PHẦN 2. ĐIỀU KHOẢN THAM CHIẾU
CHƯƠNG V. ĐIỀU KHOẢN THAM CHIẾU

I. Giới thiệu về dự án gói thầu:

1. Khái quát về gói thầu:

- Tên gói thầu: Đánh giá An toàn thông tin phần mềm nội bộ.

Thuộc các công trình:

Công trình 1: Nâng cấp phần mềm Quản lý công cụ dụng cụ

Công trình 2: Bổ sung Module đăng ký, tiếp nhận và giải quyết các yêu cầu dịch vụ điện gia tăng 24/7 trên hệ thống Quản trị chăm sóc khách hàng và hệ thống Tích hợp ứng dụng hiện trường Kinh doanh

Công trình 3: Bổ sung Module Báo cáo phục vụ công tác kinh doanh điện năng lấy dữ liệu đo xa tích hợp vào hệ thống "Tích hợp các ứng dụng phần mềm khối Kinh doanh và Dịch vụ khách hàng"

- Giá dự toán gói thầu: 159.244.615 đồng;
- Nguồn vốn: Khấu hao cơ bản;
- Thời gian tổ chức lựa chọn nhà thầu: 60 ngày;
- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý IV/2025;
- Hình thức, phương thức lựa chọn nhà thầu: Đấu thầu rộng rãi qua mạng, một giai đoạn hai túi hồ sơ;
- Loại hợp đồng: Trọn gói;
- Thời gian thực hiện gói thầu: 90 ngày;

2. Mô tả mục đích tuyển chọn nhà thầu:

- Việc tuyển chọn nhà thầu nhằm các mục đích sau:

o Lựa chọn được nhà thầu có đủ năng lực và kinh nghiệm, đáp ứng các yêu cầu của Bên mời thầu để thực hiện *Kiểm tra, đánh giá an toàn thông tin; Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống phần mềm công tác quản lý An toàn giai đoạn 3* trên cơ sở cạnh tranh, công bằng, minh bạch và hiệu quả kinh tế.

- Đảm bảo an toàn thông tin và đưa ra các cảnh báo trong quá trình khai thác và vận hành hệ thống công tác quản lý an toàn:
  + Phân tích kết quả dò quét, xác minh lỗ hổng tìm được và tấn công kiểm thử xâm nhập;
  + Đánh giá mức độ nguy hiểm của các lỗ hổng, các thành phần bị ảnh hưởng
  + Báo cáo, phân loại lỗ hổng. Phối hợp hỗ trợ khắc phục các lỗ hổng
  + Sau khi các lỗ hổng đã được khắc phục, tiến hành tái đánh giá các lỗ hổng đã tìm được trên các mục tiêu để đảm bảo các lỗ hổng đã được khắc phục hoàn toàn, không thể bị khai thác.

II. Phạm vi công việc:

1. Phạm vi công việc của nhà thầu:

– Đánh giá kiểm thử an toàn thông tin mức hạ tầng (VAPT – Vulnerabilty Assessment Penetration Testing):

- Thiết bị cân bằng tải, tường lửa ứng dụng.
- Máy chủ hệ thống ứng dụng: App, API, AI và cơ sở dữ liệu Database.

– Đánh giá an toàn thông tin mức ứng dụng (AST – Application Security Testing):
- Ứng dụng web.
- App trên thiết bị di động (Android/iOS).
- API kết nối đến các ứng dụng dịch vụ.

– Đánh giá an toàn mã nguồn ứng dụng:
- FrontEnd: Web, mobile (Android/iOS).
- Backend: API, AI, các service

