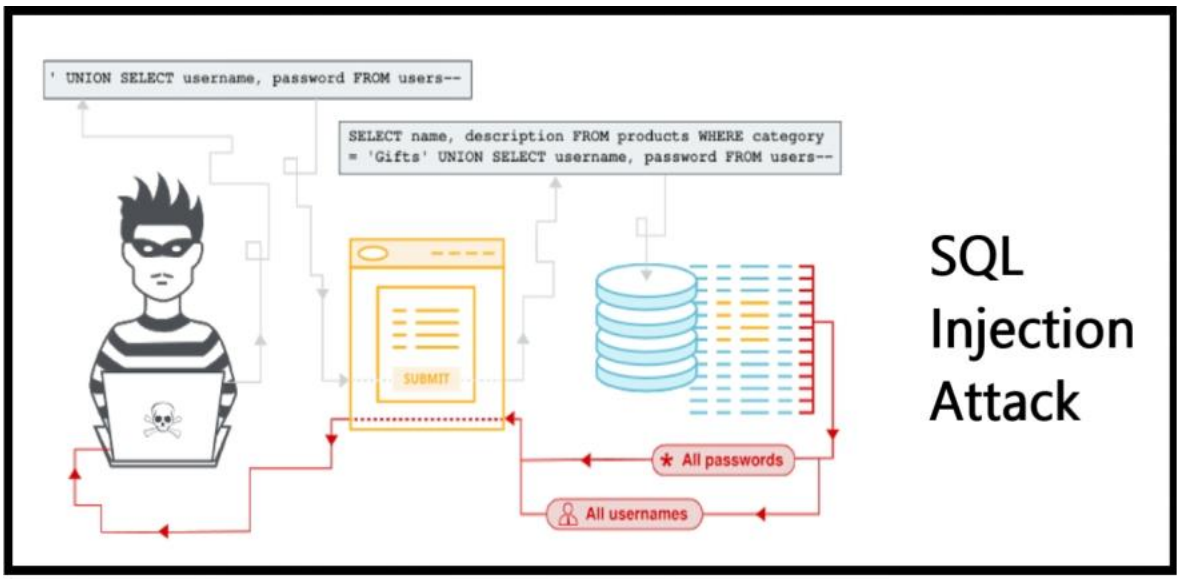


*Figure 7: SQL injection attack*

**2.3.2.3 Some common attacks with web applications**

There are 4 common types of attacks including: bypassing the login check, using SELECT statements, using INSERT statements, using Stored-Procedures .

**In this**

type of attack, an attacker can easily bypass login pages through errors when using SQL statements to manipulate the web application's database.

**Type of attack using SELECT statement**

This type of attack is more complex. To perform this type of attack, an attacker must be able to understand and take advantage of loopholes in error messages from the system to detect weaknesses that initiate attacks

**. INSERT**

Usually web applications allow users to register an account to participate. An indispensable function is that after successful registration, users can view and edit input information.

**Type of attack using Stored procedures**

An attack with stored procedures will cause great harm if the application is executed with 'sa' system administrator privileges.

#### 2.3.2.4 Consequences of

SQL Injection cause many serious consequences for users, most notably:

- Leaking data in the database, depending on the importance of the data, the consequences can be moderate. to a serious extent.
- Revealing customer data, affecting the company and customers. Customers can switch to other services, leading to bankruptcy of the company.
- In many cases, hackers can not only access the data but can also modify the data.

#### 2.3.2.5 Prevention

There are several ways that can be used to prevent SQL Injection vulnerabilities:

- Filtering data from users: ta Use filter to filter special characters or keywords (SELECT, UNION) entered by the user.
- Use Store procedures in the database. Briefly understood as putting SQL queries into the procedure (almost like functions in programming languages), data is passed into the procedure through parameters separating the data from the code.

- Do not display exception or error message: because hackers rely on error messages to find out the structure of the database and then find a method to penetrate the user's database.
- Regularly back up data: if a hacker deletes data, we still have a "backup" to be able to restore lost data.
- Decentralize access in the database: this makes it impossible for hackers to read the data. Just create an account in the database and assign access rights only to that account.

### *2.3.3 CSRF*

Website security is very important. There are many common types of attacks that seriously affect websites, CSRF is one of them. If we are a programmer, we need to understand CSRF to ensure the security of our website.

#### 2.3.3.1 Concept of CSRF

CSRF (Cross Site Request Forgery) is an attack technique by using user authentication rights to a website.

