

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TPHCM

KHOA CÔNG NGHỆ THÔNG TIN



HCMUTE

BÁO CÁO CUỐI KỲ

MÔN: AN NINH MẠNG

HỆ THỐNG TƯỜNG LỬA WEB

Sinh viên thực hiện:

1. Nguyễn Lưu Gia Bảo - 22162005

2. Nguyễn Thắng Lợi - 22162023

TP. Hồ Chí Minh, tháng 05 năm 2025

MỤC LỤC

PHẦN 1: MỞ ĐẦU.....	1
1. Mục tiêu nghiên cứu.....	1
2. Đối tượng nghiên cứu.....	2
3. Phương pháp nghiên cứu.....	2
4. Phạm vi nghiên cứu.....	3
PHẦN 2: NỘI DUNG.....	4
Chương 1: Tổng Quan Về Cơ Chế Hoạt Động Của WAF.....	4
1.1. Cấu trúc và nguyên lý hoạt động của WAF.....	4
1.2. Các phương pháp nhận diện tấn công.....	6
1.2.1. Phòng thủ dựa trên thông tin tình báo và các quy tắc cơ bản.....	6
1.2.2. Phân tích hành vi nâng cao và học máy.....	6
1.2.3. Bảo vệ chuyên sâu logic và dữ liệu ứng dụng.....	7
1.2.4. Đánh giá và quản lý lỗ hổng chủ động.....	8
Chương 2: Giới Thiệu Thiết Bị FortiWeb-100D.....	9
2.1. Thông số kỹ thuật của FortiWeb-100D.....	9
2.2. Các tính năng của FortiWeb-100D.....	10
Chương 3: Triển Khai Cấu Hình Và Thủ Nghiêm.....	14
3.1. Cấu hình các đối tượng máy chủ.....	15
3.2. DoS Protection.....	18
3.3. Known Attacks.....	21
3.3.1. Cross Site Scripting.....	21
3.3.2. SQL Injection.....	23
3.4. Advanced Protection.....	27
3.4.1. Client Side Request Forgery.....	27

3.4.2. HTTP Header Security.....	31
3.5. <i>Cookie Security</i>	33
3.6. <i>Input Validation</i>	36
3.6.1. File Security.....	36
3.6.2. Parameter Validation.....	39
3.7. <i>URL Access control</i>	41
3.8. <i>Áp dụng Machine Learning trong nhận diện bất thường</i>	44
3.8.1. Kích hoạt và giai đoạn học.....	46
3.8.2. Giai đoạn phát hiện và thực thi.....	49
3.9. <i>Thực hành khả năng scan lỗ hổng web</i>	51
PHẦN 3: KẾT LUẬN.....	55
1. Ưu nhược điểm của FortiWeb-100D.....	55
2. Tổng Kết.....	56
TÀI LIỆU THAM KHẢO.....	58

PHẦN 1: MỞ ĐẦU

Trong kỷ nguyên số hóa hiện nay, các ứng dụng web đã trở thành một phần không thể thiếu trong hoạt động của hầu hết các tổ chức và doanh nghiệp, từ việc cung cấp thông tin, dịch vụ trực tuyến, thương mại điện tử đến việc quản lý nội bộ. Sự phổ biến và tầm quan trọng ngày càng tăng của chúng cũng đi kèm với những thách thức lớn về an ninh mạng. Các ứng dụng web liên tục là mục tiêu của vô số các cuộc tấn công tinh vi, nhằm mục đích đánh cắp dữ liệu nhạy cảm, chiếm quyền kiểm soát hệ thống, phá hoại hoạt động hoặc làm tổn hại đến uy tín của tổ chức. Các mối đe dọa như SQL Injection, Cross-Site Scripting (XSS), tấn công Từ chối Dịch vụ (DoS/DDoS), tấn công vào API, và nhiều kỹ thuật khác không ngừng phát triển, đòi hỏi các biện pháp bảo vệ chuyên dụng và hiệu quả.

Trước bối cảnh đó, Tường lửa Ứng dụng Web (Web Application Firewall - WAF) đã nổi lên như một giải pháp bảo mật thiết yếu, đóng vai trò như một lá chắn quan trọng giữa người dùng internet và các ứng dụng web. Khác với tường lửa mạng truyền thống, WAF được thiết kế đặc biệt để hiểu và phân tích lưu lượng truy cập ở tầng ứng dụng (Lớp 7), qua đó phát hiện và ngăn chặn các cuộc tấn công nhắm vào logic và lỗ hổng của chính ứng dụng web.

Báo cáo này tập trung vào việc nghiên cứu và tìm hiểu sâu về công nghệ WAF, lấy trường hợp nghiên cứu cụ thể là thiết bị FortiWeb-100D của hãng bảo mật Fortinet. Thông qua việc kết hợp giữa lý thuyết và thực hành, báo cáo sẽ đi từ việc khám phá các nguyên tắc hoạt động cơ bản, các phương pháp nhận diện tấn công tiên tiến, đến việc triển khai cấu hình chi tiết và kiểm nghiệm hiệu quả bảo vệ của FortiWeb-100D trong một môi trường giả lập. Báo cáo được cấu trúc thành ba phần chính: Mở đầu, Nội dung (bao gồm tổng quan về WAF, giới thiệu thiết bị, triển khai cấu hình, kiểm nghiệm và đánh giá),

1. Mục tiêu nghiên cứu

Nghiên cứu này được thực hiện nhằm đạt được các mục tiêu chính sau đây:

- Hiểu rõ các nguyên tắc cơ bản: Nắm vững cấu trúc, nguyên lý hoạt động và các mô hình triển khai phổ biến của Tường lửa Ứng dụng Web (WAF).
- Khám phá các kỹ thuật phát hiện tấn công: Tìm hiểu và phân tích các phương pháp nhận diện tấn công đa dạng được các WAF hiện đại, đặc biệt là FortiWeb, sử dụng (ví dụ: dựa trên chữ ký, phân tích hành vi, học máy, chống bot, bảo vệ API).
- Tích lũy kinh nghiệm thực tế: Có được kinh nghiệm thực hành trong việc cấu hình, triển khai và quản lý một thiết bị WAF cụ thể là FortiWeb-100D để bảo vệ một ứng dụng web mẫu (DVWA) trong môi trường lab.
- Đánh giá hiệu quả bảo vệ: Kiểm nghiệm và đánh giá một cách khách quan khả năng của thiết bị FortiWeb-100D đã được cấu hình trong việc phát hiện và ngăn chặn các loại tấn công web phổ biến thông qua các kịch bản tấn công mô phỏng.
- Nhận định về giải pháp: Đưa ra những đánh giá về ưu điểm, nhược điểm và sự phù hợp của giải pháp FortiWeb-100D dựa trên kết quả nghiên cứu và thực hành.

2. Đối tượng nghiên cứu

Đối tượng nghiên cứu trọng tâm và bao quát của báo cáo này là công nghệ Tường lửa Ứng dụng Web (Web Application Firewall - WAF). Việc lựa chọn WAF làm đối tượng chính xuất phát từ vai trò ngày càng quan trọng của công nghệ này trong việc đảm bảo an ninh cho các ứng dụng web - một thành phần cốt lõi của hạ tầng công nghệ thông tin và hoạt động kinh doanh của hầu hết các tổ chức hiện nay. Trong bối cảnh các cuộc tấn công mạng nhắm vào ứng dụng web ngày càng gia tăng về số lượng và mức độ tinh vi, việc hiểu rõ và triển khai hiệu quả các giải pháp WAF là một yêu cầu cấp thiết.

Để nghiên cứu công nghệ WAF một cách cụ thể và thực tiễn, báo cáo tập trung vào một sản phẩm đại diện là thiết bị phần cứng FortiWeb-100D của hãng bảo mật Fortinet. Lý do lựa chọn FortiWeb-100D làm đối tượng nghiên cứu chính bao gồm:

- Tính sẵn có trong môi trường thực hành: Đây là thiết bị được sử dụng trong các bài thực hành của môn học, cho phép sinh viên có cơ hội trực tiếp cấu hình và kiểm nghiệm.
- Tính đại diện: FortiWeb là một dòng sản phẩm WAF phổ biến trên thị trường, tích hợp nhiều công nghệ bảo vệ tiên tiến (như Machine Learning, Bot Mitigation, API Protection) đại diện cho các xu hướng WAF hiện đại. Model 100D, dù thuộc phân khúc cho doanh nghiệp vừa và nhỏ, vẫn cung cấp đầy đủ các tính năng cốt lõi.
- Hệ sinh thái Fortinet: Việc tìm hiểu FortiWeb cũng mang lại cái nhìn về cách một sản phẩm WAF tích hợp vào hệ sinh thái bảo mật rộng lớn hơn (Fortinet Security Fabric).

Đối tượng thứ ba và không kém phần quan trọng là ứng dụng web Damn Vulnerable Web Application (DVWA). DVWA được chọn làm ứng dụng mục tiêu để FortiWeb-100D bảo vệ và cũng là đối tượng để thực hiện các kịch bản tấn công kiểm nghiệm. Sự lựa chọn này dựa trên các đặc điểm phù hợp của DVWA:

- Thiết kế cho mục đích giáo dục và thử nghiệm: DVWA được xây dựng một cách có chủ đích với nhiều lỗ hổng bảo mật web phổ biến (SQLi, XSS, File Upload, CSRF, Command Injection...), tạo ra một môi trường lý tưởng để kiểm tra và đánh giá hiệu quả của các biện pháp bảo vệ WAF.
- Môi trường kiểm soát được: Việc sử dụng DVWA cho phép thực hiện các cuộc tấn công mô phỏng một cách an toàn trong môi trường lab mà không gây ảnh hưởng đến các hệ thống thực tế.
- Phản ánh các lỗ hổng thực tế: Mặc dù là một ứng dụng thử nghiệm, các lỗ hổng trong DVWA mô phỏng khá sát với các điểm yếu thường gặp trong các ứng dụng web ngoài đời thực.

Như vậy, việc nghiên cứu kết hợp ba đối tượng này - công nghệ WAF nói chung, thiết bị FortiWeb-100D cụ thể, và ứng dụng mục tiêu DVWA - cho phép báo cáo vừa có cái nhìn tổng quan về lý thuyết, vừa đi sâu vào thực hành và đánh giá thực tiễn một cách hiệu quả.

3. Phương pháp nghiên cứu

Để đạt được các mục tiêu đã đề ra và đảm bảo tính khoa học, khách quan cho báo cáo, các phương pháp nghiên cứu sau đây đã được áp dụng một cách kết hợp:

- Nghiên cứu tài liệu: Phương pháp này bao gồm việc thu thập, tổng hợp và phân tích thông tin từ các nguồn tài liệu đa dạng và đáng tin cậy. Các nguồn này bao gồm tài liệu kỹ thuật chính thức của nhà sản xuất Fortinet (như datasheet, administration guide, concept guide cho FortiWeb), tài liệu

hướng dẫn thực hành cụ thể (huong-dan.pdf), các bài báo khoa học, bài viết chuyên ngành về an ninh ứng dụng web và công nghệ WAF, cũng như các tài liệu và hướng dẫn từ các tổ chức uy tín như OWASP.

- Thực nghiệm trong phòng lab: Đây là phương pháp cốt lõi, bao gồm việc trực tiếp thao tác, cấu hình và triển khai thiết bị FortiWeb-100D trong một môi trường mạng ảo hóa được kiểm soát. Quá trình này tuân theo các bài thực hành đã được hướng dẫn (huong-dan.pdf) và mở rộng thêm các cấu hình nâng cao dựa trên tìm hiểu lý thuyết. Việc tương tác với giao diện quản lý đồ họa (GUI) của FortiWeb để thiết lập các chính sách, profile bảo mật và theo dõi hoạt động là trọng tâm của phương pháp này.
- Kiểm thử và mô phỏng: Sau khi cấu hình, báo cáo tiến hành kiểm thử hiệu quả bảo vệ bằng cách thiết kế và thực hiện các kịch bản tấn công có kiểm soát nhắm vào ứng dụng web DVWA đã được bảo vệ bởi FortiWeb. Các công cụ và kỹ thuật tấn công phổ biến như trình duyệt web, công cụ tạo tải ApacheBench, và các payload tấn công thủ công được sử dụng để mô phỏng các mối đe dọa thực tế.
- Phân tích và đánh giá định tính: Cuối cùng, các kết quả thu được từ quá trình thực nghiệm và kiểm thử được phân tích một cách cẩn thận. Phương pháp này bao gồm việc xem xét và diễn giải các bản ghi nhật ký (logs) hệ thống và sự kiện tấn công của FortiWeb, quan sát hành vi thực tế của WAF và ứng dụng web khi đối mặt với tấn công, từ đó đưa ra những nhận định, so sánh và đánh giá về hiệu quả, ưu điểm, nhược điểm của giải pháp FortiWeb-100D.

4. Phạm vi nghiên cứu

Phạm vi của báo cáo được giới hạn trong các khía cạnh sau:

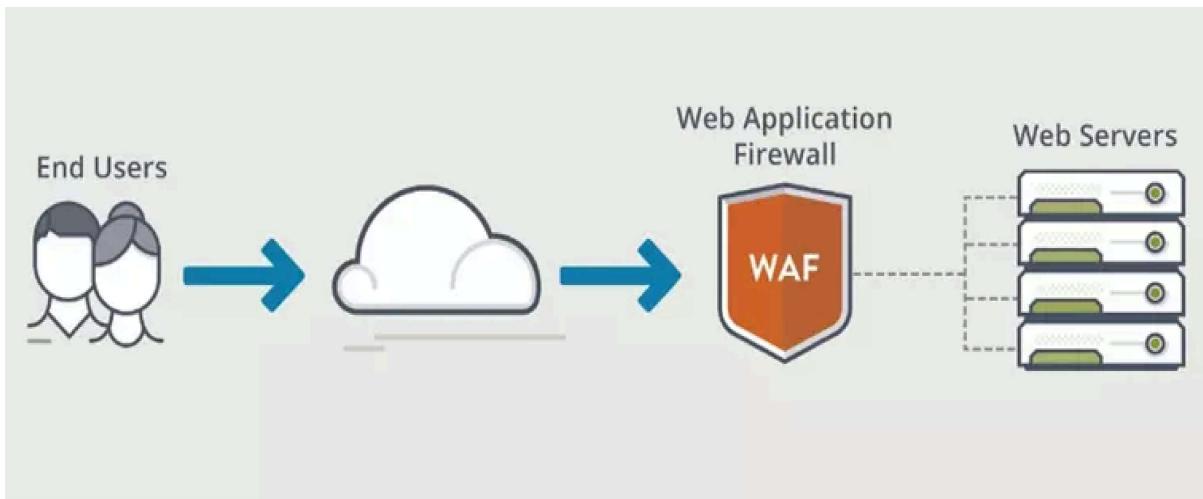
- Về lý thuyết: Báo cáo tập trung vào các khái niệm cơ bản và nâng cao của công nghệ Tường lửa ứng dụng Web (WAF), bao gồm nguyên tắc hoạt động, các mô hình triển khai, và đặc biệt là các phương pháp nhận diện tấn công chính như nhận diện dựa trên chữ ký, dựa trên hành vi bất thường (bao gồm Machine Learning), chống Bot, bảo vệ API, xác thực đầu vào và quét lỗ hổng. Các thông số kỹ thuật và tính năng cơ bản của thiết bị FortiWeb-100D cũng được trình bày. Báo cáo không đi sâu vào so sánh chi tiết với tất cả các sản phẩm WAF khác trên thị trường hoặc các khía cạnh quá chuyên sâu về thuật toán Machine Learning.
- Về thực hành: Phạm vi thực hành giới hạn trong việc cấu hình thiết bị FortiWeb-100D trong môi trường lab mô phỏng, sử dụng chế độ Reverse Proxy. Các cấu hình chính bao gồm thiết lập các đối tượng mạng cơ bản, triển khai các chính sách và profile bảo vệ cho các loại tấn công phổ biến (DoS, SQLi, XSS, CSRF, File Upload, Parameter Tampering, Cookie/Header issues), kích hoạt và quan sát hoạt động của Machine Learning, và thực hiện Web Vulnerability Scan. Báo cáo không bao gồm việc cấu hình các chế độ triển khai khác (Transparent, Offline Sniffing) hoặc các tính năng rất nâng cao không có trong bài lab (ví dụ: tích hợp FortiSandbox, cấu hình cân bằng tải phức tạp).
- Về kiểm nghiệm: Quá trình kiểm nghiệm tập trung vào việc mô phỏng các cuộc tấn công phổ biến và một số kỹ thuật tấn công zero-day cơ bản nhắm vào ứng dụng DVWA. Việc đánh giá hiệu quả dựa trên khả năng phát hiện và ngăn chặn của FortiWeb trong môi trường lab. Báo cáo không thực hiện kiểm thử hiệu năng (performance testing) chi tiết của thiết bị dưới tải trọng lớn hoặc kiểm thử trong môi trường ứng dụng production thực tế với các tình huống phức tạp hơn.

PHẦN 2: NỘI DUNG

Chương 1: Tổng Quan Về Cơ Chế Hoạt Động Của WAF

1.1. Cấu trúc và nguyên lý hoạt động của WAF

Tường lửa Ứng dụng Web (Web Application Firewall - WAF) là một giải pháp bảo mật được thiết kế đặc biệt để bảo vệ các ứng dụng web và máy chủ web khỏi các cuộc tấn công mạng ở tầng ứng dụng (Lớp 7 trong mô hình OSI). Khác với tường lửa mạng truyền thông (Network Firewall) chủ yếu hoạt động ở tầng mạng và tầng giao vận (Lớp 3 và 4), tập trung vào việc kiểm soát lưu lượng dựa trên địa chỉ IP, cổng và giao thức, WAF đi sâu hơn vào nội dung của chính các giao tiếp HTTP/HTTPS. Mục tiêu chính của WAF là phân tích lưu lượng truy cập giữa người dùng và ứng dụng web để phát hiện và ngăn chặn các hoạt động đáng ngờ hoặc độc hại có thể khai thác lỗ hổng của ứng dụng, đánh cắp dữ liệu, hoặc gây gián đoạn dịch vụ.



Về mặt cấu trúc, một WAF thường bao gồm các thành phần chính sau:

- Bộ máy phân tích (Analysis Engine): Đây là "trái tim" của WAF, chịu trách nhiệm kiểm tra và phân tích sâu các yêu cầu HTTP/HTTPS gửi đến ứng dụng web và các phản hồi HTTP/HTTPS từ ứng dụng trả về. Bộ máy này sử dụng một loạt các quy tắc, chữ ký, thuật toán phân tích hành vi, và các kỹ thuật học máy để xác định xem lưu lượng có chứa dấu hiệu của các cuộc tấn công hay không.
- Bộ quy tắc và chữ ký (Rule Set and Signatures): WAF dựa vào một tập hợp các quy tắc (policies) và chữ ký (signatures) để nhận diện các mẫu tấn công đã biết. Các quy tắc này có thể được định nghĩa trước bởi nhà cung cấp WAF, được cập nhật thường xuyên để đối phó với các mối đe dọa mới, hoặc được quản trị viên tùy chỉnh để phù hợp với đặc thù của ứng dụng web cần bảo vệ. Chữ ký là các mẫu cụ thể của mã độc hoặc các dấu hiệu đặc trưng của một kiểu tấn công (ví dụ: chuỗi ký tự thường thấy trong tấn công SQL Injection).
- Cơ chế thực thi (Enforcement Mechanism): Khi bộ máy phân tích phát hiện một mối đe dọa, cơ chế thực thi sẽ được kích hoạt để áp dụng hành động đã được cấu hình. Các hành động này có thể bao gồm:
 - Chặn (Block): Ngăn chặn hoàn toàn yêu cầu/phản hồi đáng ngờ tiếp cận ứng dụng hoặc người dùng.

- Ghi log (Log): Ghi lại chi tiết về sự kiện đáng ngờ để phục vụ cho việc điều tra và phân tích sau này.

- Cảnh báo (Alert): Gửi thông báo đến quản trị viên hệ thống về mối đe dọa vừa được phát hiện.

- Thách thức (Challenge): Yêu cầu người dùng thực hiện thêm một bước xác thực (ví dụ: CAPTCHA) để chứng minh họ không phải là bot.

- Chuyển hướng (Redirect): Chuyển hướng yêu cầu đến một trang thông báo hoặc một tài nguyên khác.

• Giao diện quản lý (Management Interface): Cung cấp cho quản trị viên công cụ để cấu hình WAF, cập nhật bộ quy tắc, theo dõi nhật ký hoạt động, xem báo cáo và chỉnh sửa các chính sách bảo mật.

Nguyên lý hoạt động cơ bản của WAF là kiểm tra mọi yêu cầu HTTP/HTTPS trước khi chúng đến được máy chủ ứng dụng web và kiểm tra các phản hồi trước khi chúng được gửi lại cho người dùng. Quá trình này diễn ra theo các bước:

• Tiếp nhận lưu lượng: WAF được triển khai trên đường đi của lưu lượng truy cập web, có thể ở dạng thiết bị phần cứng, máy ảo, hoặc dịch vụ đám mây.

• Giải mã và phân tích: Nếu lưu lượng được mã hóa SSL/TLS, WAF có thể được cấu hình để giải mã lưu lượng này (SSL Offloading/Inspection) nhằm kiểm tra nội dung bên trong. Sau đó, WAF phân tích các thành phần của yêu cầu/phản hồi như URL, header, cookie, tham số biểu mẫu (form parameters), và nội dung JSON/XML.

• Đòi hỏi với chính sách bảo mật: Bộ máy phân tích của WAF áp dụng các chính sách bảo mật, bao gồm các quy tắc dựa trên chữ ký, quy tắc dựa trên hành vi, và các mô hình học máy, để đánh giá xem lưu lượng có an toàn hay không.

• Thực thi hành động: Dựa trên kết quả phân tích, WAF sẽ thực hiện hành động tương ứng (chặn, ghi log, cảnh báo, v.v.).

• Chuyển tiếp lưu lượng hợp lệ: Nếu lưu lượng được xác định là an toàn, WAF sẽ chuyển tiếp nó đến máy chủ ứng dụng web (đối với yêu cầu) hoặc đến người dùng (đối với phản hồi).

WAF có thể được triển khai theo nhiều mô hình khác nhau, bao gồm:

• Reverse Proxy: WAF hoạt động như một proxy ngược, đứng trước các máy chủ web, tiếp nhận tất cả lưu lượng truy cập đến và chuyển tiếp các yêu cầu hợp lệ. Đây là mô hình triển khai phổ biến.