2. Nhiệm vụ cụ thể nhà thầu cần thực hiện như sau:

TT	Hạng mục
1	**Khảo sát mục tiêu và thu thập thông tin về các thành phần thực hiện đánh giá bảo mật**
1.1	Khảo sát mục tiêu
1.2	Thu thập thông tin về các thành phần thực hiện đánh giá bảo mật
2	**Dò quét điểm yếu thông qua các công cụ dò quét điểm yếu thương mại, và dò quét theo các kịch bản nghiệp vụ ứng dụng**
2.1	Dò quét điểm yếu thông qua các công cụ dò quét điểm yếu thương mại
2.2	Dò quét theo các kịch bản nghiệp vụ ứng dụng
3	**Phân tích kết quả dò quét, xác minh lỗ hổng tìm được và tấn công kiểm thử xâm nhập**
3.1	Phân tích kết quả dò quét
3.2	Xác minh lỗ hổng tìm được
3.3	Tấn công kiểm thử xâm nhập
4	**Đánh giá mức độ nguy hiểm của các lỗ hổng, các thành phần bị ảnh hưởng**
4.1	Đánh giá mức độ nguy hiểm của các lỗ hổng, các thành phần bị ảnh hưởng
5	**Tái đánh giá các lỗ hổng đã báo cáo sau khi thực hiện khắc phục**
5.1	Tái đánh giá các lỗ hổng đã báo cáo sau khi thực hiện khắc phục

2.1. Nội dung thực hiện:

TT	Hạng mục	Đơn vị	Số lượng
A	**Nâng cấp phần mềm Quản lý công cụ dụng cụ**		
I	**Đánh giá an toàn thông tin hệ thống**		
	Kiểm thử hệ thống cân bằng tải, tường lửa ứng dụng	Thiết bị	03

1	- Kiểm tra, đánh giá cấu hình quản trị - Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị - Kiểm tra, đánh giá cấu hình chính sách tài khoản - Kiểm tra chính sách kết nối quản trị - Kiểm tra cấu hình log, giám sát		
2	**Kiểm thử hệ thống máy chủ** - Kiểm tra bản vá hệ điều hành - Kiểm tra, đánh giá cấu hình cập nhật hệ điều hành - Kiểm tra các cấu hình chính sách nội bộ (local policy) - Kiểm tra, đánh giá cấu hình chính sách tài khoản - Kiểm tra chính sách kết nối quản trị - Kiểm tra cấu hình log, giám sát	Máy chủ	02
II	**Đánh giá an toàn thông tin ứng dụng**		
1	**Ứng dụng trên nền tảng web** - Kiểm tra Quản lý cấu hình & triển khai - Kiểm tra Quản lý định danh - Kiểm tra Xác thực - Kiểm tra Phân quyền - Kiểm tra Quản lý phiên - Kiểm tra Sàng lọc dữ liệu đầu vào - Kiểm tra Cơ chế xử lý lỗi - Kiểm tra Thuật toán mã hóa - Kiểm tra Logic nghiệp vụ Kiểm tra Xử lý phía người dùng	Ứng dụng	01
3	**API ứng dụng** - Kiểm tra quản lý cấu hình và triển khai - Kiểm tra chứng thực & quản lý phiên - Kiểm tra phân quyền - Kiểm tra chơ chế mã hoá & ký API - Kiểm tra sàng lọc dữ liệu đầu vào Kiểm tra logic nghiệp vụ	Ứng dụng	01
III	**Đánh giá an toàn mã nguồn ứng dụng**		
	- Kiểm tra Sàng lọc dữ liệu đầu vào - Kiểm tra An toàn dữ liệu đầu ra - Kiểm tra Xác thực & Quản lý mật khẩu - Kiểm tra Quản lý phiên - Kiểm tra Quản lý truy cập - Kiểm tra Thuật toán mã hóa	Mã nguồn	02