CSRF refers to a web request authentication attack through the use of Cookies. This is where hackers use some tricks to make requests without the user's knowledge.

=> This is an attack technique based on unauthorized borrowing.

#### 2.3.3.2 How it works

First, the user must log in to the website they need. After that, the hacker will carefully study the URLs and create a malicious website. When the user accesses that malicious website, a request will be sent to the page that the hacker wants to attack (through forms, images, ...) Since this request contains cookies of the user, the destination website will be mistaken. that this is a request made by the user. Hackers rely on it to impersonate users and perform intrusive actions, stealing user data information.

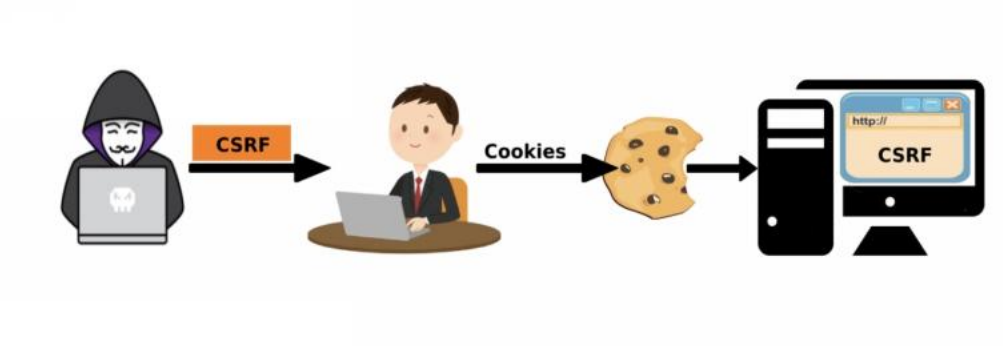


Figure 8: CSRF attack

#### 2.3.3.3 Ways to prevent

- User side:

Should log out from important websites: Bank account, online payment, social networks, gmail... when the transaction is done.

Do not click on links that you receive via email, via facebook.

Do not save password information in your browser. Do not choose the methods "login next time", "save password" ...

In the process of making transactions or visiting important websites, do not visit other websites, which may contain exploit codes of attackers. . .

- Server side:

Using captcha, confirmation messages: Captcha is used to identify whether the object that is working with the system is human or not.

Important functions such as resetting the password, confirming the change of account information should also send the URL via the registered email so that the user can click to confirm.

Use CSRF_token: this token will change continuously during the session, and when changing information, attach this token information. If the token generated and the token sent do not match, discard the request.

Use separate cookies for the admin page: It is recommended to leave the admin page in a separate subdomain so that they do not share cookies with the product front-end

IP inspection: Some important systems only allow access from designated IPs built-in, or only allow administrative access via local IP or VPN.

### *2.3.4 DDOS*

#### 2.3.4.1 DDOS concept

DDOS is a distributed denial of service attack (distributed denial of service attack) that prevents legitimate users of a certain service from accessing and using the service, attackers Work does not come from one computer but from many machines.

#### 2.3.4.2 How to attack

- Hackers take control of computers on the network, download and install malicious programs on that computer, the hacker will have a network of computers for attack
- . , then redirect to attack that target.
- Hacker issues an attack command from his computer, all networks of computers to attack that target will simultaneously attack the target.