• Transparent Bridge/Proxy: WAF được đặt inline giữa người dùng và máy chủ web, hoạt động một cách trong suốt mà không yêu cầu thay đổi cấu hình mạng phức tạp.

• Cloud-based WAF: Dịch vụ WAF được cung cấp bởi các nhà cung cấp đám mây, giúp doanh nghiệp dễ dàng triển khai và quản lý bảo vệ cho ứng dụng web mà không cần đầu tư vào phần cứng.

Nhìn chung, WAF đóng vai trò như một người gác cổng thông minh cho các ứng dụng web, giúp phát hiện và vô hiệu hóa nhiều loại tấn công phổ biến như SQL Injection, Cross-Site Scripting (XSS), Command Injection, tấn công từ chối dịch vụ (DoS/DDoS) ở tầng ứng dụng, và nhiều mối đe dọa khác, qua đó bảo vệ dữ liệu nhạy cảm, duy trì hoạt động kinh doanh và tuân thủ các quy định bảo mật.

1.2. Các phương pháp nhận diện tấn công

FortiWeb là một giải pháp Tường lửa Ứng dụng Web (WAF) toàn diện, được Fortinet phát triển với mục tiêu cung cấp khả năng bảo vệ đa lớp chống lại các mối đe dọa ngày càng phức tạp nhắm vào ứng dụng web. Thay vì dựa vào một kỹ thuật đơn lẻ, FortiWeb kết hợp một loạt các phương pháp phát hiện và ngăn chặn tấn công, từ các cơ chế truyền thống dựa trên thông tin tình báo về mối đe dọa đến các công nghệ phân tích hành vi và học máy tiên tiến. Sự phối hợp của các lớp bảo vệ này giúp FortiWeb không chỉ đối phó hiệu quả với các cuộc tấn công đã biết mà còn có khả năng phát hiện và ngăn chặn các mối đe dọa mới, bao gồm cả các cuộc tấn công zero-day và các hành vi bất thường khó lường.

1.2.1. Phòng thủ dựa trên thông tin tình báo và các quy tắc cơ bản

Lớp phòng thủ nền tảng của FortiWeb tập trung vào việc sử dụng thông tin tình báo về mối đe dọa được cập nhật liên tục và các quy tắc bảo mật cơ bản để nhận diện và chặn các cuộc tấn công phổ biến cũng như các nguồn tấn công đã được định danh. Các cơ chế chính trong lớp này bao gồm việc phát hiện dựa trên chữ ký tấn công (Attack Signature Detection), được cung cấp và làm mới thường xuyên bởi FortiGuard Labs. Cơ sở dữ liệu chữ ký này chứa hàng ngàn mẫu nhận dạng của các biến thể tấn công đã biết như SQL Injection, Cross-Site Scripting (XSS), OS Command Injection, Path Traversal và nhiều loại mã độc khác. Khi lưu lượng truy cập đi qua, FortiWeb sẽ đối chiếu nội dung yêu cầu/phản hồi với các chữ ký này; nếu có sự trùng khớp, hành động ngăn chặn tương ứng sẽ được thực thi. Bên cạnh các chữ ký được cập nhật tự động, FortiWeb cho phép quản trị viên tạo các chữ ký tùy chỉnh (Custom Signatures) để giải quyết các mối đe dọa đặc thù cho ứng dụng của họ.

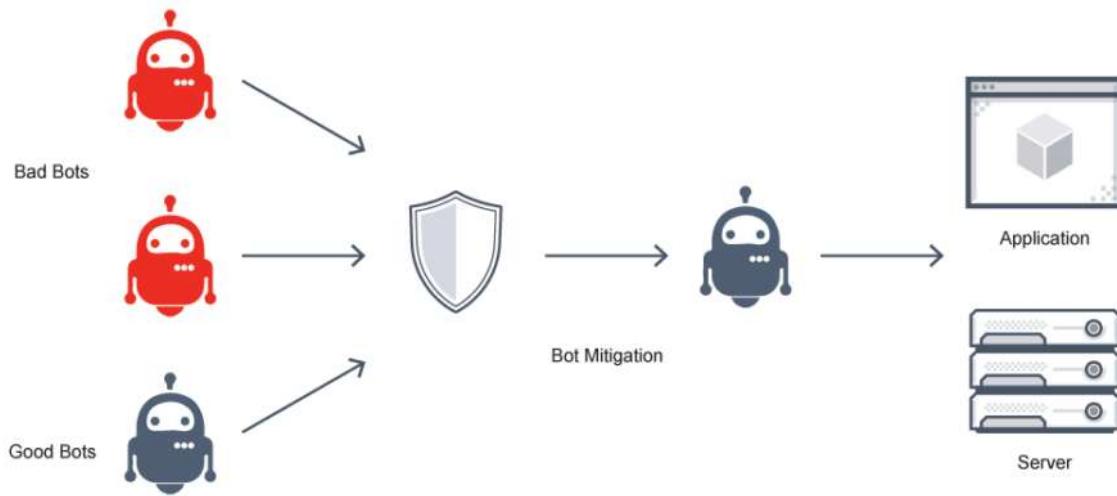
Tiếp theo, FortiWeb tăng cường lớp phòng thủ này bằng dịch vụ danh tiếng IP (IP Reputation Service) và khả năng chặn theo vị trí địa lý (GeoIP Blocking). Dịch vụ danh tiếng IP, cũng từ FortiGuard, giúp FortiWeb xác định và chặn lưu lượng từ các địa chỉ IP được biết là có liên quan đến các hoạt động độc hại (botnet, spam, proxy ẩn danh...). Tính năng chặn theo vị trí địa lý cho phép quản trị viên kiểm soát truy cập từ các quốc gia hoặc khu vực cụ thể, hữu ích cho việc tuân thủ quy định hoặc giới hạn bờ mặt tấn công. Một thành phần quan trọng khác là kiểm tra và ràng buộc giao thức (Protocol Validation and Constraints). FortiWeb thực hiện kiểm tra nghiêm ngặt tính hợp lệ của giao thức HTTP/HTTPS, đảm bảo các yêu cầu tuân thủ tiêu chuẩn RFC. Bất kỳ yêu cầu nào có định dạng không hợp lệ, chứa ký tự bất thường, hoặc vi phạm các quy tắc giao thức (ví dụ: header quá dài, phương thức HTTP không được phép) đều có thể bị chặn, giúp ngăn chặn các kỹ thuật tấn công dựa trên việc khai thác điểm yếu trong xử lý giao thức. Cuối cùng, đối với các ứng dụng cho phép tải tệp lên, FortiWeb có thể tích hợp khả năng quét mã độc Anti-virus (Integrated Antivirus Scanning). Sử dụng bộ máy và chữ ký anti-virus từ FortiGuard, FortiWeb kiểm tra các tệp tải lên để phát hiện và chặn virus, trojan, và các phần mềm độc hại khác, ngăn chặn ứng dụng web trở thành một kênh phát tán mã độc.

1.2.2. Phân tích hành vi nâng cao và học máy

Để đối phó với các mối đe dọa tinh vi hơn mà các phương pháp dựa trên quy tắc và chữ ký có thể bỏ sót, FortiWeb triển khai các kỹ thuật phân tích hành vi và học máy tiên tiến. Trọng tâm của lớp phòng thủ này là khả năng phát hiện bất thường và tấn công zero-day bằng học máy hai lớp (Dual-Layer Machine Learning for Anomaly and Zero-Day Detection). FortiWeb không chỉ tìm kiếm các mẫu tấn công đã biết mà còn tự động xây dựng một mô hình hành vi "bình thường" của từng ứng dụng web. Lớp học máy đầu tiên quan sát lưu lượng truy cập hợp lệ, phân tích các yếu tố

như URL, tham số, kiểu dữ liệu, tần suất, và phương thức HTTP để tạo ra một hồ sơ hành vi chi tiết. Bất kỳ yêu cầu nào sai lệch đáng kể so với hồ sơ này sẽ được đánh dấu là một "bất thường". Sau đó, lớp học máy thứ hai sẽ xác minh xem bất thường đó có thực sự là một mối đe dọa hay không bằng cách đối chiếu với các mô hình mối đe dọa đã được huấn luyện trước (pre-trained threat models) từ hàng ngàn mẫu tấn công thực tế. Cách tiếp cận này giúp FortiWeb phát hiện các cuộc tấn công mới với độ chính xác cao và giảm thiểu đáng kể tỷ lệ báo động giả.

Một thành phần quan trọng khác trong lớp này là khả năng nhận diện và giảm thiểu bot tinh vi (Sophisticated Bot Detection and Mitigation). FortiWeb sử dụng nhiều kỹ thuật kết hợp như phân tích hành vi của bot, chữ ký bot, thử thách thông minh (CAPTCHA, JavaScript challenge), kỹ thuật đánh lừa bot (Bot Deception), và nhận dạng dựa trên sinh trắc học để phân biệt giữa người dùng thực, bot hợp pháp, và bot độc hại. Mục tiêu là chặn các hoạt động tự động có hại như web scraping, credential stuffing, và tấn công DoS mà không làm ảnh hưởng đến trải nghiệm người dùng hợp pháp. Cuối cùng, FortiWeb cung cấp các cơ chế mạnh mẽ để phòng chống tấn công từ chối dịch vụ tầng ứng dụng (Application-Layer DoS/DDoS Prevention). Các biện pháp này bao gồm giới hạn tốc độ truy cập (Rate Limiting), phát hiện HTTP flood (HTTP Flood Detection), kiểm tra tính hợp lệ của client, và quản lý phiên để theo dõi các hành vi bất thường.



1.2.3. Bảo vệ chuyên sâu logic và dữ liệu ứng dụng

Lớp bảo vệ này đi sâu vào việc bảo vệ các thành phần và logic cụ thể của ứng dụng web, đảm bảo tính toàn vẹn và bảo mật của dữ liệu người dùng cũng như chính ứng dụng. FortiWeb cung cấp khả năng bảo mật giao diện lập trình ứng dụng (API Security) bằng cách cho phép xác thực các yêu cầu API dựa trên định nghĩa schema (ví dụ: OpenAPI), bảo vệ nội dung JSON/XML khỏi các tấn công như XXE hay JSON Injection, và áp dụng các chính sách WAF chung cho lưu lượng API. Việc kiểm soát và xác thực đầu vào người dùng (User Input Validation and Sanitization) là một biện pháp cực kỳ quan trọng, được FortiWeb hỗ trợ thông qua việc cho phép định nghĩa các quy tắc chi tiết cho từng tham số (Parameter Validation Rules), giới hạn kiểu dữ liệu, độ dài, giá trị cho phép. Đồng thời, FortiWeb cũng bảo vệ việc tải tệp lên (Secure File Uploads / File Security) bằng cách giới hạn loại tệp, kích thước, và quét virus như đã đề cập, ngăn chặn việc tải lên shell độc hại.

FortiWeb còn chú trọng đến bảo vệ cookie và quản lý phiên (Cookie Protection and Session Management). Thiết bị có thể mã hóa cookie (Cookie Encryption) để bảo vệ nội dung nhạy cảm, ký cookie (Cookie Signing) để chống giả mạo, và tự động thêm các cờ bảo mật quan trọng như HttpOnly và Secure. Một cơ chế quan trọng khác là thực thi chính sách bảo mật HTTP Header (HTTP Header Security Policy Enforcement). FortiWeb có thể tự động thêm các header bảo mật như X-Frame-Options, Strict-Transport-Security (HSTS), Content-Security-Policy (CSP) vào phản hồi từ máy chủ, hoặc xóa các header không mong muốn có thể tiết lộ thông tin hệ thống (Source 136 final-term-project.docx). Cuối cùng, để chống lại tấn công giả mạo yêu cầu liên trang, FortiWeb triển khai CORS Protection và các cơ chế ngăn chặn tấn công Cross-Site Request Forgery (CSRF Protection) bằng cách sử dụng CSRF token, đảm bảo rằng các hành động nhạy cảm chỉ được thực hiện bởi người dùng đã xác thực và có chủ đích.

1.2.4. Dánh giá và quản lý lỗ hổng chủ động

Ngoài các cơ chế phòng thủ phản ứng và ngăn chặn theo thời gian thực, FortiWeb còn cung cấp công cụ để các tổ chức có thể chủ động đánh giá và quản lý lỗ hổng ứng dụng web (Proactive Web Application Vulnerability Assessment and Management). Tính năng nổi bật nhất trong lớp này là quét lỗ hổng ứng dụng web (Web Application Vulnerability Scanning). FortiWeb tích hợp một trình quét lỗ hổng cho phép quản trị viên thực hiện các cuộc kiểm tra bảo mật tự động, định kỳ hoặc theo yêu cầu, trên các ứng dụng web của họ. Trình quét này sẽ thu thập thông tin về cấu trúc ứng dụng và cố gắng phát hiện các điểm yếu phổ biến như SQL Injection, XSS, cấu hình sai máy chủ, các thành phần phần mềm lỗi thời và các lỗ hổng khác. Sau khi quét, FortiWeb sẽ tạo ra một báo cáo chi tiết, phân loại các lỗ hổng theo mức độ nghiêm trọng và cung cấp các khuyến nghị để khắc phục. Điều này giúp các tổ chức xác định và vá các lỗ hổng trước khi chúng bị kẻ tấn công khai thác.

Scan Summary		
Target	10.1.1.252	
Request Count	11133	
Requests per Minute	816	
Total Alerts Found	8	
Alerts Found		
#	Category	Vulnerabilities
1	Server header	1
2	Powered-by header	1
3	Favicon identification failed	1
4	Cross site tracing vulnerability	1
5	Non existent methods default to GET	1
6	Internal hostname in HTML link	1
7	Strange HTTP response code	1
8	Webserver fingerprint	1

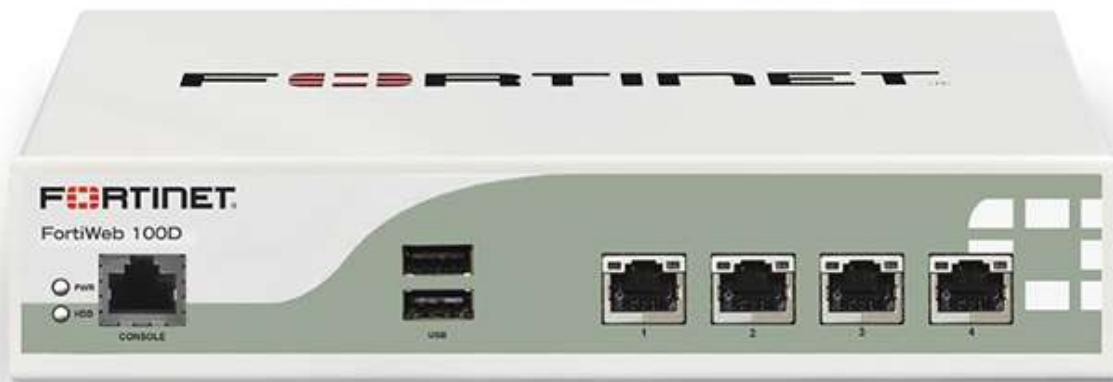
Bằng cách kết hợp các lớp phòng thủ đa dạng này, FortiWeb tạo ra một giải pháp bảo mật ứng dụng web mạnh mẽ và linh hoạt, có khả năng thích ứng với bối cảnh mới đe dọa không ngừng thay đổi và bảo vệ hiệu quả các tài sản ứng dụng web quan trọng của tổ chức.

Chương 2: Giới Thiệu Thiết Bị FortiWeb-100D

Sau khi tìm hiểu về cấu trúc, nguyên lý hoạt động chung của Tường lửa Ứng dụng Web (WAF) và các phương pháp nhận diện tấn công tiên tiến mà FortiWeb tích hợp, chương này sẽ đi sâu vào giới thiệu cụ thể về thiết bị FortiWeb-100D. Đây là một trong những model thuộc dòng sản phẩm FortiWeb của Fortinet, được thiết kế để cung cấp giải pháp bảo mật ứng dụng web mạnh mẽ và hiệu quả cho các doanh nghiệp vừa và nhỏ, cũng như các văn phòng chi nhánh. Việc hiểu rõ về thông số kỹ thuật và các tính năng của FortiWeb-100D sẽ giúp chúng ta có cái nhìn thực tế hơn về khả năng và phạm vi ứng dụng của thiết bị này trong việc bảo vệ các tài sản web quan trọng.

2.1. Thông số kỹ thuật của FortiWeb-100D

FortiWeb-100D là một thiết bị phần cứng chuyên dụng (appliance) được Fortinet tối ưu hóa cho nhiệm vụ bảo vệ ứng dụng web, cung cấp một sự cân bằng giữa hiệu suất, mật độ công và các tính năng bảo mật tiên tiến. Để đánh giá đầy đủ khả năng của thiết bị này, việc xem xét các thông số kỹ thuật cụ thể là điều cần thiết.



Về hiệu suất xử lý, FortiWeb-100D được thiết kế để đáp ứng nhu cầu của các doanh nghiệp có lưu lượng truy cập web ở mức vừa phải. Thiết bị này cung cấp thông lượng WAF (WAF Throughput), tức là tốc độ xử lý tối đa khi tất cả các tính năng bảo mật WAF được kích hoạt, vào khoảng 250 Mbps đến 500 Mbps tùy thuộc vào phiên bản firmware và điều kiện kiểm thử cụ thể. Đối với lưu lượng HTTP thuần túy (HTTP Throughput), con số này có thể cao hơn. Một chỉ số quan trọng khác là khả năng xử lý giao dịch HTTP mỗi giây ở tầng 7 (Layer 7 HTTP Transactions Per Second - TPS), FortiWeb-100D có thể xử lý hàng ngàn TPS, đảm bảo khả năng đáp ứng nhanh chóng các yêu cầu của người dùng. Số lượng kết nối đồng thời HTTP (HTTP Concurrent Connections) mà thiết bị có thể duy trì cũng lên đến hàng trăm ngàn, cho phép phục vụ một lượng lớn người dùng cùng lúc mà không làm giảm hiệu suất. Độ trễ (Latency) do FortiWeb-100D thêm vào thường ở mức rất thấp, chỉ vài mili giây, đảm bảo không ảnh hưởng đáng kể đến trải nghiệm người dùng.

Về giao diện phần cứng và kết nối mạng, FortiWeb-100D được trang bị khá đa dạng các cổng kết nối để dễ dàng tích hợp vào nhiều mô hình mạng khác nhau. Thiết bị này thường bao gồm 4 cổng Gigabit Ethernet RJ45 (GE RJ45), cho phép thiết lập các kết nối dự phòng, phân tách các vùng mạng (ví dụ: mạng quản lý, mạng cho máy chủ, mạng cho người dùng) hoặc triển khai ở các chế độ khác nhau như Reverse Proxy hay Transparent Inline. Ngoài ra, một số biến thể hoặc các model

tương đương trong cùng phân khúc có thể có thêm các cổng quang SFP để hỗ trợ kết nối cáp quang tốc độ cao hoặc khoảng cách xa. Thiết bị cũng được trang bị 1 cổng Console RJ45 cho việc truy cập quản trị trực tiếp qua dòng lệnh (CLI) và thường có ít nhất 2 cổng USB cho các mục đích như cập nhật firmware, sao lưu/khôi phục cấu hình, hoặc kết nối các thiết bị ngoại vi khác (ví dụ: USB token). Một cổng quản lý chuyên dụng (dedicated management port) cũng thường có mặt để tách biệt lưu lượng quản trị khỏi lưu lượng dữ liệu.

Đối với khả năng lưu trữ, FortiWeb-100D tích hợp bộ nhớ trong, thường là ổ cứng thể rắn (SSD), với dung lượng đủ để lưu trữ hệ điều hành FortiWeb OS, các bản cập nhật firmware, cấu hình hệ thống, và quan trọng nhất là nhật ký (logs) chi tiết về các sự kiện hệ thống, lưu lượng truy cập, và các sự kiện tấn công. Dung lượng lưu trữ này cũng được sử dụng để lưu trữ các báo cáo bảo mật và các tệp tin được đưa vào quarantine.

Về yếu tố hình thức và môi trường hoạt động, FortiWeb-100D có thiết kế dạng rack-mountable 1U, một kích thước tiêu chuẩn cho việc lắp đặt trong các tủ rack tại trung tâm dữ liệu hoặc phòng máy chủ của doanh nghiệp, giúp tối ưu hóa không gian. Kích thước vật lý của thiết bị thường vào khoảng 44 mm (Cao) x 432 mm (Rộng) x 254 mm (Sâu) và trọng lượng khoảng 3-4 kg, tùy thuộc vào cấu hình cụ thể. Thiết bị này được thiết kế để hoạt động ổn định trong dải nhiệt độ môi trường từ 0°C đến 40°C và độ ẩm tương đối từ 10% đến 90% (không ngưng tụ), phù hợp với điều kiện phòng máy chủ tiêu chuẩn.

Nguồn điện cung cấp cho FortiWeb-100D là nguồn AC, với dải điện áp đầu vào phổ biến (ví dụ: 100–240V AC, 50–60 Hz). Công suất tiêu thụ của thiết bị thường ở mức vừa phải, phản ánh hiệu quả năng lượng của nó. Một số model trong dòng này có thể được trang bị nguồn đơn (single power supply) hoặc có tùy chọn nguồn dự phòng (redundant power supply) ở các model cao cấp hơn trong cùng series để tăng cường độ tin cậy và tính sẵn sàng của hệ thống.

Việc quản lý thiết bị FortiWeb-100D rất linh hoạt, bao gồm giao diện người dùng đồ họa (GUI) trực quan dựa trên trình duyệt web, cho phép người quản trị dễ dàng cấu hình, giám sát và quản lý các chính sách bảo mật. Bên cạnh đó, giao diện dòng lệnh (CLI) mạnh mẽ cũng có sẵn cho các chuyên gia muốn thực hiện các cấu hình chi tiết, tự động hóa tác vụ hoặc khắc phục sự cố ở mức độ sâu. Thiết bị hỗ trợ đầy đủ các giao thức quản lý mạng tiêu chuẩn như SNMP, cho phép tích hợp vào các hệ thống giám sát mạng (NMS) hiện có của doanh nghiệp, cũng như khả năng gửi log đến máy chủ Syslog hoặc các nền tảng SIEM (Security Information and Event Management) như FortiAnalyzer để phân tích và lưu trữ tập trung.