	- Kiểm tra Cơ chế xử lý lỗi & Ghi nhật ký - Kiểm tra An toàn kênh truyền - Kiểm tra Cấu hình hệ thống - Kiểm tra An toàn cơ sở dữ liệu - Kiểm tra Quản lý tập tin Kiểm tra Quản lý bộ nhớ		
B	**Bổ sung Module đăng ký, tiếp nhận và giải quyết các yêu cầu dịch vụ điện gia tăng 24/7 trên hệ thống Quản trị chăm sóc khách hàng và hệ thống Tích hợp ứng dụng hiện trường Kinh doanh**		
I	**Đánh giá an toàn thông tin hệ thống**		
1	Kiểm thử hệ thống cân bằng tải, tường lửa ứng dụng - Kiểm tra, đánh giá cấu hình quản trị - Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị - Kiểm tra, đánh giá cấu hình chính sách tài khoản - Kiểm tra chính sách kết nối quản trị - Kiểm tra cấu hình log, giám sát	Thiết bị	03
2	Kiểm thử hệ thống máy chủ - Kiểm tra bản vá hệ điều hành - Kiểm tra, đánh giá cấu hình cập nhật hệ điều hành - Kiểm tra các cấu hình chính sách nội bộ (local policy) - Kiểm tra, đánh giá cấu hình chính sách tài khoản - Kiểm tra chính sách kết nối quản trị - Kiểm tra cấu hình log, giám sát	Máy chủ	8
II	**Đánh giá an toàn thông tin ứng dụng**		
1	**Ứng dụng trên nền tảng web** - Kiểm tra Quản lý cấu hình & triển khai - Kiểm tra Quản lý định danh - Kiểm tra Xác thực - Kiểm tra Phân quyền - Kiểm tra Quản lý phiên - Kiểm tra Sàng lọc dữ liệu đầu vào - Kiểm tra Cơ chế xử lý lỗi - Kiểm tra Thuật toán mã hóa - Kiểm tra Logic nghiệp vụ Kiểm tra Xử lý phía người dùng	Ứng dụng	02
	API ứng dụng	Ứng	02

2	- Kiểm tra quản lý cấu hình và triển khai - Kiểm tra chứng thực & quản lý phiên - Kiểm tra phân quyền - Kiểm tra chơ chế mã hoá & ký API - Kiểm tra sàng lọc dữ liệu đầu vào - Kiểm tra logic nghiệp vụ	dụng	
3	**Ứng dụng trên nền tảng mobile** - Kiểm tra Lưu trữ dữ liệu - Kiểm tra Mã hóa - Kiểm tra Xác thực cục bộ - Kiểm tra Giao tiếp mạng - Kiểm tra Tương tác nền tảng ứng dụng - Kiểm tra Chất lượng mã nguồn và cấu hình - Kiểm tra Khả năng chống dịch ngược Kiểm tra Logic nghiệp vụ	Ứng dụng	02
III	**Đánh giá an toàn mã nguồn ứng dụng**		
	- Kiểm tra Sàng lọc dữ liệu đầu vào - Kiểm tra An toàn dữ liệu đầu ra - Kiểm tra Xác thực & Quản lý mật khẩu - Kiểm tra Quản lý phiên - Kiểm tra Quản lý truy cập - Kiểm tra Thuật toán mã hóa - Kiểm tra Cơ chế xử lý lỗi & Ghi nhật ký - Kiểm tra An toàn kênh truyền - Kiểm tra Cấu hình hệ thống - Kiểm tra An toàn cơ sở dữ liệu - Kiểm tra Quản lý tập tin Kiểm tra Quản lý bộ nhớ	Mã nguồn	06
C	**Bổ sung Module Báo cáo phục vụ công tác kinh doanh điện năng lấy dữ liệu đo xa tích hợp vào hệ thống "Tích hợp các ứng dụng phần mềm khối Kinh doanh và Dịch vụ khách hàng"**		
I	**Đánh giá an toàn thông tin hệ thống**		
1	Kiểm thử hệ thống cân bằng tải, tường lửa ứng dụng - Kiểm tra, đánh giá cấu hình quản trị - Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị - Kiểm tra, đánh giá cấu hình chính sách tài khoản - Kiểm tra chính sách kết nối quản trị	Thiết bị	03

