

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

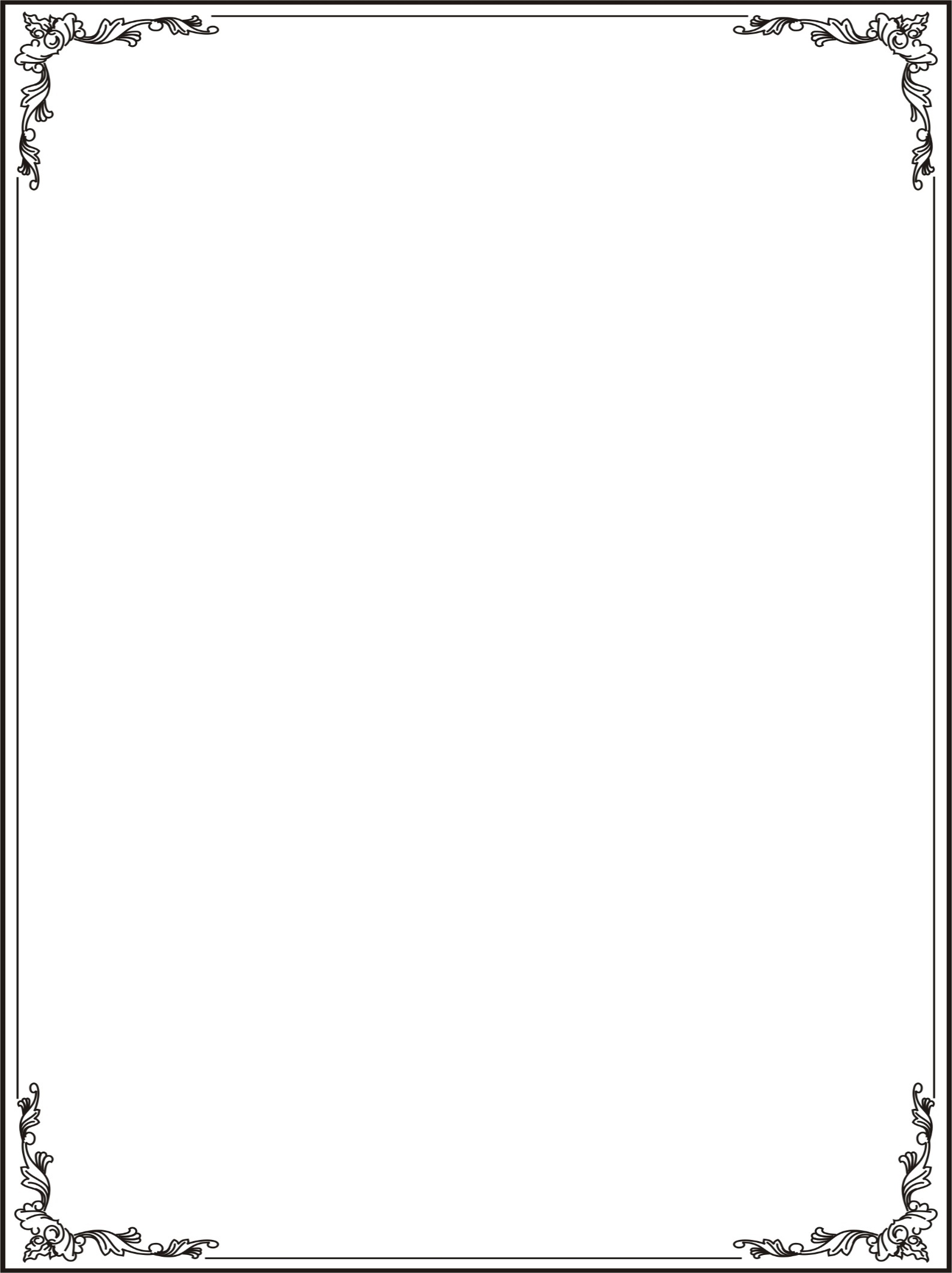
Hoàng Hữu Ánh AT170604

Tạ Quang Chiến AT170607

Nhóm 1

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

Hà Nội, 13-11-2023



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 CẢM ƠN



Nhóm chúng em xin gửi lời cảm ơn chân thành tới các thầy giáo, cô giáo trong Khoa An toàn thông tin đã tạo điều kiện thuận lợi cho nhóm em trong quá trình thực hiện bài tập này.

Chúng em xin gửi lời cảm ơn đặc biệt đến Tiến sĩ thầy: Nguyễn Mạnh Thắng đã nhiệt tình hướng dẫn và chỉ bảo nhóm trong suốt thời gian thực hiện bài tập, giúp chúng em có thể hoàn thành tốt bài tập lớn lần này.

|  |  |
| --- | --- |
| **GIẢNG VIÊN HƯỚNG DẪN** | **NHÓM SINH VIÊN THỰC HIỆN** |
|  | Vũ Tiến Đạt |
|  | Đặng Xuân Đức |
|  | Hoàng Hữu Ánh |
| TS. Nguyễn Mạnh Thắng | Tạ Quang Chiến |

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.

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 Remote Code Execution. Bên cạnh đó, chúng em 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.

Với mong muốn có thêm hiểu biết và nghiên cứu sâu hơn về các lỗ hổng phần mềm thông qua khai thác mã định danh CVE, nhóm chúng em đã thống nhất và thực hiện nghiên cứu CVE-2021-34257, CVE-2020-7246 làm bài tập báo cáo.

Trong quá trình làm bài tập, cũng như là trong quá trình làm bài báo cáo, khó tránh khỏi sai sót, rất mong các thầy bỏ qua. Đồng thời do trình độ cũng như kinh nghiệm thực tiễn còn hạn chế nên bài báo cáo không thể tránh khỏi những thiếu sót, chúng em rất mong nhận được góp ý của thầy để chúng em học thêm được nhiều kinh nghiệm và hoàn thành tốt hơn trong các bài báo cáo sắp tới.

Báo cáo được chia làm 3 chương, với các nội dung sau:

**Chương I: Cơ sở lý thuyết**

**Chương II: Giới thiệu về CVE-2021-34257 và CVE-2020-7246**

**Chương III: Triển khai khai thác CVE**

DANH MỤC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| Từ viết tắt | Tiếng Anh | Tiếng Việt |
| CVE | Common Vulnerabilities and Exposures | Các lỗ hổng và phơi nhiễm phổ biến |
| RCE | Remote Code Execution | Thực thi mã từ xa |
| CMS | Content Management System | Hệ thống quản trị nội dung |
| HTTP | Hyper Text Transfer Protocol | **Giao thức Truyền tải Siêu Văn Bản** |
| ACE | Arbitrary code execution | Thực thi mã tùy ý |
| SQL | Structured Query Language | Ngôn ngữ truy vấn có cấu trúc |
| PHP | Hypertext Preprocessor | Trình tiền xử lý siêu văn bản |
| DoS | Denial of Service | Tấn công từ chối dịch vụ |

DANH MỤC HÌNH VẼ

[Hình 1.1 Cơ chế hoạt động của RCE 5](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995002)

[Hình 2.1 CVE-2020-7246 11](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995003)

[Hình 2.2 Chức năng cập nhật tài khoản của qdPM 12](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995004)

[Hình 2.3 Đăng nhập vào user 14](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995005)

[Hình 2.4 Loại bỏ biện pháp baoe vệ 14](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995006)

[Hình 2.5 My Details của qdPM 15](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995007)

[Hình 2.6 Up file 15](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995008)

[Hình 2.7 Nội dung tệp .htacces 16](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995009)

[Hình 2.8 Xóa ảnh hồ sơ 16](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995010)

[Hình 2.9 Request xóa hình ảnh 16](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995011)

[Hình 2.10 Thay đổi giá trị users[photo\_preview] 17](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995012)

[Hình 2.11 file .htaccess đã bị xóa 17](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995013)

[Hình 2.12 File .htaccess tồn tại trong thư mục gốc 17](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995014)

[Hình 2.13 Bước xác minh tệp hình ảnh 18](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995015)

[Hình 2.14 Các vị trí tải được tệp tùy ý 20](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995016)

[Hình 2.15 Tải lên ảnh đại diện 20](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995017)

[Hình 2.16 New record 20](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995018)

[Hình 2.17 Folder image 21](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995019)

[Hình 3.1 Mô hình CVE 2020-7246 22](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995020)

[Hình 3.2 Gửi yêu cầu 23](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995021)

[Hình 3.3 Thực hiện yêu cầu backdoor 24](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995022)

[Hình 3.4 Đặt users[photo\_preview] thành .htaccess 24](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995023)

[Hình 3.5 Chạy file python 24](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995024)

[Hình 3.6 Thực hiện thành công lệnh shell qua backdoor 25](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995025)

[Hình 3.7 Đổi url, email, password 26](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995026)

[Hình 3.8 Đổi ip của attacker 26](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995027)

[Hình 3.9 Chạy file python3 50255.py 27](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995028)

