**View access\_log lên ta thấy địa chỉ 192.168.1.1 đang cố gắng thực hiện SQL INJECTION vào trang Web** [**http://192.168.1.5**](http://192.168.1.5)

* **Thực hiện lọc nội dung và đếm bằng lệnh Grep trên Linux  
  => Grep -c -w “192.168.1.1” access\_log.log**
* **\* -c là đếm số dòng**
* **-w là tìm chính xác**

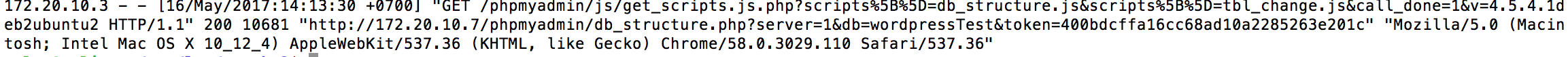
**Giới thiệu về log file của apache trên linux**

* File log của apache server nằm ở thư mục /var/log/apache2 (đối với ubuntu) và ở /var/log/httpd (đối với centOs)
* Bao gồm 2 file chính đó là access log và error log

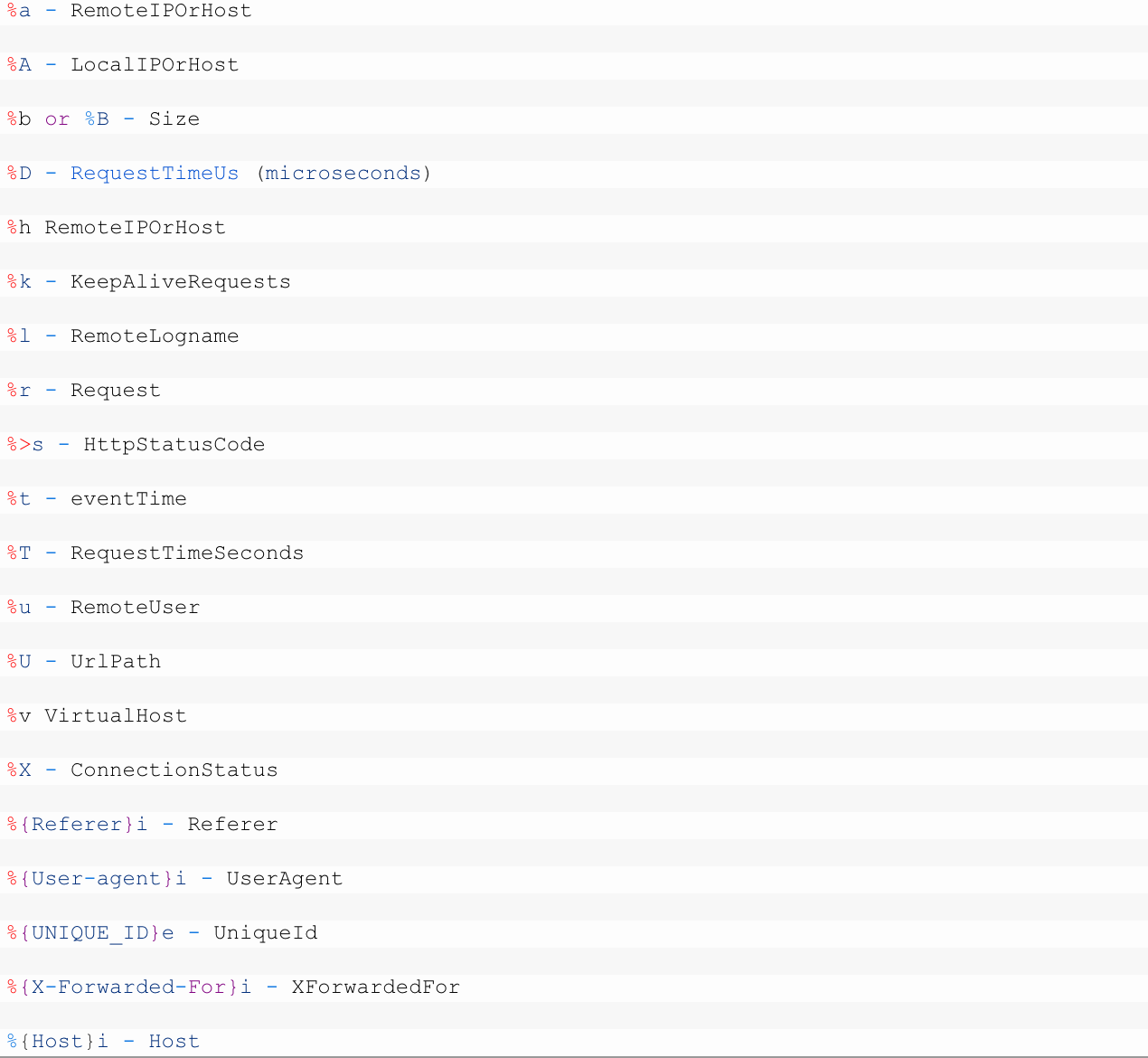
**1.Access log**

* Có chức năng ghi lại những lần sử dụng, truy cập, yên cầu đến apache server

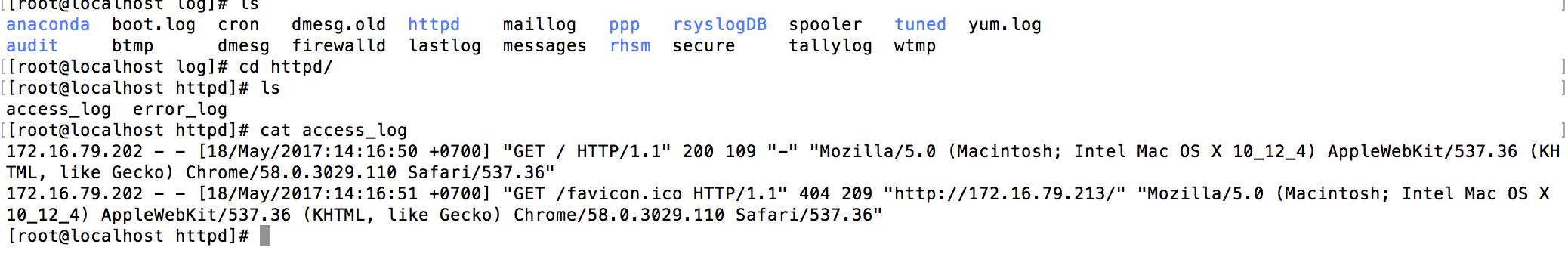
[https://camo.githubusercontent.com/de7998f6f5d87dccf4985845a34666ce1475529a/687474703a2f2f692e696d6775722e636f6d2f35506d6865586c2e706e67](https://camo.githubusercontent.com/de7998f6f5d87dccf4985845a34666ce1475529a/687474703a2f2f692e696d6775722e636f6d2f35506d6865586c2e706e67)

[](https://camo.githubusercontent.com/0e8821f53a0c695a099ae875c754bb1f5b62879f/687474703a2f2f692e696d6775722e636f6d2f34733245365a772e706e67)