2.2. Các tính năng của FortiWeb-100D

FortiWeb-100D không chỉ là một thiết bị phần cứng với các thông số kỹ thuật ấn tượng mà còn là một nền tảng bảo mật ứng dụng web toàn diện, được trang bị hàng loạt các tính năng tiên tiến. Các tính năng này được thiết kế để cung cấp một hệ thống phòng thủ đa lớp, từ việc ngăn chặn các mối đe dọa đã biết đến việc phát hiện và ứng phó với các kỹ thuật tấn công mới và tinh vi.

- Bảo vệ Toàn diện Chống lại Mối Đe dọa Ứng dụng Web: Đây là chức năng cốt lõi của FortiWeb-100D, bao gồm một loạt các cơ chế phòng thủ đã được đề cập chi tiết:
 - Phòng thủ dựa trên chữ ký (Signature-based Protection): Sử dụng cơ sở dữ liệu chữ ký từ FortiGuard Labs, được cập nhật liên tục để chống lại các cuộc tấn công đã biết như SQL Injection,

Cross-Site Scripting (XSS), OS Commanding, Path Traversal, và nhiều loại mã độc khác. FortiWeb cho phép tùy chỉnh và tạo các bộ chữ ký riêng để phù hợp với từng ứng dụng cụ thể.

- Học máy (Machine Learning) phát hiện bất thường và tấn công Zero-day: FortiWeb-100D tích hợp công nghệ học máy hai lớp. Lớp đầu tiên tự động học hành vi bình thường của ứng dụng web để phát hiện các bất thường. Lớp thứ hai xác minh các bất thường này bằng cách sử dụng các mô hình mới đe dọa đã được huấn luyện trước, giúp phát hiện các cuộc tấn công mới và giảm thiểu báo động giả.
- Phòng chống tấn công Từ chối Dịch vụ (DoS/DDoS Prevention) ở tầng ứng dụng: Bảo vệ ứng dụng khỏi các cuộc tấn công làm quá tải tài nguyên máy chủ bằng cách giới hạn tốc độ truy cập, phát hiện lũ lụt HTTP, và các cơ chế kiểm soát hành vi khác.
- Chống Bot tinh vi (Advanced Bot Mitigation): Sử dụng nhiều kỹ thuật như phân tích hành vi, chữ ký bot, thử thách thông minh, và nhận dạng sinh trắc học để phân biệt và chặn các bot độc hại gây ra các hoạt động như web scraping, credential stuffing, và tấn công tự động.
- Bảo vệ API (API Protection): Cung cấp các cơ chế bảo vệ chuyên dụng cho API, bao gồm xác thực schema API (ví dụ: OpenAPI), bảo vệ nội dung JSON/XML khỏi các tấn công cụ thể, và áp dụng các chính sách WAF chung cho lưu lượng API.
- Xác thực và Kiểm soát Đầu vào (Input Validation): Cho phép định nghĩa các quy tắc chặt chẽ đối với dữ liệu đầu vào từ người dùng, bao gồm kiểm tra tính hợp lệ của tham số (Parameter Validation Rules) về kiểu dữ liệu, độ dài, định dạng, và bảo vệ việc tải tệp lên (File Security) bằng cách giới hạn loại tệp, kích thước, và tích hợp quét mã độc.
- Bảo mật Cookie (Cookie Security): Cung cấp các tùy chọn mã hóa cookie (Cookie Encryption) để bảo vệ nội dung nhạy cảm và ký cookie (Cookie Signing) để đảm bảo tính toàn vẹn, chống lại việc giả mạo hoặc đánh cắp cookie.
- Bảo mật HTTP Header (HTTP Header Security): Cho phép quản trị viên thực thi các chính sách liên quan đến HTTP header, tự động thêm các header bảo mật quan trọng (HSTS, CSP, X-Frame-Options) và loại bỏ các header có thể tiết lộ thông tin hệ thống.
- Chống CSRF (Cross-Site Request Forgery - CSRF Protection): Triển khai các cơ chế sử dụng CSRF token để ngăn chặn các cuộc tấn công CSRF, đảm bảo các hành động nhạy cảm được thực hiện một cách hợp lệ.
- Kiểm tra tính hợp lệ của Giao thức (Protocol Validation): Đảm bảo rằng tất cả lưu lượng truy cập HTTP/HTTPS tuân thủ các tiêu chuẩn giao thức, chặn các yêu cầu dị dạng hoặc có dấu hiệu khai thác giao thức.

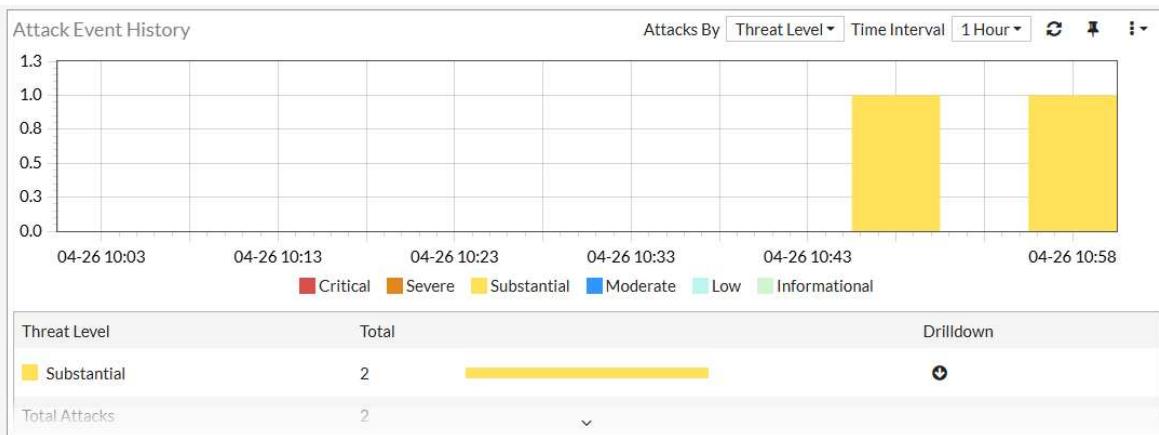
- Quét lỗ hổng ứng dụng web tích hợp (Integrated Web Vulnerability Scanning):

FortiWeb-100D không chỉ phòng thủ bị động mà còn cung cấp khả năng chủ động tìm kiếm điểm yếu. Tính năng quét lỗ hổng tích hợp cho phép quản trị viên lên lịch hoặc thực hiện quét theo yêu cầu để kiểm tra các ứng dụng web, phát hiện các lỗ hổng phổ biến như SQL Injection, XSS, cấu hình sai, và các vấn đề bảo mật khác. Kết quả quét được trình bày dưới dạng báo cáo chi tiết, kèm theo mức độ nghiêm trọng và khuyến nghị khắc phục, giúp các tổ chức và lối trước khi chúng bị khai thác.

- Quản lý, giám sát và báo cáo trực quan:

FortiWeb-100D được thiết kế với giao diện quản lý thân thiện và các công cụ giám sát mạnh mẽ:

- Giao diện người dùng đồ họa (GUI) và giao diện dòng lệnh (CLI): Cung cấp GUI trực quan dựa trên web để dễ dàng cấu hình và quản lý, cùng với CLI cho các tác vụ nâng cao và tự động hóa.



- FortiView: Một công cụ trực quan hóa và phân tích lưu lượng mạnh mẽ, cho phép quản trị viên theo dõi các sự kiện tấn công, nguồn gốc mối đe dọa, các vi phạm chính sách phổ biến, và hành vi người dùng trong thời gian thực hoặc theo lịch sử.

- Ghi log chi tiết và hệ thống báo cáo (Comprehensive Logging and Reporting): Ghi lại đầy đủ các sự kiện hệ thống, lưu lượng truy cập, và các sự kiện tấn công. Các log này có thể được lưu trữ cục bộ, gửi đến máy chủ syslog, hoặc tích hợp với FortiAnalyzer để phân tích sâu và tạo báo cáo tùy chỉnh, hỗ trợ việc điều tra sự cố và tuân thủ quy định.

- Tích hợp Hệ sinh thái Bảo mật Fortinet (Fortinet Security Fabric Integration):

FortiWeb-100D là một phần của kiến trúc Fortinet Security Fabric, cho phép nó tương tác và chia sẻ thông tin tình báo mối đe dọa với các giải pháp bảo mật khác của Fortinet như FortiGate (tường lửa mạng), FortiSandbox (phân tích mã độc nâng cao), FortiAnalyzer (phân tích và báo cáo tập trung), và FortiSIEM. Sự tích hợp này tạo ra một hệ thống phòng thủ đồng bộ và tự động hóa, nâng cao khả năng phát hiện và phản ứng với các cuộc tấn công phức tạp.

- Dịch vụ FortiGuard Security Services:

Thiết bị được hỗ trợ bởi các dịch vụ FortiGuard, bao gồm:

- FortiGuard Antivirus: Cập nhật chữ ký virus để bảo vệ chống lại các phần mềm độc hại trong các tệp tải lên.
- FortiGuard Web Application Security Service: Cung cấp các bản cập nhật chữ ký WAF, quy tắc phát hiện bot, và các thông tin tình báo khác liên quan đến mối đe dọa ứng dụng web.
- FortiGuard IP Reputation & Anti-botnet Service: Cập nhật danh sách các địa chỉ IP độc hại và các botnet đã biết.
- FortiGuard Vulnerability Management Service: Cung cấp thông tin cập nhật cho tính năng quét lỗ hổng.

- Các Chế độ Triển khai Linh hoạt:

FortiWeb-100D hỗ trợ nhiều chế độ triển khai để phù hợp với các yêu cầu và kiến trúc mạng khác nhau:

- Reverse Proxy: Chế độ phổ biến nhất, FortiWeb hoạt động như một proxy ngược, đứng trước các máy chủ web.
- Transparent Inline Mode: FortiWeb được chèn vào luồng lưu lượng mà không yêu cầu thay đổi địa chỉ IP của máy chủ web.
- True Transparent Proxy Mode: Tương tự như transparent inline nhưng với một số khác biệt về xử lý mạng.
- Offline Sniffing Mode: FortiWeb phân tích một bản sao của lưu lượng truy cập mạng để phát hiện tấn công mà không ảnh hưởng trực tiếp đến luồng dữ liệu chính (thường dùng cho mục đích giám sát hoặc kiểm thử).

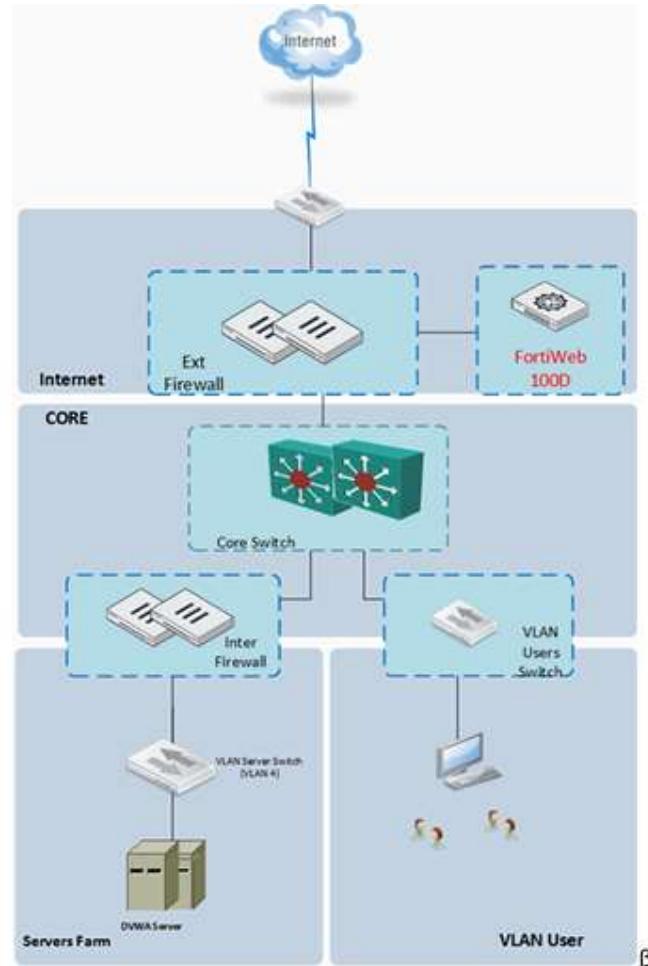
- Hỗ trợ Chứng chỉ Số và Mã hóa SSL/TLS:

FortiWeb-100D có khả năng xử lý lưu lượng SSL/TLS, bao gồm SSL Offloading (giải mã SSL trước khi chuyển đến máy chủ web để giảm tải cho máy chủ) và SSL Inspection (giải mã, kiểm tra, rồi mã hóa lại). Thiết bị hỗ trợ quản lý chứng chỉ số, bao gồm việc tạo CSR, nhập chứng chỉ, và hỗ trợ các giao thức mã hóa mạnh.

Các tính năng này kết hợp lại làm cho FortiWeb-100D trở thành một giải pháp mạnh mẽ, cung cấp khả năng bảo vệ chuyên sâu và toàn diện cho các ứng dụng web chống lại một loạt các mối đe dọa hiện đại.

Chương 3: Triển Khai Cấu Hình Và Thủ Nghiệm

Sau khi đã tìm hiểu tổng quan về WAF, các phương pháp nhận diện tấn công, cũng như thông số kỹ thuật và tính năng của thiết bị FortiWeb-100D, chương này sẽ đi vào mô tả các bước triển khai cấu hình cơ bản và nâng cao trên thiết bị. Mục tiêu là giúp người đọc hình dung được quy trình thiết lập FortiWeb để bảo vệ một ứng dụng web cụ thể, trong trường hợp này là máy chủ DVWA (Damn Vulnerable Web Application) được sử dụng cho mục đích thử nghiệm.



Trước khi đi vào chi tiết các bước cấu hình trên thiết bị FortiWeb-100D, điều quan trọng là phải hiểu rõ mô hình mạng được sử dụng trong môi trường thực hành. Sơ đồ mạng này mô tả cách các thành phần khác nhau được kết nối và vai trò của từng thiết bị trong hệ thống. Mạng được chia thành các vùng chính như Internet, vùng CORE, vùng Servers Farm và vùng VLAN User. Kết nối từ Internet đi qua một tường lửa bên ngoài (Ext Firewall) trước khi vào vùng CORE. Tại đây, Core Switch đóng vai trò trung tâm, kết nối đến một tường lửa nội bộ (Inter Firewall) và một switch cho người dùng (VLAN Users Switch). Tường lửa nội bộ sẽ kiểm soát truy cập vào vùng Servers Farm, nơi chứa máy chủ ứng dụng web DVWA (Damn Vulnerable Web Application). Vùng VLAN User chứa các máy tính của người dùng cuối (PC). Đặc biệt, thiết bị FortiWeb-100D được đặt trong vùng CORE, kết nối với tường lửa bên ngoài và có nhiệm vụ chính là đóng vai trò tường lửa chuyên dụng cho ứng dụng web, bảo vệ máy chủ DVWA khỏi các cuộc tấn công từ bên ngoài. Máy chủ DVWA Server trong vùng Servers Farm là mục tiêu cần được bảo vệ và cũng là nơi để kiểm thử các lỗ hổng bảo mật web. Máy tính PC trong vùng VLAN User sẽ được sử dụng để truy cập vào trang web DVWA (qua FortiWeb) nhằm kiểm tra kết quả cấu hình và thực hiện các cuộc tấn công mô

phỏng. Mô hình này tạo ra một môi trường giả lập tương đối đầy đủ, cho phép triển khai và kiểm nghiệm các tính năng của FortiWeb một cách hiệu quả.

3.1. Cấu hình các đối tượng máy chủ

Bước đầu tiên và cơ bản nhất để FortiWeb có thể bảo vệ một ứng dụng web là phải khai báo cho FortiWeb biết về máy chủ web thực sự (Real Server) mà nó cần bảo vệ và cách thức người dùng sẽ truy cập vào ứng dụng đó thông qua FortiWeb (Virtual Server).

Đầu tiên, chúng ta cần định nghĩa Real Server, đại diện cho máy chủ web vật lý hoặc máy ảo chứa ứng dụng DVWA. Trong FortiWeb, điều này thường được thực hiện bằng cách tạo một "Server Pool". Server Pool cho phép nhóm một hoặc nhiều Real Server lại với nhau, hữu ích cho việc cân bằng tải (load balancing) nếu có nhiều máy chủ backend. Tuy nhiên, trong trường hợp đơn giản với một máy chủ DVWA duy nhất như trong bài lab, chúng ta sẽ cấu hình một Server Pool với một thành viên duy nhất là địa chỉ IP (ví dụ: 172.16.1.241) và cổng dịch vụ (ví dụ: port 80) của máy chủ DVWA.

Tiếp theo, để người dùng có thể truy cập ứng dụng web thông qua FortiWeb, chúng ta cần tạo một Virtual Server. Virtual Server là một địa chỉ IP và cổng trên FortiWeb mà người dùng sẽ kết nối đến. FortiWeb sẽ lắng nghe trên Virtual Server này, xử lý các yêu cầu và sau đó chuyển tiếp chúng đến Real Server đã được định nghĩa trong Server Pool. Trong bài lab, một Virtual Server (DVWA-VIP) được tạo, sử dụng một địa chỉ IP trên một trong các cổng của FortiWeb (IP của port2 là 10.1.1.252).

Edit Virtual Server

Name	DVWA-VIP		
<button>OK</button> <button>Cancel</button>			
<button>+ Create New</button> <button>Edit</button> <button>Delete</button>			
ID	Use Interface IP	Interface/Virtual IP	Status
1	Enable	port2(10.1.1.252/24,::/0)	Enable

Kiểu hoạt động được chọn là "Reverse Proxy", có nghĩa là FortiWeb sẽ hoạt động như một proxy ngược, tiếp nhận yêu cầu từ người dùng và chuyển tiếp đến máy chủ DVWA.

New Server Pool

Name	Nhom1_DVWA					
Protocol	HTTP					
Type	Reverse Proxy					
Single Server/Server Balance	<input checked="" type="radio"/> Single Server <input type="radio"/> Server Balance					
Comments	0/199 (bytes)					
<button>OK</button> <button>Cancel</button>						
<button>+ Create New</button> <button>Edit</button> <button>Delete</button>						
ID	IP/Domain	Status	Port	HTTP/2	SSL	Connection Limit
No results						

New Server Pool Rule

ID	auto
Status	<input checked="" type="button"/> Enable <input type="button"/> Disable <input type="button"/> Maintenance
Server Type	<input checked="" type="radio"/> IP <input type="radio"/> Domain
IP	172.16.4.241
Port	80
Connection Limit <small>i</small>	0 (Concurrent Connections)(0 - 1048576)
Proxy Protocol	<input type="checkbox"/>
HTTP/2	<input type="checkbox"/>
SSL <small>i</small>	<input type="checkbox"/>
Show advanced settings	
<input type="button"/> OK <input type="button"/> Cancel	

Edit Server Pool

Name	Nhom1_DVWA														
Protocol	HTTP														
Type	<input checked="" type="radio"/> Reverse Proxy <input type="radio"/> Single Server <input type="radio"/> Server Balance														
Comments	0/199 [bytes]														
<input type="button"/> OK <input type="button"/> Cancel															
<input type="button"/> + Create New <input type="button"/> Edit <input type="button"/> Delete															
<table border="1"> <thead> <tr> <th>ID</th> <th>IP/Domain</th> <th>Status</th> <th>Port</th> <th>HTTP/2</th> <th>SSL</th> <th>Connection Limit</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>172.16.4.241</td> <td>Enable</td> <td>80</td> <td>Disable</td> <td>Disable</td> <td>0</td> </tr> </tbody> </table>		ID	IP/Domain	Status	Port	HTTP/2	SSL	Connection Limit	1	172.16.4.241	Enable	80	Disable	Disable	0
ID	IP/Domain	Status	Port	HTTP/2	SSL	Connection Limit									
1	172.16.4.241	Enable	80	Disable	Disable	0									

Một cấu hình quan trọng khi FortiWeb hoạt động ở chế độ Reverse Proxy là X-Forwarded-For (XFF). Do FortiWeb thực hiện Full NAT, máy chủ web backend sẽ chỉ thấy địa chỉ IP của FortiWeb thay vì IP gốc của client. Để máy chủ backend có thể ghi nhận được IP thật của người dùng (ví dụ, cho mục đích ghi log hoặc phân tích), XFF header cần được cấu hình. FortiWeb sẽ chèn địa chỉ IP gốc của client vào XFF header trước khi chuyển tiếp yêu cầu đến Real Server. Việc này đòi hỏi tạo một X-Forwarded-For Profile và quy tắc tương ứng.

New X-Forwarded-For Rule

Name	<input type="text" value="XFF-Rule"/>
Add X-Forwarded-For	<input checked="" type="checkbox"/>
Add Source Port <small>i</small>	<input checked="" type="checkbox"/>
Add X-Forwarded-Port <small>i</small>	<input checked="" type="checkbox"/>
Add X-Real-IP <small>i</small>	<input checked="" type="checkbox"/>
Add X-Forwarded-Proto <small>i</small>	<input checked="" type="checkbox"/>
Use X-Header to Identify Original Client's IP	<input checked="" type="checkbox"/> <input type="text" value="X-FORWARDED-FOR"/>
IP Location in X-Header	<input type="radio" value="Left"/> Left <input type="radio" value="Right"/> Right
Block Using Original Client's IP <small>i</small>	<input checked="" type="checkbox"/>

OK **Cancel**

Create New **Edit** **Delete**

ID	Trusted X-Header Sources
No results	

Edit X-Forwarded-For Rule

Name	<input type="text" value="XFF-Rule"/>
Add X-Forwarded-For	<input checked="" type="checkbox"/>
Add Source Port <small>i</small>	<input checked="" type="checkbox"/>
Add X-Forwarded-Port <small>i</small>	<input checked="" type="checkbox"/>
Add X-Real-IP <small>i</small>	<input checked="" type="checkbox"/>
Add X-Forwarded-Proto <small>i</small>	<input checked="" type="checkbox"/>
Use X-Header to Identify Original Client's IP	<input checked="" type="checkbox"/> <input type="text" value="X-FORWARDED-FOR"/>
IP Location in X-Header	<input type="radio" value="Left"/> Left <input type="radio" value="Right"/> Right
Block Using Original Client's IP <small>i</small>	<input checked="" type="checkbox"/>

OK **Cancel**

Create New **Edit** **Delete**

ID	Trusted X-Header Sources
1	10.1.1.252
2	172.16.4.241

Sau khi hoàn tất các cấu hình cơ bản này, một Server Policy sẽ được tạo để liên kết Virtual Server, Server Pool, dịch vụ HTTP/HTTPS, và các Protected Hostnames lại với nhau. Đây là chính sách trung tâm điều khiển luồng truy cập và là nơi áp dụng các profile bảo mật khác nhau.

