

Số: /TB-STTTT

Tây Ninh, ngày tháng 8 năm 2022

THÔNG BÁO

Về việc chào giá cung cấp dịch vụ “Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh năm 2022 (Hệ thống thông tin cấp độ 3)”

Căn cứ Quyết định số 848/QĐ-UBND ngày 07/4/2022 của Chủ tịch Ủy ban nhân dân tỉnh Tây Ninh Ban hành Kế hoạch chuyển đổi số và đảm bảo an toàn thông tin mạng tỉnh Tây Ninh năm 2022;

Sở Thông tin và Truyền thông Tây Ninh thông báo mời các đơn vị chào giá cung cấp dịch vụ “**Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh năm 2022 (Hệ thống thông tin cấp độ 3)**” chi tiết như phụ lục đính kèm.

Sở Thông tin và Truyền Thông kính mời quý đơn vị tham gia chào giá cạnh tranh cung cấp dịch vụ nêu trên.

Hồ sơ chào giá bao gồm Bảng chào giá cung cấp gói dịch vụ (Giá chào hàng bằng VNĐ, đã bao gồm thuế và chi phí triển khai, hỗ trợ cài đặt).

Thời gian nhận hồ sơ chào giá là 7 ngày tính từ ngày ra thông báo. Địa điểm nhận hồ sơ: 06 Trần Quốc Toản, Phường 2, Thành phố Tây Ninh, tỉnh Tây Ninh. Điện thoại: 0276 3 824666.

Trân trọng./.

Nơi nhận:

- Các Công ty cung cấp dịch vụ tin học, CNTT;
- Đăng thông báo lên cổng TTĐT Sở;
- Lưu: VT, TTGSĐH.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

PHỤ LỤC
Cung cấp dịch vụ “Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh năm 2022
(Hệ thống thông tin cấp độ 3)”

- Địa điểm thực hiện: Trung tâm tích hợp dữ liệu tỉnh Tây Ninh
- Nội dung thực hiện:

DANH SÁCH CÁC ỨNG DỤNG TRÊN NỀN TẢNG WEBSITE VÀ MOBILE CẦN ĐÁNH GIÁ AN TOÀN THÔNG TIN			
Stt	Ứng dụng	Ngôn ngữ lập trình	Ghi chú
Ứng dụng trên nền tảng Website			
1	https://ttgsdh.tayninh.gov.vn	Asp.net	Trang thông tin điện tử của Trung tâm Giám sát điều hành
2	https://chukyso.tayninh.gov.vn	Asp.net	Trang cung cấp thông tin về Đăng ký/cập nhật/xóa chữ ký số
3	https://hdnd1.tayninh.gov.vn	Asp.net	Hệ thống Hợp không giấy Hội đồng nhân dân tỉnh
4	https://rauquaantoan.tayninh.gov.vn	Php	Trang thông tin điện tử quảng bá rau sạch tỉnh Tây Ninh
5	https://bqlnuiba.tayninh.gov.vn	Php	Trang thông tin Ban Quản lý núi Bà
6	https://chuthapdo.tayninh.gov.vn	Php	Trang thông tin Hội Chũ thập đồ tỉnh
7	https://hoinongdan.tayninh.gov.vn	Php	Trang thông tin Hội Nông dân tỉnh
8	https://matrantuoc.tayninh.gov.vn	Php	Trang thông tin Mặt trận tổ quốc tỉnh
9	https://nganhangnhanuoc.tayninh.gov.vn	Php	Trang thông tin Ngân hàng nhà nước tỉnh
10	https://tinhdolan.tayninh.gov.vn	Php	Trang thông tin Tỉnh đoàn
11	https://ttxtdt.tayninh.gov.vn	Php	Trang thông tin Trung tâm xúc tiến đầu tư
12	https://trogiupphaply.tayninh.gov.vn	Php	Trang thông tin Trung tâm trợ giúp pháp lý

