

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 2023-39147**

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

Đặng Xuân Đức AT170612

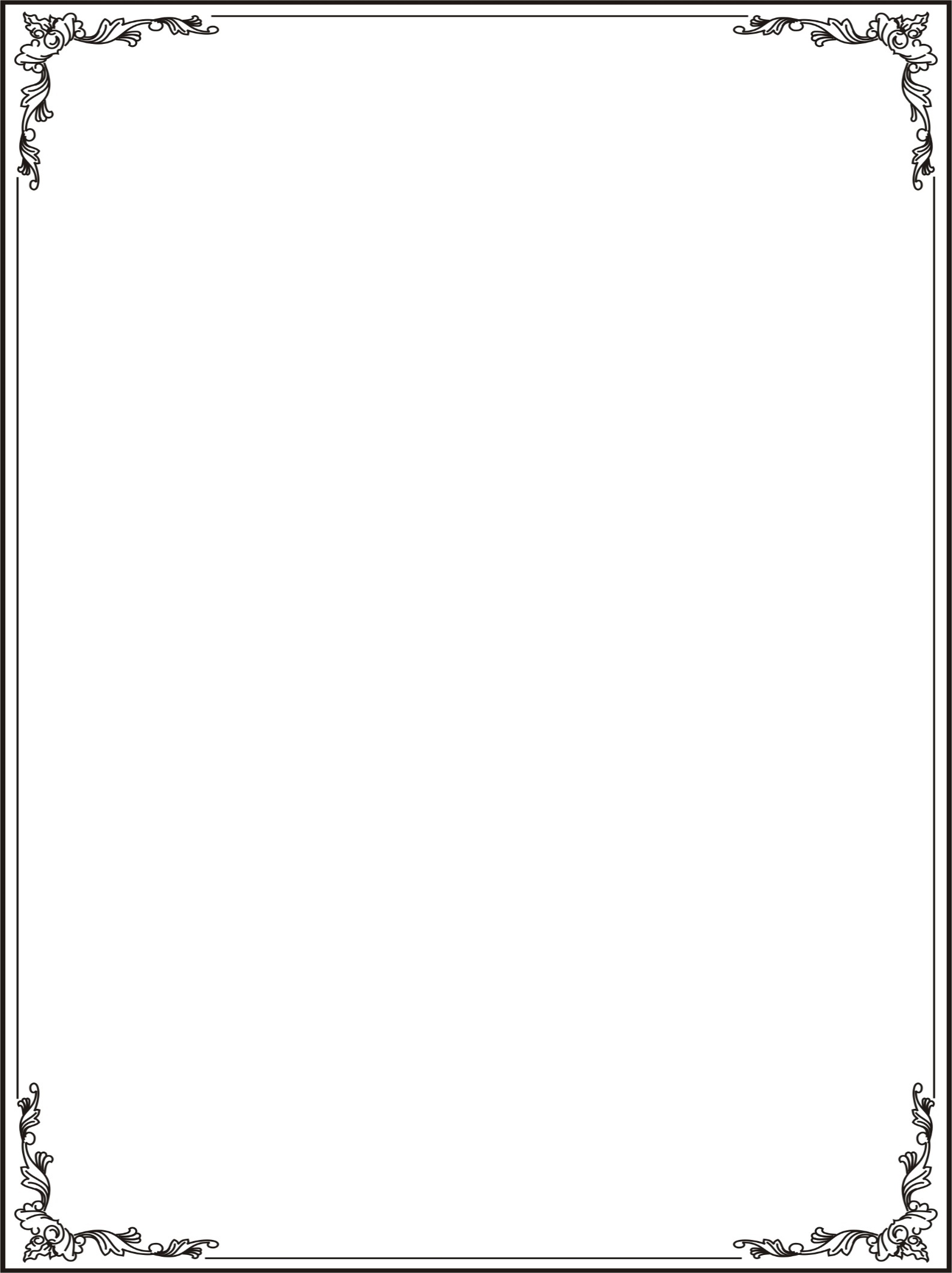
Hoàng Hữu Ánh AT170604

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 2023-39147**

***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-2023-39147, 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-2023-39147và 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:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183949)

[Hình 1.2 Giao diện qdPM 11](#_Toc155183950)

[Hình 1.3 Giao diện Tasks Priorities 11](#_Toc155183951)

[Hình 1.4 Giao diện New Report 12](#_Toc155183952)

[Hình 1.5 Giao diện User Time Report 12](#_Toc155183953)

[Hình 1.6 Giao diện Tickets 13](#_Toc155183954)

[Hình 2.1 CVE-2020-7246 15](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183955)

[Hình 2.2 Chức năng cập nhật tài khoản của qdPM 16](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183956)

[Hình 2.3 Đăng nhập vào user 18](#_Toc155183957)

[Hình 2.4 Loại bỏ biện pháp baoe vệ 19](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183958)

[Hình 2.5 My Details của qdPM 19](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183959)

[Hình 2.6 Up file 19](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183960)

[Hình 2.7 Nội dung tệp .htaccess 20](#_Toc155183961)

[Hình 2.8 Xóa ảnh hồ sơ 20](#_Toc155183962)

[Hình 2.9 Request xóa hình ảnh 21](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183963)

[Hình 2.10 Thay đổi giá trị users[photo\_preview] 21](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183964)

[Hình 2.11 file .htaccess đã bị xóa 21](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183965)

[Hình 2.12 File .htaccess tồn tại trong thư mục gốc 21](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183966)

[Hình 2.13 Bước xác minh tệp hình ảnh 22](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183967)

[Hình 2.14 Giao diện uvdesk 24](#_Toc155183968)

[Hình 2.15 Giao diện thêm folder 25](#_Toc155183969)

[Hình 2.16 Tải lên tệp php 25](#_Toc155183970)

[Hình 2.17 Thay đổi nội dung file 26](#_Toc155183971)

[Hình 2.18 Tải tệp php 26](#_Toc155183972)

[Hình 2.19 Xác minh thành công 27](#_Toc155183973)

[Hình 2.20 Mở tệp thành công 27](#_Toc155183974)

[Hình 3.1 Mô hình CVE 2020-7246 29](#_Toc155183975)

[Hình 3.2 Chọn phiên bản php 30](#_Toc155183976)

[Hình 3.3 Chỉnh sửa dir.conf 30](#_Toc155183977)

[Hình 3.4 Gửi yêu cầu 31](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183978)

[Hình 3.5 Thực hiện yêu cầu backdoor 32](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183979)

[Hình 3.6 Đặt users[photo\_preview] thành .htaccess 32](file:///C:\Users\chieu\Downloads\Nhóm1_CVE-2023-39147-CVE-2020-7246.docx#_Toc155183980)

[Hình 3.7 Chạy file python 33](#_Toc155183981)

[Hình 3.8 Thực hiện thành công lệnh shell qua backdoor 33](#_Toc155183982)

[Hình 3.9 Mô hình CVE 2023-39147 34](#_Toc155183983)

[Hình 3.11 Mở file thành công 38](#_Toc155183984)

MỤC LỤC

[LỜI CẢM ƠN iii](#_Toc155183985)

[LỜI NÓI ĐẦU iv](#_Toc155183986)

[DANH MỤC TỪ VIẾT TẮT v](#_Toc155183987)

[DANH MỤC HÌNH VẼ vi](#_Toc155183988)

[CHƯƠNG 1. CƠ SỞ LÝ THUYẾT 3](#_Toc155183989)

[1.1 Giới thiệu về lỗ hổng RCE 3](#_Toc155183990)

[1.1.1 Khái niệm 3](#_Toc155183991)

[1.1.2 Cơ chế hoạt động của RCE 4](#_Toc155183992)

[1.1.3 Tác động của lỗ hổng RCE 6](#_Toc155183993)

[1.1.4 Phân loại tấn công RCE 7](#_Toc155183994)

[1.1.5 Giảm thiểu và phát hiện cuộc tấn công RCE 8](#_Toc155183995)

[1.1.6 Phương pháp ngăn chặn cuộc tấn công RCE 8](#_Toc155183996)

[1.2 Giới thiệu về Uvdesk và những điểm yếu của Uvdesk 9](#_Toc155183997)

[1.2.1 Tổng quan về Uvdesk 9](#_Toc155183998)

[1.2.2 Những điểm yếu của Uvdesk 10](#_Toc155183999)

[1.3 Giới thiệu về qdPM v9.1 và những điểm yếu của qdPM v9.1 10](#_Toc155184000)

[1.3.1 Tổng quan về qdPM v9.1 10](#_Toc155184001)

[1.3.2 Những điểm yễu của qdPM v9.1 13](#_Toc155184002)

[CHƯƠNG 2. GIỚI THIỆU VỀ CVE-2023-39147VÀ CVE-2020-7246 15](#_Toc155184003)

[2.1 CVE-2020-7246 15](#_Toc155184004)

[2.1.1 Mô tả lỗ hổng 15](#_Toc155184005)

[2.1.2 Cách thức hoạt động 16](#_Toc155184006)

[2.1.3 Cách thức khai thác 18](#_Toc155184007)

[2.1.4 Biện pháp khắc phục 22](#_Toc155184008)

[2.2 CVE- 2023-39147 22](#_Toc155184009)

[2.2.1 Mô tả lỗ hổng 22](#_Toc155184010)

[2.2.2 Cách thức hoạt động 23](#_Toc155184011)

[2.2.3 Cách thức khai thác 24](#_Toc155184012)

[2.2.4 Biện pháp khắc phục 27](#_Toc155184013)

[CHƯƠNG 3. THỰC NGHIỆM 29](#_Toc155184014)

