BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính nâng cao**

**Lab 2: Improving Mod Security WAF**

*GVHD: Đỗ Thị Phương Uyên*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT522.O21.ATCL.1- Nhóm 3

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Ngọc Trà My | 21520353 | [21520353@gm.uit.edu.vn](mailto:21520353@gm.uit.edu.vn) |
| 2 | Bùi Hoàng Trúc Anh | 21521817 | [21521817@gm.uit.edu.vn](mailto:21521817@gm.uit.edu.vn) |
| 3 | Lê Hoàng Oanh | 21521253 | [21521253@gm.uit.edu.vn](mailto:21521253@gm.uit.edu.vn) |
| 4 | Huỳnh Minh Tân Tiến | 21521520 | 21521520@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | **Yêu cầu 1** | 100% |
| 2 | **Yêu cầu 2** | 100% |
| 3 | **Yêu cầu 3** | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

**Yêu cầu 1:** Tìm hiểu cơ chế hoạt động của việc tính điểm bất thường của bộ Core Rule Set và giải thích tại sao cơ chế này lại dẫn đến sự xuất hiện của False Positive. Tham khảo: <https://coreruleset.org/docs/concepts/anomaly_scoring/>

Cơ chế hoạt động của việc tính điểm bất thường (anomaly scoring) trong Core Rule Set (CRS) là một phương pháp được sử dụng để đánh giá mức độ rủi ro của các yêu cầu web dựa trên các biểu hiện không bình thường hoặc không được mong đợi. Cụ thể, khi một yêu cầu web đến, CRS sẽ theo dõi các biểu hiện không phù hợp hoặc không bình thường trong yêu cầu này và gán điểm dựa trên mức độ nghi ngờ về mức độ độc hại hoặc nguy hiểm của yêu cầu.

Cơ chế tính điểm bất thường trong CRS có thể bao gồm các phần như sau:

1. Quy tắc (rules): CRS bao gồm một tập hợp các quy tắc được thiết kế để phát hiện các hoạt động bất thường hoặc tiềm ẩn của các cuộc tấn công web. Mỗi quy tắc sẽ đánh giá các yêu cầu web dựa trên các tiêu chí nhất định và gán điểm dựa trên mức độ rủi ro được đánh giá.
2. Trọng số (weights): Mỗi quy tắc có thể có một trọng số tương ứng, biểu thị mức độ nghiêm trọng của một vi phạm có thể xảy ra nếu quy tắc được kích hoạt.
3. Thang điểm (scoring scale): CRS sử dụng một thang điểm để đánh giá mức độ nghi ngờ của các hoạt động không bình thường. Các điểm này thường được tính dựa trên các yếu tố như trọng số của quy tắc, số lần xảy ra vi phạm, hoặc các yếu tố khác.

Tuy nhiên, cơ chế tính điểm bất thường có thể dẫn đến sự xuất hiện của False Positive, tức là các báo động bất thường được kích hoạt nhưng thực tế không phải là mối đe dọa thực sự. Có một số lý do chính dẫn đến việc này:

1. Quy tắc không chính xác: Có thể có trường hợp một số quy tắc được kích hoạt dựa trên các biểu hiện không phù hợp hoặc không chính xác, dẫn đến việc kích hoạt các báo động bất thường không chính xác.
2. Môi trường phức tạp: Trong môi trường web phức tạp, các hoạt động bình thường có thể được đánh giá nhầm là bất thường do sự phức tạp của hệ thống và ứng dụng web.
3. Thiết lập không chính xác: Cài đặt không chính xác của CRS hoặc không tinh chỉnh cẩn thận có thể dẫn đến việc kích hoạt các báo động bất thường không mong muốn.

Để giảm thiểu False Positive, quan trọng để cân nhắc và tinh chỉnh cài đặt của CRS, đảm bảo rằng các quy tắc được chọn và cấu hình phù hợp với môi trường web cụ thể của bạn. Đồng thời, việc theo dõi và phản hồi đối với các báo động cũng là một phần quan trọng của việc quản lý rủi ro trong bảo mật web.

**Yêu cầu 2:** Tìm hiểu cách viết rule, giải thích ý nghĩa của ít nhất 3 rule trong bộ Core Rule Set

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Description automatically generated

Ảnh có chứa văn bản, ảnh chụp màn hình, tài liệu, Phông chữ

Description automatically generated

Rule trên được sử dụng để xử lý các trường hợp đặc biệt khi có yêu cầu từ máy chủ Apache mà có thể gây ra các cảnh báo sai (false positives) khi sử dụng Core Rule Set (CRS) để bảo vệ ứng dụng web. Dưới đây là giải thích ý nghĩa của từng phần trong các rule:

1. Bộ xử lý ngoại lệ cho Apache SSL pinger:

- Rule này được áp dụng trong `phase:1`, tức là trong phase kiểm tra yêu cầu (request).