New Policy

Name: Nhóm1_Policy

Network Configuration

Deployment Mode	Single Server/Server Balance
Virtual Server	DVWA-VIP
Server Pool	Nhom1_DVWA
Protected Hostnames	DVWA
Client Real IP	Off
HTTP Service	HTTP
HTTPS Service	
Redirect HTTP to HTTPS	Off

Application Delivery

Proxy Protocol	Off
Retry On	Off

Security Configuration

Monitor Mode	Off
--------------	-----

OK **Cancel**

3.2. DoS Protection

Bảo vệ ứng dụng web khỏi các cuộc tấn công từ chối dịch vụ (DoS) và Từ chối dịch vụ phân tán (DDoS) ở tầng ứng dụng là một trong những nhiệm vụ quan trọng của FortiWeb. Quá trình cấu hình bao gồm việc định nghĩa các ngưỡng giới hạn truy cập và các biện pháp phát hiện lũ lụt HTTP, sau đó áp dụng chúng vào chính sách bảo vệ.

Đầu tiên, một profile giới hạn truy cập HTTP, được tạo trong mục DoS Protection > Application > HTTP Access Limit. Profile này đặt ra giới hạn về số lượng yêu cầu HTTP mỗi giây mà một địa chỉ IP đơn lẻ (Standalone IP) hoặc một địa chỉ IP được chia sẻ (Shared IP) có thể gửi đến máy chủ. Ví dụ, giới hạn có thể là 200 hoặc 300 yêu cầu/giây. Khi ngưỡng này bị vượt qua, FortiWeb sẽ thực hiện hành động đã định, chẳng hạn như "Block Period" (chặn trong một khoảng thời gian nhất định, ví dụ 600 giây) hoặc "Alert & Deny".

New HTTP Access Limit

Name: Nhóm1_DOS

HTTP Request Limit/sec (Standalone IP)	300	(0~65536)
HTTP Request Limit/sec (Shared IP)	300	(0~65536)
Bot Confirmation	Off	
Action	Alert & Deny	
Block Period	600	Seconds (1 - 10000)
Severity	High	
Trigger Policy		

OK **Cancel**

Tiếp theo, một profile chống lũ lụt HTTP (trong mục HTTP Flood Prevention), được cấu hình tại DoS Protection > Application > HTTP Flood Prevention. Profile này cũng đặt ra giới hạn số lượng yêu cầu HTTP mỗi giây và có thể kích hoạt các biện pháp xác thực bổ sung như "Bot Confirmation" (ví dụ, sử dụng CAPTCHA Enforcement) nếu phát hiện lưu lượng truy cập tăng đột biến nghi ngờ là tấn công flood. Hành động khi phát hiện cũng tương tự như chặn hoặc cảnh báo và từ chối.

Name	Nhom1_HTTP_Flood_Protect
HTTP Request Limit/sec i	200 (0 - 4096)
Bot Confirmation	<input checked="" type="checkbox"/>
Verification Method	CAPTCHA Enforcement
Max Attempt Times	3 (1 - 5)
Validation Timeout i	20 Seconds (5 - 30)
Action	Alert & Deny
Block Period	600 Seconds (1 - 10000)
Severity	High
Trigger Policy	

OK Cancel

Sau khi tạo các profile riêng lẻ này, chúng được tập hợp lại trong một DoS Protection Policy (ví dụ, "Nhom1_DOS_Policy" hoặc "Test-DOS" Policy). Chính sách này cho phép chọn các profile HTTP Access Limit và HTTP Flood Prevention đã tạo, cùng với các tùy chọn khác như HTTP Session Based Prevention hoặc TCP Flood Prevention.

New DoS Protection Policy

Name	Nhom1_DOS_Policy
HTTP Session Based Prevention	<input checked="" type="checkbox"/>
HTTP Flood Prevention	Nhom1_HTTP_Flood_Protect i
Malicious IPs	
HTTP DoS Prevention	<input checked="" type="checkbox"/>
HTTP Access Limit	Nhom1_DOS i
TCP Flood Prevention	
Layer3 Fragment Protection	<input type="checkbox"/>

OK Cancel

Cuối cùng, DoS Protection Policy này cần được áp dụng vào thực tế. Điều này được thực hiện bằng cách chỉnh sửa Web Protection Profile (tạo một profile mới "Nhom1_DOS_Profile") và chọn DoS Protection Policy vừa tạo trong mục DoS Protection của profile đó. Web Protection Profile này sau đó được gán vào Server Policy đã được thiết lập ở 3.1.

DoS Protection

DoS Protection Policy: Nhom1_DOS_Policy

Application Delivery

URL Rewriting
 HTTP Authentication
 Site Publish
 File Compress

IP Protection

IP Reputation

Name	Status	Action	Severity	Trigger Policy
FortiGate Quarantined IPs	<input type="button" value="Edit"/>	Alert <input type="button" value="Edit"/>	High <input type="button" value="Edit"/>	<input type="button" value="Edit"/>

IP List

Edit Policy

HTTP Service
 HTTPS Service
 Redirect HTTP to HTTPS

Application Delivery

Proxy Protocol
 Retry On

Security Configuration

Monitor Mode
 Syn Cookie
 Web Protection Profile: Nhom1_DOS_Profile
 Replacement Message: Predefined
 URL Case Sensitivity

Machine Learning

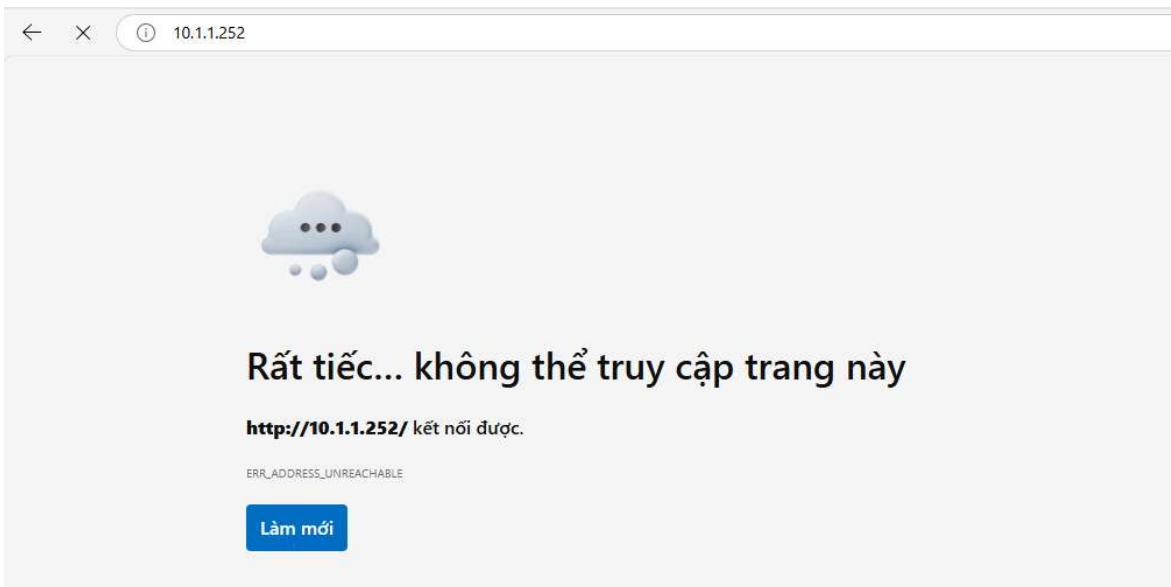
Comments 0/999 (bytes)

Sau khi cấu hình hoàn tất, việc kiểm tra được tiến hành bằng cách sử dụng các công cụ tạo tải như ApacheBench (ab) để mô phỏng một cuộc tấn công DoS bằng cách gửi một lượng lớn yêu cầu đồng thời đến Virtual Server. Nếu cấu hình đúng, FortiWeb sẽ phát hiện và chặn các yêu cầu vượt ngưỡng, và kết quả là công cụ tấn công sẽ báo lỗi kết nối hoặc chỉ hoàn thành một số lượng rất nhỏ yêu cầu, đồng thời trình duyệt truy cập vào trang web cũng có thể không kết nối được trong thời gian bị chặn.

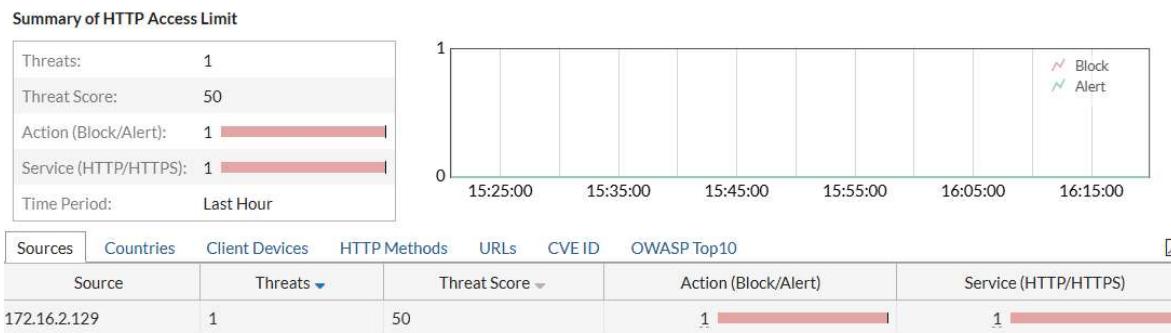
```
nhoclahola@DESKTOP-LSRCB6H d:\Program Files\XAMPP
# ab -c 1000 -n 10000 http://10.1.1.252:80/
This is ApacheBench, Version 2.3 <$Revision: 1903618 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 10.1.1.252 (be patient)
apr_socket_recv: An existing connection was forcibly closed by the remote host. (730054)

nhoclahola@DESKTOP-LSRCB6H d:\Program Files\XAMPP
```



Kiểm tra trên server, nhật ký tấn công trên FortiWeb cũng sẽ ghi lại các sự kiện này.



3.3. Known Attacks

Bên cạnh việc phòng chống các cuộc tấn công làm suy giảm tính sẵn sàng của dịch vụ như DoS/DDoS, một trong những nhiệm vụ trọng yếu của FortiWeb là bảo vệ ứng dụng web khỏi các cuộc tấn công khai thác lỗ hổng bảo mật phổ biến, thường được gọi là "Known Attacks". Đây là những kỹ thuật tấn công đã được biết đến rộng rãi, có các mẫu đặc trưng và thường nhắm vào các điểm yếu trong cách ứng dụng xử lý dữ liệu đầu vào từ người dùng hoặc tương tác với cơ sở dữ liệu. Hai trong số những loại tấn công đã biết nguy hiểm và phổ biến nhất là Cross-Site Scripting (XSS) và SQL Injection (SQLi). FortiWeb sử dụng cơ chế nhận diện dựa trên chữ ký (Signature-based Detection) để phát hiện và ngăn chặn các loại tấn công này.

3.3.1. Cross Site Scripting

Cross-Site Scripting (XSS) là một loại lỗ hổng bảo mật web cho phép kẻ tấn công chèn các đoạn mã độc (thường là JavaScript) vào các trang web mà người dùng khác sẽ xem. Khi người dùng truy cập vào trang web bị ảnh hưởng, mã độc này sẽ được thực thi trên trình duyệt của họ. Hậu quả của XSS có thể rất đa dạng, từ việc đánh cắp cookie phiên của người dùng (session hijacking), thay đổi nội dung trang web, chuyển hướng người dùng đến các trang lừa đảo, đến việc cài cắm keylogger hoặc thực hiện các hành động trái phép dưới danh nghĩa của người dùng bị tấn công. Có ba loại XSS chính: Reflected XSS (XSS phản chiếu), Stored XSS (XSS lưu trữ), và DOM-based XSS.

Để bảo vệ ứng dụng web DVWA khỏi các cuộc tấn công XSS, FortiWeb được cấu hình để sử dụng các chữ ký tấn công XSS. Quá trình này tương tự như việc cấu hình cho các loại tấn công đã biết khác, tập trung vào việc tạo hoặc tùy chỉnh một Signature Policy và áp dụng nó vào Web Protection Profile.

Đầu tiên, một Custom Signature Policy được tạo. Trong policy này, các nhóm chữ ký liên quan đến Cross Site Scripting (bao gồm cả các biến thể như XSS (Extended)) sẽ được kích hoạt, trong khi các nhóm chữ ký khác có thể được tắt nếu mục tiêu chỉ là tập trung chống XSS cho profile này. Hành động khi phát hiện tấn công thường được đặt là "Alert & Deny" hoặc tương đương, và mức độ nghiêm trọng (Severity) được thiết lập phù hợp.

	Name	Status	False Positive Mitigation	Action	Block Period	Severity	Trigger Policy
Cross Site Scripting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert & Deny	600	High	<input type="button"/>
Cross Site Scripting (Extended)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert & Deny	600	Medium	<input type="button"/>
SQL Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert & Deny	600	High	<input type="button"/>
SQL Injection (Extended)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	Medium	<input type="button"/>
Generic Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert & Deny	600	High	<input type="button"/>
Generic Attacks(Extended)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	Medium	<input type="button"/>
Known Exploits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert & Deny	600	High	<input type="button"/>
Trojans	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	Medium	<input type="button"/>
Information Disclosure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	Low	<input type="button"/>
Personally Identifiable Information	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	High	<input type="button"/>

OK **Cancel**

Sau khi Signature Policy "XSS" được định nghĩa, nó cần được áp dụng vào một Web Protection Profile. Tại mục "Known Attacks - Signatures", Signature Policy "XSS" vừa tạo sẽ được chọn.

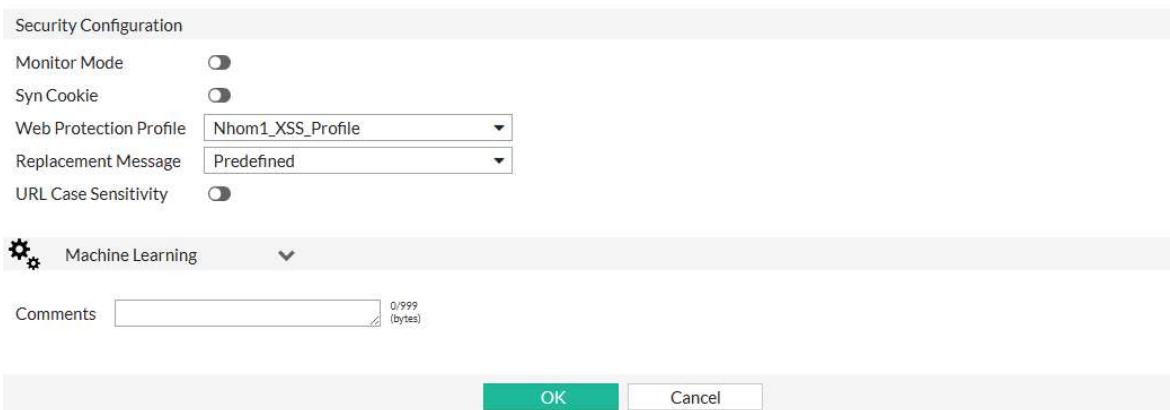
Web Protection Profile này (đã chứa chính sách chống XSS) phải được đảm bảo đã liên kết với Server Policy đang bảo vệ cho Virtual Server của DVWA.

New Policy

Name

Network Configuration

Deployment Mode	<input type="button" value="Single Server/Server Balance"/>
Virtual Server	<input type="button" value="DVWA-VIP"/>
Server Pool	<input type="button" value="Nhom1_DVWA"/>
Protected Hostnames	<input type="button" value="DVWA"/>
Client Real IP <small>?</small>	<input checked="" type="checkbox"/>
HTTP Service	<input type="button" value="HTTP"/>
HTTPS Service	<input type="button"/>
Redirect HTTP to HTTPS	<input checked="" type="checkbox"/>

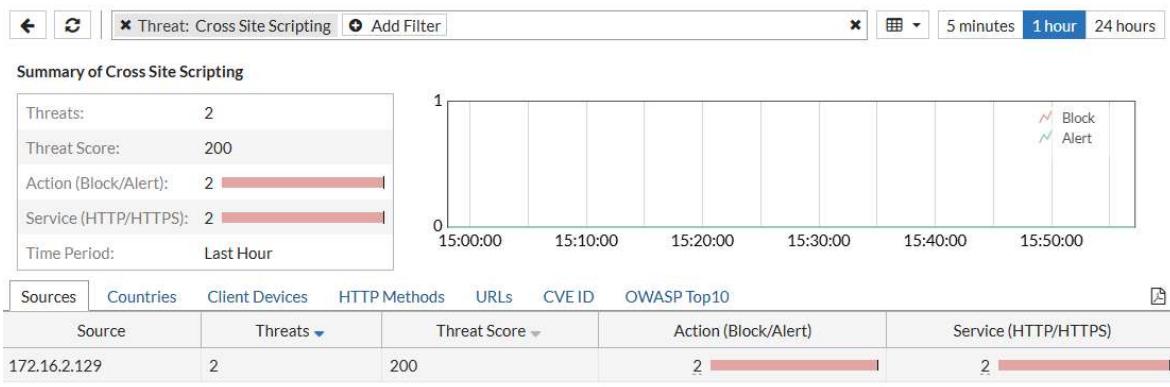


Để kiểm tra, các payload XSS được thử nghiệm trên ứng dụng DVWA. Ví dụ, đối với Reflected XSS, một đoạn mã như <script>alert(1)</script> được chèn vào một trường nhập liệu.

Các yêu cầu chứa những payload này sẽ bị chặn, và người dùng sẽ thấy trang thông báo "Web Page Blocked!".



Nhật ký tấn công (Attack Log) trên FortiWeb cũng sẽ ghi lại chi tiết về các sự kiện tấn công XSS bị ngăn chặn này.



3.3.2. SQL Injection

SQL Injection là một trong những kỹ thuật tấn công web nguy hiểm và phổ biến nhất. Lỗ hổng này xảy ra khi kẻ tấn công có thể chèn hoặc "tiêm" các câu lệnh SQL độc hại vào các truy vấn SQL mà ứng dụng web gửi đến cơ sở dữ liệu. Bằng cách này, kẻ tấn công có thể vượt qua cơ chế xác thực, đọc, sửa đổi, hoặc xóa dữ liệu nhạy cảm trong cơ sở dữ liệu, thậm chí là chiếm quyền kiểm soát hoàn toàn máy chủ cơ sở dữ liệu và trong một số trường hợp là cả máy chủ web. Lỗ hổng SQLi

thường xuất phát từ việc ứng dụng không kiểm tra hoặc làm sạch (sanitize) đúng cách dữ liệu đầu vào từ người dùng trước khi sử dụng chúng để xây dựng các câu lệnh SQL.

Tương tự như XSS, việc bảo vệ chống SQL Injection trên FortiWeb chủ yếu dựa vào việc cấu hình các chữ ký tấn công SQLi. Đầu tiên, một Custom Signature Policy được tạo hoặc chỉnh sửa. Trong chính sách này, các nhóm chữ ký liên quan đến SQL Injection (ví dụ: "SQL Injection", "SQL Injection (Extended)") và có thể cả "Generic Attacks" (vì một số kỹ thuật SQLi có thể được phát hiện bởi các chữ ký tấn công chung) sẽ được kích hoạt. Các tùy chọn như hành động (Action), thời gian chặn (Block Period), và mức độ nghiêm trọng (Severity) được thiết lập theo yêu cầu.

Name	Nhom1_SQLi						
Custom Signature Group	<input type="button" value=""/>						
Comments	0/199 (bytes)						
	Name	Status	False Positive Mitigation	Action	Block Period	Severity	Trigger Policy
	Cross Site Scripting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert & Deny	600	High	<input type="button" value=""/>
	Cross Site Scripting (Extended)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	Medium	<input type="button" value=""/>
	SQL Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block Period	600	High	<input type="button" value=""/>
	SQL Injection (Extended)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block Period	600	Medium	<input type="button" value=""/>
	Generic Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block Period	600	High	<input type="button" value=""/>
	Generic Attacks(Extended)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block Period	600	Medium	<input type="button" value=""/>
	Known Exploits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert & Deny	600	High	<input type="button" value=""/>
	Trojans	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	Medium	<input type="button" value=""/>
	Information Disclosure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	Low	<input type="button" value=""/>
<input checked="" type="checkbox"/>	Personally Identifiable Information	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alert	600	High	<input type="button" value=""/>

Signature Policy "SQL-Injection" này sau đó được chọn và áp dụng vào Web Protection Profile tại mục "Standard Protection - Signatures"

Inline Protection Profile	<input type="button" value=""/>
New Inline Protection Profile	
Name	Nhom1_SQLi_Profile
Standard Protection	
Client Management	<input checked="" type="checkbox"/>
Signatures	Nhom1_SQLi
HTTP Protocol Constraints	<input type="button" value=""/>
X-Forwarded-For	XFF-Rule
Cookie	
Cookie Security Policy	<input type="button" value=""/>
Advanced Protection	
Custom Policy	<input type="button" value=""/>
CSRF Protection	<input type="button" value=""/>
HTTP Header Security	<input type="button" value=""/>
Man in the Browser Protection	<input type="button" value=""/>
URL Encryption Policy	<input type="button" value=""/>

Web Protection Profile này, nay đã được trang bị khả năng chống SQLi, cần được liên kết với Server Policy.

New Policy

Name: Nhóm1_SQLi_Profile

Network Configuration

Deployment Mode	Single Server/Server Balance
Virtual Server	Test
Server Pool	Nhom1_DVWA
Protected Hostnames	DVWA
Client Real IP	Off
HTTP Service	HTTP
HTTPS Service	
Redirect HTTP to HTTPS	Off

Application Delivery

Proxy Protocol	Off
Retry On	Off

Security Configuration

Monitor Mode	Off
Syn Cookie	Off
Web Protection Profile	Nhom1_SQLi_Profile
Replacement Message	Predefined
URL Case Sensitivity	Off

Machine Learning

Comments: 0/999 bytes

OK Cancel

Việc kiểm tra được thực hiện bằng cách thử các payload SQL Injection khác nhau trên ứng dụng DVWA. Ví dụ, một payload phổ biến như ' or '1'='1' # hoặc ' UNION SELECT @@version, database() # được nhập vào các trường đầu vào của ứng dụng. Trước khi FortiWeb bảo vệ, payload này có thể thực thi thành công và trả về thông tin từ cơ sở dữ liệu.

