**TRƯỜNG ĐẠI HỌC AN GIANG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO TIỂU LUẬN AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG**

**CÁC KỸ THUẬT TẤN CÔNG WEBSERVER**

**Họ và tên :Huỳnh Quốc Huy DTH225650**

**Họ và tên :Bùi Nguyễn Minh Huy DTH225647**

**AN GIANG, THÁNG 08 NĂM 2025**

**MỤC LỤC**

[**1.** **GIỚI THIỆU TỔNG QUAN** 1](#_Toc208343436)

[**1.1.** **Các khái niệm cơ bản về an toàn thông tin** 1](#_Toc208343437)

[***1.1.1.*** ***Tam giác bảo mật CIA (Confidentiality, Integrity, Availability)*** 1](#_Toc208343438)

[***1.1.2.*** ***Phân loại đối tượng tấn công*** 1](#_Toc208343439)

[**1.2.** **Vòng đời tấn công mạng (Cyber Kill Chain)** 1](#_Toc208343440)

[**1.3.** **Tổng quan về các lỗ ổng bảo mật Web phổ biến** 1](#_Toc208343441)

[**1.3.1.** **Giới thiệu về OWASP Top 10** 1](#_Toc208343442)

[**1.3.2.** **Phân tích các lỗ hổng chính trong OWASP Top 10-2021** 1](#_Toc208343443)

[**2.** **CÁC KỸ THUẬT TẤN CÔNG WEB SERVER** 1](#_Toc208343444)

[**2.1.** **Tấn công SQL Injection (SQLi)** 1](#_Toc208343445)

[***2.1.1.*** ***Cơ chế hoạt động*** 1](#_Toc208343446)

[***2.1.2.*** ***Các dạng tấn công phổ biến*** 1](#_Toc208343447)

[***2.1.3.*** ***Hậu quả và ví dụ thực tế*** 1](#_Toc208343448)

[**2.2.** **Tấn công Cross-Site Scripting (XSS)** 1](#_Toc208343449)

[**2.2.1.** **Cơ chế hoạt động** 2](#_Toc208343450)

[***2.2.2.*** ***Các dạng tấn công và dặc điểm*** 2](#_Toc208343451)

[***2.2.3.*** ***Hậu quả*** 2](#_Toc208343452)

[**2.3.** **Tấn công Directory Traversal và File Inclusion** 2](#_Toc208343453)

[***2.3.1.*** ***Cơ chế hoạt động và phân loại*** 2](#_Toc208343454)

[***2.3.2.*** ***Hậu quả*** 2](#_Toc208343455)

[**2.4.** **Lỗ hổng tải lên tệp (File Upload Vulnerability)** 2](#_Toc208343456)

[**2.4.1.** ***Nguyên nhân và cách thức khai thác*** 2](#_Toc208343457)

[***2.4.2.*** ***Hậu quả*** 2](#_Toc208343458)

[**2.5.** **Tấn công từ chối dịch vụ (DoS/DDoS)** 2](#_Toc208343459)

[***2.5.1.*** ***Phân biệt DoS và DDoS*** 2](#_Toc208343460)

[***2.5.2.*** ***Các dạng tấn công theo lớp*** 2](#_Toc208343461)

[***2.5.3.*** ***Hậu quả và các case study nổi tiếng*** 2](#_Toc208343462)

[**2.6.** **Tấn công dò mật khẩu (Brute-Force Attack)** 2](#_Toc208343463)

[***2.6.1.*** ***Cơ chế hoạt động và các biến thể*** 2](#_Toc208343464)

[***2.6.2.*** ***Hậu quả và các công cụ tấn công*** 2](#_Toc208343465)

[**3.** **BIỆN PHÁP PHÒNG CHỐNG VÀ BẢO VỆ** 2](#_Toc208343466)

[**3.1.** **Phòng chống ở cấp độ Ứng dụng** 2](#_Toc208343467)

[***3.1.1.*** ***Tiểu mục cấp 3*** 2](#_Toc208343468)

[*3.1.1.1.* *Tiểu mục cấp 4* 2](#_Toc208343469)

[**3.2.** **Phòng chống ở cấp độ Hạ tầng** 2](#_Toc208343470)

[***3.2.1.*** ***Tường lửa Ứng dụng Web (WAF)*** 2](#_Toc208343471)

[***3.2.2.*** ***Các giải pháp chống DDoS*** 2](#_Toc208343472)

[**3.3.** **Các biện pháp an toàn cho Tài khoản và Quản trị** 2](#_Toc208343473)

[**4.** **THỰC HÀNH VÀ ĐÁNH GIÁ BẢO MẬT** 3](#_Toc208343474)

