Path traversal attack

Overview

Path traversal attack hay còn gọi là directory traversal nó nhằm mục đích truy cập các tệp và thư nục được lưu trữ phía bên ngoài thư mục gốc của ứng dụng Web. Bằng cách thao tác với các biến tham chiếu tệp có trình tự như “dot-dot-slash (../)” hay các biến thể của nó hoặc bằng cách sử dụng đường dẫn tệp tuyệt đối kẻ tấn công có thể truy cập được vào các tệp hay thư mục tuỳ ý được lưu trữ trên hệ thống .

Impact

Đây là 1 lỗ hổng nguy hiểm có thể gây ảnh hưởng đến hệ thống. Ở mức độ bình thường thì kẻ tấn công có thể đọc được các file trong thư mục web hay là các file nhạy cảm được lưu bên trong của hệ thống.

Với 1 số ảnh hưởng ở mức độ cao hơn kẻ tấn công có thể ghi file vào hệ thống từ đó sẽ chèn thêm vào các mã độc. Điều xấu nhất có thể xảy ra đó là kẻ tấn công có thể dẫn đến việc RCE.

How to check?

Việc kiểm tra xem 1 trang web có bị path traversal hay không thì có khá là nhiều cách nhưng thì thông thường ta sẽ chú ý về các endpoint. Các endpoint này sẽ truy cập file thông qua tên file, các endpoint upload file. Đây là những endpoint có nguy cơ cao dễ xuất hiện lỗ hổng này nhất.

Các endpoint này có thể sẽ không xuất hiện trên URL nên ta cần kiểm tra các kỹ trang web, trong source code, trong các function call api hay thậm trí là trong cookie.

How to pass the filter?

Nhiều ứng dụng đặt các đầu vào của người dùng vào đường dẫn tệp sẽ thực hiện 1 số loại phòng thủ chống lại các cuộc tấn công path traversal và chúng có thể bị phá vỡ. Nếu 1 ứng dụng tách hoặc chặn trình tự duyệt thư mục từ tên tệp do người cung cấp thì có thể vượt qua đuược sự bảo vệ bằng nhiều cách khác nhau:

- Khi mà bộ lọc chặn "../" thì ta có thể dùng các tringh tự duyệt lồng nhau như "….//" hay "….\/" thì có thể vượt qua.
- Ta có thể dùng các loại mã hoá không chuẩn khác nhau như: "%c0af%", "%252f", …
- Nếu ứng dụng yêu cầu tên tệp do người dùng cung cấp thì ta có thể thêm vào các phụ tải vào sau tên tệp.
- Nếu ứng dụng yêu cầu phần kết thức của tên tệp phải bằng các phần mở rộng dự kiến thì ta có thể dùng nullbyte(%00) để kết thúc hiệu quả đường dẫn tệp được trước phần mở rộng được yêu cầu.

Prevent

- Cách hiệu quả nhất để ngăn chặn các lỗ hổng truyền tải đường dẫn tệp là tránh chuyển hoàn toàn đầu vào do người dùng cung cấp tới các API hệ thống tệp
- Nếu việc chuyển đầu vào do người dùng cung cấp tới các API hệ thống tệp được coi là không thể tránh khỏi, thì hai lớp bảo vệ nên được sử dụng cùng nhau để ngăn chặn các cuộc tấn công:
    - Ứng dụng phải xác thực đầu vào của người dùng trước khi xử lý. Tốt nhất, việc xác thực phải so sánh với danh sách trắng các giá trị được phép.
    - Sau khi xác thực đầu vào được cung cấp, ứng dụng sẽ thêm đầu vào vào thư mục cơ sở và sử dụng API hệ thống tệp nền tảng để chuẩn hóa đường dẫn. Nó sẽ xác minh rằng đường dẫn được chuẩn hóa bắt đầu với thư mục cơ sở dự kiến.

Reference

- https://portswigger.net/web-security/file-path-traversal
- https://owasp.org/www-community/attacks/Path_Traversal
- https://viblo.asia/p/tim-hieu-ve-tan-cong-path-travelsal-m68Z0xQ2ZkG