**CVE-2023-32243**

- Plugin : Essential Addons for Elementor

- Phiên bản lỗi:5.7.1

- Lỗi: Broken Authentication and Session Management

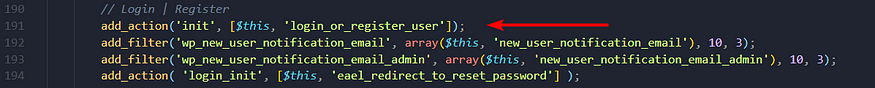
a) Mô tả

- Essential Addons for Elementor là bộ addons cung cấp thêm các widget và thư viện mẫu giúp quá trình chỉnh sửa được dễ dàng hơn, plugin hoạt động tốt ngay cả trên phiên bản Elementor miễn phí

- Plugin không xác thực khóa đặt lại mật khẩu, điều này có thể cho phép kẻ tấn công không được xác thực đặt lại mật khẩu của tài khoản tùy ý thành bất kỳ thứ gì chúng muốn, bằng cách biết email hoặc tên người dùng liên quan, giành quyền truy cập vào chúng

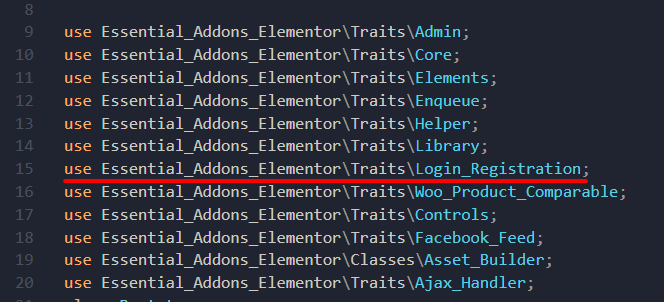
b)hàm xử lý bị lỗi

- Nhìn vào tệp **Bootstrap.php** nằm trong **Bao gồm\Lớp,** chúng ta có thể thấy hành động **init** . Hành động này kích hoạt một chức năng gọi là **login\_or\_register\_user** .



Khởi tạo hành động — Đăng nhập hoặc đăng ký Chức năng người dùng

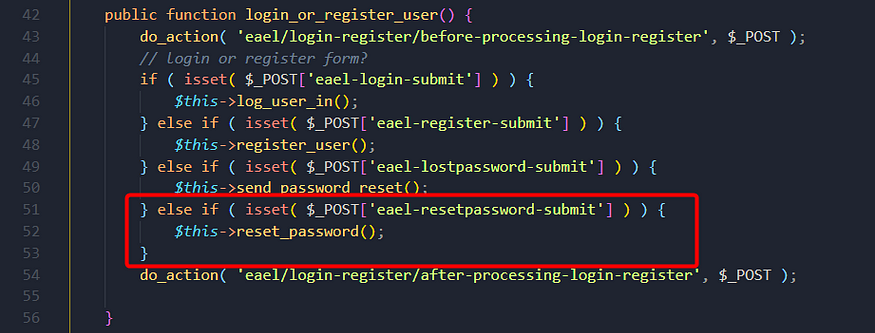
- Hàm này nằm trong tệp PHP Đăng nhập\_Registration, được nhập trước đó trong tệp Bootstrap trên dòng 15.



Đặc điểm Đăng ký Đăng nhập

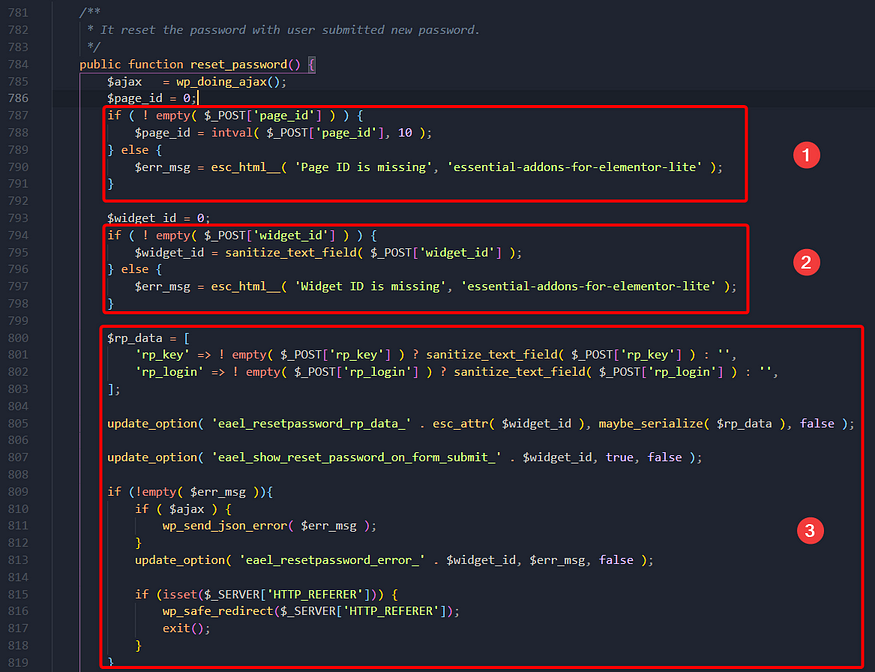
- Theo dõi hàm trong tệp Đăng nhập\_Đăng ký, chúng ta có thể thấy nó nằm ở dòng 42. Hàm này chỉ cần kiểm tra hàm nào sẽ kích hoạt dựa trên giá trị tham số yêu cầu mà nó nhận được.

