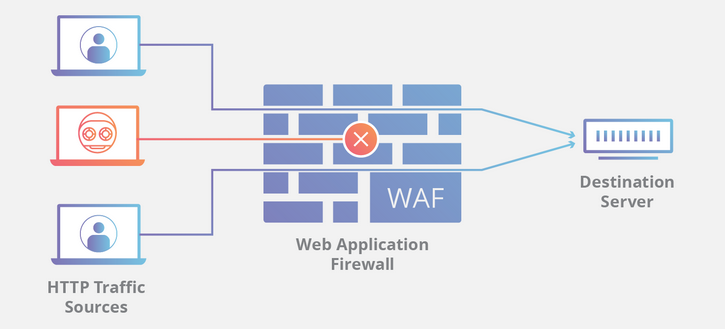
Tìm hiểu WAF và Modsecurity

1. WAF là gì?

* WAF (Web application firewall) hay còn gọi là tưởng lửa ứng dụng web là một loại tường lửa làm nhiệm vụ lọc, giám sát và chặn các lưu lượng HTTP đến và đi một ứng dụng Web. WAF khác với tường lửa thông thường ở chỗ nó có thể lọc được các lưu lượng cụ thể của một ứng dụng web trong khi các tường lửa thông thường thường chỉ bảo vệ các server. Bằng cách chặn bắt và kiểm tra các gói tin, WAF có thể phát hiện và ngăn chặn các dạng lỗ hổng xuất phát từ lỗi bảo mật của ứng dụng như SQL Injection, XSS, LFI … .
* Các WAF có thể là một thiết bị phần cứng, một phần mềm hoặc chạy như một dịch vụ và thường có một tập luật cụ thể để bảo vệ một hoặc nhiều ứng dụng.
* Hiện nay, khoảng 70% các cuộc tấn công mạng là nhằm vào ứng dụng web, do đó các tổ chức cần các biện pháp có thể giúp họ phòng tránh và giảm thiểu hậu quả trước những cuộc tấn công này. WAF là một biện pháp khả thi và thường được sử dụng để thiết lập một lớp bảo vệ đứng trước các ứng dụng web làm nhiệm vụ phát hiện và ngăn chặn tấn công.
* Mô hình:

1. Modsecurity

* Modsecurity là một WAF mã nguồn mở, đa nền tảng và được phát triển bởi Trustwave's SpiderLabs. Nó cung cấp khả năng bảo vệ ứng dụng web khỏi nhiều loại hình tấn công cũng như cho phép giám sát và phân tích lưu lượng mạng thời gian thực mà không cần can thiệp quá nhiều vào kiến trúc hạ tầng hệ thống.
* Một số chức năng của modsecurity:
  + Giám sát thời gian thực và phát hiện tấn công
  + Ngăn chặn tấn công và vá lỗi ảo.
  + Cung cấp một bộ ngôn ngữ luật cho phép dễ dàng tùy chỉnh, cài đặt để phát hiện, ngăn chặn các dạng tấn công nói chung hoặc với một hệ thống cụ thể nói riêng.
* OWASP Modsecurity Core rule set
  + Modsecurity đã cung cấp nhiều chức năng để giám sát quản lý cũng như một ngôn ngữ luật mạnh mẽ và linh hoạt, vì vậy nó có thể hoạt động rất hiệu quả nếu như có một bộ luật phù hợp. Do dó Trustwave's SpiderLabs đã tạo dự án OWASP ModSecurity Core Rule Set (CRS) mã nguồn mở bao gồm các luật để ngăn chặn các hình thức tấn công phổ biến nhất hiện nay và có độ chính xác tương đối cao. Tuy nhiên để bảo vệ ứng dụng web được tốt nhất, nên có một bộ luật được viết chuyên biệt cho chính ứng dụng web đó để đảm bảo ngăn chặn được các hình thức tấn công dựa trên những lỗi CVE hoặc các lỗ hổng 0-day để đảm bảo an toàn cho ứng dụng web.
* Mô hình hoạt động: