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

**MSV: 22810310159**

## **1. Tắt các phương thức HTTP không cần thiết**

IIS hỗ trợ nhiều phương thức HTTP (GET, POST, TRACE, PUT, DELETE…). Một số phương thức, như TRACE hoặc PUT, có thể gây rủi ro bảo mật.

**Cách thực hiện:**

1. Mở **IIS Manager**.
2. Chọn website cần cấu hình.
3. Vào **“HTTP Response Headers”** hoặc **“Request Filtering”**.
4. Chọn tab **“HTTP Verbs”** (Request Filtering → HTTP Verbs).
5. Chặn các phương thức không cần thiết, ví dụ:  
   * TRACE
   * PUT
   * DELETE

**Ví dụ chặn TRACE và PUT:**

* Trong IIS Manager → Site → Request Filtering → HTTP Verbs → “Deny Verb” → nhập TRACE và PUT.

**Kiểm tra:**

Invoke-WebRequest -Uri http://yourdomain.com -Method TRACE

Nếu trả về lỗi 405 → phương thức đã bị chặn.

**2. Bắt buộc HTTPS**

Đảm bảo mọi kết nối tới IIS đều sử dụng HTTPS để chống **MITM (Man-in-the-middle)** và các tấn công downgrade.

**Cách bật HTTPS bắt buộc:**

1. Mở IIS Manager → Chọn site → **SSL Settings**.
2. Chọn **Require SSL**.
3. Nếu muốn, tick **Require 128-bit SSL** để tăng cường bảo mật.
4. Thiết lập **HTTP → HTTPS Redirect**:  
   * Cài đặt module **HTTP Redirect**.
   * Tick **Redirect requests to this destination** → nhập https://yourdomain.com.
   * Tick **Redirect all requests** và **Permanent (301)**.
5. Kiểm tra: Truy cập http://yourdomain.com → tự động chuyển sang https://.

**Tăng cường HSTS trên IIS:**

* Vào **HTTP Response Headers** → “Add…”:

Name: Strict-Transport-Security

Value: max-age=31536000; includeSubDomains; preload

**3. Thiết lập quyền truy cập thư mục**

Ngăn chặn truy cập trái phép vào các thư mục nhạy cảm.

### **a) Giới hạn quyền theo NTFS**

* Chuột phải vào thư mục → **Properties → Security**.
* Chỉ cho phép các user hoặc nhóm cần thiết (IIS\_IUSRS, admin, hoặc nhóm cụ thể) có quyền **Read/Write**.
* Xóa quyền **Everyone** nếu không cần.

### **b) Giới hạn quyền truy cập trong IIS**

* IIS Manager → Chọn site → **Authentication**.
* Kích hoạt **Anonymous Authentication** nếu cho public, hoặc **Windows Authentication** / **Basic Authentication** cho user có mật khẩu.
* Với thư mục nhạy cảm (ví dụ /admin), có thể bật **Basic Authentication** và tắt **Anonymous Authentication**.

### **c) Chặn truy cập thư mục mặc định**

* Chặn các thư mục nhạy cảm (ví dụ /App\_Data, /bin) bằng **Request Filtering → Hidden Segments**.
* Thêm tên thư mục cần chặn để không ai có thể truy cập trực tiếp qua trình duyệt.

**4. Kiểm tra bảo mật thêm**

* **Kiểm tra các HTTP header bảo mật:**

Invoke-WebRequest -Uri https://yourdomain.com -Method GET

Header nên có:

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