Câu 1. Mô tả “Cross-Site Scripting”

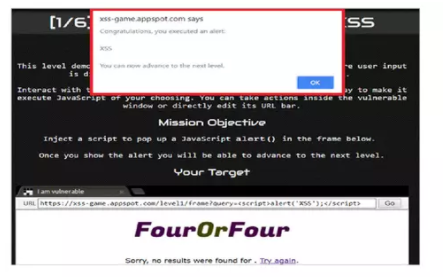
Trả lời: Tấn công Cross-Site Scripting là một cuộc tấn công được thực hiện từ phía Client, nó thường là một đoạn mã độc để khai thác lỗ hổng XSS, các hacker thường chèn các mã độc thông qua các đoạn script để thực thi chúng. Mục đích của những cuộc tấn công này là ăn cắp dữ liệu nhận dạng của người dùng.

Nguyên nhân : Nguyên nhân chính của loại tấn công này là xác thực đầu vào dữ liệu người dùng không phù hợp, dữ liệu độc hại từ đầu vào có thể xâm nhập vào dữ liệu đầu ra. Mã độc có thể nhập một script và được chèn vào mã nguồn của website. Khi đó trình duyệt không thể biết mã thực thi có phải độc hại hay không. Do đó mã độc hại có thể đang được thực thi trên trình duyệt của nạn nhận hoặc bất kỳ hình thức giả nào đang được hiển thị cho người sử dụng

Cách thức các cuộc tấn công Cross-Site Scripting được thực hiện: Giả sử trên một trang web có một ô input



Sau khi chèn đoạn script vào ô inp Search ut và nhấn nut



đoạn đã được chèn vào ô input đã được thực thi → trang web này có lỗ hổng XSS . Đây chỉ là một đoạn script vô hại, tuy nhiên với những đoạn mã độc ăn cắp dữ liệu nhận dạng người dùng gửi tới hacker thì sẽ tạo ra một lỗ hổng cực kỳ nghiêm trọng.

Câu 2: Find the way to reduce the attack via “File Upload”

Trả lời:

Một số phương pháp để giảm tấn công bằng file upload

- Đảm bảo file được upload lên không có quyền thực thi

- Check extention của file upload trước khi upload : đảm bảo rằng file upload có extention nằm trong while-list   
- Đổi tên file upload theo pattern nhất định

- Kiểm tra Content-type header: đảm bảo rằng type của header nằm trong while list.

- Sử dụng virus scan để quét những tệp độc hại

Câu 3: What is “CSRF”

Trả lời:

CSRF (Cross-site Request Forgery) nói đến việc tấn công vào chứng thực request trên web thông qua việc sử dụng Cookies, nơi mà các hacker có khả năng sử dụng thủ thuật để tạo request mà bạn không hề biết. Vì vậy, một CSRF là hacker lạm dụng sự tin tưởng của một ứng dụng web trên trình duyệt của nạn nhân.

CSRF là một kiểu tấn công gây sự nhầm lẫn tăng tính xác thực và cấp quyền của nạn nhận khi gửi một request giả mạo đến máy chủ. Vì thế một lỗ hổng CSRF ảnh hưởng tới các quyền của người dùng ví dụ như quản trị viên, kết quả là chúng truy cập được quyền đầy đủ.

Cách thức tấn công: Các ứng dụng web hoạt động theo cơ chế nhận các câu lệnh HTTP từ người sử dụng, sau đó thực thi các câu lệnh này. Hacker sử dụng phương pháp CSRF để lừa trình duyệt của người dùng gửi đi các câu lệnh http đến các ứng dụng web. Điều đó có thể thực hiện bằng cách chèn mã độc hay link đến trang web mà người dùng đã được chứng thực. Trong trường hợp phiên làm việc của người dùng chưa hết hiệu lực thì các câu lệnh trên sẽ được thực hiện với quyền chứng thực của người sử dụng