[3.1 Khai thác lỗ hổng CVE 2020-7246 29](#_Toc155184015)

[3.1.1 Mô hình triển khai và cài đặt 29](#_Toc155184016)

[3.1.2 Kịch bản khai thác 31](#_Toc155184017)

[3.1.3 Đánh giá và kết luận 33](#_Toc155184018)

[3.2 Khai thác lỗ hổng CVE 2023-39147 34](#_Toc155184019)

[3.2.1 Mô hình triển khai và cài đặt 34](#_Toc155184020)

[3.2.2 Kịch bản khai thác 38](#_Toc155184021)

[3.2.3 Đánh giá và kết luận 38](#_Toc155184022)

[KẾT LUẬN 40](#_Toc155184023)

[TÀI LIỆU THAM KHẢO 41](#_Toc155184024)

[PHỤ LỤC 42](#_Toc155184025)

# 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.

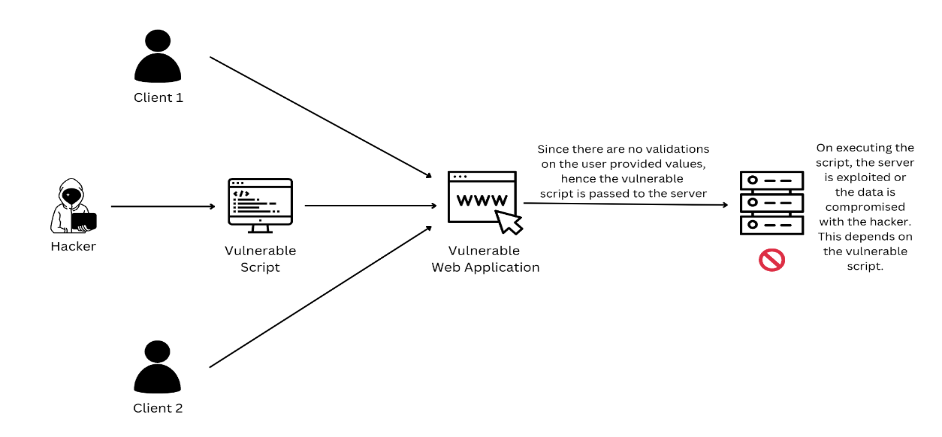
Khi phát hiện ra lỗ hổng mã từ xa, những kẻ tấn công thường khai thác lỗ hổng này ,tin tặc sử dụng các kỹ thuật như injection attacks (SQL injection, OS command injection), deserialization exploits, hay tận dụng các lỗ hổng bảo mật để chèn payload của mình vào hệ thống.

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 Uvdesk và những điểm yếu của Uvdesk

### Tổng quan về Uvdesk

Uvdesk là một hệ thống hỗ trợ khách hàng (CRM) dựa trên đám mây, cung cấp các tính năng toàn diện để giúp doanh nghiệp hỗ trợ khách hàng một cách hiệu quả.

Đặc điểm chính của Uvdesk:

* Mã nguồn mở: Uvdesk sử dụng mã nguồn mở, cho phép người dùng tùy chỉnh và mở rộng theo nhu cầu cụ thể của họ. Điều này mang lại sự linh hoạt và tích hợp dễ dàng với các hệ thống khác.
* Đa kênh hỗ trợ: Hỗ trợ nhiều kênh liên lạc bao gồm email, trò chuyện trực tuyến, hệ thống ticket, và tích hợp các kênh khác. Điều này giúp doanh nghiệp tương tác với khách hàng một cách thuận tiện và hiệu quả.
* Quản lý yêu cầu hỗ trợ: Uvdesk cung cấp các công cụ quản lý yêu cầu, bao gồm phân loại, gắn nhãn, ưu tiên hóa, và theo dõi tiến trình xử lý yêu cầu từ khách hàng.
* Tích hợp API: Hệ thống này có API mạnh mẽ, cho phép tích hợp với các ứng dụng và dịch vụ khác, giúp kết nối và chia sẻ dữ liệu một cách linh hoạt.
* Giao diện người dùng: Giao diện người dùng của Uvdesk, mặc dù mạnh mẽ, có thể được đánh giá là phức tạp đối với người mới sử dụng, yêu cầu một thời gian để làm quen và hiểu rõ.
* Cộng đồng người dùng: Uvdesk có một cộng đồng người dùng lớn, cung cấp nguồn thông tin, hỗ trợ và chia sẻ kiến thức thông qua diễn đàn, tài liệu và các nguồn thông tin khác.
* Hỗ trợ tài liệu: Cung cấp tài liệu hướng dẫn và hỗ trợ kỹ thuật, nhưng việc tìm kiếm thông tin cụ thể có thể đôi khi đòi hỏi sự cẩn thận.
* Tài nguyên hệ thống: Đối với triển khai lớn, Uvdesk có thể đòi hỏi tài nguyên hệ thống cao, và việc quản lý hiệu suất có thể trở thành một thách thức.Uvdesk là một lựa chọn tốt cho các doanh nghiệp thuộc mọi quy mô, từ các doanh nghiệp nhỏ đến các doanh nghiệp lớn. Uvdesk cung cấp các tính năng và tính linh hoạt cần thiết để hỗ trợ khách hàng một cách hiệu quả và mang lại trải nghiệm khách hàng tuyệt vời.

### Những điểm yếu của Uvdesk

Uvdesk cũng có một số điểm yếu, bao gồm:

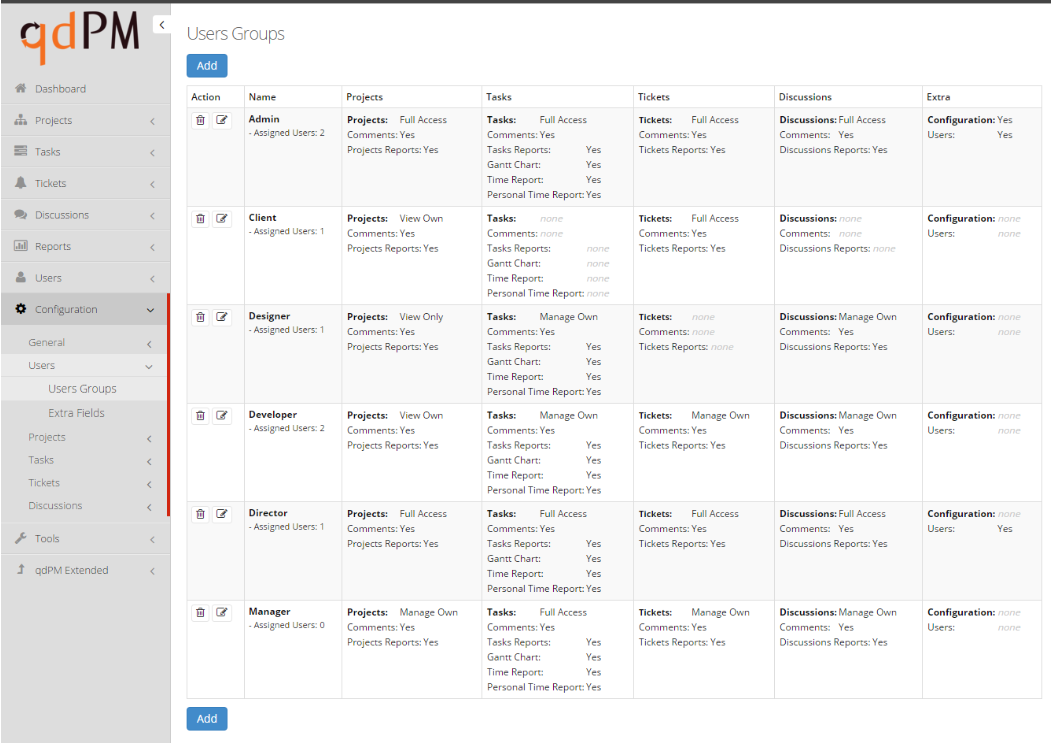
* Giao diện người dùng không thân thiện: Mặc dù có nhiều tính năng, giao diện người dùng của Uvdesk có thể khá phức tạp và khó hiểu đối với người mới sử dụng.
* Yêu cầu kiến thức kỹ thuật: Tùy chỉnh và triển khai Uvdesk có thể đòi hỏi kiến thức kỹ thuật sâu hơn đối với người không chuyên về công nghệ.
* Tài nguyên hệ thống: Khi triển khai trên một quy mô lớn hoặc có lượng yêu cầu lớn, Uvdesk có thể đòi hỏi tài nguyên hệ thống cao.
* Hỗ trợ cộng đồng có thể không đủ: Mặc dù có cộng đồng người dùng rộng lớn, việc tìm kiếm hỗ trợ cụ thể hoặc giải đáp các vấn đề phức tạp có thể không hiệu quả như mong đợi.