[Hình 3.10 Link truy cập 27](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995029)

[Hình 3.11 Sử dụng lệnh nc -lp 9000 28](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995030)

[Hình 3.12 Chuyển index.php 31](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995031)

[Hình 3.13 Cài đặt WPanel 34](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995032)

[Hình 3.14 Truy cập khu vực quản trị 34](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995033)

[Hình 3.15 Chạy thành công WPanel 35](file:///D:\Nam4\Khai%20thác%20lỗ%20hổng\nhom1\KTLHPM_CVE-2021-34257%20&%20CVE-2020-7246.docx#_Toc151995034)

**MỤC LỤC**

[LỜI CẢM ƠN iii](#_Toc151994961)

[LỜI NÓI ĐẦU iv](#_Toc151994962)

[DANH MỤC TỪ VIẾT TẮT v](#_Toc151994963)

[DANH MỤC HÌNH VẼ vi](#_Toc151994964)

[CHƯƠNG 1. CƠ SỞ LÝ THUYẾT 3](#_Toc151994965)

[1.1 Giới thiệu về lỗ hổng RCE 3](#_Toc151994966)

[1.1.1 Khái niệm 3](#_Toc151994967)

[1.1.2 Cơ chế hoạt động của RCE 4](#_Toc151994968)

[1.1.3 Tác động của lỗ hổng RCE 6](#_Toc151994969)

[1.1.4 Phân loại tấn công RCE 7](#_Toc151994970)

[1.1.5 Giảm thiểu và phát hiện cuộc tấn công RCE 8](#_Toc151994971)

[1.1.6 Phương pháp ngăn chặn cuộc tấn công RCE 8](#_Toc151994972)

[1.2 Giới thiệu về WPanel CMS và những điểm yếu của WPanel CMS 9](#_Toc151994973)

[1.2.1 Tổng quan về WPanel CMS 9](#_Toc151994974)

[1.2.2 Những điểm yếu của WPanel CMS 9](#_Toc151994975)

[1.3 Giới thiệu về qdPM v9.1 và những điểm yếu của qdPM v9.1 10](#_Toc151994976)

[1.3.1 Tổng quan về qdPM v9.1 10](#_Toc151994977)

[1.3.2 Những điểm yễu của qdPM v9.1 10](#_Toc151994978)

[CHƯƠNG 2. GIỚI THIỆU VỀ CVE-2021-34257 VÀ CVE-2020-7246 11](#_Toc151994979)

[2.1 CVE-2020-7246 11](#_Toc151994980)

[2.1.1 Mô tả lỗ hổng 11](#_Toc151994981)

[2.1.2 Cách thức hoạt động 12](#_Toc151994982)

[2.1.3 Cách thức khai thác 14](#_Toc151994983)

[2.1.4 Biện pháp khắc phục 18](#_Toc151994984)

[2.2 CVE-2021-34257 18](#_Toc151994985)

[2.2.1 Mô tả lỗ hổng 18](#_Toc151994986)

[2.2.2 Cách thức hoạt động 19](#_Toc151994987)

[2.2.3 Cách thức khai thác 19](#_Toc151994988)

[2.2.4 Biện pháp khắc phục 21](#_Toc151994989)

[CHƯƠNG 3. THỰC NGHIỆM 22](#_Toc151994990)

[3.1 Khai thác lỗ hổng CVE 2020-7246 22](#_Toc151994991)

[3.1.1 Mô hình triển khai 22](#_Toc151994992)

[3.1.2 Kịch bản khai thác 23](#_Toc151994993)

[3.1.3 Đánh giá và kết luận 25](#_Toc151994994)

[3.2 Khai thác lỗ hổng CVE 2021-34257 26](#_Toc151994995)

[3.2.1 Mô hình triển khai 26](#_Toc151994996)

[3.2.2 Kịch bản khai thác 26](#_Toc151994997)

[3.2.3 Đánh giá và kết luận 28](#_Toc151994998)

[KẾT LUẬN 29](#_Toc151994999)

[TÀI LIỆU THAM KHẢO 30](#_Toc151995000)

[PHỤ LỤC 31](#_Toc151995001)

# 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. Tin tặc sẽ sử dụng một số kỹ thuật nào đó để có thể chiếm được quyền điều khiển trên máy nạn nhân, thông qua đó có thể thực thi những câu lệnh shell, bash ..., hoặc thực thi code của những ngôn ngữ kịch bản (script) như python, perl, php, javascript, ... Điều đó có nghĩa là tin tặc có thể 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.

Trong một cuộc tấn công RCE, kẻ tấn công không cần có sự can thiệp của người dùng. Lỗ hổng thực thi mã từ xa có thể xâm phạm dữ liệu nhạy cảm của người dùng mà tin tặc không cần có quyền truy cập vật lý vào mạng của người dùng.

Lỗ hổng RCE thường xuất hiện khi các ứng dụng web hoặc phần mềm không kiểm tra, 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.

RCE được coi là một dạng của arbitrary code execution hay còn được gọi là thực thi mã tùy ý (ACE)—RCE có thể là loại lỗ hổng nghiêm trọng nhất trong ACE, vì chúng có thể bị khai thác ngay cả khi kẻ tấn công không có quyền truy cập trước vào hệ thống hoặc thiết bị và được thực thi từ xa, trong khi đó một số cuộc tấn công của ACE được thực hiện trực tiếp trên máy tính bị ảnh hưởng, thông qua việc giành quyền truy cập vật lý vào thiết bị hoặc yêu cầu người dùng tải xuống phần mềm độc hại. RCE tương đương với việc xâm phạm toàn bộ hệ thống hoặc ứng dụng bị ảnh hưởng và có thể dẫn đến hậu quả nghiêm trọng như mất dữ liệu, gián đoạn dịch vụ, triển khai khác , cài đặt các phần mềm độc hại hoặc ransomware.

### Cơ chế hoạt động của RCE

Những kẻ tấn công RCE quét mạng, xác định lỗ hổng trong phần cứng hoặc phần

mềm của mạng, điều này có thể bao gồm các lỗ hổng trong mã nguồn ứng dụng, lỗ hổng hệ điều hành, hoặc các dịch vụ mạng.

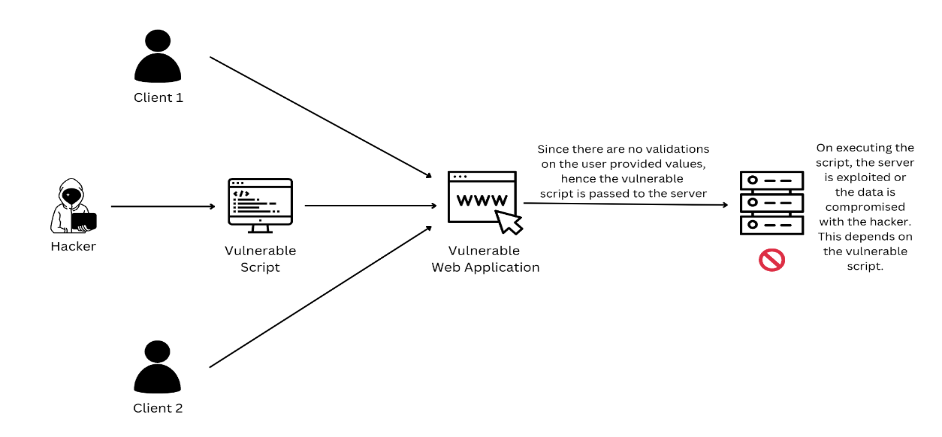
Khi phát hiện ra lỗ hổng mã từ xa, những kẻ tấn công thường khai thác lỗ hổng này ,tin tặc sử dụng các kỹ thuật như injection attacks (SQL injection, OS command injection), deserialization exploits, hay tận dụng các lỗ hổng bảo mật để chèn payload của mình vào hệ thống.

Tin tặc chèn đoạn mã độc hoặc phần mềm độc hại từ xa vào thiết bị. Đoạn mã độc này có thể được chèn vào các tham số đầu vào của ứng dụng web, các tệp tin, hay các kết nối mạng. Khi tin tặc có quyền truy cập vào mạng, tin tặc sẽ xâm phạm dữ liệu người dùng hoặc sử dụng mạng nhằm thực hiện các hành động không mong muốn, bao gồm kiểm soát hệ thống, đánh cắp dữ liệu, hoặc triển khai các hành động độc hại khác..

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. Đồng thời tin tặc sẽ cố gắng che giấu sự hiện diện của mình, làm cho việc phát hiện trở nên khó khăn.

Xem xét một tình huống trong đó tin tặc cần khám phá lỗ hổng trong một trang web.

Đầu tiên, họ sẽ bắt đầu bằng cách đưa tải trọng dễ bị tấn công vào thanh tìm kiếm trên trang web. Hơn nữa, họ sẽ tạo một truy vấn tìm kiếm có chứa mã độc và gửi nó đến trang web. Khi nhận được yêu cầu tìm kiếm, máy chủ sẽ thực thi mã độc. Cuối cùng, điều này cho phép tin tặc truy cập vào cơ sở dữ liệu và thông tin khách hàng của trang web.