Request

Pretty Raw Hex

```

1 POST /vulnerabilities/sqli/ HTTP/1.1
2 Host: 10.1.1.252
3 Content-Length: 32
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.1.1.252
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
   Safari/537.36
9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://10.1.1.252/vulnerabilities/sqli/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=Shvqbq7qikvc6a4mk5buqaiqcb; cookiesessionid=678A3E13JKMNOPQRSUWWXYZBCDEFAD9F; security=medium
14 Connection: keep-alive
15
16 id=1+OR+1#3d1+-+&Submit=Submit

```

Response

Pretty Raw Hex Render

Vulnerability: SQL Inje

User ID: 1 Submit

ID: 1 OR 1=1 -- -
First name: admin
Surname: admin

ID: 1 OR 1=1 -- -
First name: Gordon
Surname: Brown

ID: 1 OR 1=1 -- -
First name: Hack
Surname: Me

Tuy nhiên, sau khi FortiWeb được cấu hình đúng, các yêu cầu chứa payload SQLi này sẽ bị chặn, và người dùng sẽ nhận được trang thông báo "Web Page Blocked!".

Request

Pretty Raw Hex

```

1 POST /vulnerabilities/sqli/ HTTP/1.1
2 Host: 10.1.1.252
3 Content-Length: 32
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.1.1.252
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
   Safari/537.36
9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://10.1.1.252/vulnerabilities/sqli/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=Shvqbq7qikvc6a4mk5buqaiqcb; cookiesessionid=678A3E13JKMNOPQRSUWWXYZBCDEFAD9F; security=medium
14 Connection: keep-alive
15
16 id=1+OR+1#3d1+-+&Submit=Submit

```

Response

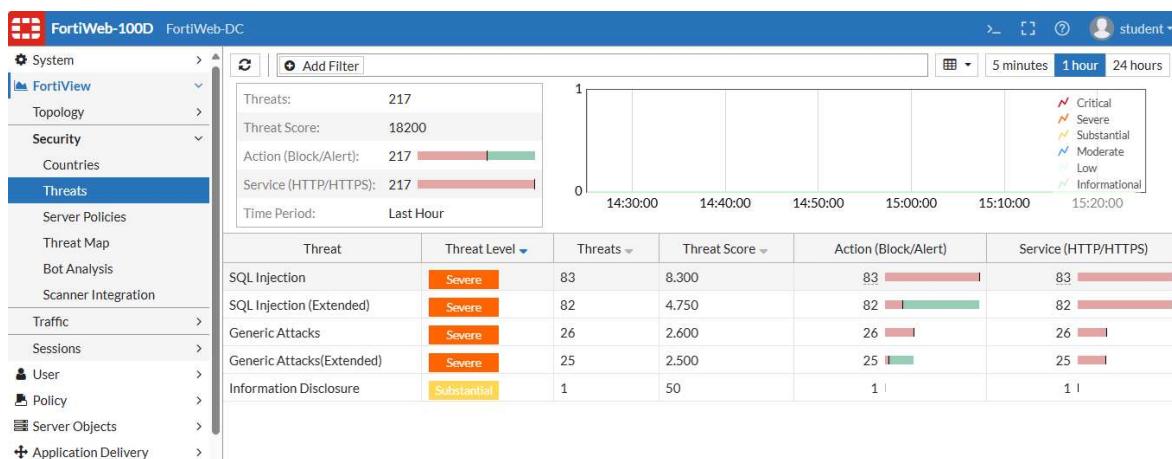
Pretty Raw Hex Render

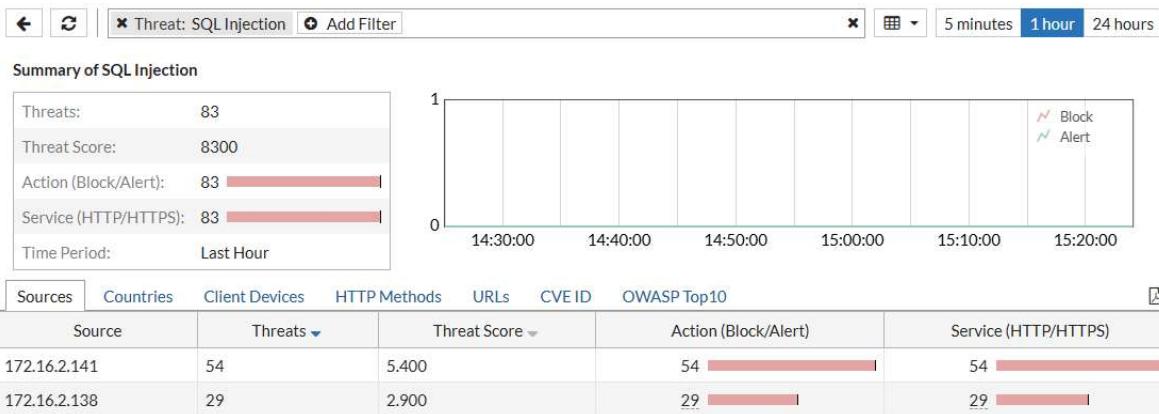
Web Page Blocked!

The page cannot be displayed. Please contact the administrator for additional information.

URL: 10.1.1.252/vulnerabilities/sqli/
Client IP: 172.16.2.129
Attack ID: 20000008
Message ID: 000003054823

Log tấn công trên FortiWeb sẽ ghi lại chi tiết về sự kiện, bao gồm chữ ký đã phát hiện ra cuộc tấn công.





3.4. Advanced Protection

Ngoài việc bảo vệ chống lại các cuộc tấn công DoS và các tấn công đã biết dựa trên chữ ký, FortiWeb còn cung cấp một loạt các tính năng bảo vệ nâng cao. Các tính năng này tập trung vào việc bảo vệ các khía cạnh cụ thể của ứng dụng web, từ việc đảm bảo tính toàn vẹn của các yêu cầu phía client, bảo mật các HTTP header, đến việc kiểm soát chặt chẽ cookie và dữ liệu đầu vào. Các cấu hình này thường được tạo dưới dạng các profile chuyên biệt và sau đó được tích hợp vào Web Protection Profile chung đang áp dụng cho Server Policy.

3.4.1. Client Side Request Forgery

Cross-Site Request Forgery (CSRF), còn được biết đến với các tên gọi khác như XSRF hay "Session Riding", là một loại tấn công mà kẻ xấu lừa người dùng đã đăng nhập và đang có phiên làm việc hợp lệ trên một ứng dụng web thực hiện một hành động không mong muốn. Kẻ tấn công tạo ra một yêu cầu độc hại (ví dụ, thông qua một đường link, một hình ảnh, hoặc một đoạn script trên một trang web khác mà người dùng truy cập) và khi người dùng tương tác với nó (thường là vô tình), trình duyệt của họ sẽ tự động gửi yêu cầu đó đến ứng dụng web đích, kèm theo cookie xác thực của người dùng. Nếu ứng dụng không có cơ chế phòng chống CSRF, nó sẽ thực thi yêu cầu này như thể chính người dùng đã chủ động thực hiện, dẫn đến các hậu quả như thay đổi thông tin tài khoản, thực hiện giao dịch trái phép, hoặc các hành động có hại khác.

FortiWeb cung cấp cơ chế bảo vệ chống CSRF hiệu quả bằng cách sử dụng kỹ thuật "CSRF token". Ý tưởng cơ bản là FortiWeb sẽ chèn một token ngẫu nhiên, duy nhất và khó đoán vào mỗi biểu mẫu web (form) hoặc các yêu cầu nhạy cảm mà ứng dụng gửi đến trình duyệt của người dùng. Khi người dùng gửi lại biểu mẫu hoặc thực hiện yêu cầu, FortiWeb sẽ kiểm tra sự hiện diện và tính hợp lệ của token này. Nếu token bị thiếu, không khớp, hoặc không hợp lệ, FortiWeb sẽ coi đó là một yêu cầu đáng ngờ và chặn lại.

Đầu tiên là tạo Rule:

Edit CSRF Protection Rule

Name	Nhom1_CSRF	
Action	Alert & Deny	
Block Period	600	Seconds (1 - 3600)
Severity	High	
Trigger Policy		

OK

Cancel

Page List Table

New CSRF URL Rule

ID	auto
Host Status	<input checked="" type="checkbox"/>
Host	<input type="text"/>
Request Type	Simple String <input checked="" type="radio"/> Regular Expression <input type="radio"/>
Full URL	<input type="text"/> /vulnerabilities/csrf/
Parameter Filter	<input checked="" type="checkbox"/>
Parameter Name	<input type="text"/> Change
Parameter Value Type	Simple String <input checked="" type="radio"/> Regular Expression <input type="radio"/>
Parameter Value	<input type="text"/> Change

OK

Cancel

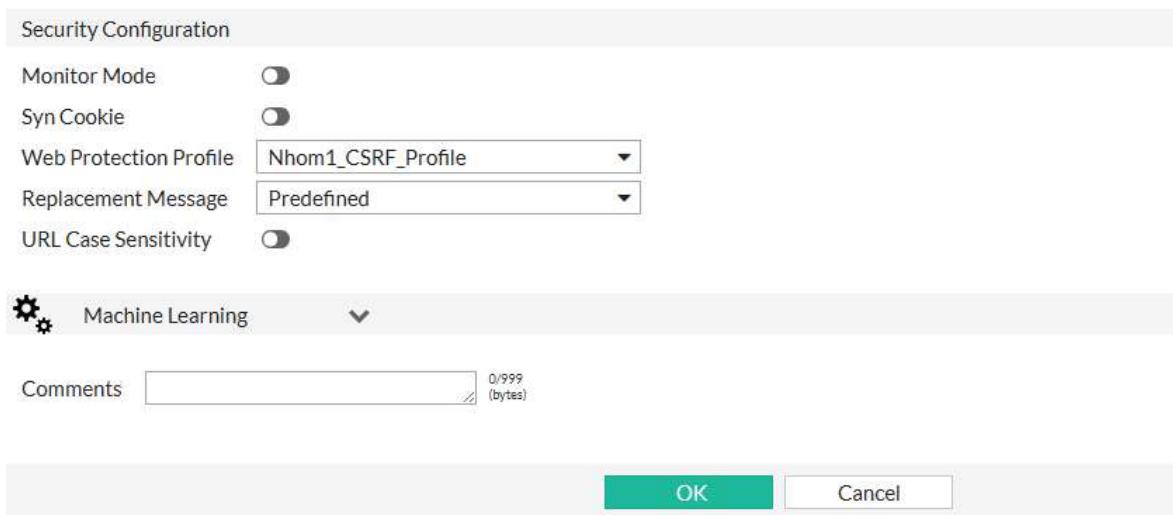
Page List Table

Page List Table					
+ Create New		Edit	Delete		
ID	Host Status	Host	Request Type	Full URL	Parameter Filter
1	Disable		Regular Expression	/vulnerabilities/csrf/	Disable

URL List Table

URL List Table					
+ Create New		Edit	Delete		
ID	Host Status	Host	Request Type	Full URL	Parameter Filter
1	Disable		Regular Expression	/vulnerabilities/csrf/	Enable

Một profile CSRF Protection được tạo trong mục Web Protection > Advanced Protection > CSRF Protection. Profile này sau đó được thêm vào Web Protection Profile đang được áp dụng cho Server Policy.



Khi tính năng này được kích hoạt, FortiWeb sẽ tự động phân tích mã HTML của các trang web được bảo vệ và chèn một trường ẩn (hidden field) chứa CSRF token vào các biểu mẫu. Khi người dùng submit biểu mẫu, token này sẽ được gửi kèm.

Trang CSRF của DVWA:

Bây giờ khi vào trang web, mã nguồn sẽ có thêm phần csrf token:

```
<script>
var csrftoken="678A3E0DWXYZBCDEFGHJKLMNOPRSAD6D";
function trim(str){return str.replace(/(\^\s+)|(\s+$)/g, "")}
function updateForms(csrftoken) {var forms = document.getElementsByName('form');for(i=0; i<forms.length; i++) {var e = forms[i];
function isSkip(e){return 0==e.length?1:0==e.toLowerCase().indexOf("http://")||0==e.toLowerCase().indexOf("https://")||0==e.getAttribute("action");}
function updateTag(element, attr, token) {var location = element.getAttribute(attr);if(location != null && location != ""){element.setAttribute(attr, location+token);
function updateTags(csrftoken) {var all = document.getElementsByTagName('a');var len = all.length;for(var i=0; i<len; i++)
updateForms(csrftoken);
updateTags(csrftoken);
</script>
</html>
```

Khi request thì sẽ có thêm phần đó:

Request to http://10.1.1.252:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 GET /vulnerabilities/csrf/?password_current=123&password_new=234&password_conf=234&Change=Change&user_token=
2 72818dafafac8577b54cc26ae842c35b&tknfv=678A3E0F45789890134ABCDEFHIJB039 HTTP/1.1
3 Host: 10.1.1.252
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://10.1.1.252/vulnerabilities/csrf/
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
10 Cookie: security=impossible; PHPSESSID=594hebglmlqpllo2e6r7hq88p; cookiesession1=678A3E0F45789890134ABCDEFHIJB039;
security_low
11 Connection: keep-alive

```

Một yêu cầu hợp lệ sẽ đi kèm với token này và được xử lý bình thường.

Response

Pretty Raw Hex Render

```

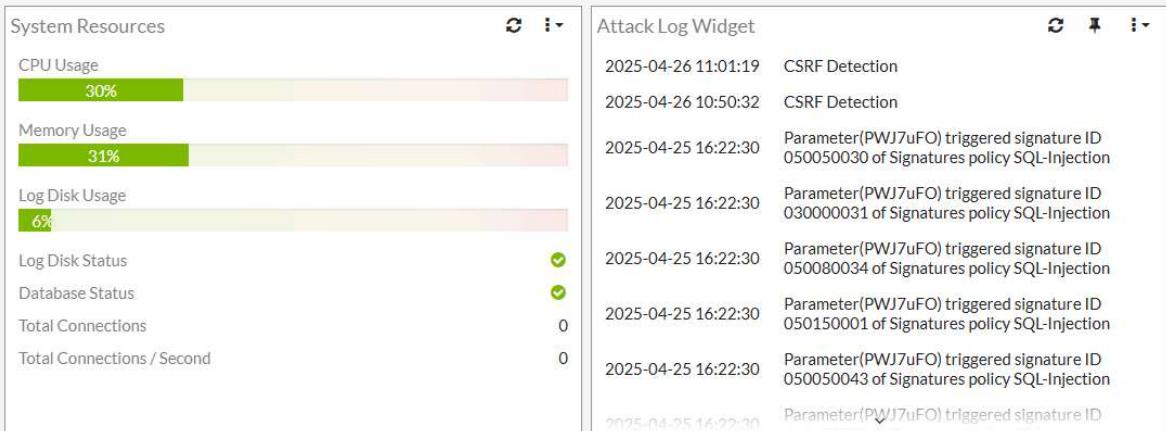
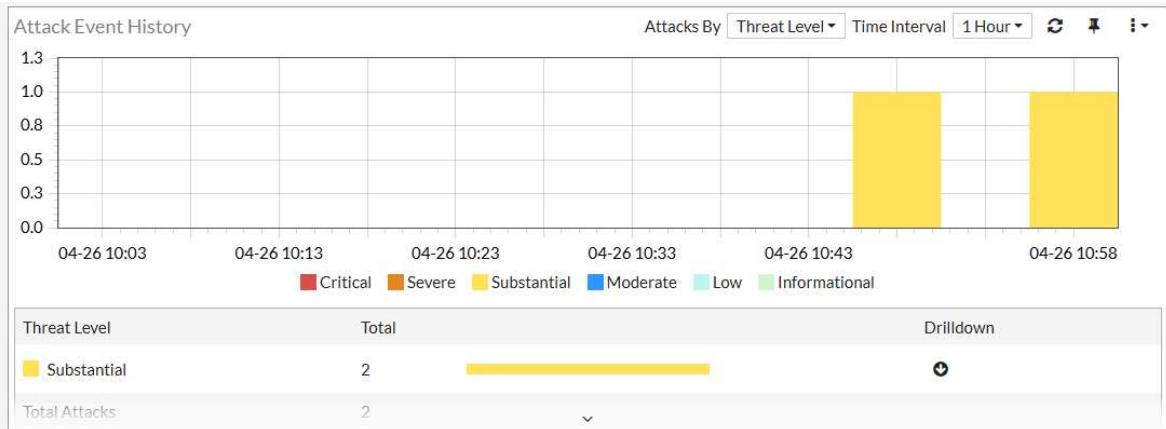
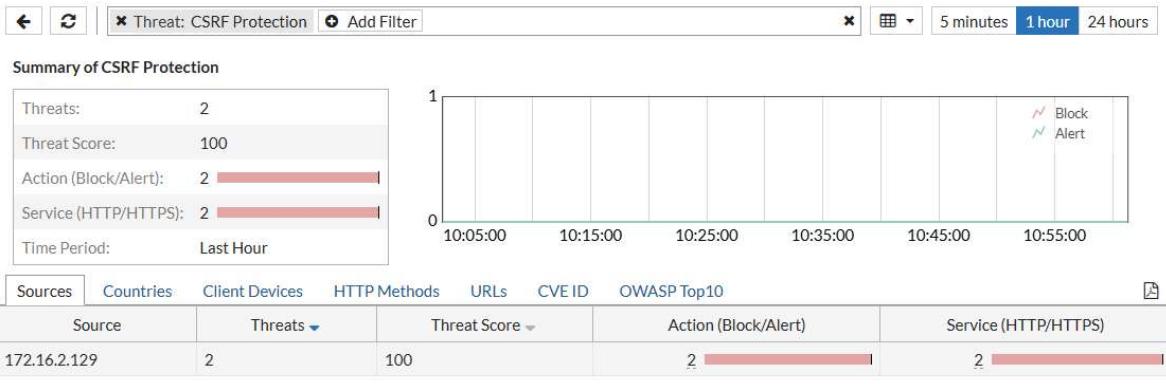
1 HTTP/1.1 200 OK
2 Date: Sat, 26 Apr 2025 03:58:40 GMT
3 Server: Apache/2.4.37 (centos)
4 X-Powered-By: PHP/7.3.24
5 Pragma: no-cache
6 Cache-Control: no-cache, must-revalidate
7 Expires: Tue, 23 Jun 2009 12:00:00 GMT
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=utf-8
11 content-length: 6078
12
13 <!DOCTYPE html>
14
15 <html lang="en-GB">

```

Tuy nhiên, nếu cố gắng thực hiện một yêu cầu mà không có token hợp lệ (ví dụ, cố gắng truy cập trực tiếp vào URL xử lý hành động mà không thông qua biểu mẫu đã được chèn token), FortiWeb sẽ chặn yêu cầu này lại.



Nhật ký "Threats" trên FortiWeb sẽ ghi lại các request bị chặn do vi phạm chính sách CSRF.



3.4.2. HTTP Header Security

HTTP header là một phần của các yêu cầu và phản hồi HTTP, chứa các thông tin meta về giao tiếp web. Một số header có thể được sử dụng để tăng cường đáng kể khả năng bảo mật của ứng dụng.

web bằng cách hướng dẫn trình duyệt của người dùng thực hiện các biện pháp bảo vệ nhất định hoặc ngăn chặn các hành vi nguy hiểm. Ngược lại, một số header mặc định do máy chủ web gửi đi có thể vô tình tiết lộ thông tin nhạy cảm về công nghệ đang sử dụng, tạo điều kiện cho kẻ tấn công.

Ví dụ như trước khi có Header Security:

Request

Pretty Raw Hex

```
1 GET /index.php HTTP/1.1
2 Host: 10.1.1.252
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
6 Chrome/125.0.6422.112 Safari/537.36
7 Accept:
8   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
9     .8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.1.1.252/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=qom9hq453egkvu2ag14k629f5h; security=impossible; cookieselession1=
14   678A3E0E34ACDEFCHIKLMN0PQSTU09AD
15 Connection: keep-alive
```

Phản hồi của web sẽ gồm các header sau:

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 09 May 2025 07:38:59 GMT
3 Server: Apache/2.4.37 (centos)
4 X-Powered-By: PHP/7.3.24
5 Pragma: no-cache
6 Cache-Control: no-cache, must-revalidate
7 Expires: Tue, 23 Jun 2029 12:00:00 GMT
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=utf-8
11 content-length: 6348
```

FortiWeb cho phép quản trị viên kiểm soát và tùy chỉnh các HTTP header được gửi đi trong các phản hồi từ máy chủ đến client. Điều này được thực hiện bằng cách tạo một HTTP Header Security Policy trong mục Web Protection > Advanced Protection > HTTP Header Security. Trong chính sách này, quản trị viên có thể:

- Thêm các header bảo mật mới: FortiWeb có thể tự động chèn các header bảo mật quan trọng như:
 - Strict-Transport-Security (HSTS): Buộc trình duyệt chỉ giao tiếp với máy chủ qua HTTPS.
 - X-Frame-Options: Ngăn chặn tấn công clickjacking bằng cách kiểm soát việc trang web có được phép hiển thị trong một frame hoặc iframe hay không.
 - X-Content-Type-Options (thường với giá trị nosniff): Ngăn trình duyệt có gắng "đoán" kiểu MIME của tài nguyên, giảm nguy cơ tấn công liên quan đến việc thực thi nội dung không mong muốn.

- Content-Security-Policy (CSP): Một cơ chế mạnh mẽ cho phép định nghĩa các nguồn tài nguyên (script, ảnh, CSS, v.v.) mà trình duyệt được phép tải và thực thi, giúp giảm thiểu rủi ro từ XSS và các cuộc tấn công chèn mã khác.
- X-XSS-Protection: Kích hoạt các bộ lọc XSS tích hợp sẵn trong một số trình duyệt.

- Xóa các header không mong muốn: Loại bỏ các header có thể tiết lộ thông tin như Server, X-Powered-By, X-AspNet-Version, v.v.
- Sửa đổi các header hiện có.

Ví dụ tạo Policy để thêm các header khác, ngăn chặn XSS với CSP

ID	URL Filter	Request URL Type	Request URL	Secure Header Type	Header Value
1	Disable			X-XSS-Protection	Block Mode
2	Disable			X-Frame-Options	SAMEORIGIN
3	Disable			X-Content-Type-Options	nosniff
4	Disable			Content-Security-Policy	default-src 'none'; script-src 'self'; upgrade-insecure-requests; block-all-mixed-content;

Sau khi thiết lập chính sách trên FortiWeb, các header phản hồi sẽ bao gồm các header bảo mật đã được cấu hình, giúp tăng cường khả năng phòng thủ của ứng dụng web ở phía client. Việc kiểm tra có thể được thực hiện bằng cách sử dụng các công cụ phát triển của trình duyệt (Developer Tools) để xem các header phản hồi hoặc các công cụ quét bảo mật trực tuyến chuyên kiểm tra HTTP header.