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

### Tổng quan về qdPM v9.1

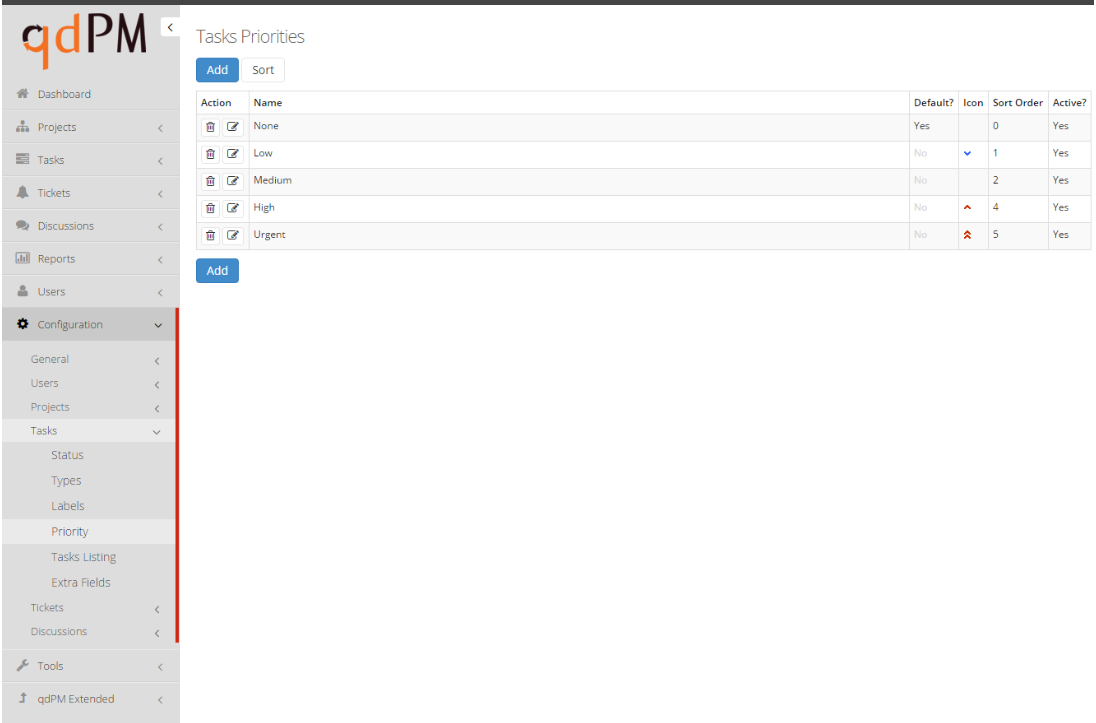
qdPM là một công cụ quản lý dự án dựa trên web miến phí phù hợp với nhóm nhỏ làm việc trên nhiều dự án. Nó có thể cấu hình đầy đủ. Người dùng có thể dễ dàng quản lý Dự án, Nhiệm vụ và Con người. Khách hàng tương tác bằng cách sử dụng Hệ thống yêu cầu được tích hợp vào Quản lý tác vụ.

* Tính năng nổi bật của qdpm:
* qdPM cho phép kiểm soát truy cập của người dùng, chỉ định người dùng cho các nhóm như Customer, Manager, Programmer và định cấu hình quyền cho từng nhóm để kiểm soát những gì họ có quyền truy cập.



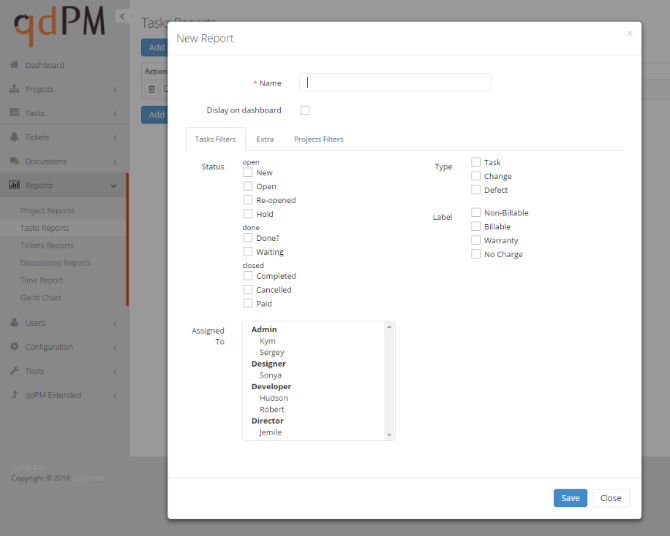
Hình . Giao diện qdPM

* Cho phép định cấu hình trạng thái nhiệm vụ, nhãn, loại, mức độ ưu tiên và các trường bổ sung tùy chỉnh cho nhiệm vụ. Mỗi mục có thứ tự sắp xếp, trạng thái hoạt động và trạng thái mặc định. Trạng thái nhiệm vụ được phân tách theo nhóm: mở/hoàn thành/đóng điều đó giúp người dùng dễ dàng lọc các nhiệm vụ theo nhóm. Người dùng có thể định cấu hình các trường bổ sung của riêng mình cho từng nhãn nhiệm vụ. Ngoài ra, bạn có thể định cấu hình danh sách cột nhiệm vụ



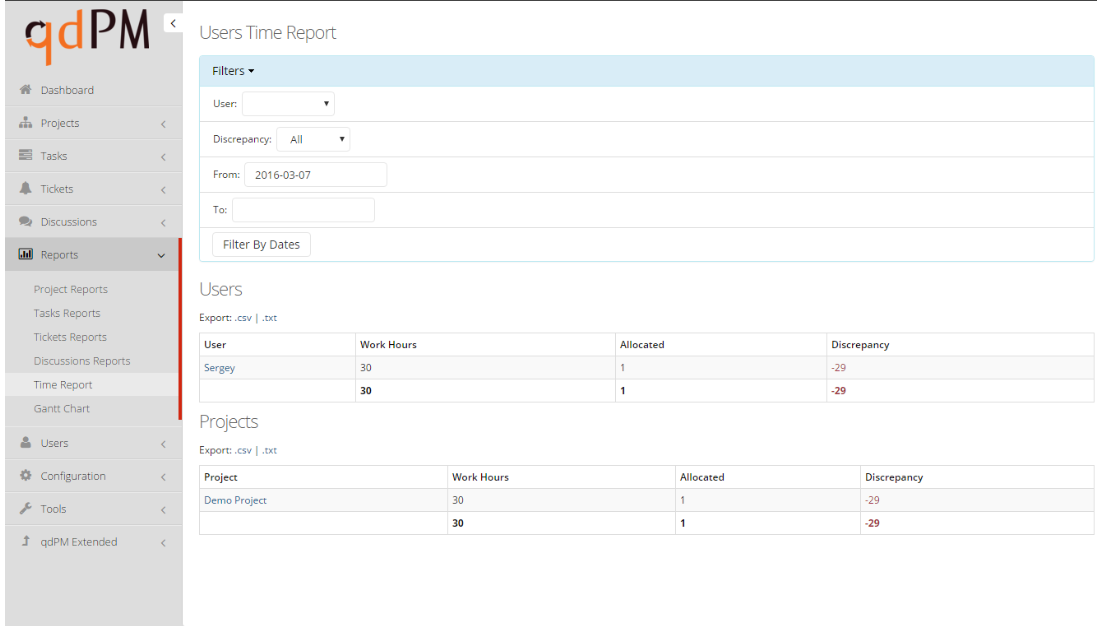
Hình . Giao diện Tasks Priorities

* Tạo báo cáo dự án, nhiệm vụ, thời gian, … tùy chỉnh theo người dùng



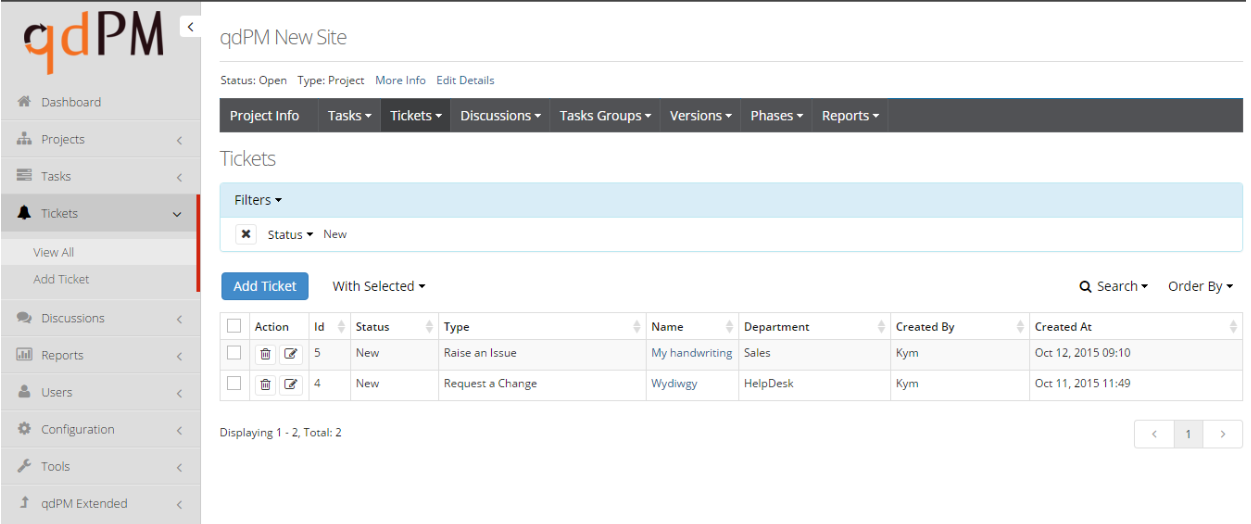
Hình . Giao diện New Report

* Cho phép xem thống kê số giờ làm việc của người dùng, thống kê thời gian ước tính và thực tế cho mỗi nhiệm vụ, lọc dữ liệu theo người dùng, dự án, trạng thái nhiệm vụ hoặc ngày.



Hình . Giao diện User Time Report

* Khách hàng tương tác bằng Hệ thống vé được tích hợp vào Quản lý nhiệm vụ. Khi phản hồi một Vé, bạn có thể dễ dàng tạo một hoặc nhiều Nhiệm vụ liên quan đến Vé đó mà Khách hàng không nhìn thấy.