* File log được lưu trữ tại /var/log/httpd/access\_log (hoặc /var/log/apache2/access.log)
* Định dạng log (LogFormat) cơ bản như sau là : %h %l %u %t %r %>s %b Refer User\_agent
* Trong đó:
  + %h: địa chỉ của máy client
  + %l: nhận dạng người dùng được xác định bởi identd (thường không SD vì không tin cậy)
  + %u: tên người dung được xác định bằng xác thức HTTP
  + %t: thời gian yêu cầu được nhận
  + %r: là yêu cầu từ người sử dụng (client)
  + %>s: mã trạng thái được gửi từ máy chủ đến máy khách
  + %b: kích cỡ phản hồi đối với client
  + Refer: tiêu đề Refeer của yêu cầu HTTP (chứa URL của trang mà yêu cầu này được khởi tạo)
  + User\_agent: chuỗi xác định trình duyệt
* Ở trên là 1 ví dụ về LogFormat của access log. Ngoài những trường trên còn có thêm 1 số trường khác như trong bảng định dạnh của file log như sau:

[](https://camo.githubusercontent.com/9ada3cd2238ebab704edbf76ee7b66bf7133d60e/687474703a2f2f692e696d6775722e636f6d2f58656e444c68432e706e67)

* Ví dụ như:

[](https://camo.githubusercontent.com/111799e7275b10e308b90468559ba5c1d79898ab/687474703a2f2f692e696d6775722e636f6d2f30364652674c632e706e67)

