UBND TỈNH TUYÊN QUANG
**SỞ KHOA HỌC VÀ CÔNG NGHỆ**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

Số: 112 /SKHCN-CĐS
V/v khắc phục lỗ hổng bảo mật Trang/Cổng thông tin điện tử

*Tuyên Quang, ngày 14 tháng 01 năm 2026*

Kính gửi: Công an tỉnh Tuyên Quang.

Ngày 06/01/2026 Sở Khoa học và Công nghệ nhận được Văn bản số 7604/CAT-ANM của Công an tỉnh Tuyên Quang về việc khắc phục lỗ hổng bảo mật Trang/Cổng thông tin điện tử trên địa bàn tỉnh;

Căn cứ Văn bản của các cơ quan, đơn vị: Số 35/SCT-VP ngày 07/01/2026 của Sở Công Thương; Số 51/SVHTTDL-VP ngày 09/01/2026 của Sở Văn hoá, Thể thao và Du lịch; Số 69/SNV-VP ngày 09/01/2026 của Sở Nội Vụ; Số 18/UBND-VP ngày 06/01/2026 của UBND xã Trường Sinh; Số 06/UBND-VHXH ngày 07/01/2026 của UBND xã Tân Mỹ; Số 13/UBND-VHXH ngày 08/01/2026 của UBND xã Tân Tiến; Số 21/UBND-VX ngày 09/01/2026 của UBND xã Lâm Bình; Số 16/UBND-VP ngày 09/01/2026 của UBND xã Tùng Bá; Số 28/UBND-HCC ngày 09/01/2026 của UBND xã Yên Phú; Số 18/CV-UBND ngày 10/01/2026 của UBND xã Tân Thanh; Số 26/UBND-VX ngày 10/01/2026 của UBND xã Tân Thành; Số 49/UBND-VP ngày 10/01/2026 của UBND xã Hùng An; Số 31/UBND-VX ngày 10/01/2026 của UBND xã Sơn Thuỷ về việc đề nghị hỗ trợ khắc phục lỗ hổng bảo mật Trang/Cổng thông tin điện tử.

Căn cứ chức năng, nhiệm vụ được giao, Sở Khoa học và Công nghệ đã rà soát, khắc phục lỗ hổng bảo mật Trang/Cổng thông tin điện tử theo đề nghị của các cơ quan, đơn vị.

*(Có danh sách kết quả xử lý gửi kèm)*

Sở Khoa học và Công nghệ trân trọng gửi Công an tỉnh tổng hợp./.

***Nơi nhận:***
- Như trên;
- Ban Giám đốc Sở (báo cáo);
- Các Sở, Ban, ngành (để biết);
- UBND các xã, phường (để biết);
- Lưu: VT, CĐS.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH TUYÊN QUANG

**Nguyễn Văn Hiến**

# DANH SÁCH KẾT QUẢ XỬ LÝ LỖ HỔNG BẢO MẬT

*(Kèm theo Công văn số 112 /SKHCN-CĐS ngày 14 /01/2026 của Sở Khoa học và Công nghệ)*

| Nội dung lỗi bảo mật | Các hoạt động đã thực hiện để khắc phục |
|---|---|
| **1. Nhóm lỗi liên quan đến SSL / TLS / Mã hóa đường truyền**<br>**1.1. Insecure Transportation Security Protocol Supported (TLS 1.0)**<br>Mô tả:<br>Máy chủ chấp nhận kết nối qua giao thức mã hóa cũ TLS 1.0. Đây là giao thức đã bị khai tử, chứa nhiều lỗ hổng và không còn an toàn theo các tiêu chuẩn bảo mật hiện đại.<br>Nguy cơ:<br>Kẻ tấn công đứng giữa (Man-in-the-middle) có thể giải mã dữ liệu truyền tải giữa người dùng và máy chủ, đánh cắp thông tin nhạy cảm (mật khẩu, cookie phiên).<br>**1.2. Insecure Transportation Security Protocol Supported (TLS 1.1)**<br>Mô tả:<br>Máy chủ vẫn hỗ trợ TLS 1.1 – một phiên bản giao thức mã hóa đã lỗi thời.<br>Nguy cơ:<br>Làm giảm mức độ an toàn của kênh truyền SSL/TLS, tăng nguy cơ bị tấn công giải mã dữ liệu.<br>**1.3. TLS/SSL Weak Cipher Suites**<br>Mô tả:<br>Máy chủ chấp nhận các bộ mã hóa yếu (Weak Cipher Suites) hoặc thuật toán mã hóa có độ dài khóa ngắn.<br>Nguy cơ:<br>Kẻ tấn công có thể khai thác để giải mã dữ liệu trao đổi giữa người dùng và máy chủ. | Cấu hình lại Web Server để vô hiệu hóa hoàn toàn giao thức TLS 1.0 và TLS 1.1. Chỉ cho phép sử dụng TLS 1.2 và TLS 1.3 để đảm bảo an toàn dữ liệu |
| **2. Nhóm lỗi Nội dung hỗn hợp (Mixed Content)**<br>**2.1. Nội dung hỗn hợp hoạt động trên giao thúc HTTPS (Active Mixed Content over HTTPS)**<br>Mô tả:<br>Trang web chạy HTTPS nhưng lại tải các tài nguyên động (script, iframe, object, media) thông qua giao thức HTTP không bảo mật.<br>Nguy cơ: | Đề xuất kiến nghị chỉ sử dụng ảnh up lên từ máy tính nội bộ, không sử dụng ảnh trực tiếp từ link trang web bên ngoài |