Response

Pretty	Raw	Hex	Render
<pre> 1 HTTP/1.1 200 OK 2 Date: Fri, 09 May 2025 07:43:02 GMT 3 Server: Apache/2.4.37 (centos) 4 X-Powered-By: PHP/7.3.24 5 Pragma: no-cache 6 Cache-Control: no-cache, must-revalidate 7 Expires: Tue, 23 Jun 2009 12:00:00 GMT 8 Keep-Alive: timeout=5, max=100 9 Connection: Keep-Alive 10 Content-Type: text/html; charset=utf-8 11 X-XSS-Protection: 1; mode=block 12 X-Frame-Options: SAMEORIGIN 13 X-Content-Type-Options: nosniff 14 Content-Security-Policy: default-src 'none'; script-src 'self'; upgrade-insecure-requests; block-all-mixed-content; 15 content-length: 6348 </pre>			

3.5. Cookie Security

Cookie là những mẩu thông tin nhỏ mà các trang web lưu trữ trên trình duyệt của người dùng để duy trì trạng thái phiên làm việc (session state), lưu trữ các tùy chọn cá nhân hóa, hoặc theo dõi

hành vi người dùng. Do cookie thường chứa các định danh phiên (session ID) hoặc các dữ liệu nhạy cảm khác, chúng trở thành mục tiêu hấp dẫn cho kẻ tấn công. Nếu cookie bị đánh cắp hoặc giả mạo, kẻ tấn công có thể chiếm quyền điều khiển phiên làm việc của người dùng (session hijacking), truy cập trái phép vào tài khoản, hoặc thực hiện các hành động gian lận khác. Do đó, việc bảo vệ cookie là một khía cạnh quan trọng của bảo mật ứng dụng web.

FortiWeb cung cấp các cơ chế mạnh mẽ để bảo vệ cookie, bao gồm mã hóa cookie (Cookie Encryption) và ký cookie (Cookie Signing), nhằm đảm bảo tính bí mật và tính toàn vẹn của thông tin được lưu trữ trong cookie.

"Cookie encrypt" (mã hóa cookie) trong Fortiweb là một tính năng bảo mật được thiết kế để bảo vệ nội dung của cookie bằng cách mã hóa nó. Điều này đảm bảo rằng thông tin nhạy cảm được lưu trữ trong cookie không thể bị đọc hoặc hiểu bởi phía client (người dùng cuối) hoặc bất kỳ kẻ tấn công nào có thể chặn được cookie.

Cách hoạt động cơ bản của Cookie Encryption trong Fortiweb:

- Server gửi Cookie: Khi máy chủ ứng dụng web (backend server) gửi một cookie đến client (through qua Fortiweb).
- Fortiweb mã hóa: Trước khi cookie này được chuyển tiếp đến trình duyệt của client, Fortiweb sẽ chặn nó lại và mã hóa toàn bộ giá trị (nội dung) của cookie bằng một thuật toán mã hóa mạnh và một khóa bí mật mà chỉ Fortiweb biết.
- Client nhận cookie mã hóa: Trình duyệt của client sẽ nhận và lưu trữ cookie ở dạng đã mã hóa này. Client không thể đọc được nội dung thực sự của cookie.
- Client gửi lại cookie mã hóa: Khi client gửi request tiếp theo đến server, nó sẽ gửi lại cookie đã được mã hóa này.
- Fortiweb giải mã: Trước khi request (cùng với cookie mã hóa) được chuyển tiếp đến backend server, Fortiweb sẽ chặn nó lại, giải mã cookie bằng khóa bí mật của mình để khôi phục lại giá trị gốc.
- Server nhận cookie gốc: Backend server sẽ nhận được cookie với nội dung gốc, giống như không có quá trình mã hóa/giải mã nào xảy ra từ phía nó.

Mục đích của Cookie Encryption:

- Đảm bảo tính bảo mật/bí mật (Confidentiality) của nội dung cookie: Ngăn chặn việc lộ thông tin nhạy cảm (ví dụ: ID phiên, thông tin người dùng, dữ liệu tạm thời, sở thích người dùng, token truy cập) được lưu trữ trong cookie. Nếu cookie bị đánh cắp hoặc chặn, kẻ tấn công cũng không thể đọc được nội dung của nó.
- Giảm thiểu rủi ro từ việc lộ thông tin phiên: Ngay cả khi cookie bị lộ, việc mã hóa làm cho nó trở nên vô giá trị đối với kẻ tấn công nếu họ không có khóa giải mã.
- Hỗ trợ tuân thủ các tiêu chuẩn bảo mật: Nhiều quy định và tiêu chuẩn bảo mật yêu cầu bảo vệ dữ liệu nhạy cảm, và mã hóa cookie là một biện pháp để đạt được điều này.

So sánh với "Cookie Signed" (Cookie được ký):

- Cookie Signed (ký cookie):

+ Mục đích chính: Đảm bảo tính toàn vẹn (integrity) và tính xác thực (authenticity) của cookie. Tức là, nó giúp phát hiện xem cookie có bị thay đổi (tampered) hay không.

+ Cách thức: Thêm một chữ ký số (hash) vào cookie. Nội dung cookie vẫn có thể đọc được (không mã hóa).

+ Tập trung vào: Ngăn chặn giả mạo cookie.

- Cookie Encrypted (Mã hóa cookie):

+ Mục đích chính: Đảm bảo tính bí mật (confidentiality) của nội dung cookie.

+ Cách thức: Mã hóa toàn bộ nội dung cookie.

+ Tập trung vào: Giữ bí mật thông tin trong cookie.

Kết hợp:

Trong một số trường hợp, cả hai kỹ thuật có thể được sử dụng đồng thời để cung cấp mức độ bảo mật cao nhất: cookie được mã hóa để bảo vệ nội dung và sau đó được ký để đảm bảo tính toàn vẹn của bản mã hóa đó. Tuy nhiên, việc lựa chọn sử dụng "Signed", "Encrypted", hoặc cả hai thường phụ thuộc vào cấu hình cụ thể trong Fortiweb và yêu cầu bảo mật của ứng dụng.

Ở đây chúng ta sẽ cấu hình bảo mật cookie với Security Mode là Cookie Encrypted.

Name	Nhom1-K22
Security Mode	Encrypted
Cookie Replay	IP
Allow Suspicious Cookies	Always
Don't Block Until	16/05/2025
Cookie Security Attributes	
Cookie Max Age	240 Minutes
Secure Cookie	<input checked="" type="checkbox"/>
HTTP Only	<input checked="" type="checkbox"/>
Action	Alert & Deny
Block Period	600 Seconds (1 - 3600)
Severity	Medium
Trigger Action	

Trước khi thiết lập, sử dụng các công cụ phát triển của trình duyệt (Developer Tools) hoặc các tiện ích mở rộng quản lý cookie, người ta có thể xem được giá trị thực (clear text) của các cookie mà ứng dụng web sử dụng (PHPSESSID, security,...).

Name	Value	Domain	Path	Expires / ...	Size
PHPSESSID	qom9hq453egkvu2agl4k629f5h	10.1.1.252	/	Session	35
cookiesession1	678A3E0E34ACDEFGHIJKLMNOPQSTU09AD	10.1.1.252	/	2026-05-...	46
security	impossible	10.1.1.252	/	Session	18

Sau khi kích hoạt tính năng Cookie Encryption trên FortiWeb và áp dụng chính sách, khi kiểm tra lại cookie trên trình duyệt, giá trị của các cookie đã được FortiWeb xử lý sẽ hiển thị dưới dạng một chuỗi ký tự mã hóa, không còn mang ý nghĩa rõ ràng nữa. Điều này chứng tỏ nội dung của cookie đã được bảo vệ thành công khỏi việc bị đọc trộm ở phía client.

Sources	Network	Performance	Memory	Application	Security	Lighthouse	Recorder	DOM Invader
Filter					Only show cookies with an issue			
Name	Value	Domain	Path	Expires / ...	Size	HttpOnly		
PHPSESSID	yQ/aoiFowjTExmKLgNwcKXzSfpQ7aoarCUb5E1ZxSIRTpu...	10.1.1.252	/	2025-05-...	117	✓		
cookiesession1	678A3E12TVWXYZACDEFGIJKLMNOPQE937	10.1.1.252	/	2026-05-...	46	✓		
security	yQ/aoiFowjTExmKLgNwcKbbquqA9RPe6BfGJygWn308DJ...	10.1.1.252	/	2025-05-...	96	✓		

Việc mã hóa cookie giúp đảm bảo tính bí mật (confidentiality) của thông tin chứa trong cookie, giảm thiểu rủi ro lộ thông tin phiên và hỗ trợ tuân thủ các tiêu chuẩn bảo mật yêu cầu bảo vệ dữ liệu nhạy cảm.

3.6. Input Validation

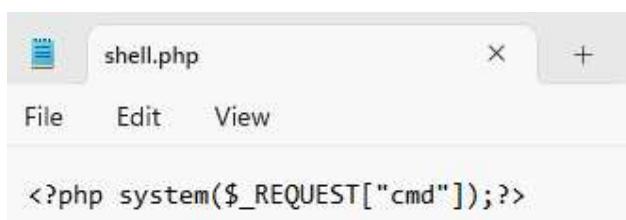
Xác thực đầu vào là quá trình kiểm tra và đảm bảo rằng tất cả dữ liệu nhận được từ người dùng (hoặc từ các nguồn bên ngoài khác) đều tuân thủ các quy tắc, định dạng, và giới hạn đã được định trước trước khi dữ liệu đó được xử lý bởi ứng dụng. Việc thiếu hoặc xác thực đầu vào không đầy đủ là một trong những nguyên nhân gốc rễ của rất nhiều lỗ hổng bảo mật web nghiêm trọng, bao gồm SQL Injection, Cross-Site Scripting (XSS), Command Injection, Buffer Overflows, và nhiều loại tấn công khác. Bằng cách kiểm soát chặt chẽ những gì được phép đi vào ứng dụng, chúng ta có thể giảm thiểu đáng kể mối đe dọa và ngăn chặn các payload độc hại.

FortiWeb cung cấp các cơ chế mạnh mẽ để thực thi các chính sách xác thực đầu vào, cho phép quản trị viên định nghĩa chi tiết các quy tắc cho từng loại dữ liệu mà ứng dụng web nhận được.

3.6.1. File Security

Nhiều ứng dụng web cho phép người dùng tải lên các tệp tin, chẳng hạn như ảnh đại diện, tài liệu, hoặc các loại phương tiện khác. Nếu không được kiểm soát cẩn thận, tính năng này có thể bị lạm dụng để tải lên các tệp độc hại, bao gồm webshell (cho phép kẻ tấn công thực thi lệnh từ xa trên máy chủ), virus, malware, hoặc các tệp tin có định dạng không mong muốn có thể gây lỗi cho ứng dụng hoặc hệ thống.

Trước khi cấu hình có thể upload shell:



```
<?php system($_REQUEST["cmd"]);?>
```

Vulnerability: File Upload

Choose an image to upload:

shell.php

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitetecurity/upload-forms-threat/>

Lúc này có thể tấn công shell lên server:

The screenshot shows two separate command-line sessions in a browser window. The top session runs 'ls' and lists files 'dvwa_email.png' and 'shell.php'. The bottom session runs 'whoami' and shows the user is 'apache'.

FortiWeb cho phép quản trị viên thiết lập các chính sách chi tiết để kiểm soát việc tải tệp lên, đảm bảo rằng chỉ các tệp hợp lệ và an toàn mới được chấp nhận. Quá trình cấu hình bao gồm:

Truy cập vào mục cấu hình liên quan đến xác thực đầu vào hoặc bảo vệ tệp, thường nằm trong Web Protection > Input Validation > File Security (hoặc đường dẫn tương tự).

Tạo một File Security Profile mới hoặc chỉnh sửa một profile có sẵn.

Trong profile này, quản trị viên có thể định nghĩa các quy tắc như:

- Chặn theo loại tệp (Block by File Type): Cho phép chỉ định các loại tệp được phép hoặc bị cấm tải lên dựa trên phần mở rộng của tệp (file extension) hoặc kiểu MIME (MIME type). Ví dụ, có thể cấm tải lên các tệp thực thi (như .exe, .php, .asp, .sh) để ngăn chặn việc tải lên webshell.
- Giới hạn kích thước tệp (File Size Restriction): Đặt giới hạn tối đa cho kích thước của tệp được phép tải lên để ngăn chặn các cuộc tấn công từ chối dịch vụ bằng cách tải lên các tệp quá lớn làm cạn kiệt tài nguyên máy chủ.
- Quét mã độc (Antivirus Scanning): Tích hợp với bộ máy antivirus của FortiGuard để quét tất cả các tệp tải lên nhằm phát hiện và chặn các phần mềm độc hại.
- Kiểm tra tên tệp (File Name Checks): Áp dụng các quy tắc cho tên tệp, ví dụ như độ dài tối đa, các ký tự được phép, để tránh các vấn đề liên quan đến việc xử lý tên tệp không hợp lệ.

Edit File Security Policy

Name	WebShell-Uploading	
Action	Alert & Deny	
Block Period	600	Seconds (1 - 3600)
Severity	Medium	
Trigger Action	<input type="text"/>	
Trojan Detection	<input checked="" type="checkbox"/>	
Antivirus Scan	<input checked="" type="checkbox"/>	
Send Files to FortiSandbox	<input checked="" type="checkbox"/>	
Scan Attachments in Email	<input checked="" type="checkbox"/>	

Return

Edit File Security Rule

Name	WebShell-Uploading
Type	Allow File Types Block File Types
Host Status	<input checked="" type="checkbox"/>
Host	<input type="text"/>
Request URL Type	Simple String Regular Expression
Request URL	<input type="text"/> ^/* »
File Upload Limit	<input type="text"/> 0 (0-102400)(Kbytes)
JSON File Support	<input checked="" type="checkbox"/>

Return

ID	File Types
1	EXE(.exe)
2	PHP(.php)
3	JSP(.jsp)
4	ASPX(.aspx)
5	SQL(.sql)

File Security Profile này sau đó được áp dụng vào Web Protection Profile chung.

Input Validation

Parameter Validation	<input type="text"/>
Hidden Fields Protection	<input type="text"/>
File Security	WebShell-Uploading

Security Configuration

Monitor Mode	<input checked="" type="checkbox"/>
Syn Cookie	<input checked="" type="checkbox"/>
Web Protection Profile	Nhom1_FileUpload_Profile
Replacement Message	Predefined
URL Case Sensitivity	<input checked="" type="checkbox"/>

Sau khi áp dụng chính sách, thử tải lại tệp PHP đó. FortiWeb sẽ chặn yêu cầu tải lên, và người dùng có thể nhận được thông báo chặn.

Vulnerability: File Upload

Choose an image to upload:

shell.php

More Information

← ⌂ ▲ Không bảo mật | 10.1.1.252/vulnerabilities/upload/#



Web Page Blocked!

The page cannot be displayed. Please contact the administrator for additional information.

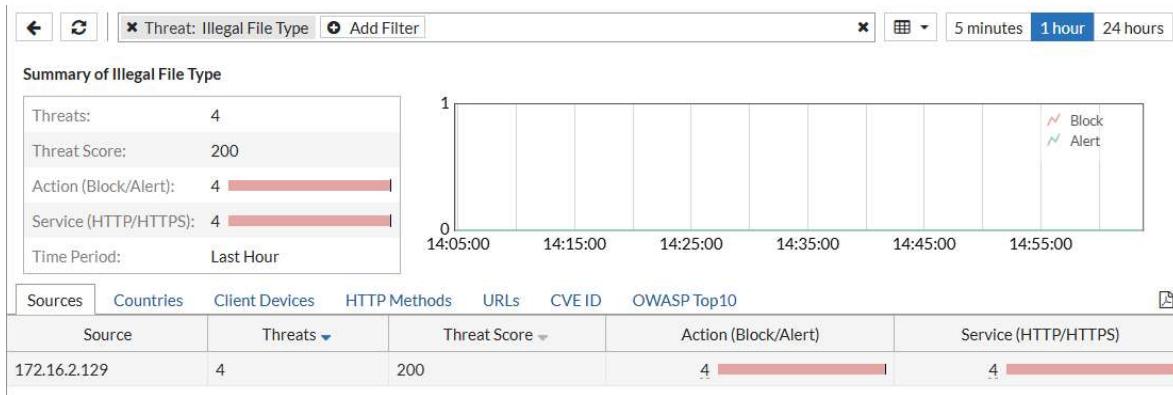
URL: 10.1.1.252/vulnerabilities/upload/

Client IP: 172.16.2.129

Attack ID: 20000017

Message ID: 000001477410





3.6.2. Parameter Validation

Hầu hết các ứng dụng web nhận dữ liệu đầu vào từ người dùng thông qua các tham số trong URL (GET request) hoặc trong thân của yêu cầu (POST request). Nếu ứng dụng không kiểm tra kỹ lưỡng các giá trị của những tham số này, kẻ tấn công có thể gửi các giá trị độc hại hoặc không mong muốn để khai thác lỗ hổng. Ví dụ, gửi một chuỗi ký tự quá dài có thể gây ra lỗi tràn bộ đệm (buffer overflow), hoặc gửi các ký tự đặc biệt có thể dẫn đến SQL Injection hoặc XSS nếu các biện pháp bảo vệ chuyên biệt khác chưa được áp dụng hoặc bị bypass.

FortiWeb cho phép quản trị viên định nghĩa các quy tắc xác thực chi tiết cho từng tham số mà ứng dụng web sử dụng. Điều này được thực hiện bằng cách tạo các Parameter Validation Rule.

Trong các quy tắc này, quản trị viên có thể chỉ định:

- Tên tham số (Parameter Name): Tham số cụ thể cần được xác thực.
- Kiểu dữ liệu (Data Type): Ví dụ: chuỗi (string), số nguyên (integer), số thực (float), boolean, địa chỉ email, URL, v.v. FortiWeb sẽ kiểm tra xem giá trị của tham số có khớp với kiểu dữ liệu đã định hay không.
- Độ dài tối thiểu và tối đa (Minimum and Maximum Length): Giới hạn độ dài cho phép của giá trị tham số.
- Biểu thức chính quy (Regular Expression): Cho phép định nghĩa một mẫu (pattern) phức tạp mà giá trị tham số phải tuân theo. Đây là một công cụ rất mạnh mẽ để xác thực các định dạng dữ liệu cụ thể (ví dụ: mã bưu điện, số điện thoại, định dạng ngày tháng cụ thể).
- Danh sách các giá trị cho phép/không cho phép (Allowed/Disallowed Values): Chỉ định một tập hợp các giá trị cụ thể mà tham số được hoặc không được phép nhận.
- Các ràng buộc khác: Ví dụ, tham số có bắt buộc hay không, có được phép lặp lại hay không.

Ví dụ ở đây là Rule chỉ cho phép tham số name tại /vulnerabilities/xss_r/ có độ dài tối đa là 50 ký tự.

Parameter Validation Policy Parameter Validation Rule

Edit Parameter Validation Rule

Name	XSS-R	
Host Status	<input checked="" type="checkbox"/>	
Host		
URL Type	<input checked="" type="radio"/> Simple String <input type="radio"/> Regular Expression	
Post URL	/vulnerabilities/xss_r/	
You can enter a precise URL, such as /floder1/index.htm or use wildcards to match multiple URLs, such as /floder1/*, or /floder1/*index.htm		
Action	<input type="button" value="Alert & Deny"/>	
Block Period	600	Seconds (1 - 3600)
Severity	<input type="button" value="Medium"/>	
Trigger Policy	<input type="button" value=""/>	

ID	Name	Max Length	Data Type	Required	Name Type	Use Type Check
1	name	50	Strings	No	Simple String	Enable

Parameter Validation Profile sau đó được áp dụng vào Web Protection Profile.

Việc nhập 30 ký tự sẽ được chấp nhận.

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

More Information

- <https://owasp.org/www-community/attacks/xss/>
 - <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
 - https://en.wikipedia.org/wiki/Cross-site_scripting
 - <http://www.cgisecurity.com/xss-faq.html>
 - <http://www.scriptalert1.com/>

Nếu nhập 51 ký tự (vượt quá giới hạn 50), FortiWeb sẽ phát hiện vi phạm quy tắc xác thực độ dài và có thể chặn yêu cầu.

The screenshot displays a network traffic capture between a client and a server. The client's request includes a GET to a URL containing a long string of 'a' characters, followed by a user token, and an upgrade-insecure-requests header. The response from the server is a single-line message: "The page cannot be displayed. Please contact the administrator for additional information." This indicates a security measure like a Content Security Policy or a custom error page is being enforced.

Bằng cách kết hợp File Security và Parameter Validation, FortiWeb giúp đảm bảo rằng chỉ những dữ liệu đầu vào hợp lệ và an toàn mới được ứng dụng web xử lý, qua đó đóng một vai trò quan trọng trong việc ngăn chặn một loạt các cuộc tấn công dựa trên đầu vào.

3.7. URL Access control

Kiểm soát truy cập URL là một cơ chế bảo mật quan trọng cho phép quản trị viên định nghĩa các quy tắc để cho phép hoặc từ chối truy cập đến các đường dẫn (URL) hoặc các phần cụ thể của một ứng dụng web dựa trên nhiều yếu tố khác nhau, phổ biến nhất là địa chỉ IP nguồn. Tính năng này rất hữu ích trong việc bảo vệ các trang quản trị, các tập tin cấu hình nhạy cảm, hoặc các chức năng đặc biệt mà chỉ một số người dùng hoặc hệ thống nhất định mới được phép truy cập. Bằng cách hạn chế quyền truy cập vào các endpoint nhạy cảm, chúng ta có thể giảm thiểu đáng kể bè mặt tấn công và ngăn chặn các truy cập trái phép.

FortiWeb cung cấp khả năng cấu hình các chính sách kiểm soát truy cập URL một cách linh hoạt, cho phép tạo ra các quy tắc chi tiết để đáp ứng các yêu cầu bảo mật cụ thể.

Cấu hình rule để cho phép IP của máy quản trị viên có thể truy cập các endpoint nhạy cảm như /setup.php, /admin,...

The screenshot shows two configuration dialogs for URL Access Control.