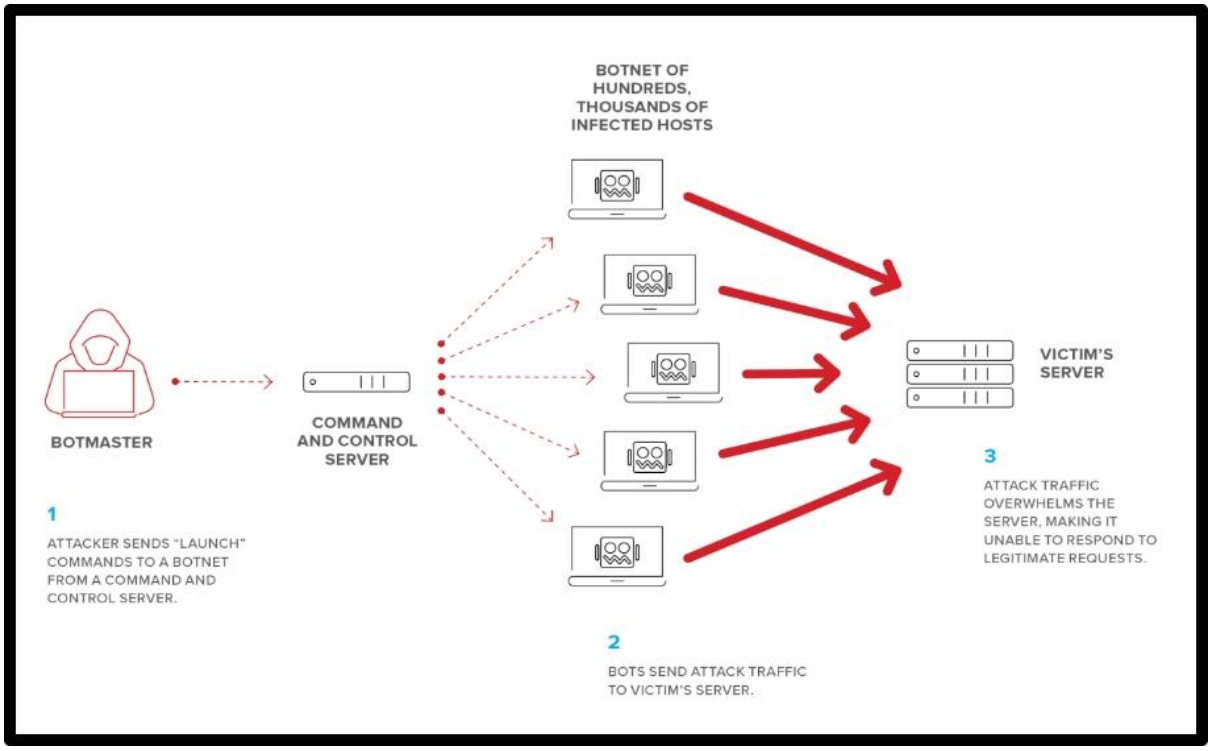


*Figure 9: Distributed Denial of Service (DDOS)*

#### 2.3.4.3 Classification

Experts often divide ddos attacks into two types

- Flood attack: Flood attack: Agents will send a large amount of packets, causing the victim system to slow down, hang, and be unable to respond to valid requests.

Amplification attack: the attacker will ping to the address of a certain network where the source address is the address of the victim. At that time, all reply packages will be transferred to the IP address of the victim machine. Amplification attacks aim to use the directed broadcast feature of routers to amplify and determine attacks. This feature allows the sender to specify an IP address for the entire recipient subnet , the router will be tasked with sending to all IP addresses in subnet that packet it gets

- Attack depletes system resources
- SYN overflow attack:

Syn flood attack is a form of denial-of-service attack, with an attacker successfully sending SYN requests to the target system. The attacker flooded the victim system with SYN packets. This results in the victim machine taking a long time to open a large number of TCP sessions, send the SYN-ACK, and wait for the ACK response never to be . come.

Once a SYN overflow attack has been carried out, the attacked system will receive a multitude of SYN packages sent in, while the system's ability to respond is restored. there are limits, and the system will deny legal access.

It is also possible to classify attacks on the 7-tier OSI model:

- IP attack aimed at bandwidth - attack on the network layer
- TCP attack on socket server - transport floor attack
- HTTP attack on web server - application floor attack
- Attack on web application - attack on application floor

**2.3.4.4 Variants**

- Flash DDoS type attack:

Hackers will directly launch a remote mass attack through a control channel. With the scale of the attack network consisting of hundreds of thousands of computers, this type of attack can take down any system . Combined with the ability to forge IP addresses , this type of attack is also quite difficult to trace the attacker.

- DRDoS type attack:

Distributed Reflection Denial of Service (DRDoS) is the most dangerous type of attack in the DdoS family. The goal of DRDoS is to take up the entire bandwidth of the victim system, i.e. completely block the connection from the server to the internet and do it. drain server resources. During the DRDoS attack, no client was able to connect to that server. All services running on the TCP/IP platform such as DNS, HTTP, FTP ... They are all disabled.

- DDoS attack on mobile phones:

Mobile DDoS attack methods also cause subscribers to constantly receive incoming calls. Other valid subscribers can't call the hacked subscription because the machine is always busy. It's also hard to make outgoing calls because there's always a phone call coming in.

