NGÂN HÀNG TMCP THỊNH VƯỢNG VÀ PHÁT TRIỂN

Hà nội, ngày 28 tháng 08 năm 2024

THƯ MỜI CHÀO HÀNG CẠNH TRANH

Kính gửi: Quý Công ty

Ngân hàng TMCP Thịnh vượng và Phát triển (PGBank) chuẩn bị tổ chức chào hàng cạnh tranh gói mua sắm ***"Triển khai thuê dịch vụ rà quét, đánh giá, kiểm thử các ứng dụng, dịch vụ quan trọng của PGBank."*** tại Tầng 24 – Tòa Mipec - 229 Tây Sơn - Quận Đống Đa - Hà Nội. Trân trọng kính mời Quý Công ty quan tâm tham gia chào hàng cạnh tranh gói mua sắm nêu trên.

Quý Công ty sẽ được cung cấp bộ hồ sơ yêu cầu tại website Ngân hàng TMCP Thịnh vượng và Phát triển: https://www.pgbank.com.vn/.

Thời gian phát hành hồ sơ yêu cầu từ 16 giờ 00 ngày 28 tháng 08 năm 2024 đến trước 16 giờ 00 ngày 12 tháng 09 năm 2024. (giờ Việt Nam)

Hồ sơ chào hàng cạnh tranh phải được gửi đến Ngân hàng TMCP Thịnh vượng và Phát triển muộn nhất là trước 15 giờ 00, ngày 12 tháng 09 năm 2024.

Hồ sơ phải được niêm phong kín bên ngoài ghi rõ "**Triển khai thuê dịch vụ rà quét, đánh giá, kiểm thử các ứng dụng, dịch vụ quan trọng của PGBank.**". Hồ sơ chào hàng cạnh tranh sẽ không hợp lệ và bị loại nếu không có niêm phong, niêm phong bị hư hại hoặc gửi tới địa chỉ trên quá giờ quy định ở trên.

PGBank thực hiện nhận HSĐX/báo giá, mở HSĐX/báo giá có thể nhiều hơn 01 lần. Sau thời hạn báo giá lần đầu, PGBank thực hiện mở HSĐX/báo giá và PGBank được quyền yêu cầu NCC đã gửi HSĐX/báo giá thực hiện đàm phán giá, điều kiện thương mại. PGBank có thể nhận HSĐX/báo giá và mở HSĐX/báo giá trong các lần tiếp theo theo thông báo bằng thư điện tử (email) của PGBank nhằm đạt được mức giá tối ưu nhất, tùy vào thực tế việc chào hàng.

Nếu Quý Công ty cần biết thêm thông tin, xin vui lòng liên hệ với đầu mối như bên dưới.
Hồ sơ đề xuất xin vui lòng gửi về địa chỉ:
Ngân Hàng TMCP Thịnh vượng và Phát triển
Tầng 24, Tòa nhà Mipec, 229 Tây Sơn, Đống Đa, Hà Nội
Người nhận: **Mr. Trần Hải Hoàng - Trung tâm mua sắm** - 0932641723

ĐẠI DIỆN NGÂN HÀNG TMCP THỊNH VƯỢNG VÀ PHÁT TRIỂN

M.S.D.N: 1400114233 - C.T.C.P - NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN THỊNH VƯỢNG VÀ PHÁT TRIỂN - Q. ĐỐNG ĐA - T.P HÀ NỘI

PHÓ TỔNG GIÁM ĐỐC ĐIỀU HÀNH

Trần Văn Luân

HỒ SƠ MỜI CHÀO HÀNG CẠNH TRANH

Gói mua sắm: **Triển khai thuê dịch vụ rà quét, đánh giá, kiểm thử các ứng dụng, dịch vụ quan trọng của PGBank.**

Bên mời chào hàng cạnh tranh: Ngân hàng TMCP Thịnh vượng và Phát triển (PGBank)