Hình . Cơ chế hoạt động của RCE

Sau đó, tin tặc có thể lấy cắp dữ liệu nhạy cảm, chẳng hạn như tên khách hàng, địa chỉ và số thẻ tín dụng. Tin tặc cũng có thể cài phần mềm độc hại vào trang web để lây nhiễm cho nhiều người dùng hơn. Trong trường hợp này, việc trang web không xác thực đúng thông tin đầu vào của người dùng đã dẫn đến lỗ hổng RCE. Kết quả là tin tặc có được quyền truy cập trái phép vào hệ thống và dữ liệu nhạy cảm.

Ví dụ: Xét biểu mẫu đăng nhập php sau:

<?php

$username = $\_POST['username'];

$password = $\_POST['password'];

$query = "SELECT \* FROM users WHERE username='$username' AND password='$password'";

$result = mysqli\_query($conn, $query);

if (mysqli\_num\_rows($result) > 0) {

// login successful

} else {

// login failed

}

?>

Trong biểu mẫu trên RCE có thể được chèn vào khi các trường đầu vào không được ứng dụng lọc hoặc xác thực đúng cách. Kẻ tấn công sử dụng đầu vào độc hại của người dùng như ‘; system('rm -rf /'); //, thì truy vấn SELECT sẽ có dạng như sau:

**SELECT \* FROM users WHERE username='''; system('rm -rf /'); //' AND password=''**

Truy vấn trên sẽ xóa tất cả các tệp, gây ảnh hưởng nghiêm trọng đến bảo mật. Để tránh kiểu tấn công này, điều quan trọng là phải lọc và xác thực thông tin đầu vào của người dùng.

RCE cũng có thể được đưa vào thông qua các lỗ hổng thông dịch ngôn ngữ. Ví dụ: nếu chúng tôi sử dụng phiên bản PHP có bất kỳ lỗ hổng nào đã biết thì kẻ tấn công có thể khai thác lỗ hổng đó bằng cách thực thi mã tùy ý.

### 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: trong nhiều trường hợp, máy chủ có lỗ hổng nội bộ mà chỉ những người có quyền truy cập bên trong mới có thể nhìn thấy. RCE cho phép kẻ tấn công khám phá và khai thác những lỗ hổng này, nâng cao đặc quyền và giành quyền truy cập vào các hệ thống được kết nối. leo thang đặc quyền cung cấp cho kẻ tấn công các quyền và đặc quyền bổ sung mà chúng cần để truy cập vào dữ liệu nhạy cảm
* Lộ dữ liệu nhạy cảm - Sensitive data exposure: RCE có thể được sử dụng để lọc dữ liệu khỏi các hệ thống dễ bị tấn công bằng cách cài đặt phần mềm độc hại đánh cắp dữ liệu hoặc thực thi trực tiếp các lệnh. Điều này có thể bao gồm từ việc sao chép đơn giản dữ liệu không được mã hóa đến phần mềm độc hại quét bộ nhớ để tìm kiếm thông tin xác thực trong bộ nhớ hệ thống.
* Từ chối dịch vụ (DoS)—lỗ hổng RCE cho phép kẻ tấn công thực thi mã trên hệ thống. Mã này có thể được sử dụng để làm làm tràn ngập máy chủ web, mạng hoặc hệ thống với lưu lượng truy cập nhiều hơn mức chúng có thể xử lý, làm cạn kiệt tài nguyên hệ thống hoặc tận dụng tài nguyên của hệ thống tạo các mạng botnet để tiến hành DoS chống lại bên thứ ba.
* Cryptomining - Khai thác tiền điện tử: bước tiếp theo phổ biến sau khi khai thác RCE là chạy phần mềm độc hại khai thác tiền điện tử hoặc đánh cắp tiền điện tử sử dụng tài nguyên máy tính của một thiết bị bị nhiễm để khai thác tiền điện tử nhằm mang lại lợi ích tài chính cho kẻ tấn công.
* Ransomware—có thể hậu quả nguy hiểm nhất của RCE là kẻ tấn công có thể triển khai ransomware trên ứng dụng hoặc máy chủ bị ảnh hưởng và phát tán ransomware qua mạng, khóa hệ thống máy tính, từ chối người dùng truy cập vào tệp của họ cho đến khi họ trả tiền chuộc.

Những lỗ hổng này có thể rất khó hoặc dễ tìm, nếu được tìm thấy thì cũng thường rất khó khai thác, tùy thuộc vào kịch bản. Tuy nhiên nếu khai thác thành công, thì có thể dấn đến mất bảo mật, mất tính khả dụng, mất tính toàn vẹn... Điển hình như Phần mềm tống tiền “WannaCry” đã làm sập mạng trên toàn thế giới từ các siêu tập đoàn đến bệnh viện vào năm 2017,ransomware này khai thác một lỗi trên hệ thống Windows có tên là EternalBlue hay tên mã là MS17-010 để xâm nhập vào hệ thống Windows, sau đó nó sẽ chạy một payload đã được hacker cài sẵn để tự động mã hóa toàn bộ dữ liệu trên máy của nạn nhân, đồng thời mở một kết nối Internet từ máy nạn nhân đến một server được hacker kiểm soát nhằm nhận lệnh của hacker. Hay vào tháng 2 năm 2016, tin tặc đã cướp gần 1 tỷ USD của Ngân hàng Bangladesh bằng cách sử dụng cuộc tấn công RCE vào mạng ngân hàng SWIFT.

### 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): Các ứng dụng thường sử dụng quá trình serialization để kết hợp một số nguồn dữ liệu thành một chuỗi duy nhất nhằm giúp truyền hoặc giao tiếp dễ dàng hơn và sau đó chương trình đích sẽ Deserialization. Dữ liệu được serialized thường được biểu diễn dưới dạng chuỗi byte hoặc chuỗi văn bản. 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 hoặc đầu vào được định dạng đặc biệt được serialization và chương trình đích sau khi deserialization hiểu là mã thực thi.
* Ghi ngoài giới hạn(Out-of-bounds write): Kiểu tấn công này lợi dụng quá trình cấp phát bộ nhớ. Với các ứng dụng sử dụng phân bổ các khối bộ nhớ có kích thước cố định để lưu trữ dữ liệu, bao gồm cả dữ liệu do người dùng cung cấp. Nếu việc cấp phát bộ nhớ này được thực hiện không chính xác, kẻ tấn công có thể thiết kế đầu vào ghi bên ngoài bộ đệm được cấp phát. Vì mã thực thi cũng được lưu trữ trong bộ nhớ nên dữ liệu do người dùng cung cấp được ghi vào đúng vị trí có thể được ứng dụng thực thi. 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.

## Giới thiệu về WPanel CMS và những điểm yếu của WPanel CMS

### 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.

## Giới thiệu về qdPM v9.1 và những điểm yếu của qdPM v9.1

### 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.

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

## CVE-2020-7246

### Mô tả lỗ hổng

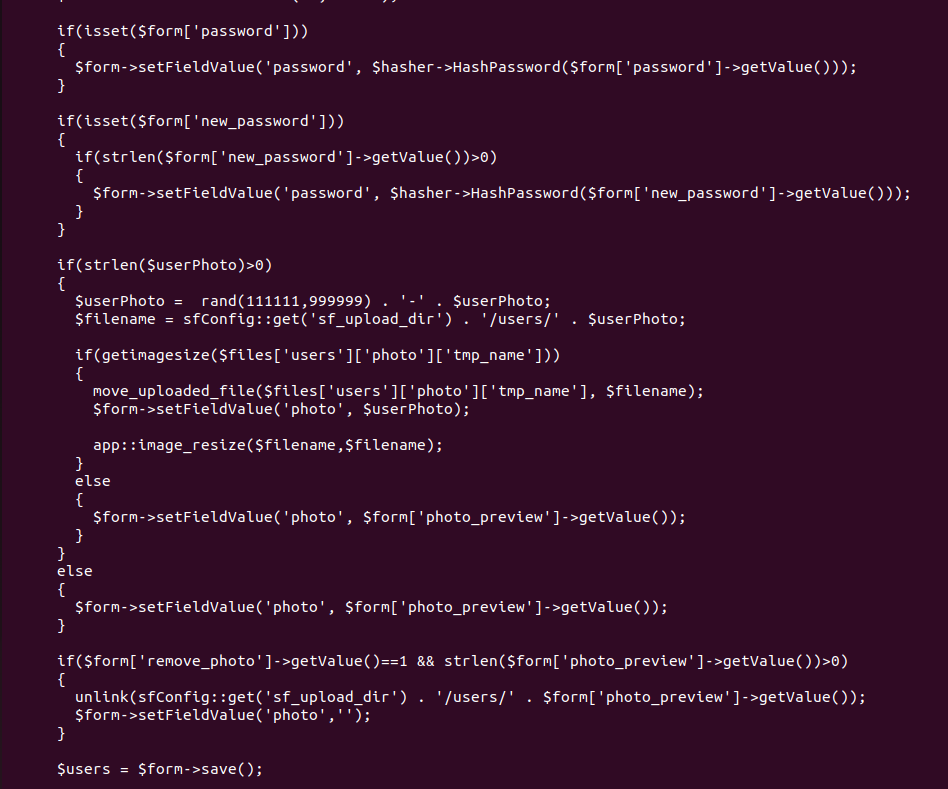
Hình . CVE-2020-7246

Lỗ hổng thực thi mã từ xa (RCE) tồn tại trong qdPM 9.1 và các phiên bản trở về trước. Kẻ tấn công có thể tải lên tệp mã PHP độc hại thông qua chức năng ảnh hồ sơ, bằng cách lợi dụng lỗ hổng path traversal trong tính năng xóa ảnh **users['photop\_preview']**, cho phép bỏ qua tính năng bảo vệ .htaccess. LƯU Ý: sự cố này tồn tại do bản sửa lỗi chưa hoàn chỉnh cho CVE-2015-3884.