	- Kiểm tra cấu hình log, giám sát		
2	Kiểm thử hệ thống máy chủ - Kiểm tra bản vá hệ điều hành - Kiểm tra, đánh giá cấu hình cập nhật hệ điều hành - Kiểm tra các cấu hình chính sách nội bộ (local policy) - Kiểm tra, đánh giá cấu hình chính sách tài khoản - Kiểm tra chính sách kết nối quản trị - Kiểm tra cấu hình log, giám sát	Máy chủ	6
II	**Đánh giá an toàn thông tin ứng dụng**		
1	**Ứng dụng trên nền tảng web** - Kiểm tra Quản lý cấu hình & triển khai - Kiểm tra Quản lý định danh - Kiểm tra Xác thực - Kiểm tra Phân quyền - Kiểm tra Quản lý phiên - Kiểm tra Sàng lọc dữ liệu đầu vào - Kiểm tra Cơ chế xử lý lỗi - Kiểm tra Thuật toán mã hóa - Kiểm tra Logic nghiệp vụ Kiểm tra Xử lý phía người dùng	Ứng dụng	01
3	**API ứng dụng** - Kiểm tra quản lý cấu hình và triển khai - Kiểm tra chứng thực & quản lý phiên - Kiểm tra phân quyền - Kiểm tra chơ chế mã hoá & ký API - Kiểm tra sàng lọc dữ liệu đầu vào Kiểm tra logic nghiệp vụ	Ứng dụng	01
III	**Đánh giá an toàn mã nguồn ứng dụng**		
	- Kiểm tra Sàng lọc dữ liệu đầu vào - Kiểm tra An toàn dữ liệu đầu ra - Kiểm tra Xác thực & Quản lý mật khẩu - Kiểm tra Quản lý phiên - Kiểm tra Quản lý truy cập - Kiểm tra Thuật toán mã hóa - Kiểm tra Cơ chế xử lý lỗi & Ghi nhật ký - Kiểm tra An toàn kênh truyền - Kiểm tra Cấu hình hệ thống - Kiểm tra An toàn cơ sở dữ liệu - Kiểm tra Quản lý tập tin	Mã nguồn	02

	- Kiểm tra Quản lý bộ nhớ		

2.2. Các phương pháp đánh giá:

2.2.1. Đánh giá an toàn thông tin hệ thống:

➢ **Phạm vi đánh giá**

STT	Hạng mục	Mô tả
1	**Đánh giá an toàn thông tin hệ thống**	
1.1	**Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập, cụ thể các hạng mục sau:** - Máy chủ ứng dụng; - Máy chủ cơ sở dữ liệu. - Máy chủ API	- Thực hiện rà soát toàn bộ máy chủ, dò quét điểm yếu hạ tầng mức mạng (OS, service port, platform), phân tích điểm yếu để lên kịch bản và thực hiện tấn công các lỗ hổng sau khi được phê duyệt. - Thực hiện đánh giá cấu hình bảo mật hệ thống máy chủ, CSDL theo tiêu chuẩn CIS.
1.2	**Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập hệ thống mạng, bảo mật, cụ thể các hạng mục sau:** - Thiết bị cân bằng tải. - Thiết bị tường lửa ứng dụng.	Thực hiện rà soát thiết bị cân bằng tải và thiết bị tường lửa ứng dụng, dò quét điểm yếu hạ tầng mức mạng (OS, service port, IP protocol), phân tích điểm yếu để lên kịch bản và thực hiện tấn công các lỗ hổng sau khi được phê duyệt. Thực hiện đánh giá cấu hình bảo mật hệ thống mạng, bảo mật theo tiêu chuẩn CIS.

➢ **Cách thức đánh giá:**

Sử dụng kết hợp Technical Guide to Information Security Testing and Assessment (SP 800-115) của Viện tiêu chuẩn và công nghệ Hoa Kỳ (NIST), Open- source Security Testing Methodology Manual (OSSTMM) và tiêu chuẩn CIS Benchmark của Center for Internet Security cho việc kiểm soát đánh giá điểm yếu các thành phần trong hệ thống như máy chủ, thiết bị mạng.

➢ **Công cụ sử dụng:**

- Các công cụ thu thập thông tin:

STT	Công việc thực hiện	Công cụ sử dụng	Kết quả thu được
1	Dò quét các cổng dịch vụ	Nmap	Danh sách cổng mở
2	Xác định phần mềm, phiên bản phần mềm của cổng dịch vụ	Netcat, Telnet, Nmap, Nessus	Danh sách cổng mở, dịch vụ sử dụng, phiên bản phần mềm

3	Xác định hệ điều hành, phiên bản hệ điều hành	Nmap, Nessus	Hệ điều hành/Phiên bản hệ điều hành (OS) của từng mục tiêu

- Các công cụ dò quét:

STT	Công việc thực hiện	Công cụ sử dụng	Kết quả thu được
1	Dò quét, bẻ khóa mật khẩu	Hydra, Ncrack, Core Impact	Danh sách mục tiêu, tài khoản bị khai thác
2	Xác nhận các lỗ hổng	Metasploit, Public exploit (exploitdb, security forcus, …), custom scripts	Danh sách lỗ hổng đã khai thác được, minh chứng cho việc khai thác thành công (PoC)
3	Leo thang đặc quyền	Metasploit, windows-privesc-check, unix-privesc-check, other public exploits	Các lỗ hổng dẫn tới leo thang đặc quyền, dữ liệu lấy được qua việc khai thác lỗ hổng

2.2.2. Đánh giá bảo mật ứng dụng Web:

➢ **Phạm vi đánh giá:**

STT	Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập cho ứng dụng Web	
1	**Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập hệ thống**	- Thực hiện dò quét điểm yếu và kiểm thử xâm nhập mức ứng dụng (theo OWASP) cho các ứng dụng web-based được kết nối qua Internet và sử dụng nội bộ

➢ **Cách thức đánh giá:**

Thực hiện Đánh giá bảo mật ứng dụng Web-based dựa trên cơ sở Top 10 các lỗ hổng thường gặp được định nghĩa bởi tổ chức OWASP. Theo OWASP Testing Guide V4, các nhóm đánh giá bao gồm:

- Thu thập thông tin
- Kiểm tra Quản lý cấu hình & triển khai
- Kiểm tra Quản lý định danh
- Kiểm tra Xác thực
- Kiểm tra Phân quyền
- Kiểm tra Quản lý phiên
- Kiểm tra Sàng lọc dữ liệu đầu vào
- Kiểm tra Cơ chế xử lý lỗi
- Kiểm tra Thuật toán mã hóa
- Kiểm tra Logic nghiệp vụ

- Kiểm tra Xử lý phía người dùng

➢ **Công cụ thực hiện dò quét**

STT	Công việc thực hiện	Công cụ sử dụng	Kết quả thu được
1	Thu thập thông tin	Nmap, Burpsuite, dirbuster, whatweb, whatcms	- Danh sách các cổng dịch vụ chạy ứng dụng web - Danh sách framework, nền tảng được sử dụng tương ứng với từng ứng dụng web - Site map các website
2	Xác minh điểm yếu, kiểm thử xâp nhập	Metasploit, Burpsuite Professionals, SQLmap, và các công cụ mã nguồn mở, tự phát triển khác	Danh sách lỗ hổng đã khai thác được, minh chứng cho việc khai thác thành công (PoC)

2.2.3. Đánh giá bảo mật ứng dụng Mobile:

➢ **Phạm vi đánh giá:**

STT	Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập cho ứng dụng Mobile	
1	**Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập hệ thống trên thiết bị di động (IOS, Android)**	- Thực hiện dò quét điểm yếu và kiểm thử xâm nhập mức ứng dụng (theo OWASP) cho các ứng dụng trên thiết bị di động được kết nối qua Internet và sử dụng nội bộ

➢ **Cách thức đánh giá:**

Thực hiện Đánh giá bảo mật ứng dụng Mobile dựa trên cơ sở Top 10 các lỗ hổng thường gặp được định nghĩa bởi tổ chức OWASP. Theo OWASP Mobile Testing Guide, các nhóm đánh giá bao gồm:

- Kiểm tra Lưu trữ dữ liệu
- Kiểm tra Mã hóa
- Kiểm tra Xác thực cục bộ
- Kiểm tra Giao tiếp mạng
- Kiểm tra Tương tác nền tảng ứng dụng
- Kiểm tra Chất lượng mã nguồn và cấu hình
- Kiểm tra Khả năng chống dịch ngược
- Kiểm tra Logic nghiệp vụ

➢ **Công cụ thực hiện dò quét:**

STT	Công việc thực hiện	Công cụ sử dụng	Kết quả thu được

1	Thu thập thông tin	Nmap, Burpsuite, dirbuster, whatweb, whatcms	- Danh sách các cổng dịch vụ chạy ứng dụng web - Danh sách framework, nền tảng được sử dụng tương ứng với từng ứng dụng web - Site map các website
2	Xác minh điểm yếu, kiểm thử xâp nhập	Metasploit, Burpsuite Professionals, SQLmap, và các công cụ mã nguồn mở, tự phát triển khác	Danh sách lỗ hổng đã khai thác được, minh chứng cho việc khai thác thành công (PoC)