M.S.D.N: 1400116233-C.T.C.P
NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN THỊNH VƯỢNG VÀ PHÁT TRIỂN
Q. ĐỐNG ĐA - T.P HÀ NỘI

PHÓ TỔNG GIÁM ĐỐC ĐIỀU HÀNH

Trần Văn Luân

ĐẠI DIỆN BÊN CHÀO HÀNG CẠNH TRANH

PHẦN A. TỪ NGỮ VIẾT TẮT

PGBANK	Ngân hàng TMCP Thịnh vượng và Phát triển
CHCT	Chào hàng cạnh tranh
HSYC	Hồ sơ yêu cầu
HSĐX	Hồ sơ đề xuất
HSĐXKT	Hồ sơ đề xuất kỹ thuật
HSĐXTC	Hồ sơ đề xuất tài chính
VND	Đồng Việt Nam

PHẦN B. CHỈ DẪN ĐỐI VỚI NHÀ CUNG CẤP

Mục 1. Nội dung mời chào hàng cạnh tranh

1. PGBank mời nhà cung cấp tham gia chào hàng cạnh tranh gói CHCT được mô tả tại **Mục 2** của phần này.
2. Tên gói CHCT: **Triển khai thuê dịch vụ rà quét, đánh giá, kiểm thử các ứng dụng, dịch vụ quan trọng của PGBank.**
3. Loại hợp đồng: trọn gói

Mục 2. Thời hạn triển khai

Trong 12 tháng từ ngày ký hợp đồng

Mục 3. Hiện trạng và mục tiêu đầu tư

1. **Hiện trạng**

PGBank đang có nhu cầu "**Triển khai thuê dịch vụ rà quét, đánh giá, kiểm thử các ứng dụng, dịch vụ quan trọng của PGBank**"

2. **Mục tiêu đầu tư**

Triển khai thuê dịch vụ rà quét, đánh giá, kiểm thử các ứng dụng, dịch vụ quan trọng này giúp PGBank:

- Phát hiện sớm nguy cơ, lỗ hổng trên các thiết bị và ứng dụng
- Kịp thời ngăn chặn kẻ tấn công, khai thác điểm yếu
- Giảm thiểu những nguy cơ mất an toàn thông tin và sự cố tấn công mạng xảy ra

Mục 4. Nội dung của HSĐX

HSĐX do nhà cung cấp chuẩn bị phải bao gồm:

1. Đơn chào hàng;
2. Tài liệu chứng minh tư cách hợp lệ của nhà cung cấp.
3. Hồ sơ đề xuất kỹ thuật đáp ứng các yêu cầu của PGBank
4. Hồ sơ đề xuất tài chính;
5. Các tài liệu khác mà nhà cung cấp thấy cần thiết để làm rõ năng lực và kinh nghiệm của mình trong việc triển khai Gói chào hàng.
6. Bảng tuyên bố đáp ứng Phần C, D (theo form như nội dung tại Phần C,D)

Mục 5. Làm rõ HSYC

1. **Làm rõ HSYC**

Trong trường hợp cần làm rõ HSYC, nhà cung cấp gửi đề nghị làm rõ đến bên mời chào hàng muộn nhất trước thời điểm đóng chào hàng. Khi nhận được đề nghị làm rõ HSYC của nhà cung cấp, bên mời chào hàng sẽ trả lời cho nhà cung cấp có yêu cầu làm rõ và tất cả các nhà cung cấp khác đã nhận HSYC từ bên mời chào hàng, trong đó mô tả nội dung yêu cầu làm rõ nhưng không nêu tên nhà cung cấp đề nghị làm rõ. Trường hợp việc làm rõ dẫn đến phải sửa đổi HSYC thì bên mời chào hàng tiến hành sửa đổi HSYC theo thủ tục quy định tại Khoản 2 Mục này.