- 172:16.79.202: là địa chỉ IP của máy client truy cập tới apache server

- 2 trường %l %u không có giá trị sẽ hiển thị “-“

- 18/May/2017…. Là thời gian nhận được yêu cầu từ client

- GET/HTTP/1.1: là yêu cầu từ client

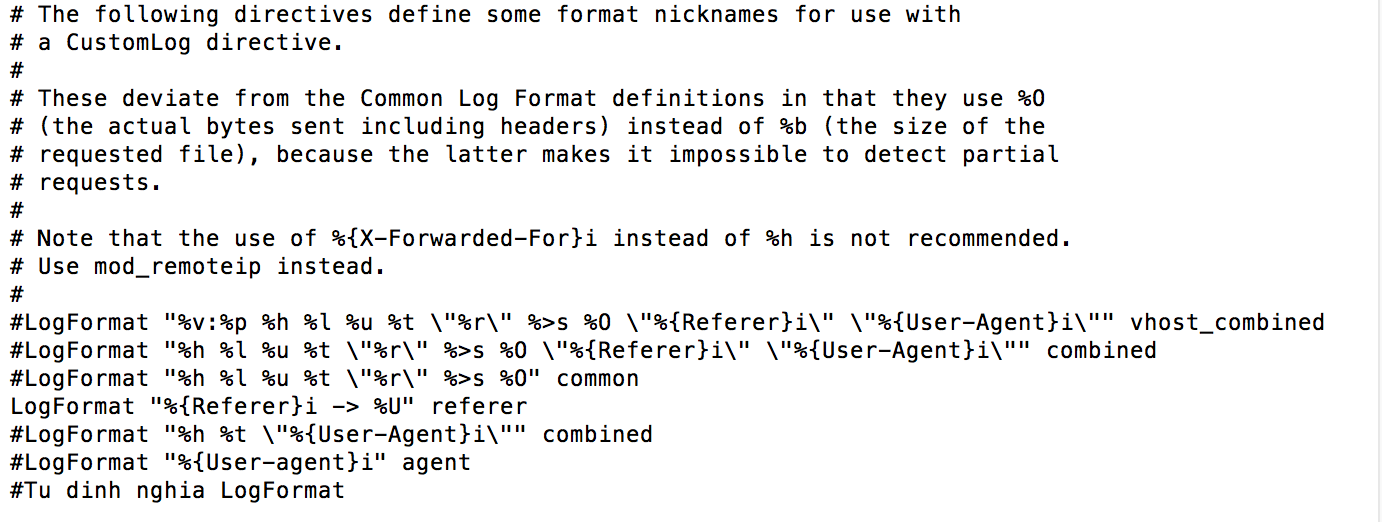
- 404: mã trạng thái gửi từ server đến client

