TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

**VIỆN CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG**



**BÁO CÁO MÔN HỌC**

# Công nghệ web và dịch vụ trực tuyến

**LAB06**

Nhóm: **H3D**

| | |
|---|---|
| Phan Thành Đạt | 20173001 |
| Hoàng Thị Hiền | 20173102 |
| Trần Văn Định | 20173017 |
| Dương Đức Điệp | 20173013 |

- Reflex xss: Điều này xảy ra khi các kết quả độc hại được trả về sau khi nhập mã độc hại. Trong một số trang web khi nhập sai thông tin đăng nhập, thông báo lỗi như “Xin lỗi tên người dùng của bạn hoặc thông tin đăng nhập của bạn sai” sẽ được hiển thị. Bằng cách này, kẻ tấn công có thể nhập tập lệnh độc hại thay vì tên người dùng hoặc địa chỉ email chính xác. => Người dùng bị dụ nhấp vào một đường link đến một trang web bình thường nhưng có gắn sau một đoạn code độc, giả sử là example.com/search.php?user=<code-độc>, phía back-end của example.com nhận request này, tìm kiếm không thấy user trên và trả về giao diện là <html> Không thấy người dùng <code-độc> </html>. Browser sẽ thực hiện file html đó, nếu <code-độc> là một đoạn script js thì script đó sẽ đc chạy. Trong ví dụ ở slide là script gửi về cho bên attack document.cookies, trong ví dụ paypal là: việc dụ người dùng click vào link thực hiện qua mail, mã gắn sau đường link đến paypal là một script  redirect đến một trang giả thông báo tài khoản người dùng có lỗi và lừa ng dùng nhập thông tin nhạy cảm
- Stored xss: thực hiện trên những trang cho phép người dùng đăng những dạng như post, storyboard, v.v. ví dụ như MySpace, Facebook hoặc Review sản phẩm. Kẻ tấn công là người dùng cố tình đăng bài nhưng ko chỉ nhập text mà cố tình nhập vào mã độc, mã thực hiện phía client v.v. Bài đăng của kẻ tấn công này vẫn đc lưu như ng dùng thông thường, và người dùng khác không may click vào thì sẽ bị tấn công. Ở ví dụ trong slide, Myspace: đăng bài là mã độc dù Myspace đã chặn ko cho đăng <html> nhưng kẻ tấn công vẫn tìm đc cách lách như ẩn “javascript” bằng “java\nscript”, vd2: một trang web  cho phép người dùng đăng ảnh, kẻ tấn công upload ảnh là một file html, nếu một người dùng khác request đến ảnh thực ra là code html đó, trình duyệt như ie sẽ coi đó là file html dù content type là image.

⇨ Giải pháp: Validates ở back-end và mã hóa trước khi gửi.