#### 2.3.4.5 How to Prevent

Install and constantly update antivirus software, it is recommended to use paid antivirus software to ensure high security

Install a firewall, configure the firewall to limit strange access from the outside and go from your computer out.

Use an e-mail filter to limit the receipt of strange emails, malicious emails, or unwanted access .

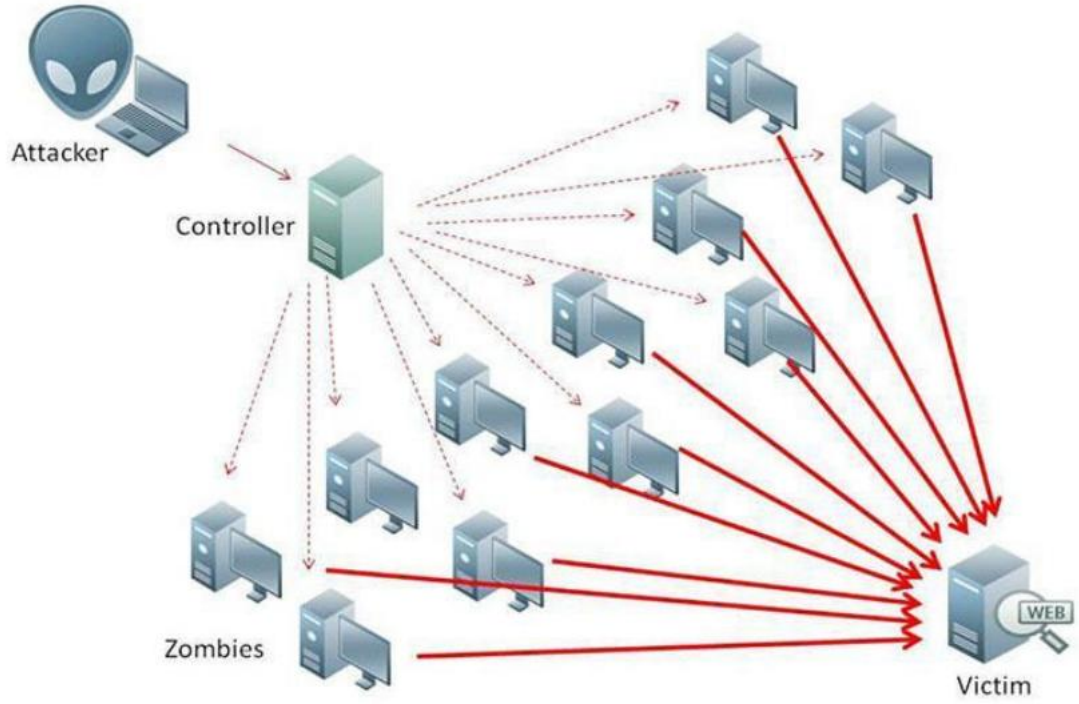


*Figure 10: Fix DDOS Vulnerability*

### *2.3.5 Clickjacking*

#### 2.3.5.1 Clickjacking Concept

Clickjacking is a form of attack that fools users by clicking on an object on the web, hackers can steal user accounts, trick clicks Go to advertising to make money.

#### 2.3.5.2 How Clickjacking Works

- Interact with a hidden frame:

Hackers will create a website, which contains a hidden frame (transparent with the user) and the displayed content will trick the user into clicking on a Or something on the website. At that time, the user did not know that they were working with a malicious website located in the iframe. And through that iframe hackers can steal the user's information or perform other operations.

- Use JavaScript:

Through JavaScript, hackers can control the location of the mouse pointer and the user's mouse clicks. At the same time, it is possible to change the location of any object on the website, making it mandatory for users to click on the locations containing the links. The malware is on that site without even knowing it. From there, hackers can also create a seamless multi-click attack, which means that after some mouse clicks, the hacker will stop attacking and strangely return control of the cursor to the user, making the user unrecognizable .

- Attack through software vulnerability.