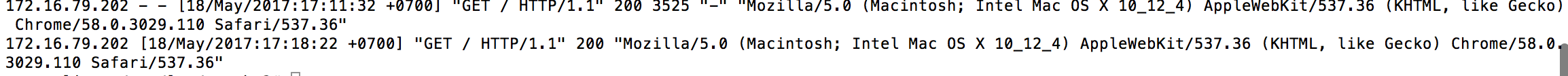
- 209: kich thước phản hồi lại client

- “http:/172.16.79.213”: url mà client yêu cầu tới server

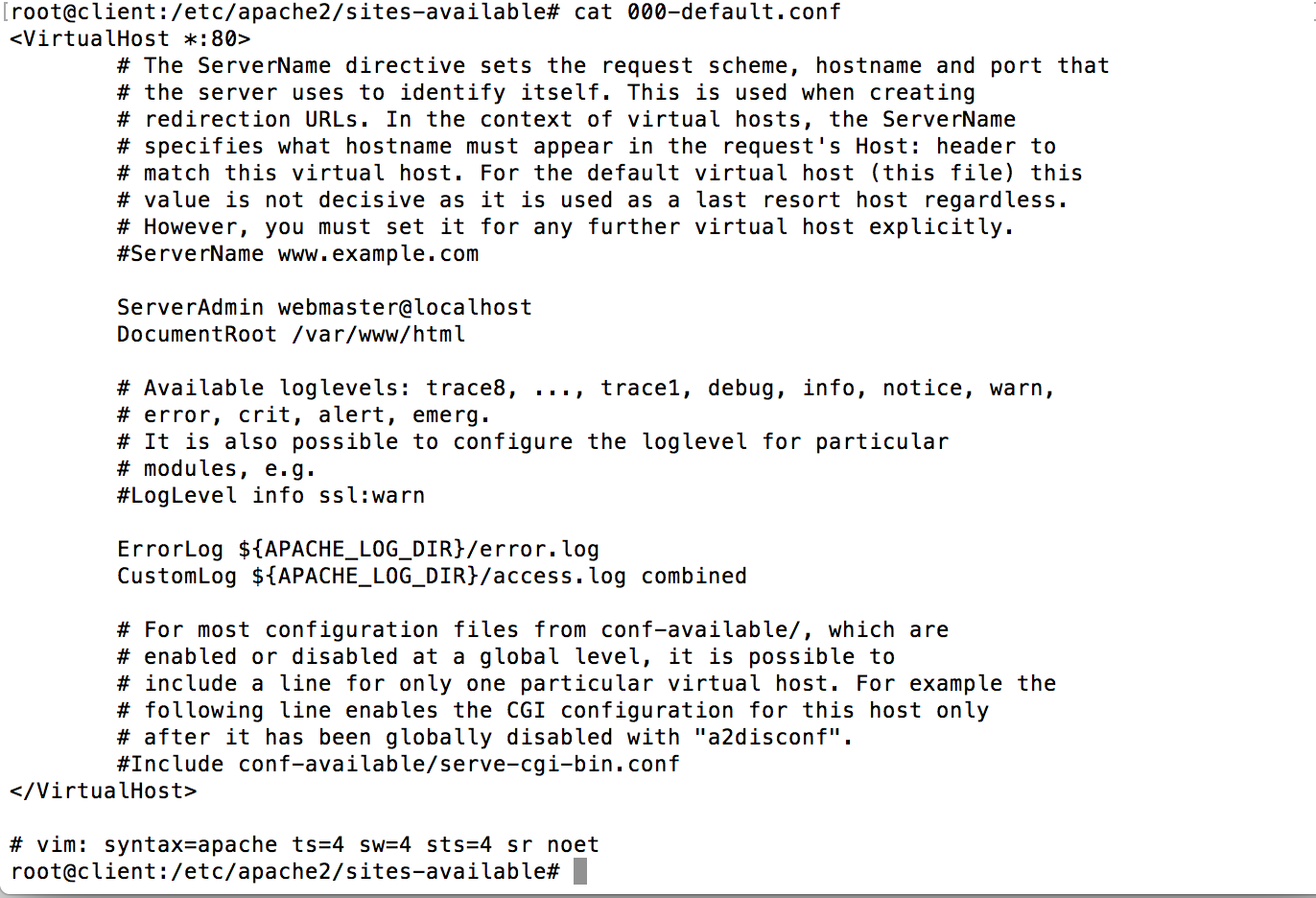
- Moliza …. Chrome, Safari: là chuỗi định danh trình duyệt

* Ngoài ra bạn còn có thể thay đổi Format của file log này trong file cấu hình của apache server đặt tại thư mục /etc/apache2/apache2.conf

[](https://camo.githubusercontent.com/6ec24a7c1b751fb10f07bb6e1ff163dad83f6ba8/687474703a2f2f692e696d6775722e636f6d2f30596858616f462e706e67)

[](https://camo.githubusercontent.com/30474ff02c890513001ded0fa8148dae78edb013/687474703a2f2f692e696d6775722e636f6d2f414d31486d73732e706e67)

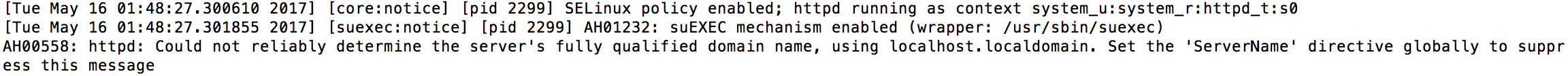
* Bạn cũng thể thay đổi vị trí lưu file log của mình bằng cách chỉnh sửa file cấu hình ở đường dẫn sau: /etc/apache2/sites-available/000-default.conf (đối với ubuntu)

[](https://camo.githubusercontent.com/45fa550f88c02b9c9de23eb7d7655fa94acca8db/687474703a2f2f692e696d6775722e636f6d2f58357a453869712e706e67)