Hình . Giao diện Tickets

### Những điểm yễu của qdPM v9.1

Lộ thông tin nhạy cảm cho những tác nhân trái phép không có quyền truy cập vào thông tin đó. Lộ thông tin hay còn gọi là rò rỉ thông tin là việc một trang web vô tình tiết lộ thông tin nhạy cảm cho người dùng. Tùy thuộc vào ngữ cảnh, các trang web có thể rò rỉ các loại thông tin quan trọng cho kẻ tấn công như Dữ liệu về những người dùng, mã nguồn, ... Điểm yếu này từng xuất hiện trong phiên bản qdPM 8.3 trước đó khi cho phép kẻ tấn công từ xa lấy thông tin nhạy cảm thông qua yêu cầu trực tiếp tới các mục tới core/config/databases.yml (chứa thông tin cấu hình như chi tiết cơ sở dữ liệu (máy chủ, cổng, tên người dùng và mật khẩu), core/log/qdPM\_prod.log (log lỗi) hoặc core/apps/qdPM/ config/settings.yml (Tiết lộ khóa csrf\_secret cùng với các thông tin quan trọng khác).

Cross-site Scripting (XSS): là một lỗ hổng bảo mật web cho phép kẻ tấn công xâm phạm các tương tác mà người dùng thực hiện với một ứng dụng dễ bị tấn công. Nó cho phép kẻ tấn công phá vỡ chính sách xuất xứ gốc, được thiết kế để tách biệt các trang web khác nhau với nhau. Các lỗ hổng XSS thường cho phép kẻ tấn công giả dạng người dùng nạn nhân, thực hiện bất kỳ hành động nào mà người dùng có thể thực hiện và truy cập bất kỳ dữ liệu nào của người dùng. Nếu người dùng nạn nhân có quyền truy cập đặc quyền vào ứng dụng thì kẻ tấn công có thể giành được toàn quyền kiểm soát tất cả chức năng và dữ liệu của ứng dụng. Cũng trong phiên bản qdPM 8.3 cho phép kẻ tấn công từ xa chèn tập lệnh script hoặc HTML tùy ý thông qua tham số search[keywords] vào trang index.php/users; "Tên ứng dụng" trên index.php/configuration; tên dự án mới trên index.php/projects; tên tác vụ trên index.php/tasks; Tên vé trên index.php/tickets; tên thảo luận trên index.php/discussions; tên báo cáo trên index.php/projectReports; hoặc tên sự kiện trên index.php/scheduler/personal.

Lỗ hổng Unrestricted file upload là khi máy chủ web cho phép người dùng tải tệp lên hệ thống tệp của nó mà không xác thực đầy đủ những thứ như tên, loại, nội dung hoặc kích thước của chúng. Việc không thực thi đúng cách các hạn chế đối với những hạn chế này có thể có nghĩa là ngay cả chức năng tải lên hình ảnh cơ bản cũng có thể được sử dụng để tải lên các tệp tùy ý và có khả năng gây nguy hiểm. Điều này thậm chí có thể bao gồm các tệp tập lệnh phía máy chủ cho phép thực thi mã từ xa. Trường hợp xấu nhất có thể xảy ra là khi một trang web cho phép bạn tải lên các tập lệnh phía máy chủ, chẳng hạn như tệp PHP, Java hoặc Python và cũng được định cấu hình để thực thi chúng dưới dạng mã. Điều này khiến việc tạo web shell của riêng người dùng trên máy chủ trở nên đơn giản. Trong myAccount, dự án, nhiệm vụ, vé, thảo luận, báo cáo và trang lập lịch trong qdPM 8.3 cho phép kẻ tấn công từ xa thực thi mã tùy ý bằng cách tải lên tệp có phần mở rộng thực thi (như PHP), sau đó truy cập tệp đó thông qua yêu cầu trực tiếp tới tệp trong uploads/attachments/ hoặc uploads/users/.

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.

Cross-site request forgery (CSRF) là một lỗ hổng bảo mật web cho phép kẻ tấn công xúi giục người dùng thực hiện các hành động mà họ không có ý định thực hiện. Nó cho phép kẻ tấn công phá vỡ một phần chính sách xuất xứ ban đầu, được thiết kế để ngăn chặn các trang web khác nhau can thiệp lẫn nhau. Trong qdPM 9.2 cho phép Giả mạo yêu cầu trên nhiều trang web (CSRF) thông qua URI index.php/myAccount/update.

# GIỚI THIỆU VỀ CVE-2023-39147VÀ CVE-2020-7246

## CVE-2020-7246

### Mô tả lỗ hổng

Hình . CVE-2020-7246

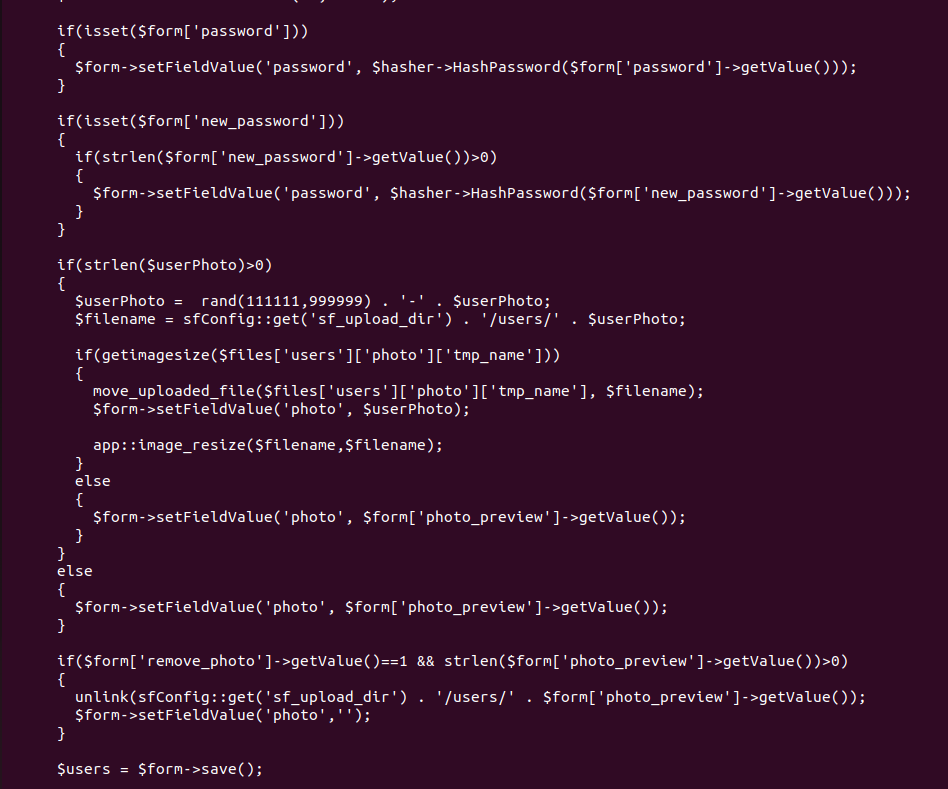
CVE-2020-7246 là một lỗ hổng nguy hiểm với điểm CVSS cao là 8.8 (CVSS- The Common Vulnerability Scoring System là hệ thống đánh giá lỗ hổng bảo mật chung– một tiêu chuẩn ngành để xếp hạng đặc điểm và mức độ nghiêm trọng của các lỗ hổng phần mềm, đã sử dụng thang điểm từ 0 đến 10), theo CVSS thì với số điểm này có khả năng gây hại đáng kể nếu bị khai thác và có thể dẫn đến hậu quả nghiêm trọng, chẳng hạn như mất dữ liệu hoặc tạo khoảng thời gian ngừng hoạt động đáng kể.

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. Kẻ tấn công sử dụng các phương pháp thao túng đường dẫn để khai thác việc xác thực đầu vào không đầy đủ của mục tiêu nhằm có được quyền truy cập vào dữ liệu mà các yêu cầu được định dạng đúng thông thường không thể truy xuất được. Một dạng điển hình của cuộc tấn công này liên quan đến việc chỉ định đường dẫn đến tệp mong muốn cùng với các ký tự dấu chấm-dấu gạch chéo, dẫn đến API hoặc chức năng truy cập tệp đi ra khỏi cấu trúc thư mục dự định và vào hệ thống tệp gốc. Bằng cách thay thế hoặc sửa đổi thông tin đường dẫn dự kiến, chức năng truy cập hoặc API sẽ truy xuất tệp mà kẻ tấn công mong muốn. Các cuộc tấn công này liên quan đến việc kẻ tấn công cung cấp đường dẫn đầy đủ đến tệp được nhắm mục tiêu hoặc sử dụng các ký tự điều khiển (ví dụ: dấu phân cách đường dẫn (/ hoặc \) và/hoặc dấu chấm (.)) để đến các thư mục hoặc tệp mong muốn. Đặc biệt với các 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.

