CVE-2022-29455

- Plugin : Elementor

- Phiên bản lỗi: 3.5.5

- Lỗi: Reflexd XSS

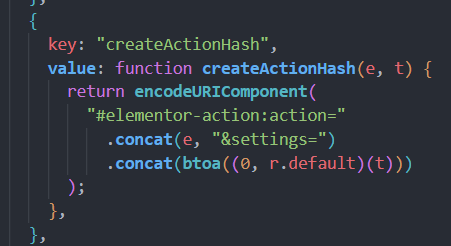
a)Mô tả

- Plugin này cho admin xây dựng trang web 1 cách nhanh gọn hơn

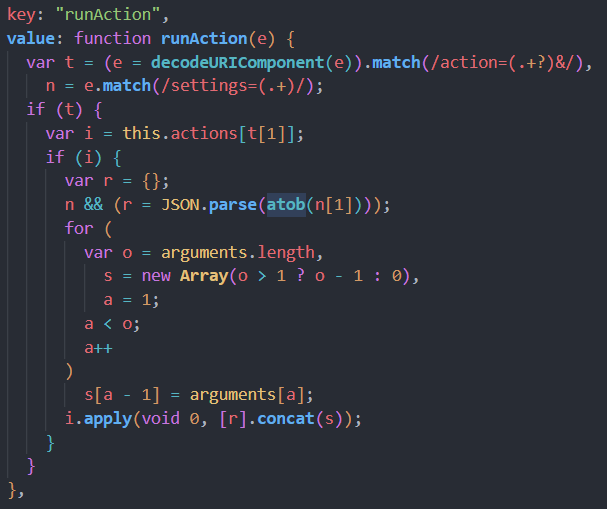
- Nhưng do 1 không kiểm soát đầu vào chặn chẽ nên hacker có thể lợi dụng để tấn công xss

b) Hàm xử lý bị lỗi

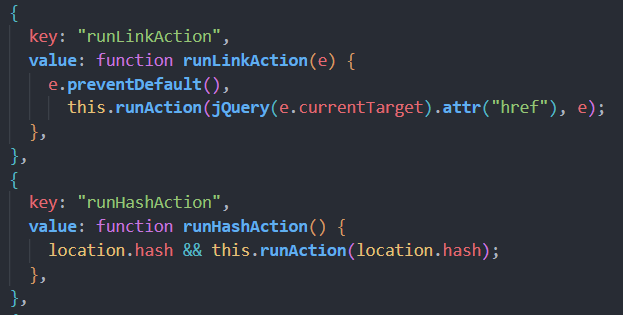
- hàm xử lý trên url



Giải mã based 64 để thực thi



Gọi hàm sử lý



c)demo