- Hàm chúng ta quan tâm là hàm **reset\_password** . Chúng ta có thể thấy nó được gọi thông qua $this, trong trường hợp này nó được tìm thấy trong cùng một tệp.



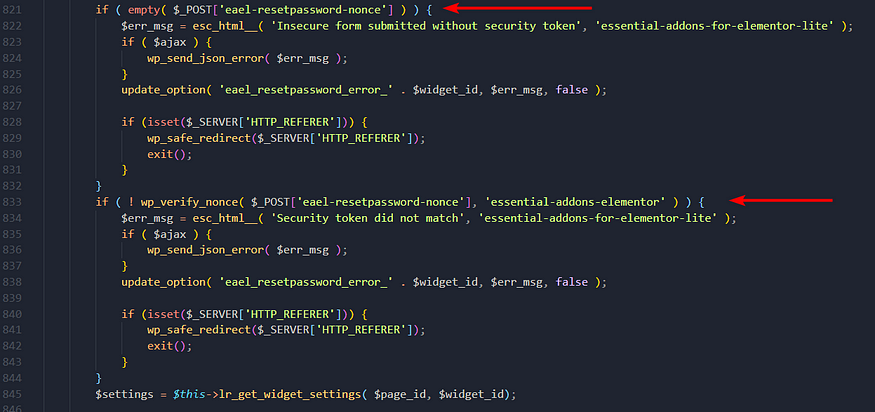
Đăng nhập hoặc Đăng ký chức năng người dùng

- Hàm **reset\_password** có thể được tìm thấy ở dòng 784. Đoạn đầu tiên của hàm này khá đơn giản. Chúng tôi đang kiểm tra xem thông số **page\_id** và **widget\_id** có trống hay không. Không có giá trị cụ thể nào đang được kiểm tra chéo.



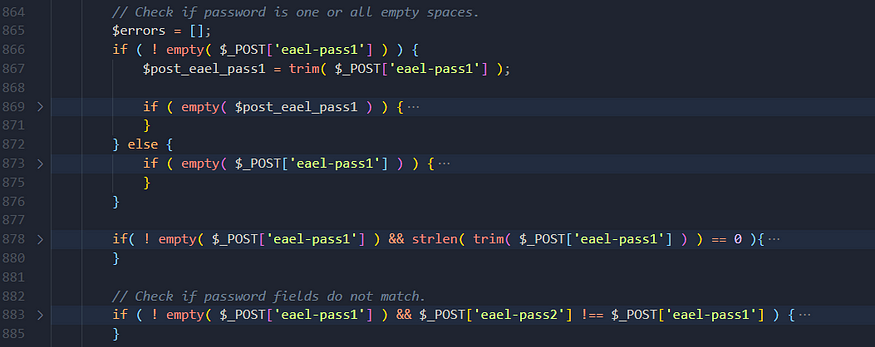
Kiểm tra các thông số cần thiết

- Tiếp theo, mã sẽ kiểm tra xem có giá trị nonce nào được chuyển trong yêu cầu thông qua tham số **eael\_resetpassword\_nonce hay không** . Nếu giá trị không trống, nó sẽ được xác minh thông qua hàm **wp\_verify\_nonce** trên dòng 833.