[**4.1.** **Giới thiệu về Kiểm thử Xâm nhập (Pentesting)** 3](#_Toc208343475)

[***4.1.1.*** ***Tiểu mục cấp 3*** 3](#_Toc208343476)

[*4.1.1.1.* *Tiểu mục cấp 4* 3](#_Toc208343477)

[**4.2.** **Các công cụ và môi trường thực hành** 3](#_Toc208343478)

[**4.3.** **Mô phỏng các bước thực hiện demo** 3](#_Toc208343479)

[**TÀI LIỆU THAM KHẢO** 4](#_Toc208343480)

**DANH MỤC HÌNH**

[Hình 1: Tiêu đề (Caption) nằm ở phía dưới của hình. 1](#_Toc207867296)

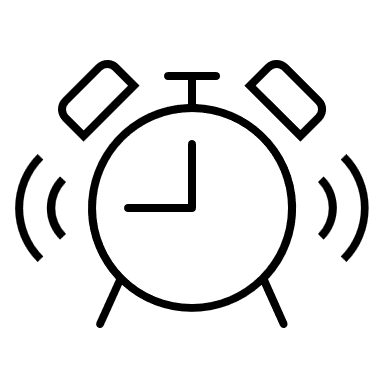
**DANH MỤC BẢNG**

[Bảng 1: Tiêu đề (Caption) của bảng nằm ở phía trên của bảng. 1](#_Toc207867335)

**DANH MỤC TỪ VIẾT TẮT**

|  |  |
| --- | --- |
| **TỪ VIẾT TẮT (SẮP XẾP THEO ABC)** | **TÊN ĐẦY ĐỦ/DIỄN GIẢI** |
|  |  |
|  |  |

1. **GIỚI THIỆU TỔNG QUAN**
   1. **Các khái niệm cơ bản về an toàn thông tin**



Hình 1: Tiêu đề (Caption) nằm ở phía dưới của hình.(để copy)

* + 1. ***Tam giác bảo mật CIA (Confidentiality, Integrity, Availability)***

Mô hình tam giác CIA là mô hình cốt lõi và nền tảng của an toàn thông tin [1]. Nó định nghĩa ba mục tiêu chính mà mọi chiến lược bảo mật cần hướng tới để bảo vệ thông tin và hệ thống [2]:

**Confidentiality (Tính bảo mật):** Mục tiêu này đảm bảo rằng thông tin được bảo vệ khỏi sự truy cập, sử dụng, hoặc thay đổi không được phép [1], [2]. Một cuộc tấn công SQL Injection thành công, nơi tin tặc có thể lấy được dữ liệu người dùng như email và mật khẩu, là một ví dụ điển hình về việc vi phạm tính bảo mật này [3], [4].

**Integrity (Tính toàn vẹn): data-type):** Tính toàn vẹn của dữ liệu đề cập đến việc đảm bảo tính chính xác và đầy đủ của thông tin, ngăn chặn việc sửa đổi hoặc phá hủy trái phép. Khi một kẻ tấn công SQL Injection có thể sửa, xóa hoặc thay đổi toàn bộ dữ liệu trong cơ sở dữ liệu, tính toàn vẹn của hệ thống đã bị phá vỡ hoàn toàn [5], [6].

**Availability (Tính sẵn sàng):** Mục tiêu cuối cùng của tính sẵn sàng là đảm bảo rằng các hệ thống, ứng dụng và dữ liệu luôn có thể truy cập được cho người dùng được ủy quyền vào bất cứ lúc nào họ cần [2]. Các cuộc tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS) trực tiếp nhắm vào mục tiêu này. Bằng cách làm quá tải hệ thống với một lượng lớn lưu lượng truy cập, chúng khiến dịch vụ không thể phản hồi và gây gián đoạn nghiêm trọng cho người dùng hợp pháp [7].

Bảng 1: Tiêu đề (Caption) của bảng nằm ở phía trên của bảng.

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **MSSV** | **Họ và tên** | **Lớp** |
|  |  |  |  |
|  |  |  |  |

* + 1. ***Phân loại đối tượng tấn công***
  1. **Vòng đời tấn công mạng (Cyber Kill Chain)**
  2. **Tổng quan về các lỗ ổng bảo mật Web phổ biến**
     1. **Giới thiệu về OWASP Top 10**
     2. **Phân tích các lỗ hổng chính trong OWASP Top 10-2021**

1. **CÁC KỸ THUẬT TẤN CÔNG WEB SERVER**
   1. **Tấn công SQL Injection (SQLi)**
      1. ***Cơ chế hoạt động***
      2. ***Các dạng tấn công phổ biến***
      3. ***Hậu quả và ví dụ thực tế***

Nội dung của tiểu mục cấp 3

* + - 1. *Tiểu mục cấp 4*

Nội dung của tiểu mục cấp 4(để copy)

