LỖI BẢO MẬT WEB 2.0 ĐẦU TIÊN LỘ DIỆN

Các ch

Các chuyên gia của Fortify Software tuyên bố phát hiện được lỗ hổng bảo mật đầu tiên trong Web 2.0 và ứng dụng AJAX.

Trước đây các nhà phát triển web thường sử dụng Javascript để thực hiện các tác vụ đơn giản như thay đổi hình ảnh hiển thị mỗi con trỏ chuột đi qua hay trong các web forms. Nhưng trong thế giới Web 2.0 Javascript ngày càng được sử dụng rộng rãi cả trong việc truyền tải dữ liệu. Đó chính là nguyên nhân làm phát sinh hàng loạt các vấn đề bảo mật.

Brian Chess - chuyên gia nghiên cứu hàng đầu của Fortify Software - cho biết tin tặc có thể lừa người dùng truy cập vào một website độc hại và đánh cắp dữ liệu bí mật của họ từ chính các ứng dụng web chạy trên nền tảng trình duyệt. Đơn giản là bởi các máy chủ thường không áp dụng các giải pháp bảo mật Javascript ngay cả khi chúng được sử dụng để truyền tải dữ liệu.

"Chúng tôi đặt tên cho phương thức tấn công trên là Javascript Hijacking. Hậu quả của nó là toàn bộ thông tin lưu trữ trên máy chủ sẽ rơi vào tay tin tặc".

Các chuyên gia nghiên cứu của Fortify đã tiến hành thử nghiệm hàng chục nền tảng Web 2.0 khác nhau và đưa ra kết luận rằng mọi nền tảng đều mắc lỗi Javascript Hijacking.

"Nếu chúng ta nhìn sâu vào các ứng dụng Web 2.0 chúng ta sẽ phát hiện được những lỗi bảo mật cho dù đó là nền tảng AJAX của Google, Microsoft hay một hãng mã nguồn mở nào đó," ông Chess cho biết.

Các ứng dụng web truyền thống lại không mắc lỗi như trên, ông Chess khẳng định, đơn giản là bởi chúng không dùng Javascript để truyền tải dữ liệu.

Hiện công nghệ Web 2.0 đã trở nên ngày một phổ biến và hầu hết các website thương mại điện tử giờ đều ứng dụng công nghệ này. Chính vì thế mà cần phải đầu tư thời gian thích hợp để nghiên cứu và khắc phục mọi lỗi bảo mật.

Hoàng Dũng