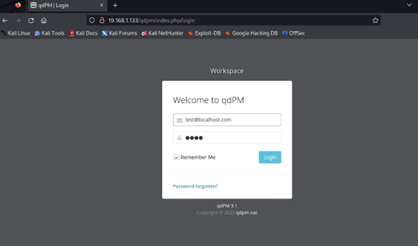
Kiểm Tra và Xử Lý Yêu Cầu Xóa Ảnh:

|  |
| --- |
| 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



Hình . Đăng nhập vào user

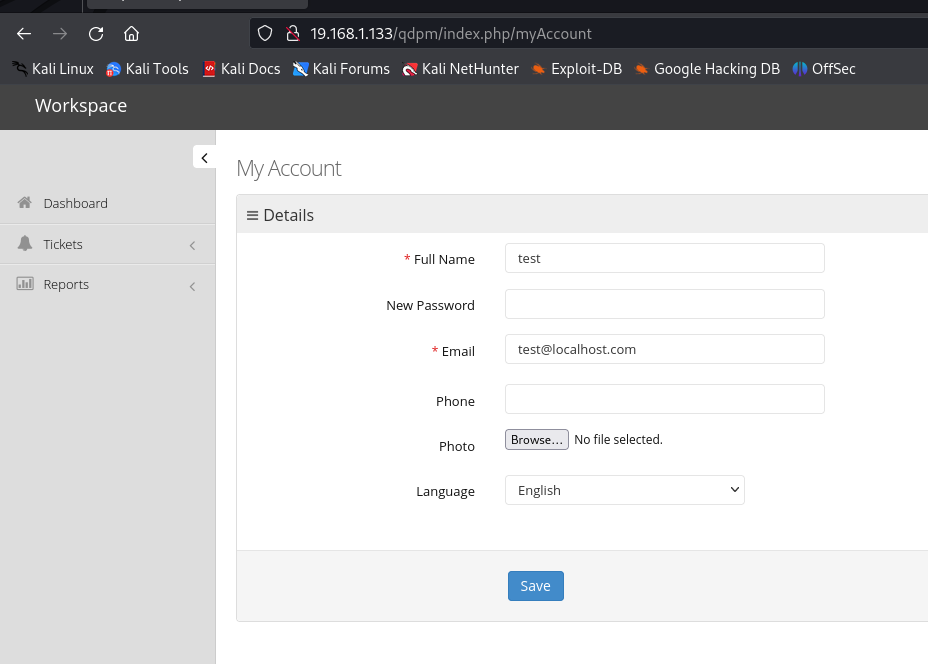
* Thăm dò:

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

Email: test@localhost

Password: test

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)

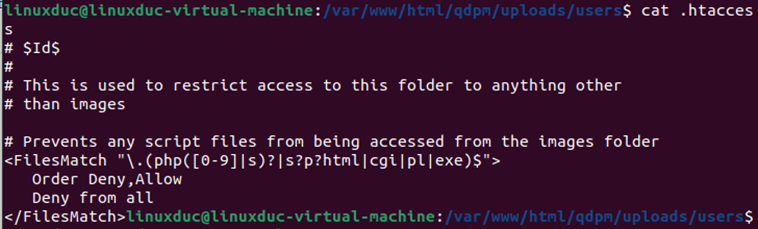
• upload.py (A simple Python file)

• upload.php (A simple PHP file)

• .php

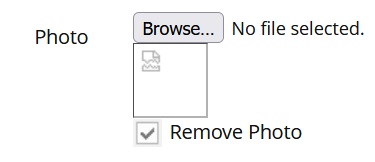
Hình . Up file

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 .htaccess

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

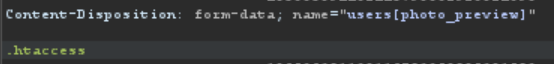


Hình . Xóa ảnh hồ sơ

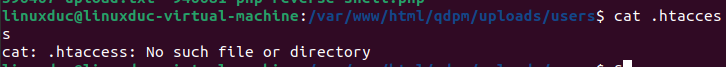
Trong yêu cầu thứ 2 là nơi thông tin dễ bị tấn công với 2 giá trị **users[photo\_preview]** và **users[remove\_photo]**

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

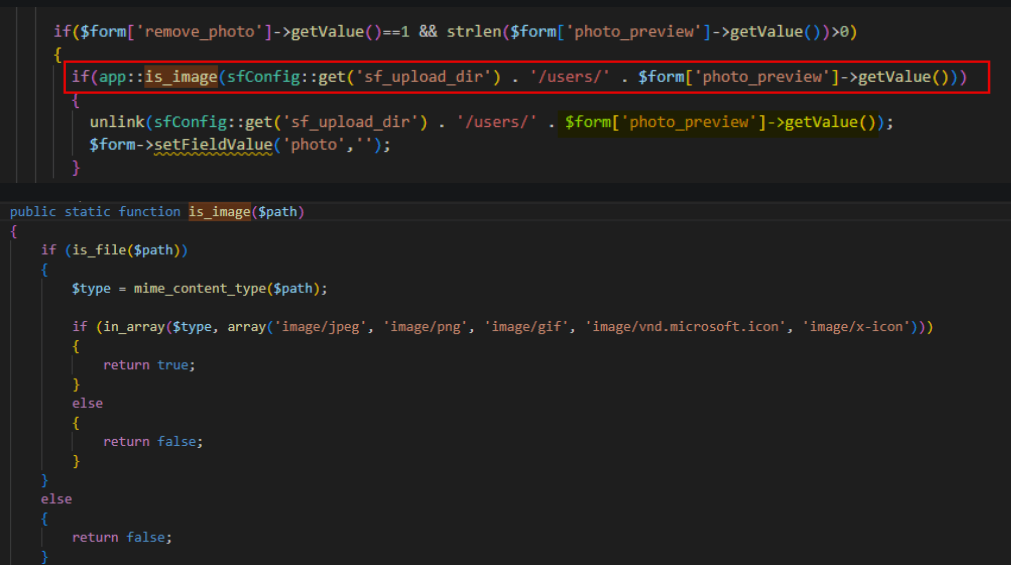
Do tệp .htaccess vẫn tồn tại trong thư mục gốc /uploads/ nên cần thực hiện yêu cầu Burp với **users[photo\_preview]** thành ../.htaccess

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

Cập nhật lên phiên bản mới nhất

 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- 2023-39147

### Mô tả lỗ hổng

Lỗ hổng RCE (Remote Code Execution) trong Uvdesk phiên bản 1.1.3 là một vấn đề bảo mật nghiêm trọng, cung cấp khả năng cho tin tặc thực hiện mã từ xa trên hệ thống của người dùng được xác thực. Lỗ hổng này cho phép người dùng tấn công đăng nhập có thể tải lên các tệp độc hại và sau đó thực thi chúng trên máy chủ hệ thống.

Quá trình khai thác thường diễn ra như sau:

- Tin tặc xác định lỗ hổng và tìm cách tạo tệp độc hại, thường là một tệp có thể thực thi mã (ví dụ: PHP, Python, hoặc tệp tải lên ẩn thông tin bất hợp pháp).

- Tin tặc đăng nhập vào Uvdesk bằng tài khoản có quyền truy cập, sau đó sử dụng lỗ hổng tải lên tệp để đưa tệp độc hại lên hệ thống.

- Khi tệp độc hại được tải lên thành công, tin tặc có thể thực thi mã từ xa thông qua tệp đó, tiềm ẩn nguy cơ kiểm soát hoặc xâm nhập vào hệ thống.

Vấn đề này đặc biệt nguy hiểm vì nó cho phép kẻ tấn công có thể tiến hành thực hiện các hành động không được ủy quyền trên hệ thống, có thể dẫn đến việc chiếm quyền kiểm soát hoặc xâm nhập vào dữ liệu nhạy cảm.

### Cách thức hoạt động

Mã này có vẻ là một đoạn mã Python sử dụng thư viện requests để tạo và gửi các yêu cầu HTTP, đặc biệt là gửi yêu cầu POST và GET đến một URL được cung cấp qua tham số dòng lệnh

* Hàm get\_args() sử dụng thư viện argparse để lấy thông tin từ dòng lệnh khi chương trình được gọi.
* Hai đối số được yêu cầu:

-u hoặc --url: Để cung cấp URL của mục tiêu.

-c hoặc --command: Để cung cấp lệnh cần thực thi.

* Gọi hàm get\_args() để lấy thông tin từ dòng lệnh, như URL và lệnh cần thực thi.

args = get\_args()

* base\_url: Lưu trữ URL của mục tiêu.
* command: Lưu trữ lệnh cần thực thi.
* login\_data: Thông tin đăng nhập để truy cập vào hệ thống Uvdesk.
* files: Định dạng dữ liệu cần gửi trong yêu cầu POST để tải lên tệp shell.php lên hệ thống Uvdesk.
* Tạo một phiên sử dụng thư viện requests để duy trì trạng thái đăng nhập.

s = requests.session()

* Gửi yêu cầu POST để đăng nhập vào hệ thống Uvdesk với thông tin đăng nhập đã được cung cấp.s.post(base\_url + "/en/member/login", data=login\_data)
* Gửi yêu cầu POST để tải lên tệp shell.php lên hệ thống Uvdesk.s.post(base\_url + "/en/member/knowledgebase/folders/new", files=files):
* url\_cmd: Tạo URL chứa lệnh để thực thi thông qua tệp shell.php.
* Gửi yêu cầu GET đến URL tạo ra để thực hiện lệnh từ xa thông qua tệp

shell.php.s.get(url\_cmd)

* In kết quả của lệnh thực thi từ xa trên hệ thống Uvdesk.