2.2.4. Đánh giá bảo mật API ứng dụng:

➢ **Phạm vi đánh giá:**

STT	Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập cho API ứng dụng	
1	**Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập ứng dụng API**	- Thực hiện dò quét điểm yếu và kiểm thử xâm nhập mức API (theo OWASP) cho các API được kết nối qua Internet và sử dụng nội bộ

Cách thức đánh giá:

Thực hiện Đánh giá bảo mật ứng dụng API dựa trên cơ sở Top 10 các lỗ hổng thường gặp được định nghĩa bởi tổ chức OWASP. Các bước đánh giá bao gồm:

- Thu thập thông tin
- Kiểm tra quản lý cấu hình và triển khai
- Kiểm tra chứng thực & quản lý phiên
- Kiểm tra phân quyền
- Kiểm tra cơ chế mã hoá & ký API
- Kiểm tra sàng lọc dữ liệu đầu vào
- Kiểm tra logic nghiệp vụ

➢ **Công cụ thực hiện dò quét:**

STT	Công việc thực hiện	Công cụ sử dụng	Kết quả thu được
1	Thu thập thông tin	Nmap, Burpsuite, dirbuster, whatweb, whatcms	- Danh sách các cổng dịch vụ chạy ứng dụng web - Danh sách framework, nền tảng được sử dụng tương ứng với từng ứng dụng web - Site map các website
2	Xác minh điểm yếu, kiểm thử xâp nhập	Metasploit, Burpsuite Professionals, SQLmap, và	Danh sách lỗ hổng đã khai thác được, minh chứng cho

		các công cụ mã nguồn mở, tự phát triển khác	việc khai thác thành công (PoC)

2.2.5. Đánh giá an toàn mã nguồn ứng dụng:

➢ **Phạm vi đánh giá:**

STT	Dò quét lỗ hổng bảo mật và kiểm thử xâm nhập cho ứng dụng Mobile	
1	**Đánh giá an toàn mã nguồn ứng dụng:**	- Thực hiện đánh giá an toàn mã nguồn ứng dụng cho các ứng dụng được kết nối qua Internet và sử dụng nội bộ

➢ **Cách thức đánh giá:**

Việc Đánh giá mã nguồn ứng dụng nhắm đến xác định các lỗi bảo mật của ứng dụng không thể phát hiện thông qua các phương pháp đánh giá truyền thống. Ngoài ra việc đánh giá mã nguồn còn giúp đảm bảo các cơ chế, phương pháp kiểm soát theo các tiêu chuẩn, thực tiễn tốt nhất được áp dụng để giảm thiểu các rủi ro có thể xảy ra.

Thực hiện Đánh giá mã nguồn ứng dụng dựa trên cơ sở các thực tiễn tốt nhất về lập trình an toàn (OWASP Secure Coding Practices) được định nghĩa bởi tổ chức OWASP.

3. Dự kiến thời gian chuyên gia bắt đầu thực hiện dịch vụ tư vấn:

- Thời gian dự kiến thực hiện: Sau khi hợp đồng có hiệu lực

III. Báo cáo và thời gian thực hiện:

➢ Các báo cáo sẽ cung cấp thông tin chi tiết cho các hạng mục đánh giá bao gồm 02 phần chính:

- Báo cáo tổng quan:
  + Tổng quan dự án: Phạm vi và phương pháp đánh giá.
  + Thông tin tổng quan: Tóm lược các lỗ hổng và kịch bản tấn công có thể thực hiện.
  + Thống kê: Danh sách các lỗ hổng, mức độ nghiêm trọng và khuyến nghị.
- Báo cáo chi tiết kỹ thuật:
  + Phương pháp: Cách thức phát hiện lỗ hổng (mô tả phương pháp tấn công, mã khai thác) và các công cụ thực hiện.
  + Mô tả lỗ hổng và mối đe dọa.
  + Ảnh hưởng: Các ảnh hưởng có thể xảy ra khi lỗ hổng bị khai thác (bao gồm ảnh hưởng đến hoạt động của doanh nghiệp).
  + Phân loại mức độ nghiêm trọng: Thấp, Trung Bình, Cao hay Nghiêm Trọng dựa trên múc độ ảnh hưởng và khả năng bị khai thác.
  + Các phát hiện và bằng chứng khai thác: hình ảnh, video, các gói tin bắt được.
  + Khuyến nghị: Phương pháp vá lỗ hổng, tham chiếu đến giải pháp chính thức của OWASP và cụ thể cho hiện trạng của khách hàng.