13	https://sotttt.tayninh.gov.vn	Php	Trang thông tin điện tử của Sở thông tin và Truyền thông	
14	https://tracnghiem.tayninh.gov.vn	Reactjs+asp.net	Trang tổ chức thi trắc nghiệm cho các đơn khi có nhu cầu.	
15	https://congthuong.tayninh.gov.vn	Reactjs+asp.net	Hệ thống quản lý điều hành ngành công thương	
16	https://khenthuong.tayninh.gov.vn	Reactjs+asp.net	Hệ thống quản lý hồ sơ thi đua khen thưởng điện tử	
Ứng dụng trên nền tảng Mobile				
1	Tây Ninh Smart	React-navite	Ứng dụng phản án hiện trường tỉnh Tây Ninh	
2	App Sự kiện	React-navite	Ứng dụng thông tin các sự kiện của tỉnh	
3	App GIS	React-navite	Ứng dụng Quản lý các trạm BTS trong tỉnh	
NỘI DUNG CHI TIẾT THỰC HIỆN CÔNG VIỆC				
Stt	Nội dung công việc	Chi tiết công việc	Đơn vị tính	Số lượng
A	Đánh giá ATTT hệ thống ứng dụng trên nền tảng WEB		Website	16
1	Kiểm thử, kiểm tra, đánh giá ATTT ứng dụng website			
1.1	Kiểm tra, đánh giá cấu hình			
	Khảo sát thu thập thông tin (qua search engine và web server, robot.txt)			
	Đánh giá cho ứng dụng dịch vụ front end (giao tiếp người dùng)			
	Đánh giá cho ứng dụng dịch vụ back -end (quản trị) của hệ thống Nhận diện framework, thư viện Đánh giá cấu hình			

	Đánh giá quản lý định danh			
		Đánh giá kết nối, đường truyền của ứng dụng (kiểm tra cấu hình triển khai https)		
		Kiểm tra HTTP Methods.		
		Kiểm tra HTTP Strict Transport Security (HSTS) header.		
		Kiểm tra Cross-Site Tracing (XST).		
		Kiểm tra DB Listener		
	Đánh giá quá trình xác thực			
		Kiểm tra thông tin đăng nhập truyền trên kênh truyền đã mã hóa		
		Kiểm tra thông tin đăng nhập mặc định		
		Kiểm tra cơ chế vô hiệu hóa tài khoản		
		Kiểm tra chức năng nhớ mật khẩu		
		Kiểm tra chức năng lưu cache trên trình duyệt		
		Kiểm tra chính sách đặt mật khẩu		
		Kiểm tra chính sách câu hỏi an toàn		
		Kiểm tra tính năng đổi hoặc reset mật khẩu		
		Kiểm tra cơ chế xác thực qua các kênh khác		

	Đánh giá quá trình phân quyền			
		Kiểm tra lỗ hổng directory traversal/file include)		
		Kiểm tra khả năng vượt qua cơ chế phân quyền		
	Đánh giá quản lý phiên đăng nhập			
		Kiểm tra khả năng vượt qua cơ chế quản lý phiên		
		Kiểm tra các thuộc tính của Cookies		
		Kiểm tra lỗi Session Fixation		
		Kiểm tra khả năng lộ dữ liệu trong các biến Session		
		Kiểm tra lỗi Cross Site Request Forgery		
		Kiểm tra tính năng đăng xuất		
		Kiểm tra thời gian hết hạn Session		
	Đánh giá quá trình kiểm soát dữ liệu đầu vào			
		Kiểm tra lỗi Reflected Cross Site		
		Scripting Kiểm tra lỗi Stored Cross Site Scripting		
		Kiểm tra lỗi HTTP Verb Tampering		
		Kiểm tra lỗi HTTP Parameter pollution		

		Kiểm tra lỗi SQL Injection		
		Kiểm tra lỗi LDAP Injection		
		Kiểm tra lỗi ORM Injection		
		Kiểm tra lỗi XML Injection		
		Kiểm tra lỗi SSI Injection		
		Kiểm tra lỗi XPath Injection		
		Kiểm tra lỗi IMAP/SMTP Injection		
		Kiểm tra lỗi Code Injection		
		Kiểm tra lỗi Local File Inclusion		
		Kiểm tra lỗi Remote File Inclusion		
		Kiểm tra lỗi Command Injection		
		Kiểm tra lỗi Buffer overflow		
		Kiểm tra lỗi Heap overflow		
		Kiểm tra lỗi Stack overflow		
		Kiểm tra lỗi Format string		
		Kiểm tra các lỗ hổng tiềm ẩn lâu dài		
		Kiểm tra lỗi HTTP Splitting/Smuggling		
	Đánh giá độ an toàn của mã hóa			
		Kiểm tra các thuật toán mã hóa yếu trong giao thức SSL/TLS, các cơ chế bảo vệ tầng vận chuyển không hiệu quả		

		Kiểm tra dữ liệu nhạy cảm bị truyền qua kênh không mã hóa		
	Đánh giá nền tảng ứng dụng (Improper Platform Usage)			
	Kiểm tra chức năng ngoài (Extraneous Functionality)			
1.2	Dò quét lỗ hổng tồn tại trên ứng dụng			
	Tấn công thử nghiệm khai thác lỗ hổng và khai thác thông tin:			
	<i>Dò quét chủ động</i>			
	<i>Dò quét thụ động</i>			
	<i>Kiểm tra false positive</i>			
	Đánh giá an toàn thông tin cho ứng dụng trên web			
2	Lập báo cáo kết quả kiểm tra, đánh giá an toàn thông tin ứng dụng web			
	Quá trình đánh giá			
	Phạm vi đánh giá (Đối tượng đánh giá + tiêu chí đánh giá).			
	Quy mô và nội dung đánh giá			
	Công cụ đánh giá.			
	Đưa ra danh sách các lỗ hổng có trên ứng dụng			
	Hướng dẫn khắc phục các lỗ hổng an toàn thông tin.			