Kiểm tra nonce hợp lệ

- Sau đó, các tham số **eael-pass-1** và **eael-pass-2** được chạy theo một số kiểm tra tiêu chuẩn. Về cơ bản, 2 trường đó là “mật khẩu” và “xác nhận mật khẩu”. Việc kiểm tra bao gồm so sánh chuỗi để kiểm tra xem mật khẩu có trống không và chúng có khớp không.

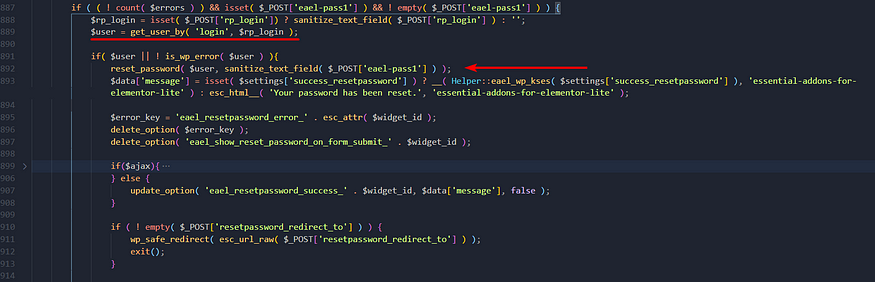


Kiểm tra mật khẩu

- Nếu tất cả các bước kiểm tra đều đạt, ở dòng 888 và 889, biến **rp\_login** đã được thiết lập. Biến **rp\_login** chỉ đơn giản là tên người dùng của nạn nhân. Sau khi biến được thiết lập, biến đó sẽ được chuyển đến hàm 'getter' **get\_user\_by** . Phản hồi sau đó được lưu trữ trong biến **người dùng** .

888 : $rp\_login = isset ( $\_POST [ 'rp\_login' ]) ? vệ sinh\_text\_field ( $\_POST [ 'rp\_login' ] ) : '' ;   
889 : $user = get\_user\_by ( 'login' , $rp\_login );

- Nếu người dùng hợp lệ và không có lỗi nào được kích hoạt, hàm **reset\_password** được gọi với các biến **người dùng** và **eael-pass-1** (mật khẩu) làm tham số trên dòng 892.

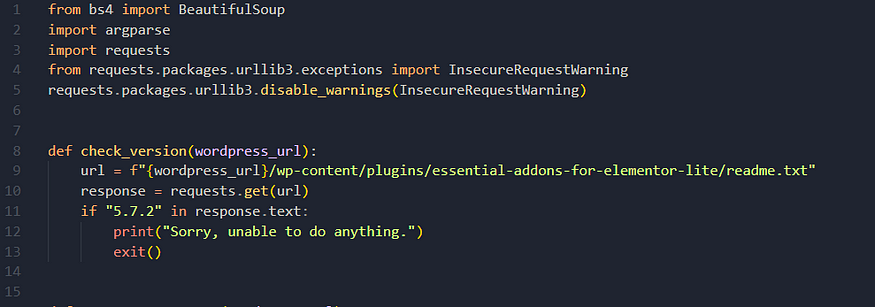


Thiết lập đặt lại mật khẩu rp\_login

c) Khai thác

- Trước tiên, bạn nhập một vài thư viện để gửi yêu cầu HTTP và phân tích dữ liệu phản hồi HTML cũng như các giá trị đối số do người dùng cung cấp.

- Tiếp theo, hàm **check\_version** được định nghĩa để kiểm tra phiên bản plugin dễ bị tấn công “ **essential addons for elementor lite** ” bằng cách nhấn vào tệp **readme.txt** và kiểm tra xem phiên bản hiện tại có phải là phiên bản đã vá hay không.