- Nó kiểm tra nếu yêu cầu là `GET /` (yêu cầu trang chủ) và địa chỉ IP của máy gửi yêu cầu là `127.0.0.1` hoặc `::1` (địa chỉ loopback của máy chủ), đây thường là các yêu cầu từ máy chủ chính nó.

- Nếu cả hai điều kiện này đều đúng, rule sẽ bỏ qua (pass) yêu cầu này (`pass`) và không ghi log (`nolog`).

- Đồng thời, nó sẽ thực hiện việc loại bỏ các cảnh báo có liên quan đến CRS bằng cách loại bỏ theo thẻ `OWASP\_CRS`.

- Cụ thể trong trường hợp này, nó sẽ loại bỏ cảnh báo nếu có (`ctl:auditEngine=Off`).

1. Bộ xử lý ngoại lệ cho kết nối giả mạo bên trong của Apache:

- Rule này cũng được áp dụng trong `phase:1`.

- Nó kiểm tra nếu địa chỉ IP của máy gửi yêu cầu là `127.0.0.1` hoặc `::1`, và trong trường hợp này, nó sẽ tiếp tục kiểm tra `User-Agent` của yêu cầu.

- Nếu `User-Agent` của yêu cầu kết thúc với chuỗi "(internal dummy connection)", điều này cho thấy yêu cầu là một kết nối giả mạo bên trong của Apache.

- Rule sẽ loại bỏ (pass) yêu cầu này và không ghi log.

- Nó cũng sẽ thực hiện loại bỏ các cảnh báo liên quan đến CRS và tắt việc ghi log cảnh báo.

Những rule này giúp loại bỏ các cảnh báo không cần thiết và cải thiện hiệu suất của hệ thống bảo mật web, đồng thời giảm thiểu việc xuất hiện các false positives.

Ảnh có chứa văn bản, tài liệu, ảnh chụp màn hình, thực đơn

Description automatically generated

Ảnh có chứa văn bản, ảnh chụp màn hình, tài liệu, Phông chữ

Description automatically generated

1. Rule về Paranoia Level (Độ Cảnh Giác):

- Rule này liên quan đến việc xác định mức độ cảnh giác (paranoia level) của hệ thống CRS. Mức độ cảnh giác này có thể được cấu hình để xác định cách mà các quy tắc CRS được áp dụng dựa trên mức độ nguy cơ ước lượng cho ứng dụng của bạn.

- Mỗi mức độ cảnh giác (paranoia level) có một tập hợp khác nhau của các quy tắc CRS áp dụng. Ví dụ, khi mức độ cảnh giác tăng lên, số lượng và nghiêm ngặt của các quy tắc có thể được áp dụng cũng tăng theo.

- Quy tắc này kiểm tra mức độ cảnh giác hiện tại của hệ thống và áp dụng các quy tắc tương ứng với mức độ cảnh giác này.

1. Rule về Phương Thức Yêu Cầu Cho Phép (Allowed Request Methods):

- Rule này kiểm tra xem phương thức yêu cầu (request method) được sử dụng có được phép hay không theo chính sách bảo mật.

- Nếu phương thức yêu cầu không nằm trong danh sách các phương thức được phép (được xác định trước trong file cấu hình), quy tắc này sẽ chặn yêu cầu và ghi log một cảnh báo với mức độ nghiêm trọng CRITICAL.

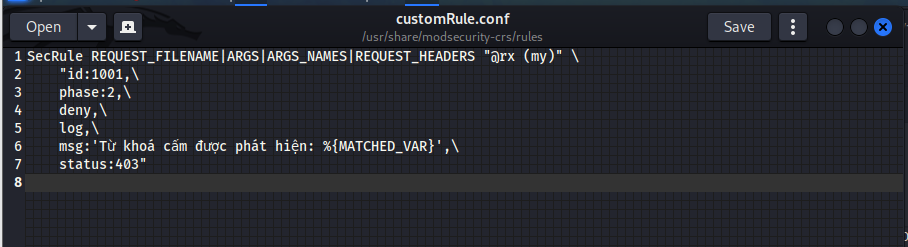
- Đồng thời, nó tăng điểm điểm bất thường (anomaly score) của yêu cầu đó.