3	Thông báo kết quả			
	Trao đổi và thống nhất kết quả đánh giá cuối cùng với đơn vị			
4	Lưu hồ sơ			
	Thực hiện lưu trữ toàn bộ hồ sơ liên quan đến quá trình kiểm tra đánh giá cho hệ thống thông tin.			
B	Đánh giá ATTT hệ thống ứng dụng trên nền tảng Mobile		Ứng dụng	03
1	Kiểm thử, kiểm tra đánh giá an toàn ứng dụng mobile			
1.1	Kiểm thử, kiểm tra, đánh giá cấu hình			
	Đánh giá cho ứng dụng dịch vụ front end (giao tiếp người dùng)			
	Đánh giá cho ứng dụng dịch vụ back end (quản trị) của hệ thống			
	Kiểm tra việc bảo vệ dữ liệu của ứng dụng			
	Kiểm tra các chức năng và kết nối mạng của ứng dụng			
	Kiểm tra việc kiểm duyệt dữ liệu đầu vào			
	Kiểm tra xác thực	Chức năng ghi nhớ thông tin xác thực.		
		Kiểm tra lỗ hổng xác thực phía người dùng.		
		Kiểm tra phiên người dùng không hợp lệ.		

		Xác thực thời gian phiên truy nhập.		
		Cookie Rotation. Thông tin đăng nhập đồng thời.		
		Nhận dạng thiết bị cụ thể trong Attacker Elements Visible.		
	Kiểm tra quản lý phiên			
		Kiểm tra phân quyền người dùng.		
		Tấn công IDOR.		
		Kiểm tra quản lý phiên.		
	Kiểm tra quản lý thông tin cá nhân			
	Thực hiện dịch ngược và phân tích			
		Dịch ngược ứng dụng (kiểm tra Obfuscating code)		
		Lộ thông tin / hardcode thông tin xác thực trong binaries.		
	Truyền dữ liệu không an toàn (Insecure Communication)			
		Sử dụng giao thức tầng vận chuyển không an toàn.		
		Sử dụng thuật toán không an toàn.		
		Kiểm tra vô hiệu hóa chứng chỉ.		
		Kiểm tra SSL pinning.		

		Mã hóa đầu cuối.		
	Mật mã kém (Insufficient Cryptography)			
		Mật mã lưu trữ.		
		Sử dụng các giao thức mã hóa.		
		Token/Tạo phiên và xử lý		
	Chất lượng client code (Client Code Quality)			
		Tấn công SQL injection vs LFI.		
		Kiểm tra tấn công injection.		
		Kiểm tra cấu trúc URL hoặc Deeplinks.		
		Kiểm tra việc che dấu thông tin nhạy cảm		
	Kiểm tra chức năng ngoài (Extraneous Functionality)			
		Kiểm tra gỡ rối ứng dụng.		
		Lộ mật khẩu/ chuỗi kết nối.		
		Kiểm tra chức năng ẩn		
1.2	Dò quét lỗ hổng tồn tại trên ứng dụng			
	Tấn công thử nghiệm khai thác lỗ hổng và khai thác thông tin:			
	<i>Dò quét chủ động</i>			
	<i>Dò quét thụ động</i>			
	<i>Kiểm tra false positive</i>			

	Đánh giá an toàn thông tin ứng dụng mobile			
2	Lập báo cáo kết quả kiểm tra, đánh giá an toàn thông tin ứng dụng mobile			
	Quá trình đánh giá Phạm vi đánh giá (Đối tượng đánh giá + tiêu chí đánh giá).			
	Quy mô và nội dung đánh giá			
	Công cụ đánh giá			
	Đưa ra danh sách các lỗ hổng có trên ứng dụng			
	Hướng dẫn khắc phục các lỗ hổng an toàn Thông tin.			
3	Thông báo kết quả			
	Trao đổi và thống nhất kết quả đánh giá cuối cùng với đơn vị			
4	Lưu hồ sơ			
	Thực hiện lưu trữ toàn bộ hồ sơ liên quan đến quá trình kiểm tra đánh giá cho hệ thống thông tin.			