

HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO BÀI TẬP LỚN

**KHAI THÁC LỖ HỔNG PHẦN MỀM**

**Đề tài:**

**CVE-2020-7246**

**WPanel 4.3.1**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

Đặng Xuân Đức AT170612

Hoàng Hữu Ánh AT170604

Tạ Quang Chiến AT170607

Nhóm 1

***Giảng viên hướng dẫn****:* TS. Nguyễn Mạnh Thắng

Hà Nội, 13-11-2023

**LỜI NÓI ĐẦU**

Lỗ hổng phần mềm là một trong những vấn đề quan trọng nhất trong lĩnh vực an ninh mạng. Việc khai thác lỗ hổng phần mềm có thể dẫn đến những hậu quả nghiêm trọng, bao gồm mất dữ liệu, sự kiểm soát của hệ thống bị chiếm đoạt, và thậm chí là tiềm ẩn nguy cơ cho tính mạng con người.

Các nhà phát triển phần mềm và các chuyên gia an ninh mạng đang cố gắng nỗ lực hết sức để tìm ra và khắc phục các lỗ hổng này trước khi chúng có thể bị khai thác. Tuy nhiên, vẫn còn rất nhiều lỗ hổng phần mềm tồn tại và tiếp tục được khai thác bởi các tin tặc.

Trong bối cảnh đó, việc tìm hiểu về khai thác lỗ hổng phần mềm là rất quan trọng. Bài viết này sẽ cung cấp cho chúng ta những kiến thức cơ bản về lỗ hổng phần mềm Cross-Site Scripting và Remote Code Execution. Bên cạnh đó, chúng tôi cũng sẽ triển khai thực nghiệm khai thác lỗ hổng trên và đề cập đến những biện pháp bảo vệ phù hợp để giúp ngăn chặn các cuộc tấn công thông qua lỗ hổng phần mềm. Mong rằng bài viết này sẽ giúp mọi người hiểu rõ hơn về mối đe dọa từ các lỗ hổng phần mềm và cách phòng chống chúng.

**MỤC LỤC**

[DANH MỤC HÌNH VẼ iii](#_Toc136180838)

[DANH MỤC KÍ HIỆU VÀ VIẾT TẮT iv](#_Toc136180839)

[CHƯƠNG 1. CƠ SỞ LÝ THUYẾT 1](#_Toc136180840)

[1.1 Giới thiệu về lỗ hổng RCE 1](#_Toc136180841)

[1.1.1 Khái niệm 1](#_Toc136180842)

[1.1.2 Cơ chế hoạt động của RCE 1](#_Toc136180843)

[1.1.3 Tác động của lỗ hổng RCE 2](#_Toc136180844)

[1.1.4 Phân loại tấn công RCE 3](#_Toc136180845)

[1.1.5 Giảm thiểu và phát hiện cuộc tấn công RCE 3](#_Toc136180846)

[1.1.6 Phương pháp ngăn chặn cuộc tấn công RCE 3](#_Toc136180847)

[1.1.7 Ví dụ về tấn công RCE 4](#_Toc136180848)

[1.2 Cơ sở lý thuyết về CVE 2017-0143 5](#_Toc136180849)

[1.2.1 Giới thiệu giao thức SMB 5](#_Toc136180850)

[1.3 Cơ sở lý thuyết về CVE 2022-28368 6](#_Toc136180851)

[1.3.1 Giới thiệu thư viện Dompdf 6](#_Toc136180852)

[CHƯƠNG 2. GIỚI THIỆU VỀ CVE 2017-0143 và CVE 2022-28368 7](#_Toc136180853)

[2.1 Giới thiệu về CVE 2017-0143 7](#_Toc136180854)

[2.1.1 Mô tả CVE 2017-0143 7](#_Toc136180855)

[2.1.2 Phạm vi ảnh hưởng 7](#_Toc136180856)

[2.1.3 Mức độ nghiêm trọng 8](#_Toc136180857)

[2.1.4 Phân tích lỗ hổng 8](#_Toc136180858)

[2.1.5 Ngăn chặn và giảm thiểu rủi ro 9](#_Toc136180859)

[2.2 Giới thiệu về CVE 2022-28368 10](#_Toc136180860)

[2.2.1 Mô tả CVE 2022-28368 10](#_Toc136180861)

[2.2.2 Phạm vi ảnh hưởng 10](#_Toc136180862)

[2.2.3 Phân tích lỗ hổng 11](#_Toc136180863)

[2.2.4 Ngăn chặn và giảm thiểu rủi ro 11](#_Toc136180864)

[CHƯƠNG 3. THỰC NGHIỆM 13](#_Toc136180865)

[3.1 Khai thác lỗ hổng CVE 2017-0143 13](#_Toc136180866)

[3.1.1 Mô hình triển khai 13](#_Toc136180867)

[3.1.2 Kịch bản khai thác 13](#_Toc136180868)

[3.1.3 Đánh giá và kết luận 21](#_Toc136180869)

[3.2 Khai thác lỗ hổng 2022-28368 22](#_Toc136180870)

[3.2.1 Mô hình triển khai 22](#_Toc136180871)

[3.2.2 Kịch bản khai thác 22](#_Toc136180872)

[3.2.3 Đánh giá và kết luận 26](#_Toc136180873)

[KẾT LUẬN 27](#_Toc136180874)

# CƠ SỞ LÝ THUYẾT

## Giới thiệu về lỗ hổng RCE

### Khái niệm

### Cơ chế hoạt động của RCE

### Tác động của lỗ hổng RCE

### Phân loại tấn công RCE

### Giảm thiểu và phát hiện cuộc tấn công RCE

### Phương pháp ngăn chặn cuộc tấn công RCE

### Ví dụ về tấn công RCE

## Cơ sở lý thuyết về 2021-34257

## Cơ sở lý thuyết về CVE 2020-7246

# GIỚI THIỆU VỀ CVE 2021-34257 và CVE 2020-7246

## Giới thiệu về CVE 2021-34257

### Mô tả CVE 2021-34257

### Phạm vi ảnh hưởng

### Mức độ nghiêm trọng

### Phân tích lỗ hổng

### Ngăn chặn và giảm thiểu rủi ro

## Giới thiệu về CVE 2020-7246

### Mô tả CVE 2020-7246

### Phạm vi ảnh hưởng

### Phân tích lỗ hổng

### Ngăn chặn và giảm thiểu rủi ro

# THỰC NGHIỆM

## Khai thác lỗ hổng CVE 2021-34257

### Mô hình triển khai

### Kịch bản khai thác

### Đánh giá và kết luận

## Khai thác lỗ hổng 2020-7246

### Mô hình triển khai

### Kịch bản khai thác

### Đánh giá và kết luận

# KẾT LUẬN