2. **Sửa đổi HSYC**

Trường hợp sửa đổi HSYC, chủ đầu tư sẽ gửi quyết định sửa đổi kèm theo những nội dung sửa đổi đến tất cả các nhà cung cấp đã nhận HSYC không muộn hơn tối thiểu 02 ngày làm việc trước ngày có thời điểm cuối nhận HSĐX, trường hợp không đủ 02 ngày làm việc thì chủ đầu tư sẽ gia hạn thời điểm cuối nhận HSĐX tương ứng.

Mục 6. Đơn chào hàng cạnh tranh

Đơn chảo hàng cạnh tranh phải có chữ ký của người đại diện hợp pháp của nhà cung cấp (người đại diện theo pháp luật của NCC hoặc người được ủy quyền kèm theo giấy ủy quyền hợp lệ)

Mục 7. Giá chào hàng cạnh tranh

Giá chào cạnh tranh bằng VNĐ, là giá đã bao gồm các loại thuế/phí theo quy định và tất cả các chi phí phát sinh liên quan mà PGBank không phải chịu thêm bất kỳ 1 chi phí nào khác.

Mục 8. Thời gian có hiệu lực của HSĐX

Thời gian có hiệu lực của HSĐX là 60 ngày, kể từ ngày có thời điểm hết hạn nộp hồ sơ chào giá HSĐX nào có thời hạn hiệu lực ngắn hơn quy định sẽ không được tiếp tục xem xét, đánh giá.

Mục 9. Chuẩn bị và nộp HSĐX

1. Nhà cung cấp phải chuẩn bị 01 bản gốc, túi đựng HSĐX phải được niêm phong và ghi rõ tên gói chào giá, tên nhà cung cấp. Bên chủ đầu tư có trách nhiệm bảo mật thông tin trong HSDX của nhà cung cấp
2. Nhà cung cấp nộp trực tiếp hoặc gửi HSDX theo đường bưu điện địa chỉ của bên chủ đầu tư nhưng phải đảm bảo bên chủ đầu tư nhận được trước thời hạn nộp hồ sơ trước … giờ ngày ….. tháng …….năm…. theo địa chỉ như sau:
    a) Ngân Hàng TMCP Thịnh vượng và Phát triển
    b) Tầng 24, Tòa nhà Mipec, 229 Tây Sơn, Đống Đa, Hà Nội
    c) Người liên hệ : Mr. Trần Hải Hoàng
    d) Email: hoangth1@pgbank.com.vn
    e) Điện thoại: 0932641723
3. Bên chủ đầu tư sẽ tiếp nhận HSĐX của tất cả nhà cung cấp nộp HSĐX trước thời hạn nộp hồ sơ. Trường hợp nhà cung cấp nộp HSĐX sau thời hạn thì HSĐX bị loại và được trả lại nguyên trưng cho nhà cung cấp.

Mục 10. Làm rõ HSĐX

Sau khi mở báo giá, nhà cung cấp có trách nhiệm làm rõ hồ sơ đề xuất theo yêu cầu của bên mời chào giá.

Việc làm tổ phải bảo đảm không làm thay đổi bản chất của nhà cung cấp, không làm thay đổi nội dung cơ bản của hồ sơ đề xuất đã nộp.

Mục 11. Mở báo giá

- Việc mở báo giá không phụ thuộc vào sự có mặt hay vắng mặt của đại diện nhà cung cấp tham dự chào hàng.
- Việc mở chào giá được thực hiện theo trình tự sau đây:

  + Kiểm tra niêm phong hoặc mở bản mềm với mật khẩu được cung cấp bởi nhà cung cấp.

+ Mở bản chào giá và đọc to, rõ tối thiểu những thông tin sau: tên nhà cung cấp, giá, thời gian có hiệu lực của chào giá và các thông tin khác mà bên mời chào hàng thấy cần thiết.

Mục 12. Điều kiện đối với nhà cung cấp được chọn

Nhà cung cấp được xem xét, đề nghị trùng chào giá kín khi đáp ứng đủ các điều kiện sau đây:

- Có Hồ sơ đề xuất hợp lệ
- Có năng lực và kinh nghiệm đáp ứng yêu cầu

Nhà cung cấp có hồ sơ hợp lệ, đáp ứng các yêu cầu sẽ tiến tới thương thảo hợp đồng.