| Nội dung lỗi bảo mật | Các hoạt động đã thực hiện để khắc phục |
|---|---|
| Kẻ tấn công có thể thay đổi các tài nguyên HTTP này để chèn mã độc, lừa đảo người dùng hoặc thực thi mã trên trình duyệt.<br><br>**2.2. Nội dung hỗn hợp thụ động (Passive Mixed Content over HTTPS)**<br>Mô tả:<br>Website tải các nội dung thụ động (hình ảnh, video) qua HTTP trên nền trang HTTPS.<br>Nguy cơ:<br>Kẻ tấn công có thể thay đổi nội dung hiển thị, gây sai lệch thông tin hoặc phục vụ mục đích lừa đảo. | |
| **3. Lỗ hổng chuyển hướng mở (URL redirection / Open Redirection)**<br>Mô tả:<br>Ứng dụng web chấp nhận dữ liệu đầu vào từ người dùng để chuyển hướng mà không kiểm tra chặt chẽ tham số đích đến (đã kiểm thử với payload như //bxss.me).<br>Nguy cơ:<br>Kẻ tấn công có thể tạo các liên kết giả mạo trông giống tên miền chính thống để chuyển hướng người dùng sang website lừa đảo hoặc chứa mã độc (Phishing). | Kiểm tra và xử lý triệt để lỗ hổng Open Redirection bằng cách xác thực kỹ tham số đích đến (target URL) trước khi chuyển hướng |
| **4. Khung nhúng bên ngoài không an toàn (Insecure Frame)**<br>Mô tả:<br>Trang web cho phép nhúng hoặc bị nhúng bởi các khung (iframe/frame) từ nguồn bên ngoài mà không có chính sách kiểm soát (X-Frame-Options hoặc CSP).<br>Nguy cơ:<br>Dễ bị tấn công Clickjacking, đánh cắp thao tác người dùng hoặc chèn nội dung giả mạo lên giao diện chính thống. | Cấu hình Content-Security-Policy để ngăn chặn tấn công Clickjacking (Insecure Frame) |
| **5. Nhóm lỗi CORS – Chia sẻ tài nguyên chéo nguồn**<br>**5.1. Access-Control-Allow-Origin header with wildcard (*)**<br>**5.2. Misconfigured Access-Control-Allow-Origin Header**<br>Mô tả:<br>Header Access-Control-Allow-Origin được cấu hình là * hoặc cho phép các nguồn gốc không xác định truy cập tài nguyên. | Cấu hình lại CORS, thay giá trị * bằng danh sách các tên miền tin cậy cụ thể. |

| Nội dung lỗi bảo mật | Các hoạt động đã thực hiện để khắc phục |
|---|---|
| Nguy cơ:<br>Có thể dẫn đến rò rỉ dữ liệu nếu website có chức năng xác thực người dùng, tạo điều kiện cho các cuộc tấn công cross-origin. | |
| **6. Nhóm lỗi Lộ thông tin (Information Disclosure)**<br>**6.1. Nghi ngờ lộ địa chỉ IP nội bộ (Internal IP Address Disclosure)**<br>Mô tả:<br>Máy chủ có dấu hiệu để lộ địa chỉ IP nội bộ trong phản hồi HTTP (Header hoặc Body).<br>Nguy cơ:<br>Kẻ tấn công có thể thu thập thông tin cấu trúc mạng nội bộ để phục vụ tấn công sâu hơn.<br>**6.2. Lộ lọt địa chỉ Email (Generic Email Address Disclosure)**<br>Mô tả:<br>Website để lộ địa chỉ email chung trong mã nguồn hoặc giao diện.<br>Nguy cơ:<br>Dễ bị các công cụ tự động thu thập để gửi thư rác (Spam) hoặc thực hiện Phishing. | Rà soát code, ẩn hiển thị địa chỉ email, IP nội bộ trong phản hồi HTTP |
| **7. Nhóm lỗi Thiếu hoặc cấu hình sai Security Headers**<br>**7.1. HTTP Strict Transport Security (HSTS) Policy Not Enabled**<br>Mô tả:<br>Chưa ép buộc trình duyệt luôn sử dụng HTTPS.<br>Nguy cơ:<br>Tạo kẽ hở cho tấn công hạ cấp giao thức (SSL Stripping).<br>**7.2. Content Security Policy (CSP) Not Implemented**<br>Mô tả:<br>Chưa triển khai chính sách CSP để kiểm soát nguồn tải tài nguyên.<br>Nguy cơ:<br>Tăng rủi ro XSS và các cuộc tấn công phía trình duyệt.<br>**7.3. Permissions-Policy header not implemented**<br>Mô tả:<br>Chưa kiểm soát quyền truy cập các tính năng phần cứng/trình duyệt.<br>**7.4. X-Content-Type-Options (Missing Security Headers)** | Bổ sung các HTTP Security Headers (HSTS, CSP) |