Edit URL Access Condition Dialog:

- ID:** 1
- Source Address:** Enabled (radio button)
- Source Address Type:** IP Resolved by Specified Domain
- Type:** IPv4 (selected)
- IP Resolved by Specified Domain:** 172.16.2.129
- URL Type:** Simple String (selected)
- URL Pattern:** /setup.php
- Note:** You can enter a precise URL, such as /folder1/index.htm or use wildcards to match multiple URLs, such as /folder1/*, or /folder1/*index.htm
- Meet this condition if:**
 - Object does not match the Source Address or the URL Pattern
 - Object matches the Source Address and the URL Pattern** (highlighted in blue)

OK **Cancel**

Edit URL Access Rule Dialog:

- Name:** Nhom01_Admin_Endpoint
- Host Status:** Enabled (radio button)
- Host:** 10.1.1.252
- Action:** Continue
- Severity:** Medium
- Trigger Policy:** (empty)

OK **Cancel**

URL Access Rule Table:

ID	URL Type	URL Pattern	Object
1	Simple String	/setup.php	match this condition

Buttons: + Create New, Edit, Delete

Sau khi đã cho phép IP quản trị, bước tiếp theo là tạo một quy tắc để chặn tất cả các địa chỉ IP khác cố gắng truy cập vào cùng các endpoint nhạy cảm đó. Thêm một rule thứ hai để chặn truy cập đến từ các máy có địa chỉ IP khác vào các endpoint nói trên.

The screenshot shows two windows side-by-side. The top window is titled 'Edit URL Access Rule' and contains fields for Name (Nhom01_Admin_Endpoint_Deny), Host Status (green circle), Host (10.1.1.252), Action (Alert & Deny), Severity (Medium), and Trigger Policy (dropdown). Below these are 'OK' and 'Cancel' buttons. The bottom window is titled 'Edit URL Access Condition' and shows a table with one row. The table has columns for ID (1), URL Type (Simple String), URL Pattern (/setup.php), and Object (match this condition). Below the table are buttons for '+ Create New', 'Edit', and 'Delete'. The condition table has columns for ID (1), Source Address (dropdown), URL Type (Simple String selected), URL Pattern (/setup.php), and a note about URL patterns. The bottom part of the condition window shows 'Meet this condition if:' with options 'Object does not match the URL Pattern' and 'Object matches the URL Pattern' (selected). At the bottom are 'OK' and 'Cancel' buttons.

Hai quy tắc vừa tạo (Allow và Deny) cần được tập hợp vào một URL Access Policy. Ví dụ, một policy có tên "Nhom01_URL_Access_Policy" được tạo.

The screenshot shows a window titled 'Edit URL Access Policy' with a 'Name' field containing 'Nhom01_URL_Access_Policy'. Below are 'OK' and 'Cancel' buttons. Underneath is a table listing two rules. The table has columns for ID (1, 2), Access Rule Name (Nhom01_Admin_Endpoint, Nhom01_Admin_Endpoint_Deny), and buttons for '+ Create New', 'Edit', 'Delete', 'Insert', and 'Move'.

ID	Access Rule Name
1	Nhom01_Admin_Endpoint
2	Nhom01_Admin_Endpoint_Deny

Từ bất kỳ máy nào, kể cả máy không phải là máy quản trị, thử truy cập vào đường dẫn /setup.php của ứng dụng. Kết quả là có thể truy cập bình thường vào trang Database Setup của DVWA.

The screenshot shows two panels from NetworkMiner. The left panel, titled 'Request', displays a GET request to '/setup.php' with various headers. The right panel, titled 'Response', shows the 'Database Setup' page of the DVWA (Damn Vulnerable Web Application) web application. The DVWA logo is at the top, followed by buttons for 'Setup DVWA', 'Instructions', and 'About'. Below these are instructions and a note about database creation.

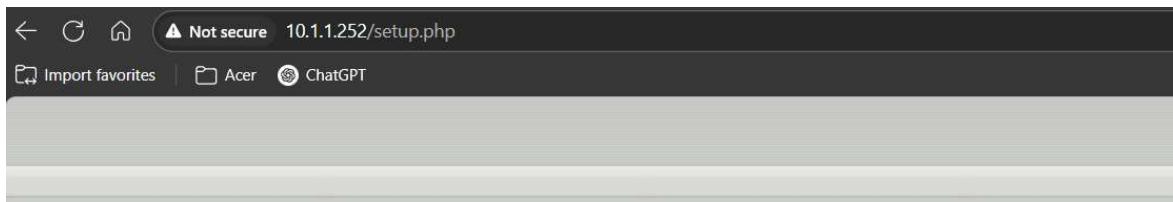
```

Request
Pretty Raw Hex
1 GET /setup.php HTTP/1.1
2 Host: 10.1.1.252
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: cookiessession1=e79a3e13jkmnopqrstuvwxyz; PHPSESSID=yQ/aoiFowjTExmLgNwcKZZ/wUMFIgmluNj8C/u3FibL/eLytsukLktn+0fiHqvriQmQJWCQpcCWXpkOTZNZgN4l8boObdjo+Vz2AryXso=; security=yQ/aoiFowjTExmLgNwcKcP0rmVPSNITz/WYIqj9wb0GcJhdJrE8Bh/dvqcMfgm0JTVYZiscVuLvb0dTZCN+Gg=; Connection: keep-alive
10

```

Sau khi đã áp dụng URL Access Policy vào Web Protection Profile và Server Policy:

- Từ máy quản trị viên (có IP 172.16.2.129), truy cập vào /setup.php vẫn thành công do khớp với quy tắc "Allow".
- Từ một máy khác (ví dụ, có IP 172.16.2.141 như trong hình ảnh), khi cố gắng truy cập vào /setup.php, yêu cầu sẽ bị FortiWeb chặn, và người dùng nhận được trang thông báo "Web Page Blocked!". Thông tin Client IP và Attack ID được hiển thị.



Web Page Blocked!



The page cannot be displayed. Please contact the administrator for additional information.

URL: 10.1.1.252/setup.php

Client IP: 172.16.2.141

Attack ID: 20000007

Message ID: 000003275596

Tính năng URL Access Control trên FortiWeb cung cấp một lớp bảo vệ hiệu quả, giúp kiểm soát chặt chẽ quyền truy cập vào các tài nguyên nhạy cảm của ứng dụng web, hạn chế nguy cơ bị khai thác hoặc truy cập trái phép từ các nguồn không đáng tin cậy.

3.8. Áp dụng Machine Learning trong nhận diện bất thường

Trong bối cảnh các kỹ thuật tấn công ngày càng trở nên tinh vi và các cuộc tấn công zero-day (khai thác các lỗ hổng chưa được công bố hoặc chưa có bản vá) xuất hiện thường xuyên, các phương pháp bảo vệ truyền thống dựa trên chữ ký không còn đủ để đảm bảo an toàn tuyệt đối. Kẻ tấn công có thể dễ dàng thay đổi một chút trong payload (tải trọng tấn công) để né tránh các chữ ký hiện có. Đây là lúc công nghệ Học máy (Machine Learning - ML) phát huy vai trò quan trọng. Bằng cách "học" hành vi bình thường của một ứng dụng web, ML có thể phát hiện ra những sai lệch (anomalies) đáng ngờ mà không cần dựa vào các mẫu tấn công cụ thể đã biết. Những sai lệch này có thể là dấu hiệu của một cuộc tấn công mới hoặc một kỹ thuật bypass tinh vi.

FortiWeb tích hợp một cơ chế Machine Learning mạnh mẽ, hai lớp, để nâng cao khả năng phát hiện và giảm thiểu báo động giả.

Các "mô hình mối đe dọa được huấn luyện trước" mà FortiWeb sử dụng ở lớp thứ hai của hệ thống Machine Learning là một thành phần trí tuệ nhân tạo tinh vi, được phát triển và duy trì bởi FortiGuard Labs, trung tâm nghiên cứu và phản ứng mối đe dọa toàn cầu của Fortinet. Đây không phải là những chữ ký tấn công tĩnh thông thường, mà là các mô hình thống kê và thuật toán được "dạy" để nhận diện các đặc điểm, hành vi, và cấu trúc tiềm ẩn của các loại tấn công phổ biến, ngay cả khi các biến thể cụ thể của những cuộc tấn công đó chưa từng xuất hiện trước đây.

Threat Model

The screenshot shows a user interface for threat modeling. At the top, there is a header "Threat Model". Below it, there are four distinct sections, each representing a different threat model:

- Well-trained Mathematical Model for Cross-site Scripting**: Described as a "Well-trained Support Vector Machine model with linear type kernel function for Cross-site Scripting attack." It includes a 3D scatter plot visualization showing data points clustered in two distinct regions separated by a decision boundary.
- Well-trained Mathematical Model for SQL Injection**
- Well-trained Mathematical Model for Code Injection**
- Well-trained Mathematical Model for Command Injection**

Các mô hình này được xây dựng dựa trên việc phân tích một khối lượng dữ liệu khổng lồ về các mối đe dọa mà FortiGuard Labs thu thập từ hàng triệu thiết bị Fortinet triển khai trên toàn cầu, từ các hệ thống honeypot, nghiên cứu mã độc, và các nguồn thông tin tình báo mối đe dọa khác. Quá trình xây dựng bao gồm:

- Thu thập và gán nhãn Dữ liệu: FortiGuard thu thập hàng triệu mẫu tấn công thực tế thuộc nhiều loại khác nhau (SQLi, XSS, Command Injection, Path Traversal, các kỹ thuật làm mờ, v.v.). Dữ liệu này được các chuyên gia phân tích và gán nhãn cẩn thận.
- Trích xuất đặc trưng (Feature Extraction): Từ các mẫu tấn công đã gán nhãn, các thuật toán sẽ trích xuất ra những đặc trưng quan trọng, những "tín hiệu" nhận biết một cuộc tấn công. Đó có thể là sự

hiện diện của các từ khóa SQL nhất định, cấu trúc của một đoạn mã JavaScript đáng ngờ, việc sử dụng các ký tự đặc biệt theo một cách cụ thể, độ dài bất thường của các tham số, hoặc các chuỗi hành động liên tiếp.

- Huấn luyện mô hình (Model Training): Sử dụng các kỹ thuật học máy có giám sát (supervised learning), các mô hình (ví dụ: Support Vector Machines, Neural Networks, Decision Trees, v.v.) được huấn luyện trên bộ dữ liệu đã trích xuất đặc trưng. Mục tiêu là để mô hình học được cách phân biệt giữa lưu lượng độc hại và lưu lượng lành tính dựa trên các đặc trưng đó. Các mô hình này được tối ưu hóa để nhận diện "bản chất" của một kiểu tấn công chứ không chỉ là một chuỗi ký tự cố định.

Khi lớp đầu tiên của Machine Learning trên FortiWeb (học hành vi bình thường của ứng dụng cụ thể) phát hiện ra một "bất thường" (anomaly) – tức là một yêu cầu đi chệch khỏi mô hình hoạt động bình thường đã học – yêu cầu bất thường này sẽ được chuyển đến lớp thứ hai. Tại đây:

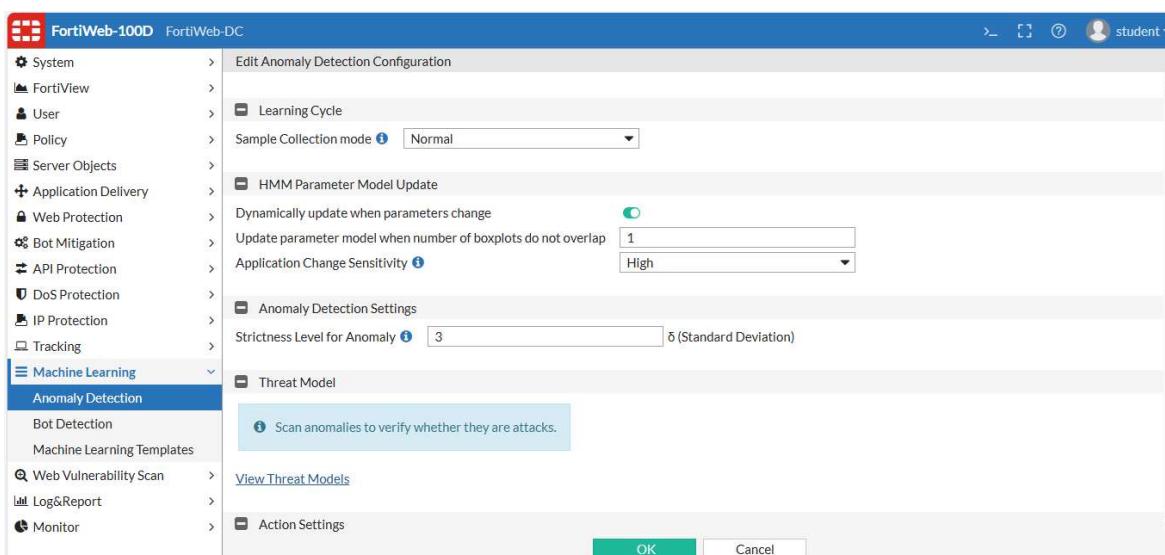
- Các đặc trưng của yêu cầu bất thường đó được trích xuất.
- Những đặc trưng này được đưa vào các mô hình mới để dọa đã được huấn luyện trước tương ứng (ví dụ, mô hình chuyên nhận diện SQLi, mô hình chuyên nhận diện XSS).
- Các mô hình này sẽ đưa ra một "điểm số" hoặc một xác suất cho biết liệu bất thường đó có mang các đặc điểm của một kiểu tấn công đã biết hay không. Ví dụ, một yêu cầu có thể không khớp với bất kỳ chữ ký SQLi nào hiện có, nhưng mô hình SQLi được huấn luyện trước vẫn có thể nhận ra rằng cấu trúc và các từ khóa trong yêu cầu đó rất giống với "hành vi" của một cuộc tấn công SQL Injection.

Việc áp dụng Machine Learning trên FortiWeb không phải là một câu hình bắt/tắt đơn giản mà là một quá trình.

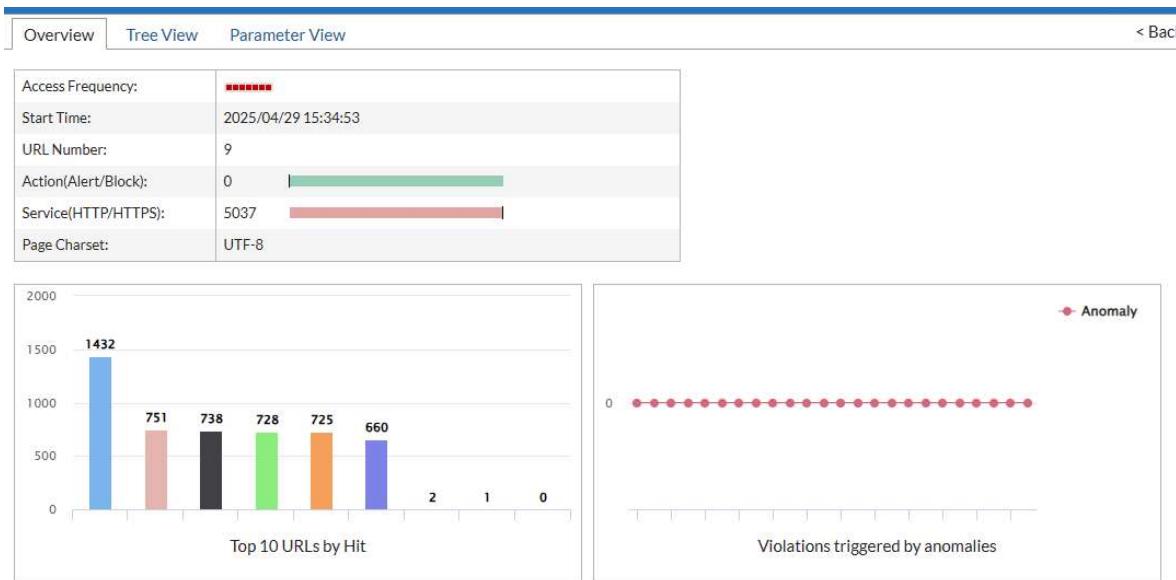
3.8.1. Kích hoạt và giai đoạn học

Đầu tiên, tính năng Machine Learning cần được kích hoạt cho Server Policy.

Sau khi kích hoạt, FortiWeb sẽ bước vào một "giai đoạn học" (learning period). Trong giai đoạn này, FortiWeb quan sát và phân tích một lượng lớn lưu lượng truy cập hợp lệ đến ứng dụng. Nó thu thập thông tin về các URL được truy cập, các tham số được sử dụng, kiểu dữ liệu của các tham số, độ dài, tần suất, các phương thức HTTP, và nhiều đặc điểm khác của các yêu cầu và phản hồi.



Mục tiêu của giai đoạn học là để FortiWeb xây dựng một "mô hình hành vi bình thường" (baseline behavior model) hoặc một "hồ sơ" (profile) chi tiết cho ứng dụng. Giai đoạn này có thể kéo dài từ vài giờ đến vài ngày hoặc thậm chí vài tuần, tùy thuộc vào độ phức tạp của ứng dụng và lượng lưu lượng truy cập.



FortiWeb-100D FortiWeb-DC

- System
- FortiView
- User
- Policy
- Server Objects
- Application Delivery
- Web Protection
- Bot Mitigation
- API Protection
- DoS Protection
- IP Protection
- Tracking
- Machine Learning**
- Anomaly Detection
- Bot Detection
- Machine Learning Templates
- Web Vulnerability Scan
- Log&Report
- Monitor

Domain: 10.1.1.252

Access Frequency:

Model Initialization Date: 2025/04/29 15:37:05

Action(Alert/Block): 0

Anomaly: 0

Violation Trend

Rebuild URL Import

Parameters

Parameter Name	HMM Learning Stage	HMM Details
user_token	Collecting	6.50%
btnSign	Collecting	6.25%
mtxMessage	Collecting	6.25%
txtName	Collecting	6.25%
btnClear	Collecting	0.00%

Overview Tree View Parameter View < Back

Access Frequency:

Start Time: 2025/04/29 15:34:53

URL Number: 14

Action(Alert/Block): 0

Service(HTTP/HTTPS): 5369

Page Charset: UTF-8

Top 10 URLs by Hit

Violations triggered by anomalies

Overview Tree View Parameter View < Back

Domain: 10.1.1.252

Refresh

Access Frequency:

Model Initialization Date: 2025/05/09 12:55:41

Action(Alert/Block): 0

Anomaly: 0

Violation Trend

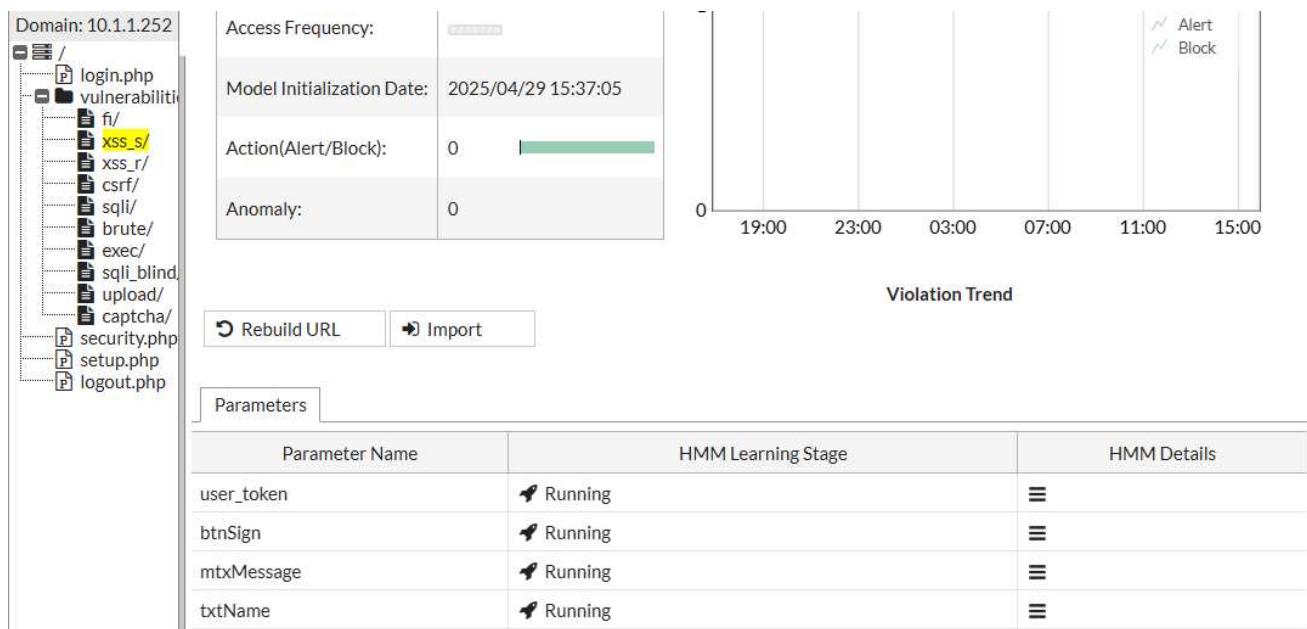
Rebuild URL Import

Parameters

Parameter Name	HMM Learning Stage	HMM Details
name	Collecting	15.00%

3.8.2. Giai đoạn phát hiện và thực thi

Sau khi học xong, mô hình hành vi bình thường đã được thiết lập. FortiWeb sẽ chuyển sang chế độ phát hiện.



Lúc này, mọi yêu cầu mới đến ứng dụng sẽ được so sánh với mô hình đã học. Nếu một yêu cầu có những đặc điểm khác biệt đáng kể so với hành vi bình thường (ví dụ: một tham số mới xuất hiện, một kiểu dữ liệu không mong muốn, một chuỗi ký tự có cấu trúc lạ, hoặc một URL chưa từng thấy được truy cập theo cách bất thường), FortiWeb sẽ đánh dấu nó là một "bất thường" (anomaly).

Nếu tắt ML, với policy ví dụ như chặn XSS, những payload thông thường sẽ không thể đi qua được:

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <script>alert(1)</script>



Web Page Blocked!

The page cannot be displayed. Please contact the administrator for additional information.

URL: 10.1.1.252/vulnerabilities/xss_r/

Client IP: 172.16.2.129

Attack ID: 20000008

Message ID: 000003248471

Nhưng những request đặc biệt như zero-day, bất thường thì sẽ không bị bắt lại (bất kể kiểu tấn công gì):

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello %%%%%%% - %%%%%%%

Qua đó có thể bypass những mẫu payload có sẵn trong Fortiweb.

Như đã đề cập trước đó, FortiWeb thường sử dụng kiến trúc ML hai lớp. Bất thường được phát hiện ở lớp đầu sẽ được lớp thứ hai kiểm tra lại bằng cách đối chiếu với các mô hình mới để dọa đã được huấn luyện trước để xác định xem đó có thực sự là một cuộc tấn công hay chỉ là một sai lệch lanh tính.