Lỗ hổng Path Traversal hoặc Directory Traversal là một lỗ hổng bảo mật xảy ra khi phần mềm sử dụng đầu vào được kiểm soát bởi kẻ tấn công để tạo ra một đường dẫn đến thư mục hoặc tệp tin nằm bên ngoài của thư mục bị hạn chế. Khi ứng dụng không vô hiệu hóa các chuỗi như " ../ " không có tác động, kẻ tấn công có thể có khả năng đọc các tệp tin tùy ý trên hệ thống mục tiêu.

Lợi dụng lỗ hổng này, kẻ tấn công có thể sử dụng các chuỗi như " ../ " để điều hướng đến các vị trí khác ngoài phạm vi của thư mục được phép và đọc các tệp tin không được ủy quyền. Điều này có thể dẫn đến việc tiết lộ thông tin nhạy cảm hoặc mã nguồn của ứng dụng, tùy thuộc vào các tệp tin mà kẻ tấn công có thể truy cập được.

### Cách thức hoạt động

* Cách hoạt động của chức năng cập nhật tài khoản của qdpm

Hình . Chức năng cập nhật tài khoản của qdPM

Kiểm tra Độ Dài của Tên Tệp ($userPhoto):

if(strlen($userPhoto)>0)

Kiểm tra xem biến $userPhoto (tên của tệp ảnh người dùng) có độ dài lớn hơn 0 hay không. Điều này đảm bảo rằng có một tệp tin đã được chọn để tải lên.

Tạo Tên Tệp Mới Nếu Có:

$userPhoto = rand(111111,999999) . '-' . $userPhoto;

Nếu có tệp được chọn, thêm một số ngẫu nhiên vào phía trước tên tệp để tạo một tên tệp mới.

Xác định Đường Dẫn và Di chuyển Tệp Lên Server:

$filename = sfConfig::get('sf\_upload\_dir') . '/users/' . $userPhoto;

Xác định đường dẫn đầy đủ của tệp trên máy chủ.

if(getimagesize($files['users']['photo']['tmp\_name']))

{

move\_uploaded\_file($files['users']['photo']['tmp\_name'], $filename);

}

Kiểm tra xem tệp đã được tải lên có phải là một hình ảnh hợp lệ không (getimagesize). Nếu có, di chuyển tệp từ thư mục tạm thời (tmp\_name) đến thư mục đích ($filename).

Thiết lập Giá Trị Của Trường photo trong Biểu Mẫu ($form->setFieldValue):

$form->setFieldValue('photo', $userPhoto);

Thiết lập giá trị của trường photo trong biểu mẫu bằng tên tệp ảnh mới.

Kiểm tra và Xử Lý Trường Hợp Không Phải Hình Ảnh:

else

{

$form->setFieldValue('photo', $form['photo\_preview']->getValue());

}

Nếu tệp không phải là hình ảnh hợp lệ (đã kiểm tra bởi getimagesize), sử dụng giá trị của trường photo\_preview trong biểu mẫu.

Kiểm Tra và Xử Lý Yêu Cầu Xóa Ảnh:

if($form['remove\_photo']->getValue()==1 && strlen($form['photo\_preview']->getValue())>0)

{

unlink(sfConfig::get('sf\_upload\_dir') . '/users/' . $form['photo\_preview']->getValue());

$form->setFieldValue('photo','');

}

Nếu người dùng đã chọn yêu cầu xóa ảnh **($form['remove\_photo']->getValue() == 1**) và có một ảnh đại diện hiện đang tồn tại (**strlen($form['photo\_preview']->getValue()) > 0**), thì sẽ xóa ảnh từ thư mục trên máy chủ và thiết lập giá trị của trường photo trong biểu mẫu thành rỗng.

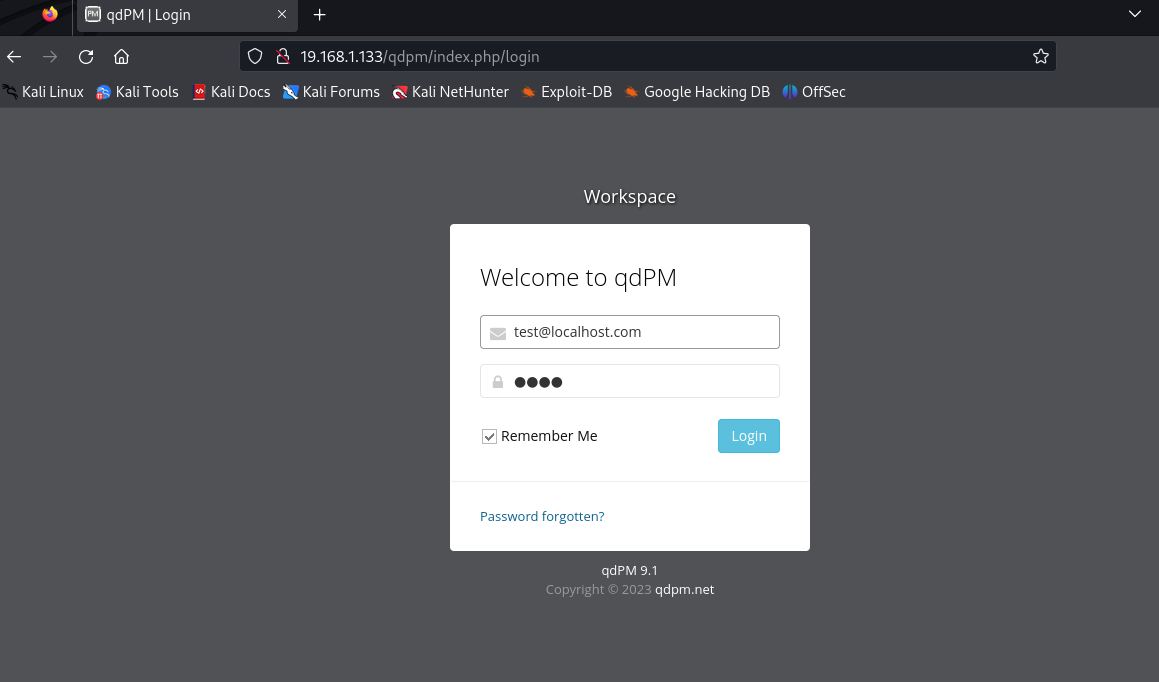
Thông qua mã nguồn có thể nhận thấy nếu thực hiện giá trị của remove\_photo là 1 và ảnh đại diện photo\_preview là chuỗi cụ thể biểu thị đường dẫn thư mục , thì sẽ gây ra lỗ hổng path traversal. Sau đó tệp sẽ bị hàm unlink() xóa.