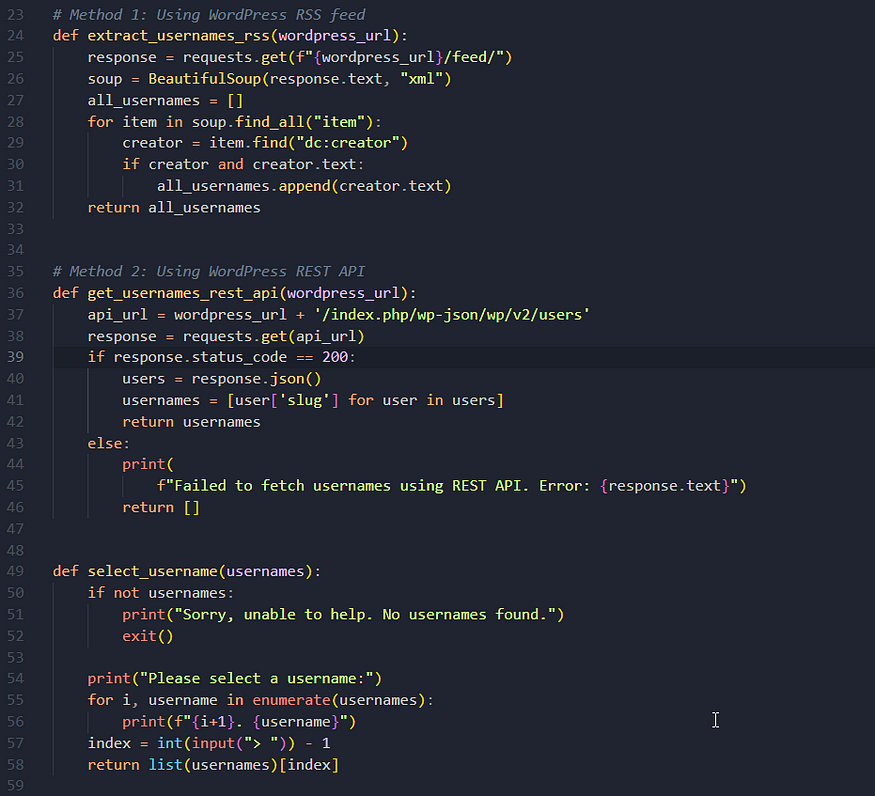


**Kiểm tra phiên bản**

- Sau đó, hàm **extract\_usernames** chạy thêm 2 hàm khác. Cái đầu tiên sử dụng nguồn cấp dữ liệu RSS của WordPress để trích xuất tên người dùng từ phản hồi XML. Cách thứ hai là nhấn vào điểm cuối API REST để truy vấn người dùng.

- Hàm **select\_username** được xác định sau đó, cho phép người dùng chọn tên người dùng từ danh sách tên người dùng được trả về (đó là một cụm từ 'tên người dùng' và 'tên người dùng' trong câu…).

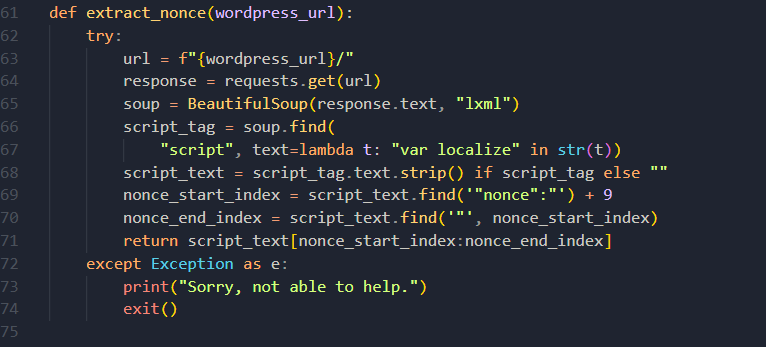
- Điều đáng chú ý là **api\_url** trong hàm **get\_usernames\_rest\_api** đã bị thay đổi. Tôi đã phải thêm “index.php” khi tôi đang thử nghiệm trên phòng thí nghiệm WordPress của mình.