- Có giá đề nghị chào hàng không vượt quá cho ngân sách được phê duyệt

Mục 13. Thông báo kết quả

Kết quả lựa chọn nhà cung cấp sẽ được gửi đến tất cả cung cấp tham dự chào hàng qua thư điện tử

Mục 14. Thương thảo, hoàn thiện và ký kết hợp đồng.

1. Thương thảo về những nội dung chưa đủ chi tiết, chưa rõ hoặc chưa phù hợp, thống nhất giữa Hồ sơ yêu cầu và Hồ sơ đề xuất, giữa các nội dung khác nhau trong Hồ sơ đề xuất có thể dẫn đến các phát sinh, tranh chấp hoặc ảnh hưởng đến trách nhiệm cánh cửa bên trong quá trình thực hiện hợp đồng.
2. Thương thảo về các sai lệch do chủ đầu tư phát hiện và đề xuất trong thồ sơ đề xuất (nếu có)
3. Thương thảo về các vấn đề phát sinh trong quá trình lựa chọn nhà cung cấp (nếu có) nhằm mục tiêu hoàn thiện các nội dung chi tiết của gói CHCT.

Mục 15. Cam kết

- Cam kết của NCC về việc tham gia chào giá minh bạch, trung thực, không đưa hối lộ cho nhân sự liên quan của PGBank dưới mọi hình thức (quà, tiền mặt, tiền chuyển khoản, lợi ích khác,...) trước, trong và sau khi công bố kết quả Chào hàng cạnh tranh.
- Cam kết bảo mật thông tin cho PGBank nếu được PGBank lựa chọn là NCC
- Cam kết chất lượng dịch vụ tốt nhất theo thỏa thuận, đúng nhận diện thương hiệu PGBank.
- Cam kết về kết quả thực hiện theo đúng tiến độ, các hạng mục tổ chức đúng yêu cầu đã thỏa thuận.

Phần C. YÊU CẦU VỀ NĂNG LỰC TÀI CHÍNH, NHÂN SỰ TRIỂN KHAI, GIẢI PHÁP CÔNG NGHỆ

STT	Nội dung	Bắt buộc/ Tùy chọn	Mức độ đáp ứng của Bên chào hàng		Ghi chú
			Đạt	Không đạt	
Mục 1	**Yêu cầu về năng lực tài chính**				
	Kinh nghiệm năng lực của nhà thầu	Bắt buộc			
1	Vốn điều lệ (căn cứ vào bản sao y chứng thực bản Đăng ký kinh doanh/chứng nhận đầu tư hiện hành): tối thiểu 5 tỷ đồng.	Bắt buộc	Có	Không	
2	Nhà thầu phải nộp báo cáo tài chính có kiểm toán của 03 năm gần nhất (2021, 2022, 2023), đã nộp cơ quan thuế hoặc báo cáo tài chính đã được kiểm toán và biên lai nộp thuế các năm (bản photo). a) Giá trị tài sản ròng (bằng tổng tài sản trừ tổng nợ) mỗi năm phải dương (> 0). b) Lợi nhuận của 03 năm liên tiếp gần nhất phải dương (> 0). Trường hợp nhà thầu liên danh: Từng thành viên liên danh phải nộp đủ báo cáo tài chính và phải thỏa mãn các yêu cầu trên.	Bắt buộc	Có	Không	Yêu cầu nêu rõ số liệu chi tiết lợi nhuận, doanh thu theo báo cáo tài chính 3 năm gần nhất
3	Kinh nghiệm lớn hơn hoặc bằng 05 năm hoạt động trong lĩnh vực Kiểm tra, đánh giá an toàn thông tin mạng được tính bằng số năm hoạt động trong lĩnh vực Kiểm tra, đánh giá an toàn thông tin mạng và được đánh giá dựa theo Hợp đồng đầu tiên về Kiểm tra, đánh giá an toàn thông tin mạng. Nhà thầu có thể tham gia với tư cách độc lập hoặc liên danh. - Nhà thầu phải kèm theo các tài liệu sau để chứng minh: Bản gốc/bản chụp được chứng thực hợp đồng chứng minh số năm kinh nghiệm.	Bắt buộc	Có	Không	
4	Uy tín của nhà thầu thông qua việc tham dự thầu (không có trường hợp không tham gia thương thảo hợp đồng, có quyết định trúng thầu nhưng không tiến hành hoàn thiện, ký kết hợp đồng; không có hợp đồng nào không hoàn thành hợp đồng do lỗi của nhà thầu), ngoài ra đáp ứng thêm các tiêu chí:	Bắt buộc	Có	Không	