### Cách thức khai thác

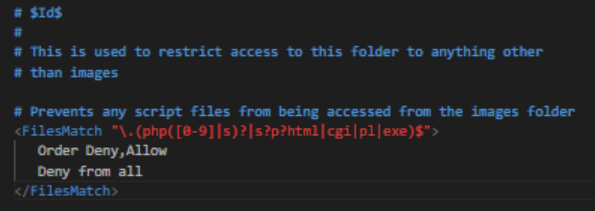
* Thăm dò:

Trên máy kali thực hiện đăng nhập vào user có quyền thấp hơn:

Email: test@localhost

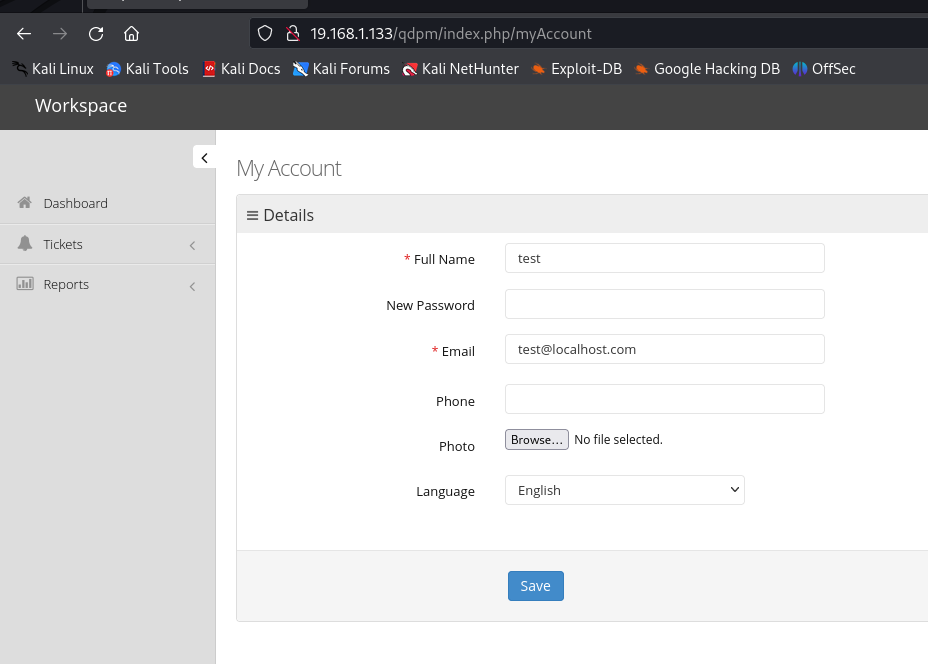
Password: test

Hình . Đăng nhập vào user



Hình . Loại bỏ biện pháp baoe vệ

Đi tới tab “My Details” (là không gian nơi người dùng có thể chỉnh sửa thông tin cá nhân và tải lên/sửa đổi ảnh hồ sơ của họ).



Hình . My Details của qdPM

Thử tải các loại file + Reverse Web Shell

Upload một số file:

• upload.txt (A simple .txt file)

• upload.py (A simple Python file)

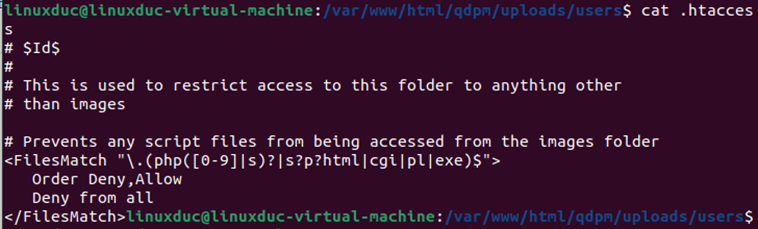
• upload.php (A simple PHP file)

• .php

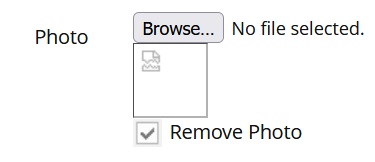


Hình . Up file

Các file đều được upload lên tùy ý , đây là loại lỗ hổng tồn tại trước đó (CVE-2015-3884) và được khắc phục bằng cách triển khai tệp .htaccess nhằm ngăn chặn các loại tệp độc hại được thực thi. Tuy nhiên cách khắc phục này không phù hợp vì có thể xóa tệp .htaccess thông qua tấn công directory traversal và tải lên tập lệnh PHP độc hại để gọi RCE.



Hình . Nội dung tệp .htacces

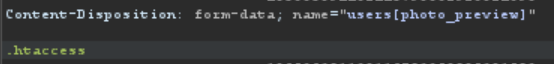
Thực hiện xóa ảnh hồ sơ. Bật burpsuite chặn tất cả các lưu lượng HTTP tới proxy BURP :

Hình . Xóa ảnh hồ sơ

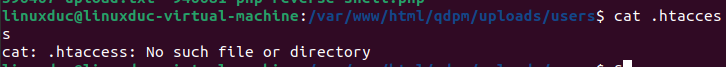
Trong yêu cầu thứ 2 là nơi thông tin dễ bị tấn công với 2 giá trị **users[photo\_preview]** và **users[remove\_photo]**

Hình . Request xóa hình ảnh

Thay đổi giá trị **users[photo\_preview]** thành .htaccess thì tập lệnh thực hiện sẽ thành unlink(“/uploads/users/.htaccess”)::



Hình . Thay đổi giá trị users[photo\_preview]

Sau khi chuyển tiếp yêu cầu .htaccess đã bị xóa khỏi thư mục /uploads/user

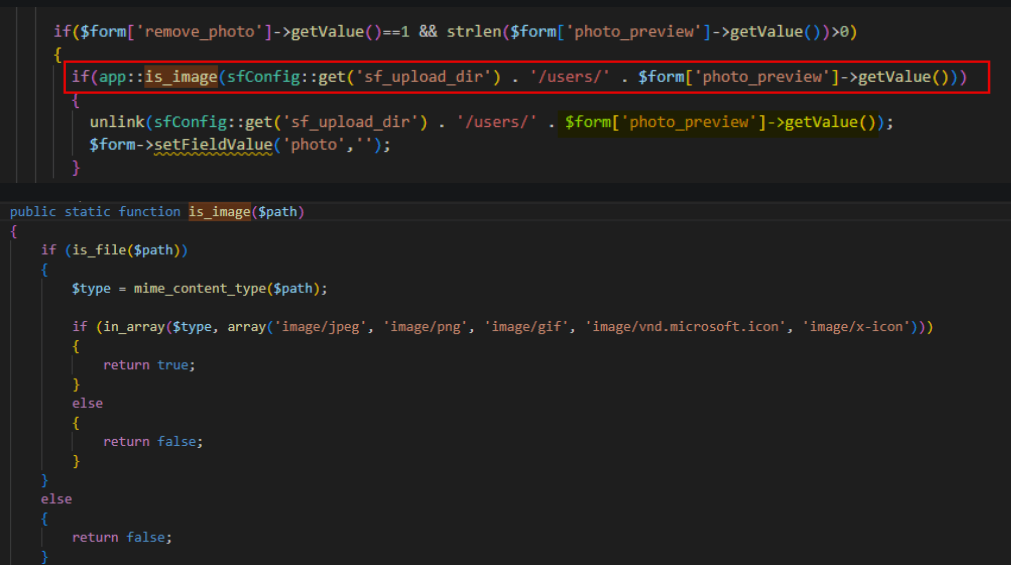
Hình . file .htaccess đã bị xóa

Do tệp .htaccess vẫn tồn tại trong thư mục gốc /uploads/ nên cần thực hiện yêu cầu Burp với **users[photo\_preview]** thành ../.htaccess

Hình . File .htaccess tồn tại trong thư mục gốc

Giờ chúng ta có khả năng bỏ qua việc truy cập các tập lệnh PHP đã tải lên

### Biện pháp khắc phục

 Chỉnh sửa mã nguồn ngăn chặn việc tải lên độc hại :

Hình . Bước xác minh tệp hình ảnh

Danh sách trắng tiện ích mở rộng (chỉ cho phép .png, .jpg, .gif, v.v.)

Kiểm tra loại nội dung của tệp được tải lên

Sử dụng thư viện PHP GD để xác thực hình ảnh mạnh mẽ hơn nữa

## CVE-2021-34257

### Mô tả lỗ hổng

CVE-2021-34257 là một lỗ hổng thực thi mã tùy ý (RCE) trong WPanel 4, một công cụ quản lý web cho WordPress. Lỗ hổng này tồn tại trong cách xử lý các tệp PHP được tải lên các thư mục hình ảnh cụ thể.

Một kẻ tấn công có thể khai thác lỗ hổng này bằng cách tải lên một tệp PHP độc hại vào một trong các thư mục hình ảnh bị ảnh hưởng. Khi người dùng truy cập tệp này, mã độc hại sẽ được thực thi với quyền của người dùng đang chạy WPanel.

Lỗ hổng này có mức độ nghiêm trọng cao và có thể được sử dụng để chiếm quyền kiểm soát hoàn toàn đối với hệ thống chạy WPanel.

Để giải quyết lỗ hổng này, nhà phát triển WPanel đã phát hành bản vá bảo mật vào ngày 16 tháng 8 năm 2021. Người dùng WPanel nên cập nhật lên phiên bản 4.3.2 hoặc cao hơn để được bảo vệ khỏi lỗ hổng này.

### Cách thức hoạt động

Quản trị viên phản hồi nhanh nhờ AdminLTE.

Quản lý tài khoản với ACL cấp quyền truy cập bằng URI.

Posts - có thể là Tin tức hoặc chỉ là Blog trên trang web của bạn.

Pages - quản lý các trang cố định trên trang web của bạn, chẳng hạn như trang 'Giới thiệu'.

Banners - Quản lý slide banner của trang chủ.

Galleries - Quản lý thư viện ảnh trên trang web.

Video Youtube.

Menu management.

Newsletters - Thu thập khách hàng tiềm năng trên trang web của bạn.