* 1. **Tấn công Cross-Site Scripting (XSS)** 
     1. **Cơ chế hoạt động**
     2. ***Các dạng tấn công và dặc điểm***
     3. ***Hậu quả***
  2. **Tấn công Directory Traversal và File Inclusion**
     1. ***Cơ chế hoạt động và phân loại***
     2. ***Hậu quả***
  3. **Lỗ hổng tải lên tệp (File Upload Vulnerability)**
     1. ***Nguyên nhân và cách thức khai thác***
     2. ***Hậu quả***
  4. **Tấn công từ chối dịch vụ (DoS/DDoS)** 
     1. ***Phân biệt DoS và DDoS***
     2. ***Các dạng tấn công theo lớp***
     3. ***Hậu quả và các case study nổi tiếng***
  5. **Tấn công dò mật khẩu (Brute-Force Attack)**
     1. ***Cơ chế hoạt động và các biến thể***
     2. ***Hậu quả và các công cụ tấn công***

1. **BIỆN PHÁP PHÒNG CHỐNG VÀ BẢO VỆ**
   1. **Phòng chống ở cấp độ Ứng dụng**

Nội dung của tiểu mục cấp 2

* + 1. ***Tiểu mục cấp 3***

Nội dung của tiểu mục cấp 3

* + - 1. *Tiểu mục cấp 4*

Nội dung của tiểu mục cấp 4

* 1. **Phòng chống ở cấp độ Hạ tầng**
     1. ***Tường lửa Ứng dụng Web (WAF)***
     2. ***Các giải pháp chống DDoS***
  2. **Các biện pháp an toàn cho Tài khoản và Quản trị**

1. **THỰC HÀNH VÀ ĐÁNH GIÁ BẢO MẬT**
   1. **Giới thiệu về Kiểm thử Xâm nhập (Pentesting)**

Nội dung của tiểu mục cấp 2

* + 1. ***Tiểu mục cấp 3***

Nội dung của tiểu mục cấp 3

* + - 1. *Tiểu mục cấp 4*

Nội dung của tiểu mục cấp 4

* 1. **Các công cụ và môi trường thực hành**
  2. **Mô phỏng các bước thực hiện demo**

Nội dung/Định dạng của tiểu mục cấp 2

* **Góp ý về môn học:** (Về nội dung môn học, cách trình bày của giáo viên, nội dung cần bổ sung, các điểm cần cải thiện của giáo viên, …).

**TÀI LIỆU THAM KHẢO**

[1] “An Toàn Thông Tin Là Gì?” Accessed: Sept. 09, 2025. [Online]. Available: https://itsystems.vn/an-toan-thong-tin-la-gi/

[2] “An toàn thông tin là gì? 4 Nội dung cần biết.” Accessed: Sept. 09, 2025. [Online]. Available: https://vnce.vn/an-toan-thong-tin-la-gi

[3] “Các Lỗ Hổng Bảo Mật của Website bị HACKER Tấn Công Nhất.” Accessed: Sept. 09, 2025. [Online]. Available: https://lanit.com.vn/cac-lo-hong-bao-mat-cua-website-bi-hacker-loi-dung-tan-cong-nhieu-nhat.html

[4] “XSS là gì? Kỹ thuật tấn công XSS, cách ngăn chặn hiệu quả.” Accessed: Sept. 09, 2025. [Online]. Available: https://vietnix.vn/xss-la-gi/

[5] “SQL Injection là gì? Cách giảm thiểu và phòng ngừa SQL Injection.” Accessed: Sept. 09, 2025. [Online]. Available: https://topdev.vn/blog/sql-injection/

[6] FPT C. ty C. phần B. lẻ K., “SQL Injection là gì? Độ nguy hiểm và cách phòng tránh hiệu quả.” Accessed: Sept. 09, 2025. [Online]. Available: https://fptshop.com.vn/tin-tuc/danh-gia/sql-injection-la-gi-159279

[7] T. Dang, “DDoS là gì và cách ngăn chặn các loại tấn công DDoS Server,” DDoS là gì và cách ngăn chặn các loại tấn công DDoS Server. Accessed: Sept. 09, 2025. [Online]. Available: https://www.vnetwork.vn/news/ddos-la-gi-va-cach-ngan-chan-cac-loai-tan-cong-ddos-server/

[Tham khảo thêm Qui định và mẫu trình bày báo cáo thực tập cuối khoá (click vào đây).](https://fit.agu.edu.vn/bai-viet/thuc-tap-khoa-luan/qui-dinh-va-mau-trinh-bay-bao-cao-thuc-tap-cuoi-khoa-dh22pm-va-dh22th-565.html)