STT	Nội dung	Bắt buộc/ Tùy chọn	Mức độ đáp ứng của Bên chào hàng		Ghi chú
			Đạt	Không đạt	
	- Có giấy phép kinh doanh dịch vụ ATTT mạng do Bộ TT và TT cấp hoặc có chức năng nhiệm vụ về cung cấp dịch vụ ATTT được cấp có thẩm quyền quy định. - Có chứng nhận phù hợp với tiêu chuẩn cơ sở TCCS02:2020/VNISA - Dịch vụ Kiểm tra, Đánh giá An toàn thông tin mạng hoặc có giấy chứng nhận ISO/IEC 27001:2013.				
5	Đã thực hiện gói thầu cung cấp dịch vụ an toàn thông tin - Có tối thiểu 01 hợp đồng có giá trị thấp nhất là từ 2.000.000.000 trở lên - Tài liệu chứng minh (bản sao được chứng thực hoặc bản gốc): Hợp đồng cung cấp dịch vụ hoặc biên bản nghiệm thu.	Bắt buộc	Có	Không	
Mục 2	**Yêu cầu về nhân sự triển khai**				
1	**Quản lý dự án (Số lượng : 01 người)** Năng lực hành nghề: - Có tối thiểu 01 nhân sự trình độ đại học về lĩnh vực CNTT, Điện tử viễn thông, An toàn thông tin. - Có 03 năm kinh nghiệm giữ vai trò Quản lý dự án/Quản trị hợp đồng về tiến độ và chất lượng của dự án, Đã thực hiện ít nhất 01 dự án/hợp đồng về dịch vụ tương đương trong vực Tài chính/ Ngân hàng.Tài liệu chứng minh: Hợp đồng tương tự/xác nhận của chủ đầu tư	Bắt buộc	Có	Không	
2	**Tư vấn trưởng (Số Lượng: 01 người)** Năng lực hành nghề: - Tốt nghiệp đại học trở lên chuyên ngành CNTT hoặc Điện tử viễn thông, An toàn thông tin.	Bắt buộc	Có	Không	