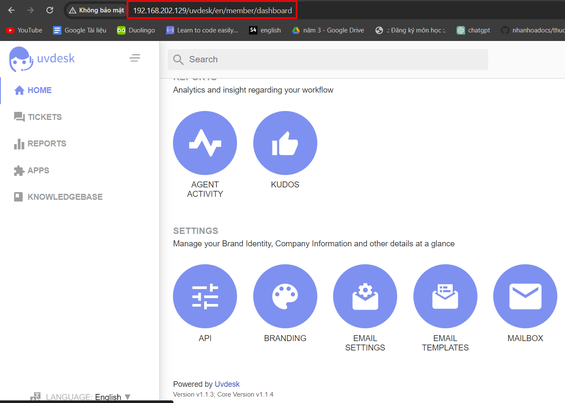
print(cmd.text)

Tổng quan, chương trình này tạo và gửi các yêu cầu HTTP để đăng nhập vào hệ thống Uvdesk, tải lên một tệp PHP có chứa mã để thực thi lệnh từ xa, sau đó gửi yêu cầu để thực thi lệnh từ xa thông qua tệp vừa tải lên. Điều này có thể tạo điều kiện cho việc tấn công vào hệ thống Uvdesk thông qua lỗ hổng RCE

### Cách thức khai thác

Thực thi mã từ xa bằng cách khai thác lỗ hổng bỏ qua loại nội dung trong quá trình tải hình ảnh lên ứng dụng đích

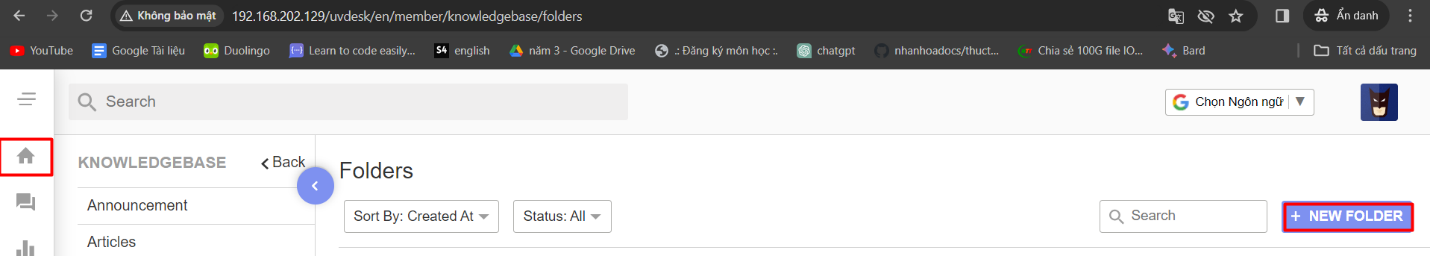
Truy cập theo đường link <http://192.168.202.129/uvdesk/en/member/login> để đăng nhập bằng email và mật khẩu đã tạo trước đó (192.168.202.129 là ip của máy victim)



Hình . Giao diện uvdesk

Lỗ hổng này được xác định trong phiên bản 1.1.3 của uvdesk.

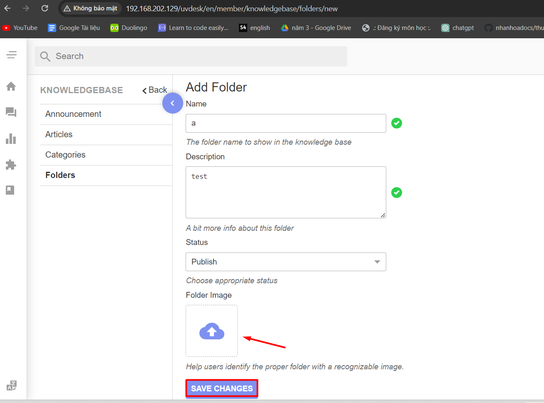
Sau khi đăng nhập vào ứng dụng, điều hướng đến phần "Home" và chọn "Folders", sau đó là "New Folder".



Hình . Giao diện thêm folder

Vì ứng dụng chỉ cho phép tải lên hình ảnh, hãy cố gắng tải lên tệp PHP.

<?php system($\_GET[“cmd”]);?>



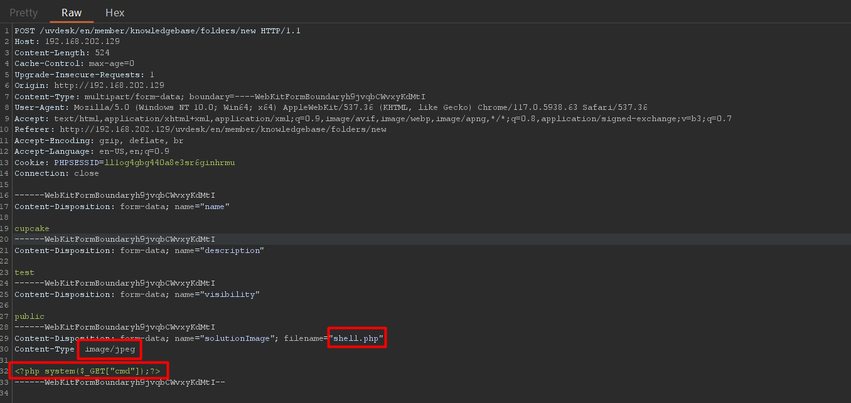
Hình . Tải lên tệp php

Nhận thấy rằng máy chủ mong muốn loại nội dung của tệp được tải lên là hình ảnh, hãy chặn yêu cầu và sửa đổi loại nội dung thành "image/jpeg"

Content-Disposition: form-data; name="solutionImage"; filename="shell.php"

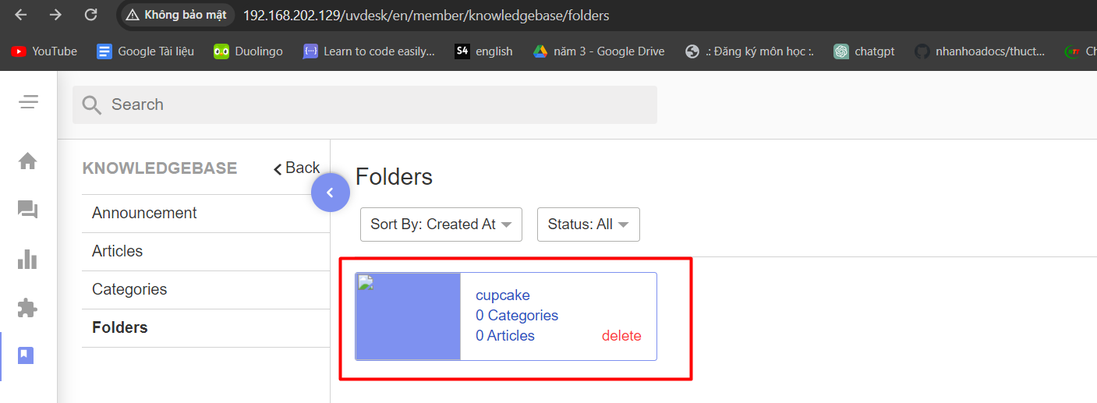
Content-Type: image/jpeg

<?php system($\_GET[“cmd”]);?>



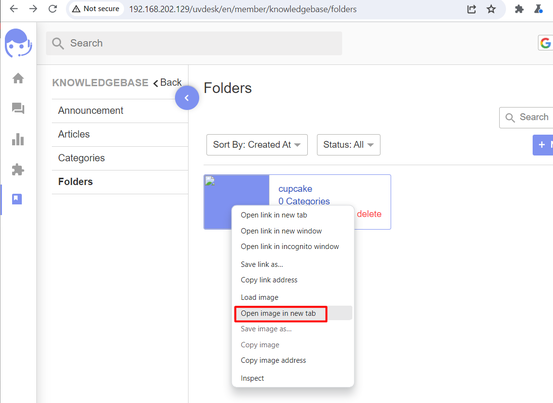
Hình . Thay đổi nội dung file

Tiếp theo, tôi tải tệp PHP lên và máy chủ đã chấp nhận nó, nhầm nó với một tệp hình ảnh hợp pháp.

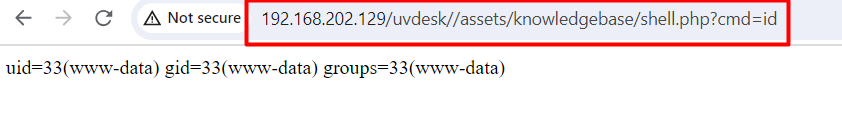


Hình . Tải tệp php

Để xác minh sự thành công của cuộc tấn công, hãy mở tệp PHP đã tải lên trong một tab mới và có thể thực thi mã từ xa.



Hình . Xác minh thành công



Hình . Mở tệp thành công

### Biện pháp khắc phục

Để khắc phục lỗ hổng RCE trong Uvdesk phiên bản 1.1.3 - File Upload Remote Code Execution (Authenticated), các biện pháp sau có thể được thực hiện:

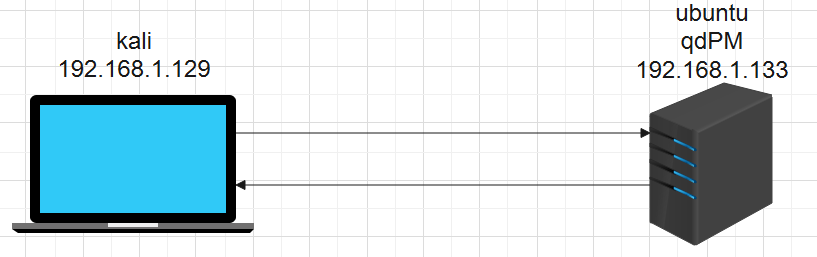
* Cập nhật lên phiên bản mới nhất: Đầu tiên và quan trọng nhất là cập nhật lên phiên bản mới nhất của Uvdesk. Nhà phát triển đã có thể phát hành bản vá lỗi cho lỗ hổng này trong các bản cập nhật sau này. Việc cập nhật sẽ loại bỏ lỗ hổng và bảo vệ hệ thống khỏi việc bị khai thác.
* Tạm ngưng chức năng tải lên tệp: Trong thời gian chờ cập nhật, tạm ngưng hoặc vô hiệu hóa chức năng tải lên tệp từ phía người dùng. Điều này có thể giúp ngăn chặn tin tặc khai thác lỗ hổng trong khi bạn đang chờ đợi bản vá từ nhà phát triển.
* Kiểm tra và xác nhận tệp tải lên: Nếu không thể vô hiệu hóa chức năng tải lên tệp, hãy thực hiện các kiểm tra kỹ thuật để xác định và chặn các tệp độc hại. Bạn có thể áp dụng các quy tắc kiểm tra loại tệp, kiểm tra ký tự hoặc phần mở rộng tệp để ngăn chặn tệp độc hại được tải lên.
* Kiểm tra lại cấu hình và phân quyền: Đảm bảo rằng cấu hình và phân quyền trên hệ thống được thiết lập chặt chẽ để hạn chế quyền truy cập và thực thi tệp từ xa chỉ cho các người dùng có quyền hợp lệ.
* Theo dõi và kiểm tra log: Thường xuyên kiểm tra log hệ thống để phát hiện bất kỳ hoạt động nào không bình thường, nhất là việc tải lên tệp và thực thi mã không xác định.
* Liên hệ với nhà phát triển hoặc cộng đồng hỗ trợ: Nếu không chắc chắn về biện pháp khắc phục hoặc không có thông tin về bản vá từ nhà phát triển, hãy liên hệ với nhà phát triển Uvdesk hoặc cộng đồng người dùng để được hỗ trợ và chỉ dẫn cụ thể.

Việc thực hiện các biện pháp trên là quan trọng để ngăn chặn hoặc giảm thiểu rủi ro từ lỗ hổng RCE trong Uvdesk phiên bản 1.1.3 cho đến khi bạn có thể cập nhật lên phiên bản mới nhất đã được vá lỗi.

# THỰC NGHIỆM

## Khai thác lỗ hổng CVE 2020-7246

### Mô hình triển khai và cài đặt



Hình 3.1 Mô hình CVE 2020-7246

Cài đặt:

- Máy kali làm máy kali làm máy attacker

- Cài đặt máy ubuntu 22.04 làm máy chủ (victim):

- Trên máy chủ ubuntu thực hiện các cài đặt sau:

* Install apache

*sudo apt install apache2 -y*

* Install mysql-server-8.0

*apt -y install mysql-server-8.0*

* Install PHP 7.4

Thêm kho lưu trữ PPA của Ondrej trên Ubuntu 22.04

*sudo apt install software-properties-common*

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

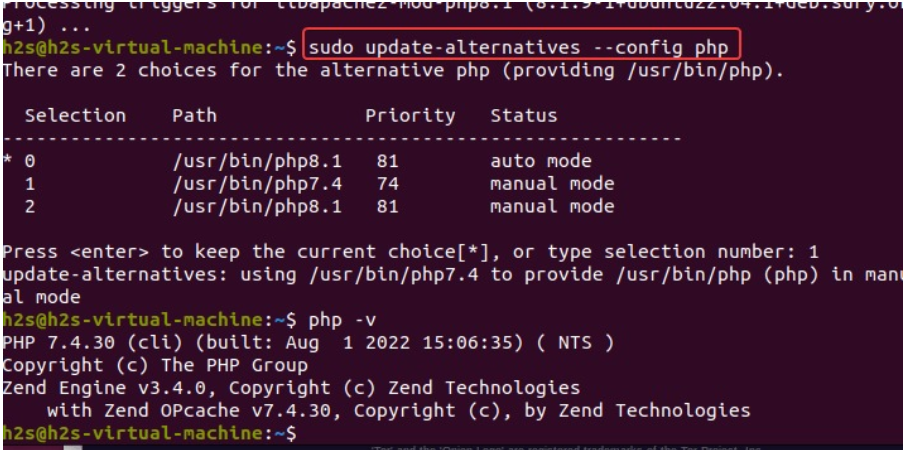
Cài đặt php7.4 và phần mở rộng

*sudo apt install php7.4*

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

Chọn phiên bản php 7.4 làm phiên bản mặc định

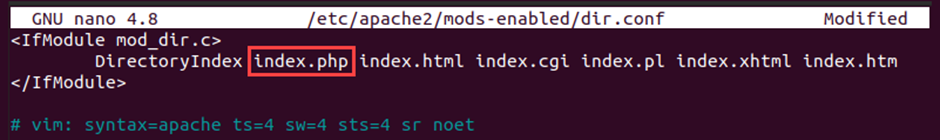
*sudo update-alternatives --config php*



Hình . Chọn phiên bản php

*sudo apt install php libapache2-mod-php7.4*

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



Hình . Chỉnh sửa dir.conf

* Tải ứng dụng qdpm9.1 có lỗ hổng trên exploitDB

*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 với tư cách là quản trị viên và tạo user có quyền thấp hơn

http://localhost/qdpm

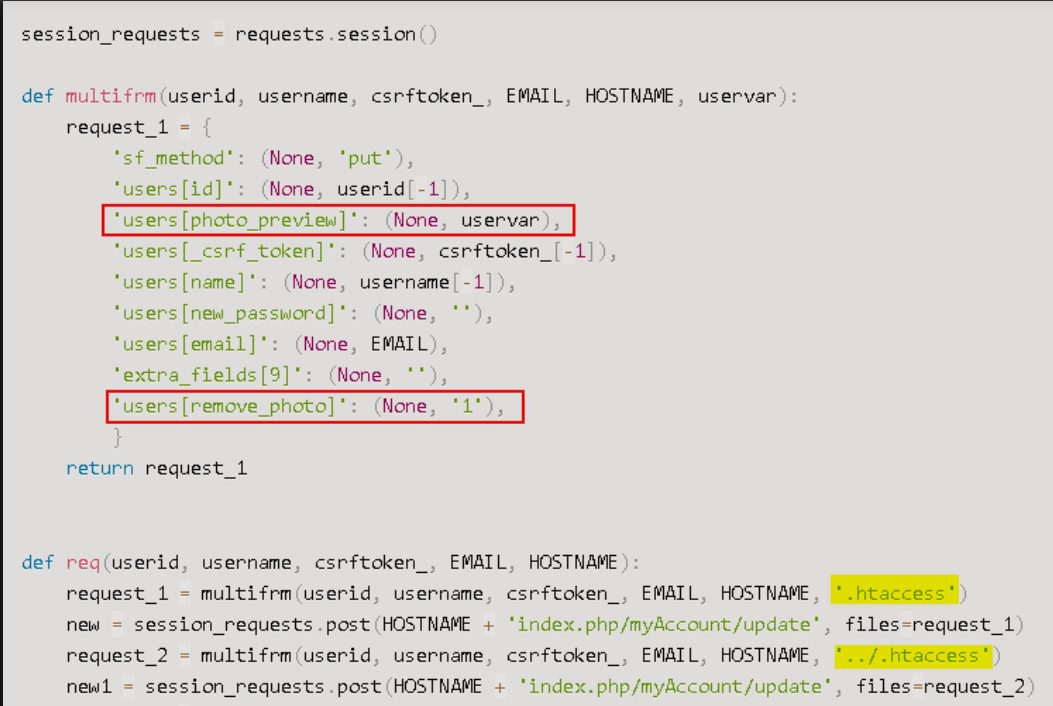
### Kịch bản khai thác

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

users[remove\_photo] được đặt thành 1

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

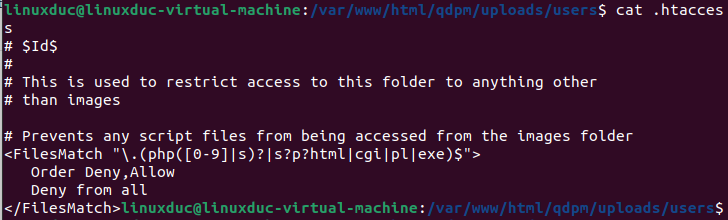
users[photo\_preview] được đặt thành ".htaccess" và "../.htaccess."

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

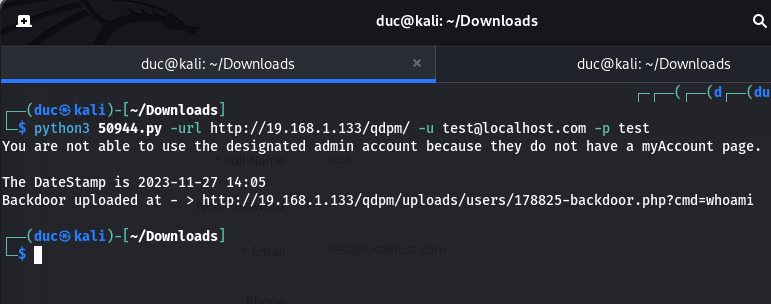
Hình . Gửi yêu cầu

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)

