## **Họ và tên : Nguyễn Thị Thùy Linh**

**MSV: 22810310159**

## **1. Chặn phương thức TRACE**

Phương thức TRACE có thể bị lợi dụng trong các tấn công **XST (Cross-Site Tracing)**. Apache thường bật TRACE mặc định, nên cần vô hiệu hóa:

**Cách thực hiện:**

* Mở file cấu hình Apache (httpd.conf hoặc các file trong sites-available/sites-enabled).
* Thêm hoặc sửa directive:

# Tắt TRACE

TraceEnable Off

* Khởi động lại Apache để áp dụng:

sudo systemctl restart apache2 # Ubuntu/Debian

sudo systemctl restart httpd # CentOS/RHEL

* **Kiểm tra:**

curl -v -X TRACE <http://yourdomain.com>

Nếu trả về lỗi 405 Method Not Allowed hoặc không phản hồi TRACE là đúng.

**2. Cấu hình HSTS (HTTP Strict Transport Security)**

HSTS bắt buộc trình duyệt chỉ kết nối HTTPS, giúp chống **downgrade attack** và **man-in-the-middle**.

**Cấu hình Apache:**

* Mở file cấu hình site HTTPS (000-default-le-ssl.conf hoặc tương tự).
* Thêm header HSTS trong <VirtualHost \*:443>:

# Kích hoạt HSTS

<IfModule mod\_headers.c>

Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"

</IfModule>

**Giải thích:**

* max-age=31536000 → trình duyệt chỉ dùng HTTPS trong 1 năm.
* includeSubDomains → áp dụng cho tất cả subdomain.
* preload → gửi yêu cầu đưa site vào danh sách preload HSTS của trình duyệt (tùy chọn).
* Khởi động lại Apache:

sudo systemctl restart apache2

* **Kiểm tra:**

curl -I <https://yourdomain.com>

Header Strict-Transport-Security phải hiển thị.

**3. Giới hạn quyền truy cập**

Đảm bảo chỉ người dùng hoặc IP được phép mới truy cập vào các thư mục nhạy cảm.

### **a) Giới hạn theo thư mục**

Trong file .htaccess hoặc cấu hình <Directory>:

<Directory /var/www/html/admin>

Require ip 192.168.1.0/24

</Directory>

### **b) Giới hạn theo mật khẩu (Basic Auth)**

* Tạo file mật khẩu:

sudo htpasswd -c /etc/apache2/.htpasswd adminuser

* Thêm vào cấu hình Apache:

<Directory /var/www/html/admin>

AuthType Basic

AuthName "Restricted Area"

AuthUserFile /etc/apache2/.htpasswd

Require valid-user

</Directory>

* Khởi động lại Apache.

**4. Một số kiểm tra bảo mật thêm**

* **Kiểm tra header bảo mật:**

curl -I https://yourdomain.com

* Header cần có: Strict-Transport-Security, X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Content-Security-Policy.
* **Quét lỗ hổng:** Sử dụng Nikto hoặc OWASP ZAP để kiểm tra cấu hình Apache.