Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

2

Lab

Improving Mod Security WAF

Thực hành môn An toàn mạng máy tính nâng cao

Tháng 3/2024

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Tìm hiểu và triển khai Web Application Firewall.
- Tìm hiểu cách viết rule

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Máy tính/máy ảo Hệ điều hành Kali Linux (Tải xuống tại: https://www.kali.org/get-kali/)
- DVWA
- Modsecurity

C. THỰC HÀNH

1. Mod Security Core Rule Set Problem:

Mod Security Core Rule Set là một công cụ quan trọng trong việc bảo vệ ứng dụng web trước các cuộc tấn công OWASP Top 10 bằng cách áp dụng các quy tắc được xác định trước để chặn các hành vi độc hại. Tuy nhiên, việc triển khai bộ Core Rule Set của Mod Security trong thực tế thường đối mặt với một số thách thức, trong đó có việc xảy ra các trường hợp False Positive - tức là các trường hợp mà hệ thống phát hiện và chặn nhầm các hoạt động không phải là mối đe doạ thực sự. Nguyên nhân của hiện tượng này xuất phát từ cơ chế tính Anomaly score (điểm bất thường) của Core Rule Set.

Task: Tìm hiểu cơ chế hoạt động của việc tính điểm bất thường của bộ Core Rule Set và giải thích tại sao cơ chế này lại dẫn đến sự xuất hiện của False Positive. Tham khảo: https://coreruleset.org/docs/concepts/anomaly_scoring/

2. Impove Mod Security:

Do sự tồn tại của vấn đề về false positive khi sử dụng bộ Core Rule Set, có nhiều cách để điều chỉnh (tuning) và cải thiện hiệu suất của ModSecurity:

- Tinh chỉnh các quy tắc có sẵn: Người quản trị có thể điều chỉnh các quy tắc có sẵn trong Core Rule Set bằng cách thay đổi các điều kiện hoặc tham số để giảm thiểu số lượng false positive. Việc này đòi hỏi hiểu biết sâu rộng về hoạt động của ứng dụng và mối đe dọa tiềm ẩn.
- Loại bỏ các quy tắc không cần thiết: Đôi khi, có những quy tắc trong Core Rule Set không phù hợp hoặc không cần thiết cho môi trường cụ thể của hệ thống. Loại bỏ các

quy tắc không cần thiết này có thể giảm thiểu số lượng false positive một cách đáng kể.

- Tạo các quy tắc tùy chỉnh (custom rules): Tạo các quy tắc tùy chỉnh cho phép người quản trị mạng xác định các mẫu hoạt động đáng nghi và đặt các biện pháp phòng ngừa cụ thể. Việc này giúp tăng cường khả năng phát hiện và giảm thiểu false positive bằng cách điều chỉnh chính sách bảo mật theo nhu cầu cụ thể của hệ thống.
- Sử dụng machine learning và AI: Kết hợp ModSecurity với các kỹ thuật machine learning và trí tuệ nhân tạo có thể giúp phát hiện các mẫu hoạt động không bình thường một cách tự động và hiệu quả hơn, từ đó giảm thiểu false positive và tăng cường bảo mật hệ thống mạng.

a. Improve Mod Security with custom rule:

Để có thể tạo được các rule custom theo nhu cầu, ta cần hiểu rõ về cấu trúc bộ quy tắc (rule) của Mod Security. Rule engine của ModSecurity, cho phép người quản trị tạo và tùy chỉnh các quy tắc để phát hiện và xử lý các mẫu tấn công phổ biến và cụ thể cho ứng dụng cụ thể của họ. Cú pháp:

SecRule VARIABLES OPERATOR ACTIONS

Ví dụ:

SecRule ARGS “<script>” log,deny,status:404

Trong đó:

VARIABLES: là một tập hợp các biến đầu vào được trích xuất từ request, cung cấp thông tin cho Mod Security. Các thông tin này có thể là request header, URI,...

OPERATOR: cung cấp cho ModSecurity cách tìm kiếm và so khớp rule

ACTIONS: các hành động sẽ thực hiện khi rule được so khớp thành công. Các hành động này có thể là ghi log, chặn, trả về status code,…

Task: Tìm hiểu cách viết rule, giải thích ý nghĩa của ít nhất 3 rule trong bộ Core Rule Set

Task: Chỉnh sửa hoặc viết mới 3 custom rule và thử nghiệm lại rule trên web DVWA.

Một vài gợi ý:

- Chặn từ một từ khoá nhất định trong form/url
- Chặn lượt truy cập tới web server từ một địa chỉ IP
- Giới hạn dung lượng upload của một file

b. Improve Mod Security with AI:

Việc kết hợp ModSecurity với trí tuệ nhân tạo (AI) đang mở ra một tiềm năng lớn trong việc cải thiện khả năng bảo mật của hệ thống mạng. AI có khả năng học từ dữ liệu lịch sử và tự động điều chỉnh mô hình để phát hiện ra các mẫu và xu hướng phức tạp hơn mà có thể bỏ qua bởi các phương pháp truyền thống. Kết hợp ModSecurity với AI giúp tăng cường khả năng phát hiện các mối đe dọa mạng và giảm thiểu số lượng false positive.

Có nhiều cách khác nhau để kết hợp trí tuệ nhân tạo với ModSecurity. Một trong những cách tiếp cận đáng chú ý để kết hợp trí tuệ nhân tạo (AI) với ModSecurity là sử dụng điểm bất

thường (anomaly score) của các quy tắc trong bộ Core Rule Set như một đặc trưng cho việc huấn luyện mô hình AI. Điều này có thể được thực hiện bằng cách kết hợp điểm bất thường với các đặc trưng khác được trích xuất từ giao thức HTTP transaction, như các thông tin về URL, phương thức HTTP, tiêu đề, thân nội dung (body), và thậm chí là thông tin về người gửi và người nhận. Bằng cách tạo thành một bộ đặc trưng huấn luyện AI từ điểm bất thường và các thông tin từ HTTP transaction, ta có thể xây dựng một mô hình AI có khả năng học và nhận biết các mẫu hành vi bất thường và tiềm ẩn trên mạng. Mô hình này có thể được sử dụng để phát hiện ra các cuộc tấn công và mối đe dọa mạng một cách tự động và hiệu quả hơn, từ đó giảm thiểu số lượng false positive và tăng cường bảo mật của hệ thống.
Ngoài ra, một cách tiếp cận khác là sử dụng các đoạn script để thực hiện việc truy xuất các thông tin của một HTTP request mà có điểm bất thường cao hơn một ngưỡng nhất định. Thông tin này sau đó có thể được sử dụng để tiến hành đánh giá lại và phân tích chi tiết về request đó trước khi thực hiện các hành động tiếp theo, như chặn hoặc ghi log. Điều này giúp đảm bảo rằng các hành động được thực hiện chỉ dựa trên các dữ liệu chính xác và đáng tin cậy, từ đó giảm thiểu rủi ro của việc chặn nhầm các request hợp lệ.
Bonus: Tham khảo các tài liệu sau, tiến hành cài đặt và thử nghiệm việc kết hợp AI vào ModSecurity:

- **https://github.com/ngoctint1lvc/waf**
- **https://github.com/coreruleset/machine-learning-integration-plugin**

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
  - Ví dụ: [NT534.K11.ANTN.1]-Lab1_1852xxxx_1852yyyy.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!