|  |  |
| --- | --- |
|  | **CHƯƠNG TRÌNH ĐÀO TẠO SINH VIÊN**  **BÀI 3: Lỗi XSS** |

|  |  |
| --- | --- |
| **Path** | Làm 3 đề CTF thể hiện các lỗi web cơ bản |
| **Phụ trách** | Khanhpv6 |
| **Thời gian** | 4 ngày |

**Yêu cầu:**

* Xây dựng trang web003 gồm các chức năng đăng nhập, đăng kí, chat message cho người dùng khác. Chức năng chat nhập tên user, title, messageContent để gửi cho người dùng khác. Trang web có sẵn một tài khoản admin là tài khoản quản trị. Tài khoản quản trị sau khi đăng nhập có thêm chức năng xem và xóa chat message của tất cả người dùng khác. (3d)
* Trang admin khi xem chat message của người dùng khác không escape messageContent dẫn tới lỗi stored XSS. Admin sau khi đăng nhập có set thêm một cookie là flag có chứa flag, không đặt httpOnly (1d)
* Viết bot để liên tục đăng nhập trang admin và xem lần lượt các chat message của từng user. Ngôn ngữ lập trình tùy chọn. Cấu hình server chạy bot chặn toàn bộ inbound, chỉ mở outbound đến web003 trên port 80 và mở outbound phép truy vấn dns trên port 53. (3d)
* Cài đặt DNS server, trỏ domain để thực hiện khai thác XSS, lấy trộm cookie thông qua tunnel dns, đọc nội dung cookie, từ đó lấy được flag (2d)

**Tài liệu tham khảo:**

* Google
* http://www.seleniumhq.org/
* Phantomjs