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

Một vài gợi ý:

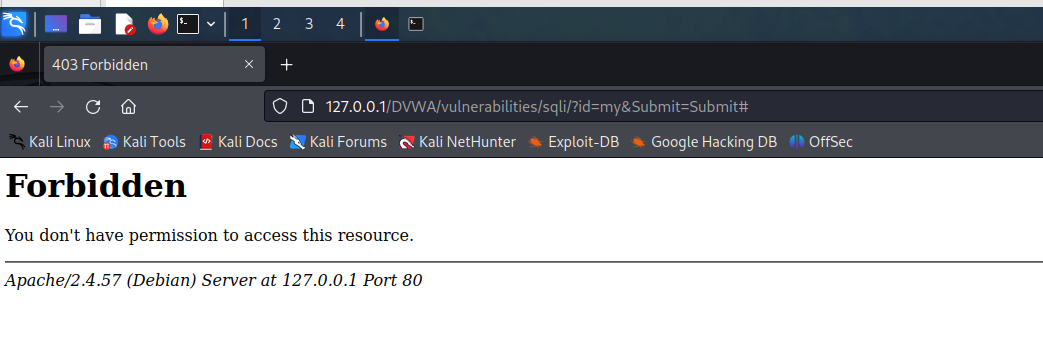
• Chặn từ một từ khoá nhất định trong form/url

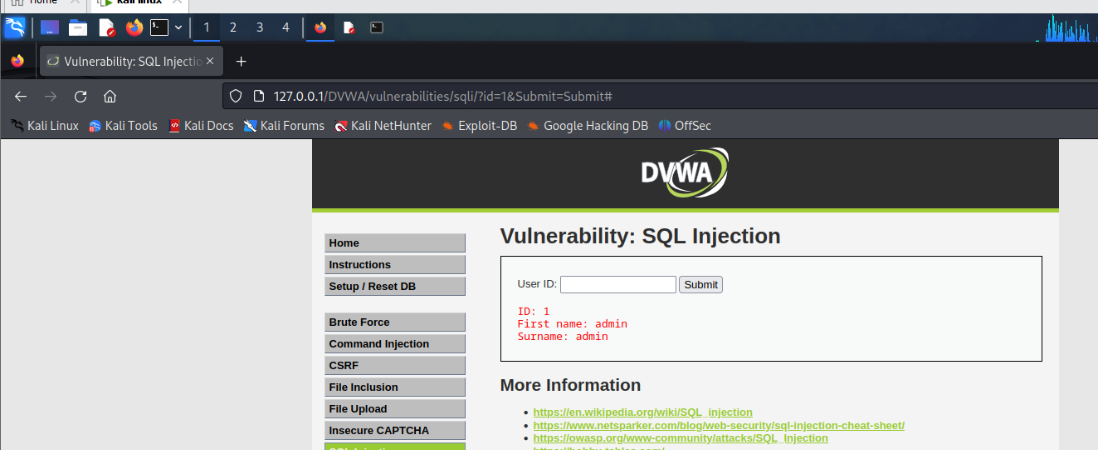
Trong thư mục /usr/share/modsecurity-crs/rules, tạo file customRule.conf



Trong đó:

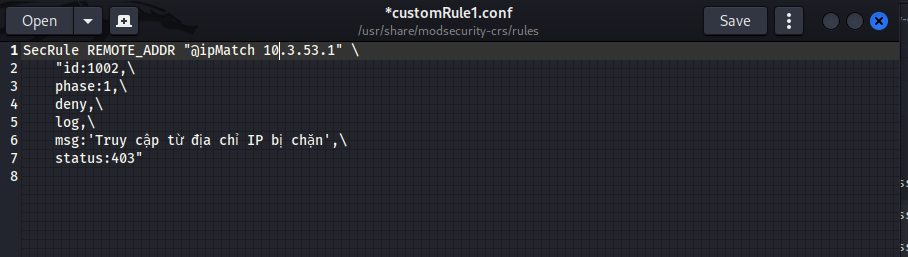
* REQUEST\_FILENAME|ARGS|ARGS\_NAMES|REQUEST\_HEADERS: Đây là phạm vi mà quy tắc sẽ kiểm tra. Trong trường hợp này, chúng ta kiểm tra tất cả các phần của yêu cầu, bao gồm tên file, tham số (ARGS), tên tham số (ARGS\_NAMES), và các tiêu đề của yêu cầu (REQUEST\_HEADERS).
* "@rx (my)": Đây là biểu thức chính quy để tìm kiếm từ khóa mà bạn muốn chặn. Trong ví dụ này, chúng ta sử dụng @rx để chỉ định biểu thức chính quy -> chặn từ khóa “my”
* id:1001: ID của quy tắc.
* phase:2: Giai đoạn mà quy tắc này sẽ được kích hoạt. Trong trường hợp này, chúng ta sử dụng giai đoạn 2, sau khi yêu cầu đã được phân tích.
* deny: Hành động của quy tắc khi điều kiện được kích hoạt. Trong trường hợp này, chúng ta đang từ chối yêu cầu.
* log: Ghi log khi quy tắc được kích hoạt.
* msg:'Từ khoá cấm được phát hiện: %{MATCHED\_VAR}': Tin nhắn được ghi vào log khi quy tắc được kích hoạt. %{MATCHED\_VAR} là biến môi trường của ModSecurity chứa giá trị từ khóa đã được phát hiện.
* status:403: Mã trạng thái HTTP được trả về khi yêu cầu bị từ chối