❖ **Các mẫu báo cáo chi tiết:**

THÔNG TIN RỦI RO	
Nhóm	LỖ HỔNG MÁY CHỦ WEB
CVE	CVE-2014-0160
CVSS	
Mô tả	Lỗ hổng Heart Bleed (cve-2014-0160) là lỗ hổng trong phần mở rộng TLS/DTLS Heartbeat (RFC6520) của OpenSSL, một thư viện phổ biến sử dụng cho SSL/TLS Lỗ hổng nghiêm trọng này đã được gán mã số ID CVE-2014-0160, cho phép kẻ tấn công có thể đọc được 64kB trong bộ nhớ của máy chủ hoặc một máy tính đang vận hành phiên bản OpenSSL bị lỗi. Nói một cách dễ hiểu, thông qua lỗ hổng này kẻ tấn công có thể đánh cắp được các chìa khóa mã hóa private keys, mật khẩu và các thông tin bí mật từ xa (remotely).
Mức độ	NGHIÊM TRỌNG

Ảnh hưởng	CAO	KHẢ NĂNG XẢY RA	CAO

Khuyến nghị	Cập nhật Open SSL lên phiên bản 1.0.1g
Tham chiếu	http://heartbleed.com/ https://www.openssl.org/news/secadv/20140407.txt https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160
CHI TIẾT VỀ RỦI RO	
Chức năng	**SSL/TLS**
Ảnh hưởng	news.abc.com.vn:443
	Kẻ tấn công có thể đọc được 64kB trong bộ nhớ của máy chủ web bao gồm cả những thông tin nhạy cảm của ứng dụng như thông tin đăng nhập và các dữ liệu quan trọng
Khuyến nghị	Cập nhật Open SSL lên phiên bản 1.0.1g hoặc cập nhật phần mềm Web Server lên phiên bản sử dụng thư viện OpenSSL không bị lỗ hổng.
Điều kiện	Người Dùng Khách/Guest

```
THREADS => 24
msf auxiliary(openssl_heartbleed) > set ShowProgress 1
ShowProgress => 1
msf auxiliary(openssl_heartbleed) > set TLSVERSION 1.0
TLSVERSION => 1.0
msf auxiliary(openssl_heartbleed) > set TCP::max_send_size 0
TCP::max_send_size => 0
msf auxiliary(openssl_heartbleed) > set ShowProgressPercent 10
ShowProgressPercent => 10
msf auxiliary(openssl_heartbleed) > set STARTTLS None
STARTTLS => None
msf auxiliary(openssl_heartbleed) > set RHOSTS
RHOSTS =>
msf auxiliary(openssl_heartbleed) > run -j
[*] Auxiliary module running as background job
[*]             - Sending Client Hello...
[*]             - Sending Heartbeat...
[*]             - Heartbeat response, checking if there is data leaked...
[+]             - Heartbeat response with leak
[*]             - Printable info leaked: @SDWdy8-j${lUf"!98532ED/A
[*] Scanned 1 of 1 hosts (100% complete)
msf auxiliary(openssl_heartbleed) >
```

Mẫu báo cáo kiểm thử xâm nhập ứng dụng

THÔNG TIN LỖ HỔNG	
Nhóm	KIỂM TRA AN TOÀN DỮ LIỆU ĐẦU VÀO
Mô tả	Chức năng chưa lọc kĩ đầu vào từ người dùng. Kẻ tấn công có thể chèn các script độc hại nhằm đánh cắp cookie, session hoặc làm bàn đạp để thực hiện các kĩ thuật tấn công khác.
Mức độ	NGHIÊM TRỌNG