Quản lý tài khoản

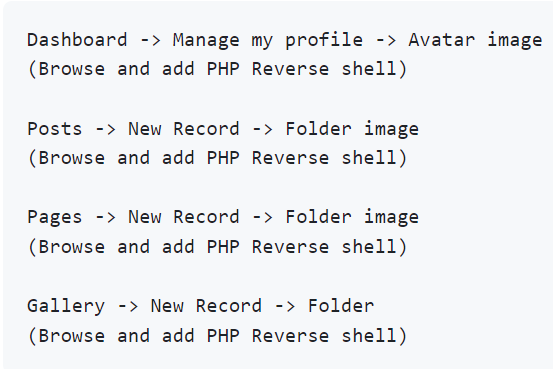
Cài đặt động

### Cách thức khai thác

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

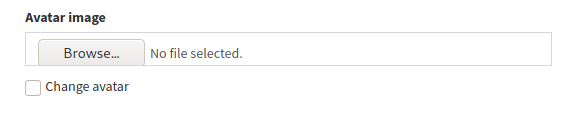
Các tệp được tải lên gây ra rủi ro đáng kể cho các ứng dụng. Tuy nhiên Không có hạn chế về loại tệp để tải lên. Người dùng được xác thực có thể tải lên bất kỳ loại tệp nào trên hệ thống và thực thi. Ví dụ: trong Galleries, người dùng được nhắc tải hình ảnh lên và nếu người dùng chọn tệp không phải hình ảnh thì nó vẫn được phép tải lên.

Ngoài ra có rất nhiều vị trí cũng có thể tải tệp lên tùy ý



Hình . Các vị trí tải được tệp tùy ý

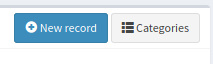
1. Tải lên hình ảnh đại diện bảng điều khiển

[](https://latestpcsolution.files.wordpress.com/2021/06/001.png)Vào Dashboard và nhấn vào Duyệt để thay đổi ảnh Avatar

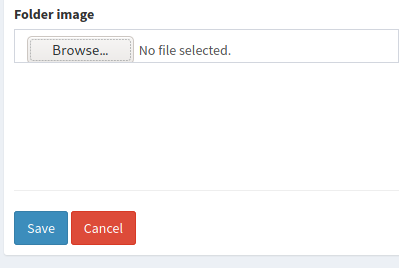
Hình . Tải lên ảnh đại diện

Thêm tệp reverse shell PHP thay vì hình ảnh, đánh dấu vào ‘change avatar< a i=4>' và nhấp vào 'save'. Bây giờ hãy tải lại Trang dashboard và đưa reverse shell trở lại máy tấn công của bạn.

1. Tải lên hình ảnh thư mục post

[](https://latestpcsolution.files.wordpress.com/2021/06/002.png)Đi tới post, nhấp vào 'new record ' và Dưới 'Folder image' nhấp vào duyệt. Một lần nữa thêm reverse shell PHP thay vì hình ảnh, hãy truy cập bài đăng và lấy lại shell.

Hình . New record

[](https://latestpcsolution.files.wordpress.com/2021/06/003.png)

Hình . Folder image

2 cách khai thác còn lại vào thư mục pages và gallery làm tương tự như trên.

### Biện pháp khắc phục

Sử dụng tường lửa để chặn lưu lượng truy cập từ các nguồn không đáng tin cậy.

Sử dụng hệ thống phát hiện xâm nhập (IDS) để phát hiện các cuộc tấn công tiềm năng.

Sử dụng hệ thống giảm thiểu tấn công từ chối dịch vụ (DDoS) để giảm thiểu tác động của các cuộc tấn công DoS.

# THỰC NGHIỆM

## Khai thác lỗ hổng CVE 2020-7246

### Mô hình triển khai

Hình . Mô hình CVE 2020-7246

Chuẩn bị :

* Máy kali làm máy kali làm máy attacker
* Máy ubuntu 22.04 làm máy chủ (victim):
* Apache2
* Mysql-server8.0
* Tạo database cho qdpm, có user database quản lý
* Php7.4
* libapache2-mod-php, php-mysql
* qdpm
* Đăng nhập với tư cách là admin tạo user có quyền thấp hơn

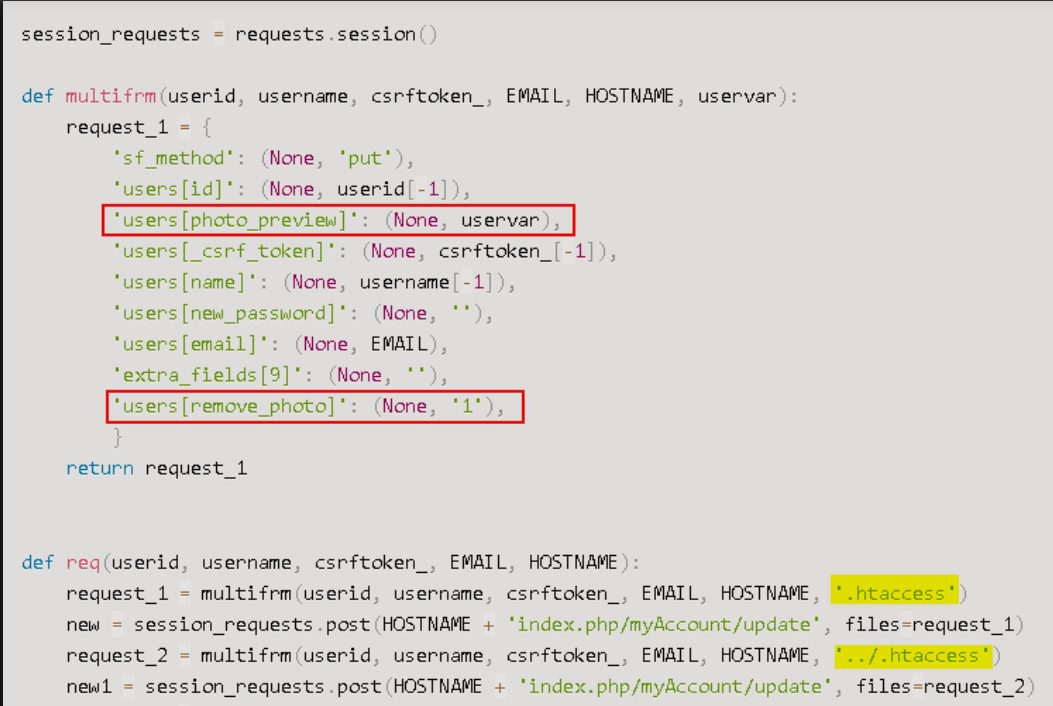
### Kịch bản khai thác

* Việc khai thác bắt đầu bằng cách gửi hai yêu cầu:

users[remove\_photo] được đặt thành 1

**'users[remove\_photo]': (None, '1')**

users[photo\_preview] được đặt thành ".htaccess" và "../.htaccess."

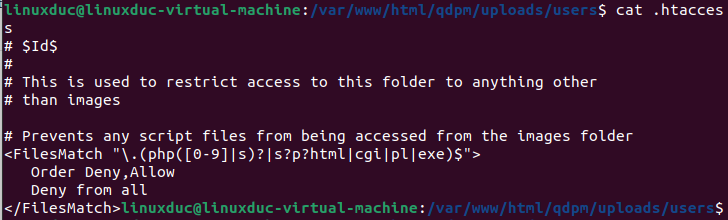
**'users[photo\_preview]': (None, uservar)**

Hình . Gửi yêu cầu

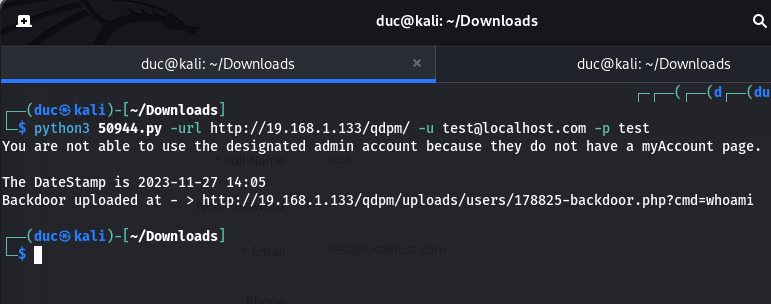
Phần thứ hai của việc khai thác liên quan đến việc tải lên tệp PHP và truy cập trực tiếp vào tệp đó backdoor.php, giúp có được khả năng thực thi các lệnh trên máy chủ. Do đã xóa tệp .htaccess nên lỗ hổng nằm ở chỗ chức năng tải lên không áp dụng bất kỳ xác thực nào đối với các tệp đã tải lên, dẫn đến việc tải tệp lên không bị hạn chế.