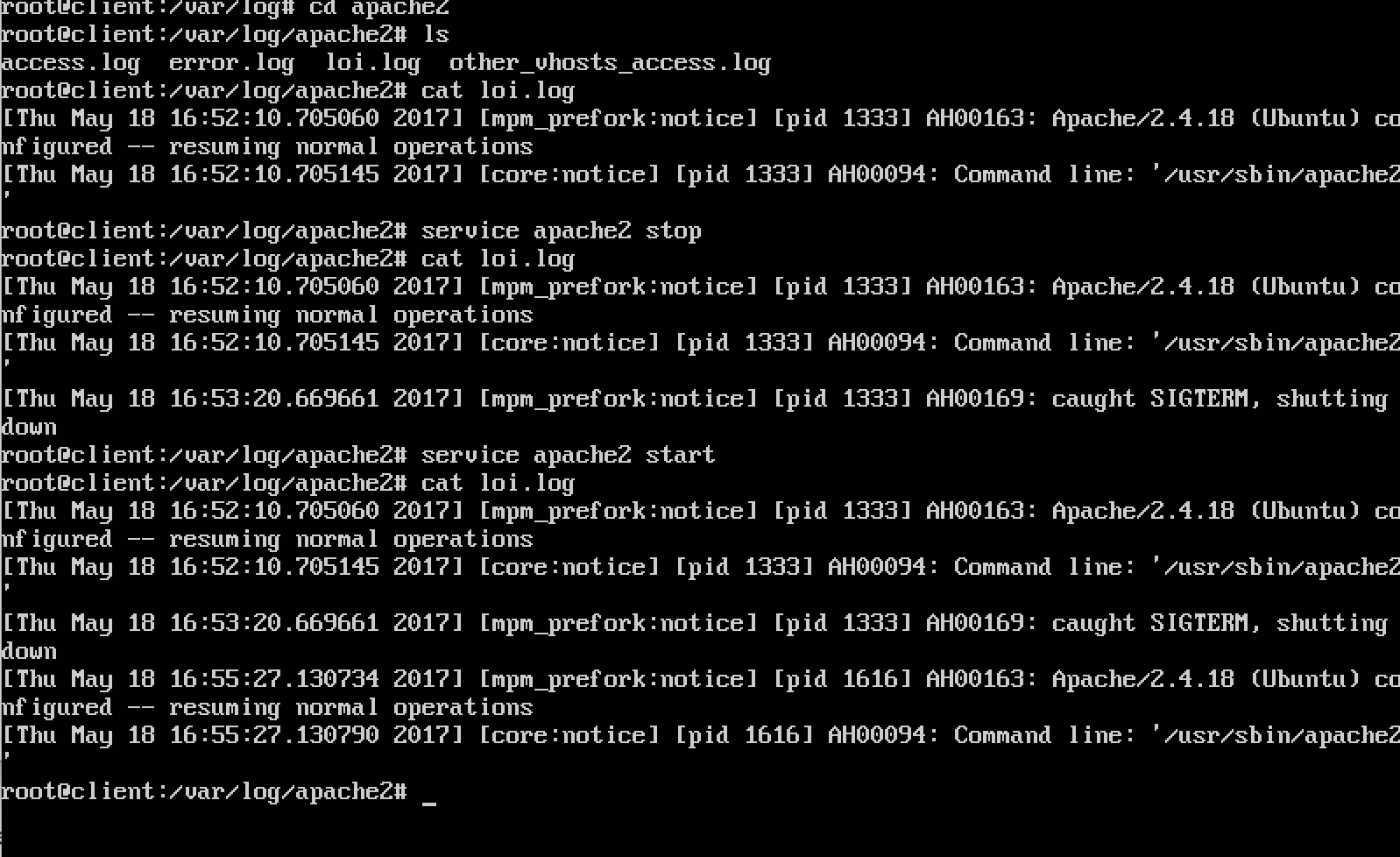
* Bạn cũng có thể thay đổi thư mục lưu file log tại trường APACHE\_LOG\_DIR trong file cấu hình /etc/apache2/envvars (file này như là 1 file thư viện định danh các biến hằng sử dụng trong các file cấu hình khác của apache)

**2. Error log**

* Chứa thông tin về lỗi mà máy chủ web gặp phải khi xử lý các yêu cầu, chẳng hạn như khi tệp bị thiếu.
* Là nơi đầu tiên để xem xét khi xảy ra sự cố khi khởi động máy chủ hoặc với hoạt động của máy chủ vì nó thường chứa thông tin chi tiết về những gì xảy ra và cách khắc phục
* Nơi lưu trữ file log là /var/log/httpd/error\_log (đối với centOs) và /var/log/apache2/error.log (đối với ubuntu)
* Định danh của error log tương đối tự do về mặt hình thức nhưng 1 số thông tin quan trọng có trong hầu hết các mục log như sau:
  + Trường thứ nhất: Trường thời gian - lưu thời gian nhận được message từ apache server
  + Trường thứ 2: liệt kê mức độ nghiêm trọng của lỗi được báo cáo
  + Trường thứ 3: Địa chỉ IP của client tạo ra lỗi
* Ví dụ:

[](https://camo.githubusercontent.com/1d5167bfd4554bfcd54ecb77500b29e09b51b66e/687474703a2f2f692e696d6775722e636f6d2f457148536c69522e706e67)

* Bạn cũng có thể thay đổi thư mục lưu trữ error log như đối với access log
* Ngoài ra bạn còn có thể đổi tên file error.log thành tên bạn mong muốn bằng cách sửa file config trong file cấu hình của apache /etc/apache2/apache2.conf:

[](https://camo.githubusercontent.com/3a489d9ff59b6dccc822e64a05304c6b37200327/687474703a2f2f692e696d6775722e636f6d2f6e6a4669714d6e2e706e67)