Ảnh hưởng	CAO	KHẢ NĂNG XẢY RA	CAO
Khuyến nghị	Nguyên nhân dẫn đến lỗ hổng SQL Injection do trong quá trình tạo thành câu truy vấn từ các tham số đầu vào, nhà phát triển nối chuỗi các tham số trực tiếp vào câu truy vấn, khiến cho các đoạn SQL được chèn thêm và thực thi. Vì vậy để khắc phục cần thực hiện theo một trong những cách sau: áp dụng cho từng ngôn ngữ, thư viện lập trình có hỗ trợ các hàm safe query sql, truyền giá trị theo tham số (parameterized query) hoặc phải làm sạch dữ liệu đầu vào. Các hướng fix: Option #1: Use of Prepared Statements (Parameterized Queries) Option #2: Use of Stored Procedures (tránh nối chuỗi trong Store) Option #3: Escaping all User Supplied Input		
Tham chiếu	https://www.owasp.org/index.php/SQL_Injections Cheatsheet: https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet		
THÔNG TIN CHI TIẾT LỖ HỔNG			
Chức năng	**View (News)**		
URL	http://localhost:8088/abc/view.php?id=1		
Kịch bản	Kẻ tấn công có thể lợi dụng lỗ hổng này thực thi câu truy vấn ở CSDL và tiến hành trích xuất dữ liệu trong đó. Có thể lấy được đầy đủ dữ liệu theo phạm vi quyền hạn của tài khoản đang sử dụng để kết nối CSDL.		
Tham số	Id		
Điều kiện	Anonymous User		

ADDITIONAL GET /abc/view.php?id=**0%20union%20select %201,version(),3,current_user** HTTP/1.1 Host: localhost:8088 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:44.0) Gecko/20100101 Firefox/44.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=tvhni9ho7qu00k37qh77iqtat1 Connection: keep-alive	
HTTP/1.1 200 OK Date: Fri, 06 May 2016 07:46:51 GMT Server: Apache/2.4.18 (Unix) OpenSSL/1.0.2g PHP/7.0.5 mod_perl/2.0.8-dev Perl/v5.16.3 X-Powered-By: PHP/7.0.5 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Content-Length: 4053 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8	

➢ **Thời hạn nộp báo cáo:**

- **Báo cáo đánh giá cho mỗi hệ thống:** Không quá 05 ngày kể từ ngày hoàn thành đánh giá cho mỗi hệ thống nhà thầu có trách nhiệm gửi Báo cáo kết quả đánh giá và hướng dẫn khắc phục các lỗ hổng đã phát hiện cho toàn bộ các hệ thống được đánh giá.
- **Báo cáo kết quả tái đánh giá cho mỗi hệ thống**: Trong vòng 05 ngày kể từ ngày nhận được yêu cầu tái đánh giá các hệ thống, nhà thầu có trách nhiệm gửi Báo cáo kết quả tái đánh giá cho hệ thống phần mềm đó.

IV. Kinh nghiệm và nhân sự của nhà thầu:

1. Năng lực kinh nghiệm của nhà thầu:

Đáp ứng quy định tại Mục 2. Tiêu chuẩn đánh giá về kỹ thuật, Chương III của E-HSMT.

2. Yêu cầu về nhân sự:

Đáp ứng quy định tại Mục 2. Tiêu chuẩn đánh giá về kỹ thuật, Chương III của E-HSMT

V. Trách nhiệm của Chủ đầu tư:

- Cử cán bộ tham gia phối hợp với nhà thầu để thực hiện công việc trong phạm vi công việc mà nhà thầu thực hiện.
- Giám sát, kiểm tra và đôn đốc Nhà thầu thực hiện gói thầu.
- Bố trí địa điểm làm việc phục vụ cho chuyên gia của Nhà thầu đến thực hiện công việc theo thỏa thuận (nếu có).
- Cung cấp các tài liệu, thông tin có liên quan đến nội dung công việc, giúp đỡ bên nhận thầu thực hiện công việc.
- Phối hợp với Nhà thầu tiến hành nghiệm thu các công việc, nghiệm thu hoàn thành gói thầu theo quy định.
- Cùng với Nhà thầu giải quyết các vướng mắc phát sinh trong quá trình thực hiện gói thầu.