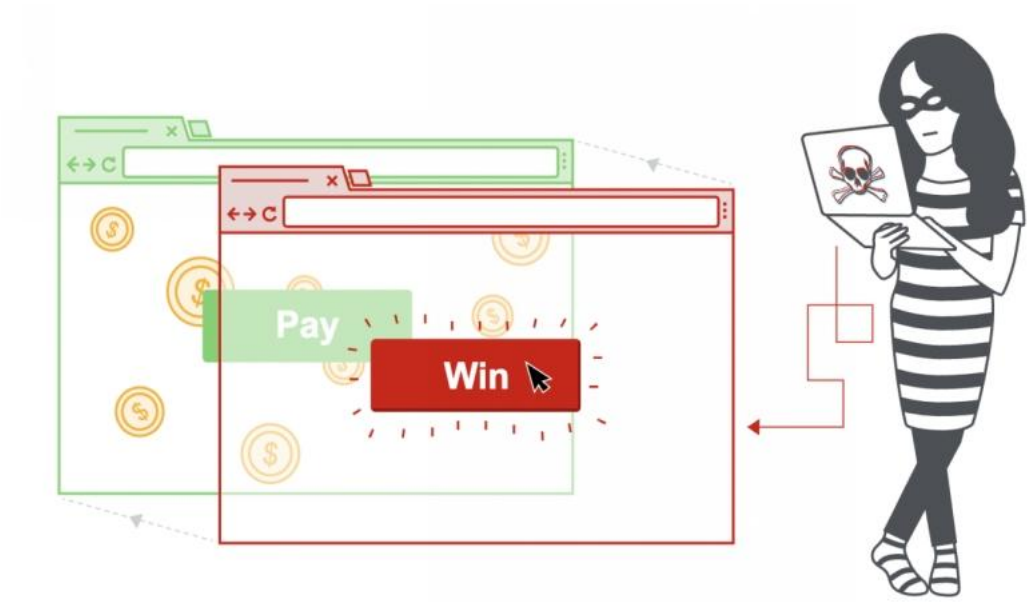


Figure 11: Clickjacking attack

#### 2.3.5.3 How to Prevent

Here are some ways to prevent clickjacking:

- Ask the user to reconfirm by displaying the dialog box announcing the operation the user has made the request and confirmation.
- Placing web objects in random locations makes it difficult for attackers because the interface is unstable.
- Set up browser policies that require frames to show up with opacity > 0.
- Using Javascript prevents another site from embedding its content into an iframe (Frame Bursting)
- Use the condition statement to check if the site is in the iframe
- Redirect the browser window to the embedded site and iframe.

# CHAPTER 3: SUMMARY

Given the current state of website security, although there are many improvements, there are still many vulnerabilities that cause websites to be taken down, leaking or stealing user information,.. causing property damage.

Proceed to give some specific statistics on the situation of websites in the countries that were attacked. specifically, the two countries with the highest number of website attacks are the US and Turkey with the numbers: 114,243 and 49,904 respectively. Although Vietnam is not in the top list, there are still 2852 attacks (According to CyStack Attack Map).

Give some harm when the website is hacked such as: theft of user data, disruption of business activities, SEO influence,...

Learn the concept, causes, and effects of security vulnerabilities

Learn the concept of the site, the classification, and the meaning of the site

Learn about some common types of security vulnerabilities such as XSS, SQL Injection, CSRF, DDOS, Clickjacking. At the same time, give the concept, classification, how to operate and preventive measures of each of the above-mentioned types of vulnerabilities.

Learn more about the XSS vulnerability with the implementation of demos.

## REFERENCES


https://www.rapid7.com/fundamentals/denial-of-service-attacks/

https://viblo.asia/p/tan-cong-xss-va-cach-phong-chong-L4x5x09O5BM

https://viblo.asia/p/ky-thuat-tan-cong-csrf-va-cach-phong-chong-amoG84bOGz8P

https://topdev.vn/blog/csrf-la-gi/

https://www.acunetix.com/websitesecurity/sql-injection/

https://cystack.net/vi/blog/lo-hong-bao-mat

https://www.newsystemvietnam.com/lo-hong-bao-mat-va-nhung-diem-yeu-thuong-thay-trong-bao-mat

https://brightsec.com/blog/error-based-sql-injection/

https://vnpro.vn/thu-vien/tong-quan-lo-hong-bao-mat-va-mot-so-ky-thuat-tan-cong-vao-mang-2443.html

https://www.imperva.com/learn/application-security/clickjacking/#:~:text=Clickjacking%20is%20an%20attack%20that,money%2C%20or%20purchase%20products%20online.

https://viblo.asia/p/lo-hong-clickjacking-aWj536e1l6m

https://securitydaily.net/csrf-phan-2-cach-khac-phuc-va-phong-tranh/

https://portswigger.net/web-security/csrf

https://owasp.org/www-community/attacks/xss/