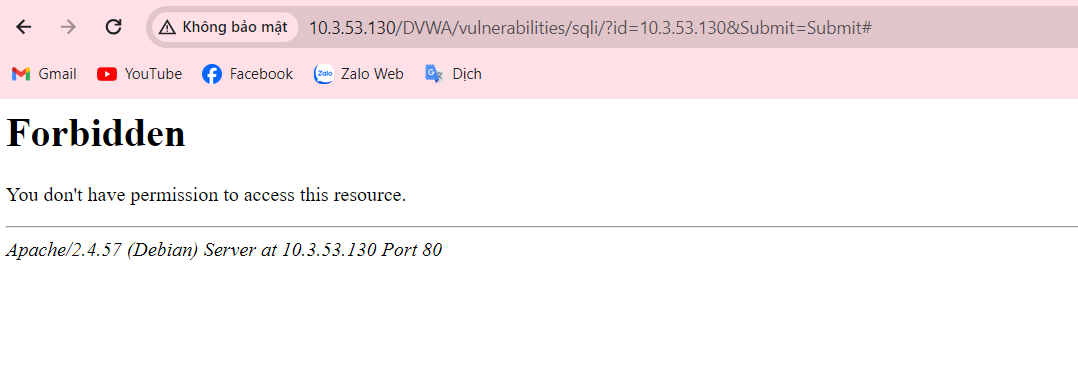
Nhập id=1 thì không bị chặn

• Chặn lượt truy cập tới web server từ một địa chỉ IP



Trong đó:

* REMOTE\_ADDR: Đây là một biến môi trường trong ModSecurity, lưu trữ địa chỉ IP của người dùng đang truy cập.
* "@ipMatch x.x.x.x": Điều kiện để so sánh địa chỉ IP của người dùng với địa chỉ IP cụ thể
* id:1002: ID của quy tắc.
* phase:1: Giai đoạn mà quy tắc này sẽ được kích hoạt. Trong trường hợp này, chúng ta sử dụng giai đoạn 1, trước khi yêu cầu được phân tích.
* deny: Hành động của quy tắc khi điều kiện được kích hoạt. Trong trường hợp này, chúng ta đang từ chối lượt truy cập từ địa chỉ IP đã chỉ định.
* log: Ghi log khi quy tắc được kích hoạt.
* msg:'Truy cập từ địa chỉ IP bị chặn': Tin nhắn được ghi vào log khi quy tắc được kích hoạt.
* status:403: Mã trạng thái HTTP được trả về khi yêu cầu bị từ chối.



• Giới hạn dung lượng upload của một file

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Description automatically generated

Giải thích:

* SecRequestBodyLimit 1048576: Giới hạn kích thước tối đa của dữ liệu yêu cầu (bao gồm cả tệp đính kèm) là 1 MB (1048576 byte).
* SecRequestBodyNoFilesLimit 1048576: Giới hạn kích thước tối đa của dữ liệu yêu cầu mà không phải là các tệp đính kèm là 1 MB.
* SecRule FILES\_TMPNAMES "@inspectFile /(\.gif|\.jpe?g|\.png)$/i": Quy tắc áp dụng cho các tệp tạm thời tải lên có phần mở rộng là .gif, .jpg, .jpeg hoặc .png.
* id:10002: ID của quy tắc.
* phase:2: Quy tắc được áp dụng trong giai đoạn 2 của xử lý yêu cầu (giai đoạn phản hồi).
* t:none: Không thực hiện biến đổi trên dữ liệu.
* deny,status:403: Từ chối yêu cầu và trả về mã trạng thái 403 (Forbidden) nếu quy tắc được kích hoạt.
* log,msg:'File upload exceeded maximum allowed size': Ghi log và gửi thông điệp lỗi "File upload exceeded maximum allowed size" nếu quy tắc được kích hoạt.

Ảnh có chứa ảnh chụp màn hình, văn bản, phần mềm, Phần mềm đa phương tiện

Description automatically generated