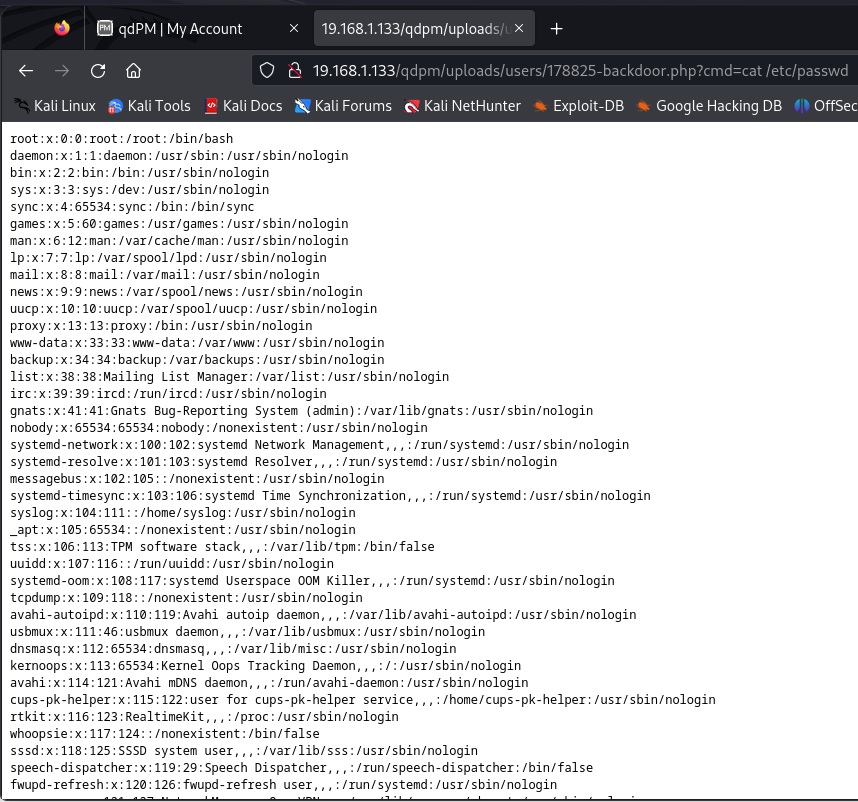
Hình . Đặt users[photo\_preview] thành .htaccess



Hình . Chạy file python

Thực hiện 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 2023-39147

### Mô hình triển khai và cài đặt

A graph paper with a black line and a red and blue arrow

Description automatically generated

Hình . Mô hình CVE 2023-39147

Cài đặt UVdesk trên Linux

Cài đặt:

1. Đăng nhập vào thiết bị Linux

2. Chạy các lệnh sau trong cửa sổ terminal:

#cập nhật kho phần mềm

sudo apt update

# cài đặt các bản cập nhật phần mềm có sẵn

sudo upgrade apt -y

# cài đặt điều kiện kiên quyết

sudo apt install curl wget zip composer -y

# cài đặt Apache HTTPD và MySQL

sudo apt install apache2 mariadb-server mariadb-client -y

# cài đặt các thành phần PHP

sudo apt install php7.4 php7.4-curl php7.4-intl php7.4-gd php7.4-dom php7.4-iconv php7.4-xsl php7.4-mbstring php7.4-ctype php7.4-zip php7.4-pdo php7.4-xml php7.4-bz2 php7.4-calendar php7.4-exif php7.4-fileinfo php7.4-json php7.4-mysqli php7.4-mysql php7.4-posix php7.4-tokenizer php7.4-xmlwriter php7.4-xmlreader php7.4-phar php7.4-soap php7.4-mysql php7.4-fpm libapache2-mod-php7.4 php7.4-gmp php7.4-bcmath php7.4-apcu php7.4-redis php7.4-imagick php7.4-imap php7.4-xdebug php7.4-mailparse -y

# cấu hình cơ sở dữ liệu MySQL

sudo su

mysql\_secure\_installation

3. Nhấn Enter để đăng nhập bằng root

4. Gõ N và nhấn Enter để không chuyển sang xác thực unix socket

5. Gõ Y và nhấn Enter để đặt mật khẩu root, gõ mật khẩu 2 lần để xác nhận

6. Gõ Y và nhấn Enter để xóa người dùng ẩn danh

7. Gõ Y và nhấn Enter để không cho phép đăng nhập root từ xa

8. Gõ Y và nhấn Enter để xóa cơ sở dữ liệu kiểm tra

9. Gõ Y và nhấn Enter để tải lại bảng đặc quyền

10. Chạy lệnh sau để đăng nhập vào MySQL:

mysql -u root -p

11. Xác thực bằng mật khẩu root đã đặt trước đó

12. Chạy các lệnh sau để tạo cơ sở dữ liệu UVdesk và người dùng cơ sở dữ liệu

CREATE DATABASE uvdesk;

GRANT ALL ON uvdesk.\* to 'uvdesk\_rw'@'localhost' IDENTIFIED BY 'admin123';

FLUSH PRIVILEGES;

EXIT;

Exit

13. Tiếp tục với các lệnh sau:

# tải xuống bản phát hành uvdesk mới nhất

wget -O uvdesk.zip https://cdn.uvdesk.com/uvdesk/downloads/opensource/uvdesk-community-current-stable.zip

# giải nén zip đã tải xuống vào /var/www

sudo unzip ./uvdesk.zip -d /var/www/

# đổi tên thư mục đã giải nén

sudo mv /var/www/uvdesk\* /var/www/uvdesk

# đặt chủ sở hữu của thư mục uvdesk

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

# tạo cấu hình apache uvdesk

sudo nano /etc/apache2/sites-available/uvdesk.conf

14. Sao chép cấu hình sau vào uvdesk.conf

Alias /uvdesk "/var/www/uvdesk/public"

<Directory /var/www/uvdesk/public>

Require all granted

Options Indexes FollowSymLinks

AllowOverride All

Order allow,deny

Allow from all

</Directory>

15. Nhấn CTRL+O, Enter, CTRL+X để viết các thay đổi

16. Chạy lệnh sau để kích hoạt trang UVdesk

# kích hoạt mô-đun

sudo a2enmod rewrite

# kích hoạt trang uvdesk

sudo a2ensite uvdesk

# khởi động lại dịch vụ apache2

sudo systemctl khởi động lại apache2

Cài đặt web UVdesk

1. Mở trình duyệt web và điều hướng đến http://192.168.202.129/uvdesk

2. Trình cài đặt web UVdesk sẽ được tải

3. Nhấp vào nút Let’s Begin

4. Nhấp vào nút Proceed

5. Hoàn thành biểu mẫu cấu hình cơ sở dữ liệu (như đã tạo ở trên)

Server: 127.0.0.1

Port: 3306

Username: uvdesk\_rw

Password: admin123

Database: uvdesk

6. Nhấp vào nút Proceed

7. Hoàn thành biểu mẫu Super Admin Account bằng cách nhập Name, Email, and Password

8. Nhấp vào nút Proceed

9. Nhấp vào nút Proceed tại màn hình cấu hình trang web

10. Nhấp vào Install Now

11. Sau khi cài đặt hoàn tất, nhấp vào nút Admin Panel

12. Đăng nhập bằng địa chỉ email quản trị viên và mật khẩu đã tạo trước đó

13. Chào mừng đến với Uvdesk

### Kịch bản khai thác

* Thực hiện download file python khai thác từ địa chỉ <https://www.exploit-db.com/exploits/51639> được file 51639.py
* Thực hiện đổi thành url vào trang web mục tiêu và tài khoản mật khâu đã có trong database của Uvdesk

login\_data = {

"\_username": "admin@admin.local",

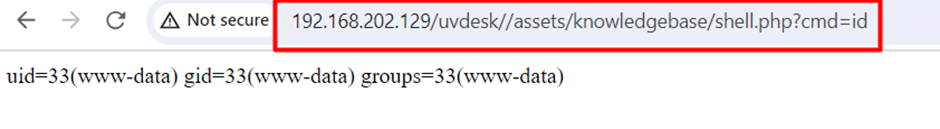
"\_password": "abcd@123",

"\_remember\_me": "off"

}

* Chạy file py và thực hiên khai thác

python3 51639.py -u "http://192.168.202.129:8000" -c "id"



Hình . Mở file thành công

### Đánh giá và kết luận

Lỗ hổng RCE (Remote Code Execution) trong Uvdesk phiên bản 1.1.3 liên quan đến khả năng tải lên tệp và thực thi mã từ xa thông qua việc tải lên tệp tin không an toàn. Đây là một vấn đề bảo mật nghiêm trọng có thể bị khai thác để chiếm quyền kiểm soát hệ thống và thực hiện các hành động không được ủy quyền. Điều này có thể dẫn đến mất dữ liệu, xâm nhập vào hệ thống, hoặc thậm chí chiếm quyền kiểm soát toàn bộ hệ thống.

#### Đánh giá:

Nghiêm trọng: Lỗ hổng này được xem là nghiêm trọng vì cho phép kẻ tấn công tải lên và thực thi mã từ xa trên hệ thống Uvdesk thông qua việc tải lên tệp tin không an toàn.

Tác động lớn: Có thể dẫn đến mất dữ liệu, chiếm quyền kiểm soát hệ thống, hoặc thậm chí làm tổn thương danh tiếng và tin cậy của doanh nghiệp sử dụng Uvdesk.

Được xác thực: Lỗ hổng này yêu cầu việc đăng nhập để thực hiện cuộc tấn công, nhưng vẫn rất nguy hiểm vì có thể bị khai thác một khi kẻ tấn công đã có thông tin đăng nhập hợp lệ.

#### Kết luận:

Lỗ hổng RCE trong Uvdesk v1.1.3 là một vấn đề bảo mật nghiêm trọng, đe dọa tính toàn vẹn và an ninh của hệ thống. Việc tận dụng lỗ hổng này có thể dẫn đến những hậu quả nguy hiểm và tiềm ẩn rủi ro lớn cho doanh nghiệp sử dụng Uvdesk. Việc áp dụng bản vá hoặc biện pháp bảo mật cần thiết để ngăn chặn cuộc tấn công từ lỗ hổng này là điều cần thiết và khẩn cấp.

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

* Cài đặt vmware
* Cài vmware tool:

Sudo apt update

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

* Cài đặt kali linux
* Cài đặt ubuntu 22.04
* Cài đặt burpsuite
* File python của CVE