

# Tìm hiểu WAF (Web Application Firewall)

Trần Nguyễn Đức Minh - 2251012095  
Lư Hiếu Trung - 2251012145  
Trần Nguyễn Xuân Khánh - 2251012078



# WAF là gì?

- Web Application Firewall viết tắt là WAF. WAF sẽ kiểm tra lưu lượng truy cập và lọc ra những yêu cầu nào có mối đe dọa xâm phạm đến trang Web trước khi đến ứng dụng Web.
- WAF được cài lên máy chủ có chức năng theo dõi các thông tin được truyền qua giao thức http/https giữa trình duyệt của người dùng và máy chủ web tại lớp 7.

# Mô hình bảo mật và Mô hình hoạt động

## Mô hình bảo mật

Có thể dựa trên hai mô hình: Positive và Negative.

**Positive:** chỉ cho phép các lưu lượng hợp lệ được định nghĩa sẵn đi qua.

**Negative:** cho phép tất cả các lưu lượng vượt qua và chỉ chặn các lưu lượng được mà WAF cho là nguy hại.

## Mô hình hoạt động

WAF có thể hoạt động ở các mô hình riêng biệt.

- Đây là một số mô hình tham khảo: *Reverse Proxy, Layer 2 Bridge, Transparent Proxy, Host/Server Based*.

# Chức năng chính của WAF

- Cung cấp ứng dụng mở rộng hoặc chọn lọc cho máy chủ dịch vụ web.
- Bảo vệ hệ thống trước các loại tấn công phổ biến như: Cross-site Scripting (XSS) and SQL Injection.
- Kiểm tra cả nội dung các truy cập Web sử dụng giao thức HTTP ở lớp ứng dụng
- Phân tích những yêu cầu và cảnh báo ngay khi có một hoạt động đáng nghi nào đó trên hệ thống.



Web Application  
Firewall

# Cách hoạt động của WAF

## Giám sát yêu cầu HTTP/HTTPS

Quản lý mọi yêu cầu HTTP/HTTPS đến ứng dụng web.

## Xác định lưu lượng độc hại

Dùng các chính sách hoặc quy tắc được thiết lập trước để xác định lưu lượng nào là độc hại và an toàn.

## Chặn lọc các lưu lượng độc hại:

WAF sẽ chặn lưu lượng này trước khi chúng xâm nhập vào ứng dụng nếu chúng không phù hợp.

## Bảo vệ dữ liệu

Đảm bảo tính toàn vẹn của ứng dụng web

# Các hình thức tấn công mà WAF có thể ngăn chặn

WAF sẽ bảo vệ bạn khỏi các cuộc tấn công độc hại như:

1 Remote Code Execution

Tấn công thực thi Code từ xa

2 SQL Injection

Công nghệ Hack trích xuất thông tin từ Database

3 Cross-Site Scripting

Đưa vào Code của một Website tin cậy, làm dữ liệu nhạy cảm bị truy cập

# WAF mã nguồn mở tốt nhất

Tường lửa ứng dụng web mã nguồn mở sau đây có thể hữu ích nếu bạn đang tìm kiếm giải pháp thay thế miễn phí cho WAF thương mại để bảo vệ trang web của mình:

- NAXSI
- WebKnight
- Shadow Daemon
- Coraza
- OctopusWAF
- IronBee
- ModSecurity