

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**

**CVE 2021-34257**

***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**

[CHƯƠNG 1. CƠ SỞ LÝ THUYẾT 3](#_Toc150799859)

[1.1 Giới thiệu về lỗ hổng RCE 3](#_Toc150799860)

[1.1.1 Khái niệm 3](#_Toc150799861)

[1.1.2 Cơ chế hoạt động của RCE 3](#_Toc150799862)

[1.1.3 Tác động của lỗ hổng RCE 3](#_Toc150799863)

[1.1.4 Phân loại tấn công RCE 3](#_Toc150799864)

[1.1.5 Giảm thiểu và phát hiện cuộc tấn công RCE 3](#_Toc150799865)

[1.1.6 Phương pháp ngăn chặn cuộc tấn công RCE 3](#_Toc150799866)

[1.1.7 Ví dụ về tấn công RCE 3](#_Toc150799867)

[1.2 Cơ sở lý thuyết về 2021-34257 3](#_Toc150799868)

[1.3 Cơ sở lý thuyết về CVE 2020-7246 3](#_Toc150799869)

[CHƯƠNG 2. GIỚI THIỆU VỀ CVE 2021-34257 và CVE 2020-7246 3](#_Toc150799870)

[2.1 Giới thiệu về CVE 2021-34257 3](#_Toc150799871)

[2.1.1 Mô tả CVE 2021-34257 3](#_Toc150799872)

[2.1.2 Phạm vi ảnh hưởng 3](#_Toc150799873)

[2.1.3 Mức độ nghiêm trọng 3](#_Toc150799874)

[2.1.4 Phân tích lỗ hổng 3](#_Toc150799875)

[2.1.5 Ngăn chặn và giảm thiểu rủi ro 3](#_Toc150799876)

[2.2 Giới thiệu về CVE 2020-7246 3](#_Toc150799877)

[2.2.1 Mô tả CVE 2020-7246 3](#_Toc150799878)

[2.2.2 Phạm vi ảnh hưởng 4](#_Toc150799879)

[2.2.3 Phân tích lỗ hổng 4](#_Toc150799880)

[2.2.4 Ngăn chặn và giảm thiểu rủi ro 4](#_Toc150799881)

[CHƯƠNG 3. THỰC NGHIỆM 4](#_Toc150799882)

[3.1 Khai thác lỗ hổng CVE 2021-34257 4](#_Toc150799883)

[3.1.1 Mô hình triển khai 4](#_Toc150799884)

[3.1.2 Kịch bản khai thác 4](#_Toc150799885)

[3.1.3 Đánh giá và kết luận 4](#_Toc150799886)

[3.2 Khai thác lỗ hổng 2020-7246 4](#_Toc150799887)

[3.2.1 Mô hình triển khai 4](#_Toc150799888)

[3.2.2 Kịch bản khai thác 4](#_Toc150799889)

[3.2.3 Đánh giá và kết luận 4](#_Toc150799890)

[KẾT LUẬN 4](#_Toc150799891)

# CƠ SỞ LÝ THUYẾT

## Giới thiệu về lỗ hổng RCE

### Khái niệm

RCE (Remote Code Execution) là một loại lỗ hổng bảo mật cho phép tin tặc thực thi mã độc từ xa trên hệ thống mà họ không có quyền truy cập. Điều này cho phép tin tặc thực hiện các hành động trái phép trên hệ thống như thay đổi dữ liệu, cài đặt phần mềm độc hại, lấy cắp thông tin nhạy cảm hoặc tạo ra các tài khoản truy cập không hợp lệ.

Lỗ hổng RCE thường xuất hiện khi các ứng dụng web hoặc phần mềm không kiểm tra và xác thực đầu vào đúng cách, cho phép tin tặc chèn mã độc vào hệ thống. Lỗ hổng này có thể được khai thác thông qua nhiều phương thức như các yêu cầu HTTP, email, tập tin đính kèm và các giao thức khác.

### Cơ chế hoạt động của RCE

Những kẻ tấn công RCE quét internet để tìm các ứng dụng dễ bị tấn công. Khi họ phát hiện ra lỗ hổng mã từ xa, họ sẽ tấn công nó qua mạng. Những kẻ tấn công thường tạo ra một command shell từ xa cho phép chúng kiểm soát một số khía cạnh của hệ thống mục tiêu từ xa.

Các lỗ hổng bảo mật mã từ xa cung cấp cho kẻ tấn công khả năng thực thi mã độc hại hoặc phần mềm độc hại và chiếm lấy một hệ thống bị ảnh hưởng. Sau khi giành được quyền truy cập vào hệ thống, những kẻ tấn công thường sẽ cố gắng nâng cao đặc quyền của chúng từ người dùng lên quản trị viên.

### Tác động của lỗ hổng RCE

Các tác nhân đe dọa sử dụng các cuộc tấn công RCE vì nhiều lý do:

* Trinh sát mạng: RCE được sử dụng để mở một cửa hậu cho phép kẻ tấn công rình mò và thu thập thông tin. RCE cũng có thể là cơ sở cho các cuộc tấn công tiếp theo.
* Leo thang đặc quyền: Các tác nhân đe dọa thực hiện các cuộc tấn công leo thang đặc quyền để cung cấp cho kẻ tấn công các quyền và đặc quyền bổ sung mà chúng cần để truy cập vào dữ liệu nhạy cảm.

Đánh cắp dữ liệu: RCE có thể được sử dụng để đánh cắp dữ liệu nhạy cảm.

* Tấn công từ chối dịch vụ: Những kẻ tấn công sử dụng các cuộc tấn công từ chối dịch vụ để làm tràn ngập máy chủ web, mạng hoặc hệ thống với lưu lượng truy cập nhiều hơn mức chúng có thể xử lý. RCE được sử dụng để tạo các mạng botnet thực hiện các loại tấn công này.
* Ransomware: Những kẻ tấn công này khóa hệ thống máy tính và sử dụng ransomware để buộc nạn nhân trả tiền để mở khóa hệ thống của họ.

### Phân loại tấn công RCE

* Tấn công injection: Nhiều loại ứng dụng khác nhau, chẳng hạn như truy vấn SQL, sử dụng dữ liệu do người dùng cung cấp làm đầu vào cho lệnh. Trong một cuộc tấn công injection, kẻ tấn công cố tình cung cấp đầu vào không đúng định dạng khiến một phần đầu vào của họ được hiểu là một phần của lệnh. Điều này cho phép kẻ tấn công định hình các lệnh được thực thi trên hệ thống dễ bị tổn thương hoặc thực thi mã tùy ý trên đó.
* Giải mã đối tượng(Deserialization): Quá trình tuần tự hóa kết hợp một số nguồn dữ liệu thành một chuỗi duy nhất mà sau đó chương trình đích sẽ giải tuần tự hóa. Giải mã đối tượng tái tạo lại dữ liệu cho mức tiêu thụ của ứng dụng. Những kẻ tấn công giấu mã độc hại trong các chuỗi dữ liệu được tuần tự hóa và chương trình đích vô tình chấp nhận mã độc hại làm đầu vào.
* Ghi ngoài giới hạn(Out-of-bounds write): Kiểu tấn công này lợi dụng quá trình cấp phát bộ nhớ. Người dùng độc hại ghi dữ liệu bên ngoài bộ đệm lưu trữ bộ nhớ được phân bổ. Điều này dẫn đến hỏng dữ liệu hoặc sự cố hệ thống.

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

Các cuộc tấn công thực thi mã từ xa có thể không bị phát hiện cho đến khi thiệt hại đã xảy ra. Có nhiều phương thức thâm nhập với các cuộc tấn công này, vì vậy có thể khó biết được cần phải tìm gì khi cố gắng phát hiện chúng. Ngoài ra, các cuộc tấn công RCE luôn phát triển.

Theo các chuyên gia an ninh mạng, phòng ngừa là cách tốt nhất để xử lý các cuộc tấn công RCE. Kiểm thử thâm nhập và các hình thức kiểm tra lỗ hổng khác có thể xác định và khắc phục các lỗ hổng mà tin tặc có thể khai thác. Chi phí cho một cuộc kiểm tra lỗ hổng thông thường thấp hơn nhiều so với chi phí tiềm tàng của một vụ vi phạm dữ liệu nghiêm trọng.