| Nội dung lỗi bảo mật | Các hoạt động đã thực hiện để khắc phục |
|---|---|
| **7.5. Missing Security Headers**<br>Mô tả:<br>Thiếu các header bảo mật quan trọng như X-Content-Type-Options, Permissions-Policy.<br>Nguy cơ:<br>Giảm khả năng phòng vệ chiều sâu của website. | |
| **8. Cấu hình Cookie và Header chưa an toàn**<br>Chi tiết:<br>- Cookies Not Marked as Secure: Cookie phiên làm việc không có cờ Secure.<br>- Subresource Integrity (SRI) Not Implemented: Thiếu xác thực toàn vẹn tài nguyên.<br>- Permissions-Policy header not implemented: Chưa kiểm soát quyền truy cập tính năng trình duyệt. | - Cookie không được gắn cờ Secure là cookie lưu trạng thái của frontend, không ảnh hưởng đến bảo mật.<br>- SRI không khả thi trong trường hợp này: Các script ngoài không được đánh version trong URL, nếu đặt SRI web sẽ sập khi các script này cập nhật.<br>- Permission-Policy không có ý nghĩa trong trường hợp này: Firefox và Safari không hỗ trợ tính năng này, các trình duyệt Chromium-based đều xin phép trước khi sử dụng các permission mà header này có hiệu lực |
| **9. Nhóm lỗi Quản lý tài nguyên & Từ chối dịch vụ (DoS)**<br>**9.1. Lỗ hổng trong thư viện Axios (Allocation of Resources Without Limits or Throttling)**<br>**9.2. Lỗ hổng phân bổ tài nguyên không giới hạn trong axios (axios Allocation of Resources Without Limits or Throttling Vulnerability)**<br>Mô tả: | Axios là một client library để khởi tạo HTTP request. Việc hạn chế Axios không làm hạn chế tấn công DoS, kẻ tấn công |

| Nội dung lỗi bảo mật | Các hoạt động đã thực hiện để khắc phục |
|---|---|
| Hệ thống sử dụng thư viện axios có lỗ hổng cho phép phân bổ tài nguyên không giới hạn, không có cơ chế throttling phù hợp.<br>Nguy cơ:<br>Kẻ tấn công có thể gửi các yêu cầu đặc biệt làm cạn kiệt CPU/RAM, dẫn đến từ chối dịch vụ (DoS). | có thể tự gọi yêu cầu bằng các API khác |
| **10. Nhóm lỗi Dịch vụ & Cấu hình máy chủ**<br>**10.1. WebDAV Enabled (Dịch vụ WebDAV đang bật)**<br>Mô tả:<br>Máy chủ đang kích hoạt tiện ích mở rộng WebDAV (Web Distributed Authoring and Versioning) cho phép quản lý, chỉnh sửa tệp tin từ xa.<br>Vị trí ảnh hưởng: Đã xác thực tại /webdav/.<br>Nguy cơ:<br>Nếu cấu hình xác thực yếu hoặc có lỗ hổng, kẻ tấn công có thể lợi dụng WebDAV để tải lên mã độc (webshell), thay đổi giao diện hoặc xóa dữ liệu trên trang web.<br>**10.2. Path traversal via misconfigured NGINX alias**<br>Mô tả:<br>Cấu hình alias của Nginx không an toàn, cho phép truy cập tệp nằm ngoài thư mục webroot.<br>Nguy cơ:<br>Có thể đọc tệp hệ thống, mã nguồn hoặc cấu hình nhạy cảm. | - Cấu hình nginx của cổng chỉ sử dụng để reverse proxy, không hỗ trợ truy cập file tại chỗ trên webserver.<br>- Webserver không hỗ trợ WebDAV, truy cập /webdav trả về trang 404. |
| **11. Nhóm lỗi XSS – Cross-Site Scripting**<br>**11.1. Odoo XSS (CVE-2023-1434) (Lỗ hổng XSS trên nền tảng Odoo)**<br>**11.2. Lỗ hổng CVE-2023-1434**<br>Mô tả:<br>Lỗ hổng Cross-site Scripting phát sinh do thiết lập sai Content-Type tại một endpoint API của Odoo.<br>Nguy cơ:<br>Cho phép chèn mã JavaScript độc hại, đánh cắp phiên làm việc người dùng. | - Cổng thông tin không sử dụng Odoo |

| Nội dung lỗi bảo mật | Các hoạt động đã thực hiện để khắc phục |
|---|---|
| **12. SQL Injection (SQLi)**<br>Mô tả:<br>Lỗ hổng cho phép kẻ tấn công can thiệp vào các truy vấn mà ứng dụng thực hiện tới cơ sở dữ liệu. | - Toàn bộ truy vấn database đều sử dụng query builder, không ghép tham số trực tiếp.<br>- Webserver đã chặn SQL injection |