Bài lab Web-xss

1. Nội dung và hướng dẫn thực hiện bài thực hành

1.1. Mục đích

- Giúp sinh viên hiểu về các lỗ hổng web (XSS)

1.2. Yêu cầu đối với sinh viên

- Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách/chủ.
- Có kiến thức về bắt gói tin, lỗ hổng web

1.3. Nội dung thực hành

- Khởi động bài lab:
  - Vào terminal, gõ:

    Labtainer web-xss

(chú ý: sinh viên sử dụng email stu.ptit.edu.vn của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy khách: web-xss, một cái là đại diện cho máy chủ: ***web-xss-server.*** Biết rằng 2 máy nằm cùng mạng LAN.

- Trên terminal ***web-xss-server*** sử dụng lệnh "ifconfig", xác định địa chỉ IP và địa chỉ mạng LAN.
- Trên máy khách ***web-xss*** sử dung ping để kiểm tra kết nối tới máy chủ

  ping <IP máy chủ>

  ví dụ IP máy: 172.25.0.2 → IP máy chủ cần điền 172.25.0.2
- Tiếp tục trên terminal ***web-xss*** sử dụng lệnh **firefox &** để kết nối tới firefox
- Sau đó tiếp tục sử dụng lệnh ***owasp-zap &*** để chạy owasp-zap
- Task1: Cấu hình firefox để kết nối proxy juiceshop trên cổng 8080
- Task2: Chỉnh sửa phần mô tả của sản phẩm bằng lệnh curl

  Trên terminal web-xss sử dụng 2 dòng lệnh:
  - *Curl –X OPTIONS –D –'http://192.168.99.100:3000/api/Products/2'*

    Lệnh này để kiểm tra các method của lệnh curl

- curl -X PUT "http://192.168.99.100:3000/api/Products/2" -H "Content-Type: application/json" --data-binary'{"description":"TEST"}'
  Lệnh này để sửa phần “description” thành TEST

- Task3: Đánh giá 0*
  - Trở về firefox với trang Custom Feedback thực hiện ghi 1 feedback mới nhưng không ấn Submit
  - Quay lại trang Owasp-zap nhấn set break on all requests and respones
  - Quay lại firefox Submit feedback vừa điền
  - Thông tin feedback hiện lên trên owasp-zap sau đó chỉnh sửa rating là 0 rồi ấn Submit and continue to next break point. Qua đó feedback vừa thực hiện sẽ là 0 sao
  - Lưu Respone của gói tin biểu thị trên về đặt tên là danhgia
- Task4: Thực hiện DOM XSS cơ bản:
  - Trên thanh tìm kiếm sử dụng đoạn mã script
    <iframe src="javascript:alert(`xss`)"> rồi nhấn enter
  - Trên owasp-zap gói tin phản hồi DOM XSS changele solved sau đó lưu Respone của gói tin này về và đặt tên là domxss
- Task5: Thực hiện tấn công XSS liên tục để chiếm quyền admin
  - Trên trang custom feedback ở phần comment điền đoạn mã script sau đó nhấn submit:
    <iframe src="javascript:alert(`xss`)">
  - Về trang đăng ký điền thông tin với email bắt buộc là mã sinh viên và thông tin còn lại là tuỳ ý nhưng chưa nhấn Register
  - Về owasp-zap nhấn set break on all requests and respones rồi quay lại trang đăng ký nhấn Register
  - Gói tin ở Break sẽ hiển thị thông tin đăng ký, chỉnh sửa email là đoạn mã scirpt rồi nhấn Submit and continue to next break point
    Đoạn mã: <iframe src="javascript:alert(`xss`)">
  - Về trang đăng nhập juiceshop với tên đăng nhập là ‘or 1=1 –
  - Lưu gói tin khi đăng nhập thành công về testfile với tên là accountxss

- Task6: Đăng ký user mới nhưng là quyền admin

- Về trang đăng ký điền thông tin với email bắt buộc là mã sinh viên và thông tin còn lại là tuỳ ý và nhấn Register
- Ở owasp-zap có gói tin đã đăng ký tài khoản, click chuột phải vào gói tin và chọn Open/Resend with Request Editor
- Thêm ký tự vào email và thêm role admin sau đó nhấn Send
- Quay về trang đăng nhập với email vừa tạo với role admin, bắt gói tin đăng nhập và lưu phản hồi với tên là admin

- Task7: Xem giỏ đồ của người khác
  - Tạo 1 tài khoản bất kỳ và đăng nhập sau đó vào phần giỏ hàng
  - Nhấn F12 ở phần Session Storage sửa bid là 7 sau đó nhấn f5 để Reload lại trang giỏ đồ
  - Giỏ đồ khác hiện ra sau đó về owasp-zap lưu gói tin của giỏ đồ đó đặt tên là basket
- Khởi động lại bài lab:
  - Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

Labtainer –r web-xss

- Kết thúc bài lab;
  - Kết thúc bài lab sinh viên dùng câu lệnh:

Stoplab web-xss