### Phương pháp ngăn chặn cuộc tấn công RCE

Có nhiều cách để thực hiện RCE, do đó, việc bảo vệ chống lại chúng đòi hỏi một phương pháp an ninh mạng nhiều lớp:

* Cập nhật bản vá: Cách tốt nhất để bảo vệ hệ thống hoặc mạng khỏi cuộc tấn công RCE là khắc phục các lỗ hổng cho phép kẻ tấn công giành quyền truy cập. Microsoft phát hành các bản vá bảo mật giải quyết các lỗ hổng thực thi mã từ xa trong các bản sửa lỗi Patch Tuesday hàng tháng.
* Làm sạch đầu vào người dùng: Các cuộc tấn công giải tuần tự hóa và tấn công injection lợi dụng lỗ hổng từ đầu vào của người dùng. Làm sạch đầu vào liên quan đến việc xác thực và lọc dữ liệu đầu vào từ người dùng, giao diện chương trình ứng dụng và dịch vụ web.
* Kiểm tra lưu lượng truy cập: Sử dụng các hệ thống phát hiện xâm nhập, trình nghe lén gói tin và tường lửa ứng dụng web là một số cách để kiểm tra lưu lượng truy cập đến để tìm hành vi đáng ngờ và ngăn chặn những kẻ tấn công.
* Bảo vệ chống tràn bộ đệm: Khi phần mềm bảo vệ chống tràn bộ đệm phát hiện lỗi tràn bộ đệm, nó sẽ chấm dứt chương trình bị ảnh hưởng để ngăn kẻ tấn công làm hỏng chương trình.
* Kiểm soát quyền truy cập: Các chính sách bảo mật mạng như không tin cậy, phân đoạn mạng và quản lý quyền truy cập có thể giảm thiểu tác động của vi phạm mạng và ngăn kẻ tấn công leo thang đặc quyền.

## Cơ sở lý thuyết về 2021-34257

### Tổng quan về WPanel CMS

WPanel là một phần mềm cho phép người dùng xây dựng Blog, trang Web và ứng dụng Web với CMS được tạo trên Codelgniter 3.x; được sinh ra từ nhu cầu tạo một trang web nhanh chóng và dễ dàng mà không cần sử dụng các giải pháp như Wordpress hoặc Joomla, do số lượng mã và plugin của bên thứ ba làm tăng độ phức tạp của bất kỳ thay đổi nào.

Mục tiêu của WPanel là hỗ trợ các nhà phát triển muốn kiểm soát mã một cách đơn giản và thiết thực.

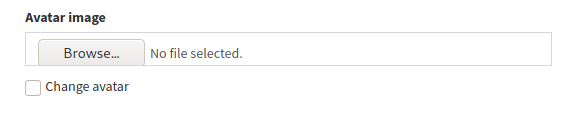
### Những điểm yếu của WPanel CMS

Sau khi đăng nhập, người dùng có nhiều cách để tải lên và thực thi tập lệnh PHP, có thể dễ dàng dẫn đến việc thực thi mã từ xa.

WPanel không có giới hạn về loại tệp được tải lên. Người dùng được xác thực có thể tải lên bất kỳ loại tệp nào trên hệ thống và thực thi.

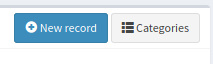
Ví dụ: Trong thư viện, người dùng được cung cấp lời nhắc tải lên hình ảnh và nếu người dùng chọn tệp khác với hình ảnh, nó vẫn được phép tải lên.

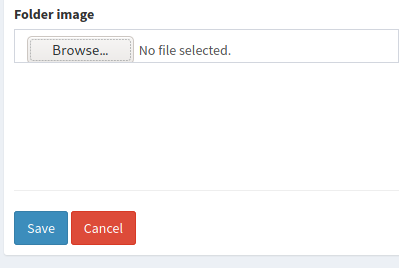
Không chỉ trên thư viện mà trên mọi lời nhắc tải lên tệp trong CMS, người dùng có thể tải lên bất kỳ loại tệp nào:

 -Vulnerable Dashboard Avatar image upload:

Đi tới Bảng điều khiển và nhấp vào Duyệt để thay đổi hình ảnh Đại diện

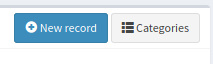
Thêm tệp **PHP reverse shell** thay vì hình ảnh, đánh dấu vào '**Thay đổi hình đại diện**' và nhấp vào '**Lưu**'. Bây giờ hãy tải lại Bảng điều khiển và lấy **reverse shell** trở lại máy tấn công của bạn.