Khi bật ML lên sau khi học, những payload zero-day sẽ được xem là khác những input thông thường thì sẽ bị xem là có hại và bị chặn lại:

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?



Web Page Blocked!

The page cannot be displayed. Please contact the administrator for additional information.

URL: 10.1.1.252/vulnerabilities/xss_r/

Client IP: 172.16.2.129

Attack ID: 20000037

Message ID: 000003250648

Hành động đối với các bất thường được xác định là mối đe dọa có thể được cấu hình là chặn (block), cảnh báo (alert), ghi log.

The screenshot shows the FortiWeb interface with two main panels. On the left is the 'Attack Log Widget' showing a list of recent attacks:

- 2025-05-10 16:10:03 Machine Learning Anomaly Detection: Remote Exploits
- 2025-05-10 16:08:48 Cookie name (PHPSESSID), signed verification failed; track lost; Domain: 10.1.1.249; Path: /dvwa/vulnerabilities/fi/
- 2025-05-10 16:08:48 Parameter(page) triggered signature ID 0600150002 of Signatures policy K22_Nhom4
- 2025-05-10 16:08:48 Parameter triggered signature ID 060070002 of Signatures policy K22_Nhom4

On the right is the 'Log Details' panel for the first attack entry:

Detailed Information

Flag	2025-05-10
Date	16:10:03
Time	Nhom1_Policy
Policy	http
Service	1.x
HTTP Version	10.1.1.252
HTTP Host	get
Method	/vulnerabilities/xss_r/?name=%X%X%X6%X%X%X%X-X-%X%X%X%X%X%X%X-X%
URL	Disabled
Monitor Mode	Action
Action	Alert_Deny
Threat Level	██████
Client Risk	Malicious
Source Country or Region	Reserved
CVE ID	N/A
OWASP Top10	N/A
Main Type	Machine Learning
Sub Type	Anomaly in http argument
Signature Subclass Type	N/A
Signature ID	N/A
Message	Machine Learning Anomaly Detection: Remote Exploits

Connection

3.9. Thực hành khả năng scan lỗ hổng web

Bên cạnh việc triển khai các lớp phòng thủ theo thời gian thực, một phương pháp quan trọng khác để đảm bảo an ninh cho ứng dụng web là chủ động tìm kiếm và xác định các lỗ hổng tiềm ẩn thông qua việc quét lỗ hổng (Vulnerability Scanning). Nhiều ứng dụng web, dù được phát triển cẩn thận đến đâu, vẫn có thể tồn tại các điểm yếu do lỗi lập trình, cấu hình sai, hoặc sử dụng các thành phần phần mềm lỗi thời. Việc phát hiện sớm các lỗ hổng này cho phép đội ngũ phát triển hoặc quản trị viên khắc phục chúng trước khi kẻ tấn công có thể tìm thấy và khai thác.

FortiWeb tích hợp sẵn một công cụ quét lỗ hổng mạnh mẽ, giúp tự động hóa quá trình kiểm tra bảo mật cho các ứng dụng web được bảo vệ. Tính năng này không chỉ giúp phát hiện các lỗ hổng đã biết mà còn có thể kiểm tra các vấn đề về cấu hình bảo mật.

Đầu tiên là tạo lịch quét (Scan Schedule - tùy chọn): Nếu muốn thực hiện quét định kỳ (ví dụ: hàng tuần, hàng tháng), một lịch quét cần được tạo trong mục Web Vulnerability Scan > Web Vulnerability Scan Schedule. Trong lịch này, chúng ta đặt tên, chọn loại lịch (Recurring) và xác định thời gian, tần suất quét. Tuy nhiên, nếu chỉ muốn quét một lần ngay lập tức, bước này có thể bỏ qua hoặc tạo lịch loại "One Time" để thử nghiệm.

Name	Nhom1_Vul_Scan
Type	One Time Recurring
Time	16 : 35
Date	25/04/2025



Sau đó tạo hồ sơ quét (Scan Profile): Đây là bước quan trọng để định nghĩa mục tiêu và phạm vi quét. Trong mục Web Vulnerability Scan > Scan Profile, một profile mới được tạo. Tại đây, cần chỉ định "Scan Target" là địa chỉ URL hoặc IP của ứng dụng web cần quét (ví dụ: địa chỉ IP của Virtual Server là 10.1.1.252). "Scan Template" xác định mức độ sâu và loại lỗ hổng cần kiểm tra; "Full Audit" là một lựa chọn phổ biến để kiểm tra toàn diện. Các tùy chọn nâng cao (Advanced Options) cho phép tinh chỉnh thêm quá trình quét, ví dụ như cấu hình thông tin xác thực nếu ứng dụng yêu cầu đăng nhập.

Scan Profile		Scan Template
New Web Vulnerability Scan Profile		
Name	Nhóm1_Scan_Profile	
Scan Target	10.1.1.252	
<small>(*) e.g. "www.mytestwvs.com", "http://www.mytestwvs.com:8080/test/login.php"</small>		
Scan Template	Full Audit	
<input checked="" type="checkbox"/> Advanced Options		
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Tạo và chạy chính sách quét (Scan Policy): Cuối cùng, một Web Vulnerability Scan Policy được tạo trong mục tương ứng. Chính sách này liên kết Scan Profile đã tạo với một lịch quét hoặc có thể được cấu hình để chạy ngay lập tức ("Run Now"). Chọn định dạng cho báo cáo kết quả (ví dụ: HTML, XML, PDF). Như của nhóm làm là "Nhóm1_Scan_Policy" được tạo, chọn Profile "Nhóm1_Scan_Profile", loại "Run Now", và định dạng báo cáo là HTML. Sau khi bấm OK, FortiWeb sẽ bắt đầu quá trình quét.

New Web Vulnerability Scan Policy	
Name	Nhóm1_Scan_Policy
Type	<input checked="" type="radio"/> Run Now <input type="radio"/> Schedule
Profile	Nhóm1_Scan_Profile
Report Format	<input checked="" type="checkbox"/> HTML <input type="checkbox"/> XML <input type="checkbox"/> PDF
Email Policy	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Trạng thái của quá trình quét có thể được theo dõi trong danh sách các Scan Policy. Trạng thái sẽ chuyển từ "Starting" sang "Scanning" và cuối cùng là "Done" khi hoàn tất

+ Create New	Edit	Delete	#	Name	Schedule	Profile	Status	Action
1	Test-DVWA	Run Now	Test-DVWA	Stopped				
2	K22_Nhom4	Run Now	K22_Nhom4	Done				
3	Nhom1_Scan_Policy	Run Now	Nhom1_Scan_Profile	Starting				

Scan Summary

Target	10.1.1.252
Request Count	4543
Requests per Minute	772
Total Alerts Found	7

Alerts Found

#	Category	Vulnerabilities
1	Server header	1
2	Powered-by header	1
3	Favicon identification failed	1
4	Cross site tracing vulnerability	1
5	Non existent methods default to GET	1
6	Internal hostname in HTML link	1
7	Strange HTTP response code	1

Refresh

Sau khi quá trình quét hoàn tất, kết quả chi tiết có thể được xem và tải về từ mục Web Vulnerability Scan > Scan History. Báo cáo sẽ liệt kê tất cả các lỗ hổng và cảnh báo được tìm thấy, phân loại chúng theo mức độ nghiêm trọng, mô tả chi tiết về từng vấn đề, và thường cung cấp các khuyến nghị hoặc liên kết tham khảo để khắc phục.

Scan Summary

Target	10.1.1.252
Request Count	11133
Requests per Minute	816
Total Alerts Found	8

Alerts Found

#	Category	Vulnerabilities
1	Server header	1
2	Powered-by header	1
3	Favicon identification failed	1
4	Cross site tracing vulnerability	1
5	Non existent methods default to GET	1
6	Internal hostname in HTML link	1
7	Strange HTTP response code	1
8	Webserver fingerprint	1

Như kết quả scan trên cho thấy một bản tóm tắt các cảnh báo được tìm thấy (Scan Summary) cho mục tiêu 10.1.1.252, bao gồm các vấn đề như thông tin Server header, Powered-by header bị lộ, lỗi xác định favicon, lỗi hỏng Cross site tracing, phương thức không tồn tại mặc định thành GET, tên máy chủ nội bộ trong link HTML, mã phản hồi HTTP lạ, và dấu vết máy chủ web (Webserver fingerprint). Số lượng cảnh báo và chi tiết cụ thể có thể thay đổi giữa các lần quét hoặc tùy thuộc vào cấu hình của ứng dụng đích.

PHẦN 3: KẾT LUẬN

Qua quá trình tìm hiểu lý thuyết, triển khai cấu hình và thực hiện kiểm nghiệm thực tế trên thiết bị Tường lửa Ứng dụng Web FortiWeb-100D, báo cáo này đã cung cấp một cái nhìn tổng quan về vai trò, cơ chế hoạt động và hiệu quả của một giải pháp WAF hiện đại trong việc bảo vệ các ứng dụng web. Từ việc phân tích các phương pháp nhận diện tấn công đa dạng mà FortiWeb tích hợp, đến việc giới thiệu chi tiết về thiết bị FortiWeb-100D và các bước cấu hình cụ thể, cuối cùng là đánh giá kết quả thông qua các kịch bản tấn công mô phỏng, chúng ta có thể rút ra những kết luận quan trọng.

1. Ưu nhược điểm của FortiWeb-100D

Dựa trên các tìm hiểu và kết quả thực hành, thiết bị FortiWeb-100D thể hiện nhiều ưu điểm đáng kể nhưng cũng có một số điểm cần cân nhắc.

Ưu điểm:

- **Khả năng bảo vệ đa lớp toàn diện:** FortiWeb-100D cung cấp một bộ tính năng bảo mật phong phú, kết hợp nhiều lớp phòng thủ từ cơ bản đến nâng cao. Việc tích hợp bảo vệ dựa trên chữ ký (Signature-based), phòng chống DoS/DDoS tầng ứng dụng, chống Bot tinh vi, bảo vệ API, xác thực đầu vào chi tiết, bảo mật cookie, bảo mật HTTP header, và đặc biệt là khả năng phát hiện bất thường bằng Machine Learning hai lớp, tạo ra một lá chắn vững chắc chống lại nhiều loại mối đe dọa.
- **Hiệu quả phát hiện cao và giảm thiểu báo động giả:** Sự kết hợp giữa chữ ký, phân tích hành vi và đặc biệt là Machine Learning hai lớp (với các mô hình mới để dọa được huấn luyện trước) giúp FortiWeb không chỉ phát hiện các tấn công đã biết mà còn cả các tấn công zero-day và biến thể mới, đồng thời giảm thiểu đáng kể tình trạng báo động giả so với các phương pháp chỉ dựa trên chữ ký hoặc phát hiện bất thường đơn thuần.
- **Tích hợp hệ sinh thái Fortinet Security Fabric:** Khả năng tích hợp liền mạch với các sản phẩm khác của Fortinet như FortiGate, FortiAnalyzer, FortiSandbox cho phép chia sẻ thông tin tình báo mối đe dọa và tự động hóa phản ứng, tạo nên một hệ thống phòng thủ đồng bộ và mạnh mẽ hơn.
- **Dịch vụ FortiGuard cập nhật liên tục:** Việc được hỗ trợ bởi các dịch vụ FortiGuard đảm bảo rằng cơ sở dữ liệu chữ ký, danh tiếng IP, mô hình mối đe dọa, và các thông tin bảo mật khác luôn được cập nhật mới nhất, giúp thiết bị đối phó hiệu quả với các mối đe dọa không ngừng thay đổi.
- **Tính năng quét lỗ hổng tích hợp:** Khả năng chủ động quét và phát hiện lỗ hổng trên ứng dụng web ngay từ chính thiết bị WAF là một điểm cộng lớn, giúp các tổ chức có cái nhìn toàn diện về tình trạng bảo mật của ứng dụng và có kế hoạch khắc phục kịp thời.
- **Giao diện quản lý trực quan và khả năng giám sát tốt:** Giao diện web (GUI) của FortiWeb tương đối thân thiện và dễ sử dụng. Công cụ FortiView cung cấp khả năng giám sát và phân tích lưu lượng, sự kiện tấn công một cách trực quan, giúp quản trị viên dễ dàng nắm bắt tình hình. Hệ thống ghi log chi tiết cũng hỗ trợ tốt cho việc điều tra và báo cáo.
- **Phù hợp cho doanh nghiệp vừa và nhỏ:** Model FortiWeb-100D cung cấp một sự cân bằng tốt giữa hiệu suất, tính năng và chi phí, là lựa chọn phù hợp cho các doanh nghiệp vừa và nhỏ hoặc các văn phòng chi nhánh cần một giải pháp WAF chuyên dụng.

Nhược điểm:

- Độ phức tạp trong cấu hình nâng cao: Mặc dù giao diện cơ bản khá thân thiện, việc cấu hình các tính năng nâng cao như Machine Learning, tùy chỉnh sâu các chính sách bảo vệ, hoặc tinh chỉnh để giảm thiểu báo động giả có thể đòi hỏi kiến thức chuyên môn sâu và thời gian tìm hiểu, thử nghiệm.
- Hiệu quả của Machine Learning phụ thuộc vào giai đoạn học: Để Machine Learning hoạt động hiệu quả nhất, nó cần có đủ thời gian và dữ liệu lưu lượng truy cập "sạch" trong giai đoạn học. Nếu giai đoạn học quá ngắn, dữ liệu không đại diện, hoặc bị "nhiễm bẩn" bởi lưu lượng tấn công, mô hình hành vi chuẩn có thể không chính xác, dẫn đến báo động giả hoặc bỏ sót tấn công.
- Yêu cầu tài nguyên cho các tính năng đầy đủ: Việc kích hoạt đồng thời nhiều tính năng bảo mật cao cấp (đặc biệt là SSL Inspection và Machine Learning) có thể ảnh hưởng đến hiệu suất tổng thể của thiết bị. Mặc dù FortiWeb-100D được tối ưu hóa, cần cân nhắc kỹ lưỡng về yêu cầu hiệu suất thực tế của ứng dụng khi lựa chọn model và cấu hình.
- Chi phí bản quyền và dịch vụ FortiGuard: Mặc dù thiết bị có thể có giá cạnh tranh, việc duy trì các dịch vụ cập nhật FortiGuard (cần thiết để đảm bảo hiệu quả bảo vệ) đòi hỏi chi phí bản quyền hàng năm, đây là một yếu tố cần xem xét trong tổng chi phí sở hữu (TCO).

2. Tổng Kết

Qua báo cáo, nhóm đã thực hiện một nghiên cứu chi tiết và thực nghiệm về Tường lửa Ứng dụng Web (WAF), tập trung vào việc triển khai và đánh giá hiệu quả của thiết bị FortiWeb-100D. Xuất phát từ nhu cầu cấp thiết trong việc bảo vệ các ứng dụng web trước bối cảnh mối đe dọa an ninh mạng ngày càng gia tăng và phức tạp, báo cáo đã đặt mục tiêu tìm hiểu sâu về cơ chế hoạt động của WAF nói chung và khám phá các khả năng cụ thể của giải pháp FortiWeb-100D.

Qua việc kết hợp giữa tìm hiểu lý thuyết về cấu trúc, nguyên lý hoạt động, các phương pháp nhận diện tấn công đa dạng (từ dựa trên chữ ký, danh tiếng IP, kiểm tra giao thức đến phân tích hành vi, học máy, chống bot, bảo vệ API, xác thực đầu vào, và quét lỗ hổng chủ động) với việc giới thiệu chi tiết về thông số kỹ thuật và tính năng của FortiWeb-100D, báo cáo đã xây dựng một nền tảng kiến thức vững chắc. Phần trọng tâm của báo cáo là việc mô tả chi tiết quá trình triển khai cấu hình các chính sách bảo mật trên FortiWeb-100D trong môi trường lab, bao gồm thiết lập các đối tượng máy chủ, cấu hình phòng chống DoS, chống các tấn công đã biết như SQL Injection và XSS, áp dụng các biện pháp bảo vệ nâng cao như chống CSRF, bảo mật HTTP Header, bảo mật Cookie, xác thực đầu vào, thực hành quét lỗ hổng, và đặc biệt là ứng dụng công nghệ Machine Learning để phát hiện các bất thường.

Quá trình kiểm nghiệm và đánh giá kết quả được thực hiện một cách có hệ thống thông qua các kịch bản tấn công mô phỏng đa dạng nhằm vào ứng dụng web DVWA. Kết quả thực nghiệm đã xác nhận một cách thuyết phục rằng FortiWeb-100D, với các cấu hình phù hợp, là một giải pháp WAF mạnh mẽ và hiệu quả. Thiết bị đã chứng minh khả năng phát hiện và ngăn chặn thành công nhiều loại tấn công phổ biến và cả các kỹ thuật tấn công mới lạ, nhờ vào kiến trúc bảo vệ đa lớp và sự hỗ trợ từ các dịch vụ tình báo mới đe dọa FortiGuard. Các tính năng như Machine Learning và quét lỗ hổng

tích hợp đã cho thấy giá trị gia tăng đáng kể, giúp nâng cao khả năng phòng thủ chủ động và thích ứng của hệ thống.

Nhìn chung, nghiên cứu này không chỉ cung cấp kiến thức về một giải pháp WAF cụ thể mà còn minh họa quy trình tiếp cận, triển khai và đánh giá một công nghệ bảo mật quan trọng. FortiWeb-100D đã được chứng minh là một công cụ bảo mật giá trị, đặc biệt phù hợp với nhu cầu của các doanh nghiệp vừa và nhỏ, góp phần đảm bảo an toàn cho các tài sản ứng dụng web trong môi trường số hóa hiện nay.

TÀI LIỆU THAM KHẢO

Tufin. "Application Firewall Review: Understanding WAFs and How They Protect Your Applications." *Tufin Blog.* Có sẵn tại: <https://www.tufin.com/blog/application-firewall-review-understanding-wafs-and-how-they-protect-your-applications>

Fortinet. "FortiGate 100D Series Data Sheet." *Senetic.* Có sẵn tại: https://www.senetic.fr/i/objects/mmo_39193334_1509459564_716_6983.pdf (Lưu ý: Mặc dù đây là tài liệu về FortiGate, nó có thể chứa thông tin liên quan đến kiến trúc bảo mật của Fortinet.)

OWASP Foundation. "Projects." *OWASP Foundation.* Có sẵn tại: <https://owasp.org/projects/> (Bao gồm các dự án quan trọng như OWASP Top Ten, ASVS, WSTG, và Cheat Sheet Series)

StrongDM. "SQL Injection Prevention: 6 Proven Ways to Prevent Attacks." *StrongDM Blog.* Có sẵn tại: <https://www.strongdm.com/blog/how-to-prevent-sql-injection-attacks>

PortSwigger. "What is cross-site scripting (XSS) and how to prevent it?" *Web Security Academy.* Có sẵn tại: <https://portswigger.net/web-security/cross-site-scripting>

Cloudflare. "What is web application security?" *Cloudflare Learning Center.* Có sẵn tại: <https://www.cloudflare.com/learning/security/what-is-web-application-security/> (Đề cập đến các khái niệm cốt lõi và các phương pháp giảm thiểu mối đe dọa)

MDN Web Docs. "Cross-site request forgery (CSRF) prevention." *MDN Web Docs.* Có sẵn tại: https://developer.mozilla.org/en-US/docs/Web/Security/Practical_implementation_guides/CSRF_prevention

Acunetix. "Strengthen Your Web Applications with HTTP Security Headers." *Acunetix Blog.* Có sẵn tại: <https://www.acunetix.com/blog/articles/http-security-headers-web-applications>

MDN Web Docs. "Using HTTP cookies." *MDN Web Docs.* Có sẵn tại: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies>

TechTarget. "Top vulnerability scanning tools." *TechTarget.* (Bài viết này thường liệt kê và mô tả các công cụ phổ biến như OpenVAS, Nessus, Acunetix, Burp Suite, Nmap, Qualys, Nikto. Bạn có thể tìm kiếm bài viết gốc hoặc một bài tương tự để trích dẫn cụ thể.)

Akamai. "What Is Bot Mitigation?" *Akamai Glossary.* Có sẵn tại: <https://www.akamai.com/glossary/what-is-bot-mitigation>

Palo Alto Networks. "API security best practices." *Palo Alto Networks.* (Tìm kiếm các bài viết hoặc white paper về chủ đề này từ các nhà cung cấp bảo mật uy tín. Kết quả tìm kiếm cung cấp một danh sách các thực tiễn tốt.)

Vercara. "What is An Application-Layer DDoS Attack, and How Do I Defend Against Them?" *Vercara Resources.* Có sẵn tại: <https://vercara.com/resources/what-is-an-application-layer-ddos-attack-and-how-do-i-defend-against-them>

ZeroThreat. "Understanding Input Validation and Its Importance." *ZeroThreat Blog*. Có sẵn tại: <https://zerothreat.ai/blog/what-is-input-validation-and-its-importance>

Cyber Advisors. "Fortinet, Fortigate, Fabric Security: Enhancing Cyber Defense Through Integrated Solutions." *Cyber Advisors Blog*. Có sẵn tại: <https://blog.cyberadvisors.com/fortinet-fortigate-fabric-security-enhancing-cyber-defense-through-integrated-solutions>

GitHub. "digininja/DVWA: Damn Vulnerable Web Application (DVWA)." *GitHub*. Có sẵn tại: <https://github.com/digininja/DVWA>

Check Point Software. "Web Application Firewall (WAF) vs. Firewall." *Check Point Cyber Hub*. Có sẵn tại: <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-web-application-firewall/what-is-waf-as-a-service/web-application-firewall-waf-vs-firewall/>

Indusface. "Web application security threats." *Indusface Blog*. (Kết quả tìm kiếm cung cấp một danh sách các mối đe dọa phổ biến. Bạn có thể tìm bài viết gốc hoặc các nguồn tương tự như OWASP Top 10 để trích dẫn.)

VIR. "Fortinet threat report reveals record surge in automated cyberattacks." *Vietnam Investment Review*. Có sẵn tại: <https://vir.com.vn/fortinet-threat-report-reveals-record-surge-in-automated-cyberattacks-128257.html> (Bạn cũng có thể tìm các báo cáo trực tiếp từ trang web của Fortinet/FortiGuard Labs.)

Ox Security. "SDLC Security: Everything You Need to Know." *Ox Security Blog*. Có sẵn tại: <https://www.ox.security/sdlc-security-everything-you-need-to-know/>