Hình . Thực hiện yêu cầu backdoor

Với việc đặt users[photo\_preview] thành ".htaccess" và "../.htaccess." sẽ xóa tệp .htaccess điều này dẫn đến loại bỏ biện pháp bảo vệ, hạn chế truy cập được áp dụng khi chạy các loại tệp nguy hiểm (php, html, exe)

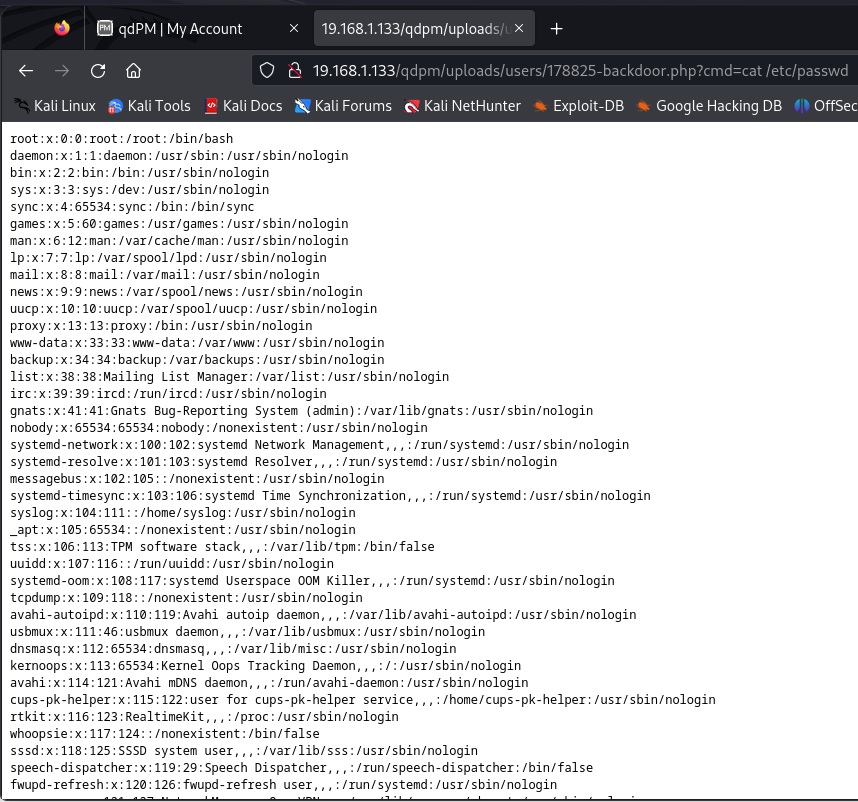
Hình . Đặt users[photo\_preview] thành .htaccess

Thực hiện chạy file python

Hình . Chạy file python

Truy cập backdoor được tạo theo đường dẫn , nhập lệnh sau cmd=

Hình . Thực hiện thành công lệnh shell qua backdoor



### Đánh giá và kết luận

CVE-2020-7246 là CVE nguy hiểm cho người dùng sử dụng ứng dụng qdpm, lỗ hổng này cho phép tin tặc thực hiện loại bỏ bất kỳ tệp nào chúng muốn khỏi máy chủ ,đồng thời tấn công từ xa và thực hiện các hoạt động độc hại trên hệ thống mà không cần đăng nhập. Lỗ hổng này đã được đánh giá với mức độ nguy hiểm cao và có thể dẫn đến các hậu quả nghiêm trọng như chiếm quyền điều khiển hệ thống, lấy cắp thông tin, phá hoại dữ liệu.

Do đã có bản cập nhật qdpm9.2 vá lỗi trên nên trong hiện tại, CVE 2020-7246 không còn là một mối đe dọa lớn đối với người dùng nếu họ đã nâng cấp và cập nhật hệ thống của mình đầy đủ. Tuy nhiên, đây là một lời nhắc nhở quan trọng về tầm quan trọng của việc đảm bảo bảo mật cho hệ thống và nâng cấp thường xuyên để bảo vệ khỏi các lỗ hổng bảo mật mới.

## Khai thác lỗ hổng CVE 2021-34257

### Mô hình triển khai

-Ubuntu 20.04:

* Apache2
* PHP 7.4
* WPanel 4.3.1 có lỗ hổng
* SQLite3

### Kịch bản khai thác (tại sao up đc file 50255.txt và đổi đc tên, ghi rõ các bước làm, vẽ sơ đồ các máy thực nghiệm, rõ ip)

-Đổi tên thư mục mới tải về và thực hiện chỉnh sửa file

mv 50255.txt 50255.py

nano 50255.py

A screen shot of a computer

Description automatically generated +Thực hiện đổi thành url vào trang web mục tiêu và tài khoản mật khâu đã có trong database của wpanel

Hình . Đổi url, email, password

A screen shot of a computer

Description automatically generated +Đổi ip của attacker

Hình . Đổi ip của attacker

+Save lại file

-Chạy file py và thực hiên khai thác

A screenshot of a computer

Description automatically generated +python3 50255.py

Hình . Chạy file python3 50255.py

+Có thể chọn 1 trong 2 link dể truy cập

A screenshot of a computer

Description automatically generated

Hình . Link truy cập

A screenshot of a computer

Description automatically generated+Sử dụng câu lệnh Nc -lp 9000

Hình . Sử dụng lệnh nc -lp 9000

### Đánh giá và kết luận

Lỗ hổng RCE trong WPanel 4.3.1 là một lỗ hổng nghiêm trọng vì nó có thể cho phép kẻ tấn công thực thi mã độc trên máy chủ chạy WPanel. Điều này có thể dẫn đến một số hậu quả nghiêm trọng, bao gồm:

Kẻ tấn công có thể chiếm quyền kiểm soát hoàn toàn máy chủ và sử dụng nó cho các mục đích bất hợp pháp, chẳng hạn như lưu trữ phần mềm độc hại hoặc tấn công các trang web khác.

Kẻ tấn công có thể truy cập và đánh cắp dữ liệu nhạy cảm, chẳng hạn như thông tin đăng nhập của người dùng hoặc dữ liệu tài chính.

Kẻ tấn công có thể thay đổi hoặc xóa dữ liệu trên máy chủ.

Lỗ hổng này có thể được khai thác bởi bất kỳ ai có quyền truy cập vào trang web WPanel. Điều này có nghĩa là kẻ tấn công có thể khai thác lỗ hổng này thông qua một cuộc tấn công phishing hoặc một cuộc tấn công xã hội khác.

KẾT LUẬN

Trong bài báo cáo này, chúng em đã nêu cơ sở lí thuyết cũng như mô tả và cách khai thác một số CVE: CVE-2022-3357 và CVE-2021-3493. Trong quá trình thực hiện bài tập báo cáo này, do kiến thức cũng như kinh nghiệm của nhóm chúng em còn hạn chế nên một số phần của bài thực tập vẫn chưa được trình bày sâu và kỹ, tuy còn nhiều thiếu sót về mặt kiến thức nhưng chúng em cũng đã thực hiện khai thác thành công hai CVE kể trên.

TÀI LIỆU THAM KHẢO

[1] [CVE - CVE (mitre.org)](https://cve.mitre.org/)

[2] [Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers (exploit-db.com)](https://www.exploit-db.com/)

[3] [https://medium.com/@tobinmshields/qdpm-v9-1-authenticated-rce-exploit-f4b84e19df00](https://l.messenger.com/l.php?u=https%3A%2F%2Fmedium.com%2F%40tobinmshields%2Fqdpm-v9-1-authenticated-rce-exploit-f4b84e19df00&h=AT0RgOLCV7huEPCZjxkexvHNDFrflfG5NoM8VM5EXZYOqOpMctylf7YFkgP0BTEitG6P0__uhDeq2ZbZtR73OCz6oJ1r3Xd_9IRZZgCNnGvRObN09aQDJn_QkV9F1liLi98wXQ)

[4] <https://breakandpray.com/cve-2020-7246-a-remote-code-execution-rce-vulnerability-in-qdpm-9-1/>

[5] [https://www.imperva.com/learn/application-security/remote-code-execution/](https://l.messenger.com/l.php?u=https%3A%2F%2Fwww.imperva.com%2Flearn%2Fapplication-security%2Fremote-code-execution%2F&h=AT0RgOLCV7huEPCZjxkexvHNDFrflfG5NoM8VM5EXZYOqOpMctylf7YFkgP0BTEitG6P0__uhDeq2ZbZtR73OCz6oJ1r3Xd_9IRZZgCNnGvRObN09aQDJn_QkV9F1liLi98wXQ)

[6]<https://docs.google.com/document/d/13ZZSm0DL1Ie6r_fU5ZdDKGZ4defFqiFXMG--zDo8S10/edit#heading=h.gjdgxs>

[7] <https://latestpcsolution.wordpress.com/2021/06/05/wpanel4-cms-authenticated-rce/>

[8] <https://avd.aquasec.com/nvd/2021/cve-2021-34257/>

PHỤ LỤC

1.CVE-2020-7246

* Cài vmware tool:

Sudo apt update

sudo apt install open-vm-tools-desktop open-vm-tools

reboot

* Install apache

sudo apt install apache2 -y

* Install mysql-server-8.0

apt -y install mysql-server-8.0

* Install PHP 7.4

sudo apt install software-properties-common

sudo add-apt-repository ppa:ondrej/php -y

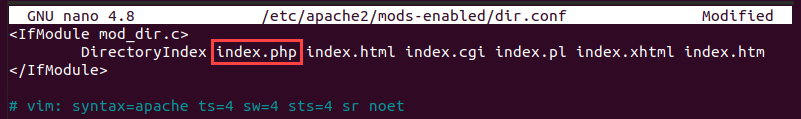
sudo apt install php7.4

sudo apt install php7.4-{cli,common,curl,zip,gd,mysql,xml,mbstring,json,intl}

sudo update-alternatives --config php (chọn phiên bản 7.4)

sudo apt install php libapache2-mod-php7.4

sudo nano /etc/apache2/mods-enabled/dir.conf (đặt index.php lên đầu như hình)



Hình . Chuyển index.php

* Tải ứng dụng qdpm9.1 có lỗ hổng

Sudo mkdir /var/www/html/qdpm

Di chuyển ứng dụng qdpm9.1 (file zip) vào thư mục /var/www/html/qdpm

Unzip f9…qdpm9.1(file trên)

sudo chown -R www-data: /var/www/html/qdpm/

sudo service apache2 restart

* Tạo CSDL

mysql -u root -p

mysql> CREATE DATABASE qdpm;

mysql>CREATE USER 'qdpm\_user'@'localhost' IDENTIFIED BY 'StrongPasswordHere';

mysql>GRANT ALL PRIVILEGES ON qdpm\_db.\* TO 'qdpm\_user'@'localhost';

mysql> FLUSH PRIVILEGES;

mysql> \q

systemctl restart apache2

* Vào qdpm

http://localhost/qdpm

2.CVE-2021-34257

Ubuntu 22.04

* Cài vmware tool:

Sudo apt update

sudo apt install open-vm-tools-desktop open-vm-tools

reboot

* Install apache

sudo apt install apache2 -y

* Install PHP 7.4

sudo apt install software-properties-common

sudo add-apt-repository ppa:ondrej/php -y

sudo apt install php7.4

sudo apt install php7.4-{cli,common,curl,zip,gd,mysql,xml,mbstring,json,intl}

sudo update-alternatives --config php (chọn phiên bản 7.4)

sudo apt install php libapache2-mod-php7.4

sudo nano /etc/apache2/mods-enabled/dir.conf

* Tải ứng dụng wpanel4.3.1 có lỗ hổng

Di chuyển ứng dụng wpanel4.3.1 (file zip) vào thư mục /var/www/html

Unzip file

sudo chown -R www-data: /var/www/html

sudo service apache2 restart

* Tạo CSDL SQLite3

sudo apt update

sudo apt install sqlite3

sqlite3 –version

sqlite3 database.db

sqlite> CREATE TABLE database(id integer NOT NULL, name text NOT NULL);

sqlite> INSERT INTO database VALUES(1, “database1”);

sqlite> INSERT INTO database VALUES(2, “database2”);

sqlite> INSERT INTO database VALUES(3, “database3”);

systemctl restart apache2

* Cài đặt wpanel

Chạy lệnh composer để tạo dự án

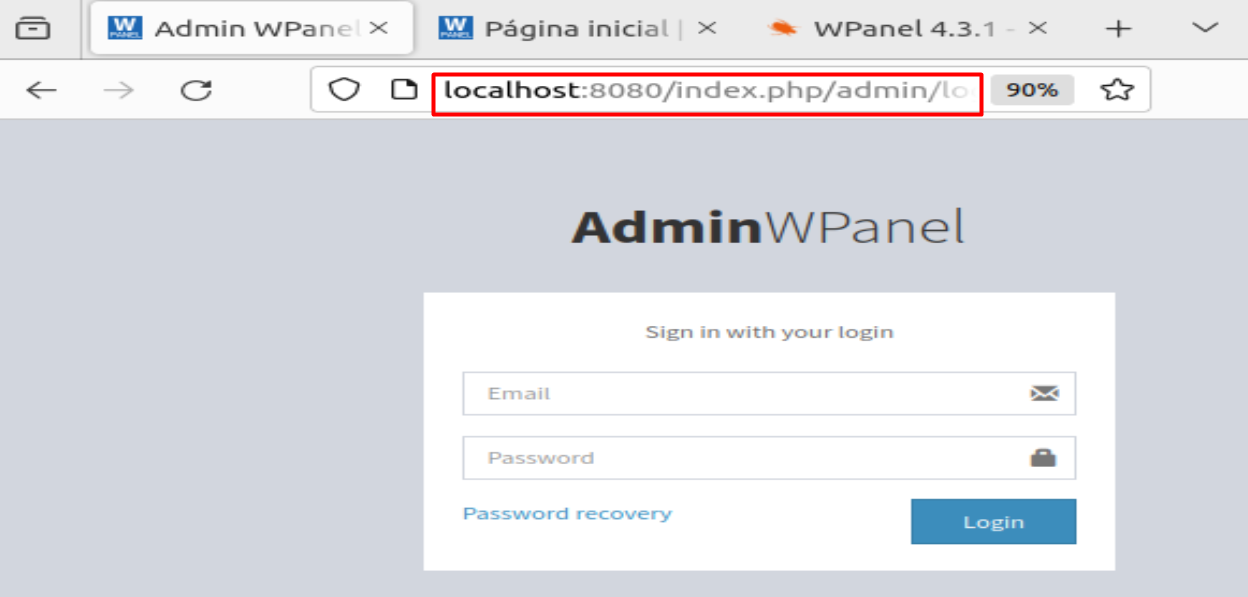
composer create-project "wpanel/wpanel4-cms" Blog

Truy cập thư mục Blog đã tạo ở bước trước và chạy tập lệnh bắt đầu:

cd Blog

composer run dev

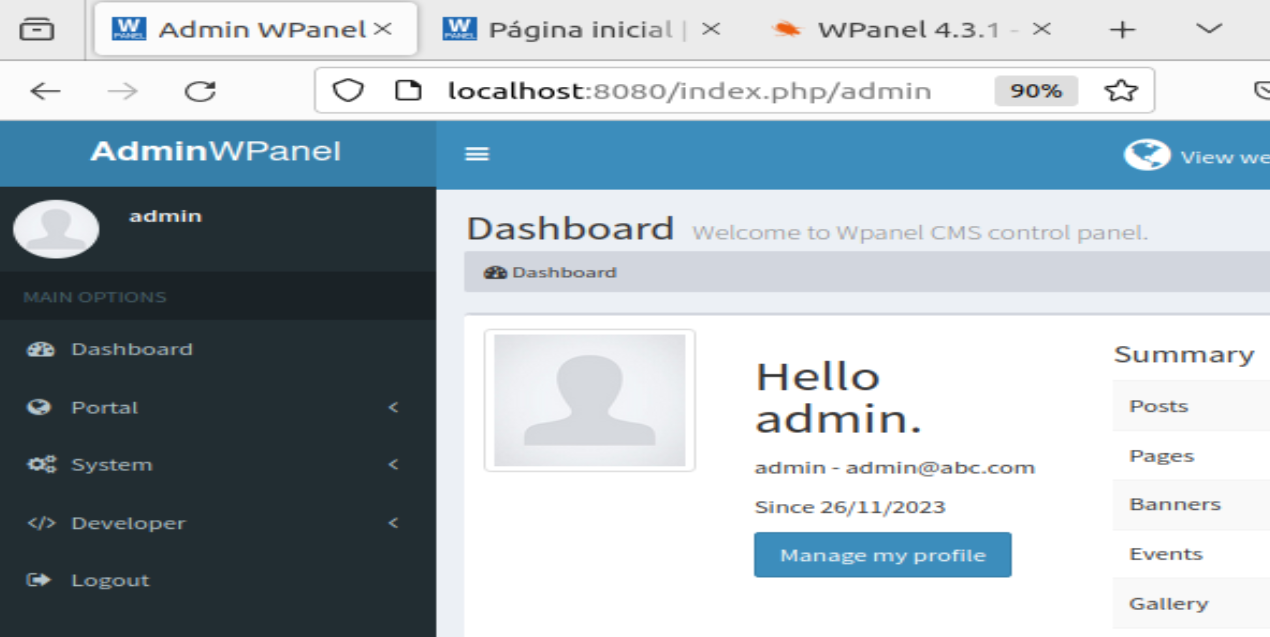
Chạy cài đặt Wpanel bằng cách truy cập <http://localhost:8080/index.php/setup>



Hình . Cài đặt WPanel

Điền vào biểu mẫu với dữ liệu quản trị viên ROOT

Truy cập khu vực quản trị bằng dữ liệu được cung cấp ở bước trước



Hình . Truy cập khu vực quản trị

Wpanel đã chạy tại <http://localhost:8080>



Hình . Chạy thành công WPanel