Trích xuất tên người dùng, Lấy tên người dùng, Chọn tên người dùng

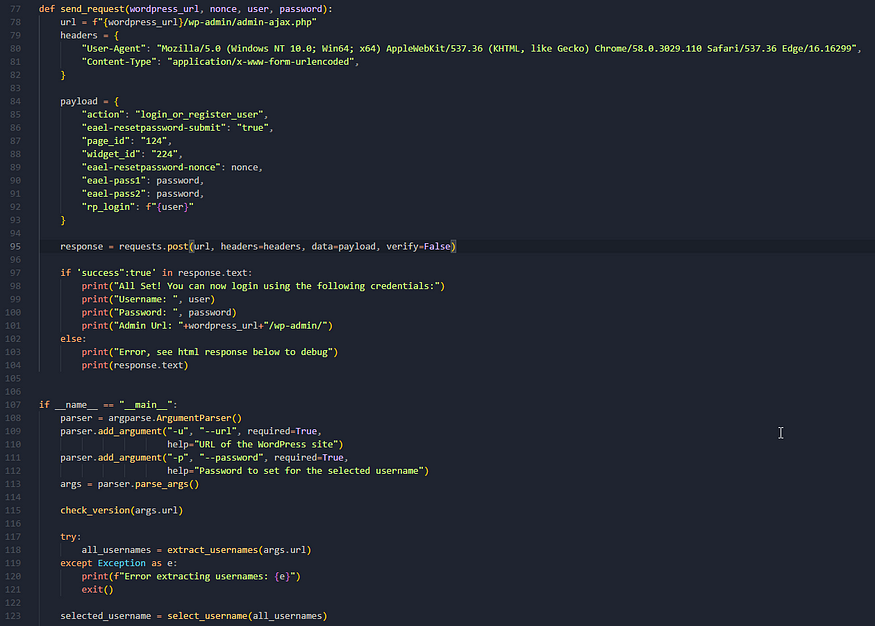
- Sau đó, hàm **extract\_nonce** được xác định. Thật đơn giản, lấy **wordpress\_url** sau đó sử dụng BeautifulSoup4 để phân tích phản hồi. Nó cố gắng tìm chuỗi “var localize” bên trong thẻ script.

- Từ đó, nó kiểm tra giá trị chuỗi “nonce” bằng cách tìm kiếm “nonce” và sau đó di chuyển bộ chọn 9 ký tự về phía trước.

****

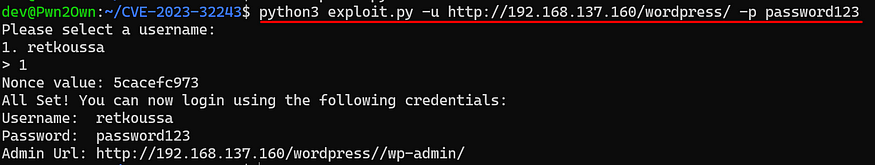
**Trích xuất nonce**

- Cuối cùng, hàm **send\_request** được xác định để gửi yêu cầu tới admin-ajax.php — phần tải trọng là phần nội dung của yêu cầu POST. Nó bao gồm số nonce được trích xuất, mật khẩu sẽ được đặt và tên người dùng của mục tiêu.



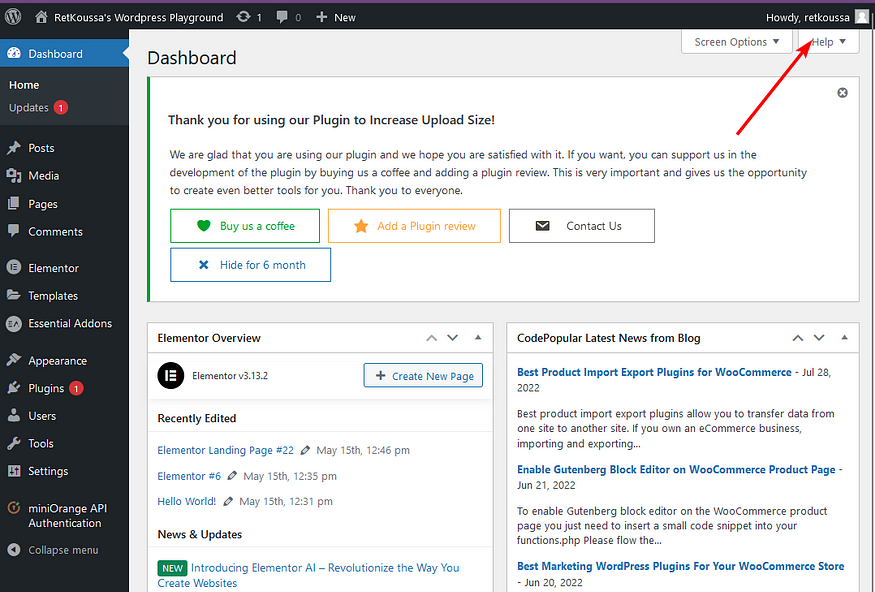
**Chức năng gửi yêu cầu**

- Và cuối cùng, kịch bản đã được sử dụng. Tôi đã lưu trữ một phiên bản WordPress có cài đặt Elementor. Tôi đảm bảo cũng cài đặt phiên bản **Essential Addons cho Elementor** đã lỗi thời .



Tập lệnh đang hoạt động

- Như bạn có thể thấy, mật khẩu đã được cập nhật. Bây giờ tôi có thể đăng nhập vào người dùng 'retkoussa' bằng mật khẩu 'password123'.



Đăng nhập WordPress thành công