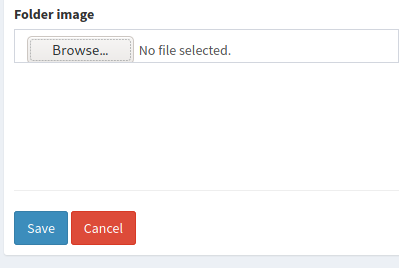
-Vulnerable Posts Folder image upload:



Đến Posts, chọn “New record” và dưới “Folder image” chọn browse.

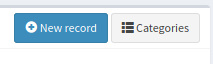
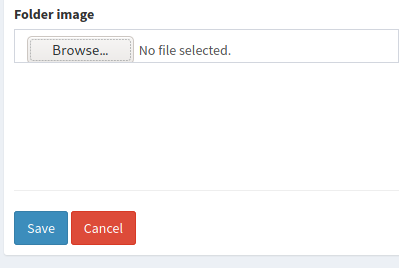
Thêm PHP reverse shell thay vì hình ảnh, truy cập bài đăng và lấy lại shell.

-Vulnerable Pages Folder image upload:



Đến Pages, chọn “New record” và dưới “Folder image” chọn browse.

Thêm PHP reverse shell thay vì hình ảnh, truy cập bài đăng và lấy lại shell.

-Vulnerable Gallery Folder Upload:

Đến Gallery, chọn “New record” và dưới “Folder image” chọn browse.

Thêm PHP reverse shell thay vì hình ảnh, truy cập bài đăng và lấy lại shell.

## Cơ sở lý thuyết về CVE 2020-7246

### Tổng quan về qdPM v9.1

qdPM là một công cụ quản lý dự án dựa trên web miến phí phù hợp với nhóm nhỏ làm việc trên nhiều dự án. Nó có thể cấu hình đầy đủ. Người dùng có thể dễ dàng quản lý Dự án, Nhiệm vụ và Con người. Khách hang tương tác bằng cách sử dụng Hệ thống yêu cầu được tích hợp vào Quản lý tác vụ.

### Những điểm yễu của qdPM v9.1

Tấn công từ chối dịch vụ (DoS): Tấn công DoS là một loại tấn công mạng nhằm mục đích làm cho một hệ thống hoặc dịch vụ không thể truy cập được. Các cuộc tấn công DoS có thể được thực hiện bằng cách gửi một lượng lớn lưu lượng truy cập đến hệ thống hoặc dịch vụ mục tiêu. Điều này có thể khiến hệ thống hoặc dịch vụ quá tải và ngừng hoạt động.

Tấn công lừa đảo (Phishing): Tấn công lừa đảo là một loại tấn công mạng nhằm mục đích đánh cắp thông tin nhạy cảm, chẳng hạn như thông tin đăng nhập hoặc thẻ tín dụng. Các cuộc tấn công lừa đảo thường sử dụng email hoặc tin nhắn văn bản giả mạo để lừa nạn nhân cung cấp thông tin cá nhân của họ.

Tấn công phần mềm độc hại (Malware): Phần mềm độc hại là một loại phần mềm được thiết kế để gây hại cho hệ thống máy tính. Phần mềm độc hại có thể được sử dụng để đánh cắp dữ liệu, phá hủy hệ thống hoặc kiểm soát hệ thống. Các cuộc tấn công phần mềm độc hại có thể được thực hiện bằng cách tải xuống phần mềm độc hại từ một nguồn không đáng tin cậy hoặc nhấp vào liên kết lừa đảo.

Tấn công xâm nhập trái phép (Hacking): Tấn công xâm nhập trái phép là một loại tấn công mạng nhằm mục đích truy cập trái phép vào một hệ thống hoặc mạng. Các cuộc tấn công xâm nhập trái phép thường được thực hiện bằng cách khai thác lỗ hổng bảo mật trong hệ thống hoặc mạng.