STT	Nội dung	Bắt buộc/ Tùy chọn	Mức độ đáp ứng của Bên chào hàng		Ghi chú
			Đạt	Không đạt	
	- Có 03 năm kinh nghiệm và có tối thiểu hai trong các chứng chỉ (còn hiệu lực tính đến thời điểm đóng thầu) sau: GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), Licensed Penetration Tester (LPT), GIAC Penetration Tester (GPEN), CISM, CTIA - Đã trực tiếp làm tư vấn trưởng tư vấn kỹ thuật hoặc tương đương ít nhất 01 dự án về dịch vụ kiểm thử ATTT - Đã trực tiếp tham gia ít nhất 02 dự án/hợp đồng về dịch vụ an toàn thông tin/ kiểm thử xâm nhập Tài liệu chứng minh: Hợp đồng lao động, Bản sao công chứng của chứng chỉ				
3	**Trưởng nhóm đánh giá an toàn thông tin (Số Lượng: 01 người)** Năng lực hành nghề: - Trình độ đại học về lĩnh vực CNTT, Điện tử viễn thông, An toàn thông tin. - Có 3 năm kinh nghiệm và có tối thiểu 01 trong các chứng chỉ bảo mật sau hoặc tương đương / cao hơn: Microsoft Azure Security Engineer - AZ-500,SC – 200, OSWE, OSCP, CPTS HTB, CEH, CRISC, CHFI, CISM , CTIA, ECIH, CySA+ còn hiệu lực tính đến thời điểm điểm chào thầu - Đã trực tiếp làm trưởng nhóm kỹ thuật hoặc tương đương ít nhất 01 dự án về dịch vụ kiểm thử ATTT - Đã trực tiếp tham gia ít nhất 02 dự án/hợp đồng về dịch vụ an toàn thông tin/ kiểm thử xâm nhập. Và đáp ứng một trong những tiêu chí sau: - Có thành tích 6 tháng liên tục trong 3 năm gần nhất được công nhận bởi các nền tảng săn tìm lỗ hổng bảo mật quốc tế (Hall of fame) như Apple, Google; hoặc có	Bắt buộc	Có	Không	

STT	Nội dung	Bắt buộc/ Tùy chọn	Mức độ đáp ứng của Bên chào hàng		Ghi chú
			Đạt	Không đạt	
	đồng thời 03 chứng chỉ OSCP, ECSA, CEH còn hiệu lực tính đến thời điểm điểm chào thầu				
4	**Chuyên gia đánh giá An Toàn Thông Tin (Số Lượng: 05 người)** Năng lực hành nghề: - Trình độ đại học về lĩnh vực CNTT, An toàn thông tin. - Có 3 năm kinh nghiệm và mỗi nhân sự có tối thiểu 1 trong các chứng chỉ bảo mật sau hoặc tương đương: Microsoft Azure Security Engineer, AZ-500, SC200, OSWE, OSCP, CPTS HTB, CEH CRISC, CHFI, CISM, CEH, CTIA, ECIH, CySA+, CompTIA Security+ còn hiệu lực tính đến thời điểm điểm chào thầu. Tối thiểu 02 nhân sự đã phát hiện 05 lỗ hổng bảo mật/CVE/Zero day….. Của các nền tảng Vmware, Cisco,Microsoft, McAfee, Hackerone, Bugcrowd, Apple, Oracle hoặc đã trực tiếp tham gia ít nhất 01 dự án/hợp đồng về dịch vụ an toàn thông tin/ kiểm thử xâm nhập.	Bắt buộc	Có	Không	
Mục 3	**Yêu cầu giải pháp công nghệ**				
1	Cung cấp dịch vụ giám sát và phát hiện các thông tin liên quan đến domain PGBank lộ lọt trên môi trường internet, diễn đàn phải sử dụng giải pháp thương mại được đánh giá mức thang điểm đánh giá từ 4.5 điểm trở lên trên Gartner Peer Insights với tối thiểu 45 phản hồi đánh giá.	Bắt buộc	Có	Không	
2	Yêu cầu nhà thầu sử dụng công cụ có bản quyền chính hãng trong quá trình cung cấp dịch vụ hỗ trợ thực hiện các thao tác mô phỏng tấn công khai thác, rà soát hệ thống: - Công cụ có chức năng cung cấp và tổng hợp mã khai thác gồm đầy đủ các mã khai thác tương đương khoảng hơn 35.000 mã khai thác trong đó bao gồm các	Bắt buộc	Có	Không	

STT	Nội dung	Bắt buộc/ Tùy chọn	Mức độ đáp ứng của Bên chào hàng		Ghi chú
			Đạt	Không đạt	
	lỗ hổng 0-day. Hỗ trợ khai thác trên nhiều nền tảng như Windows, Linux, Unix, Minix, SCO, Solaris, OSX, Mobile, Web. Có một số chức năng hỗ trợ quá trình khai thác sâu như: Hexa editor, Remote Fuzzer,… Automated attacks, Targets management, - Sử dụng công cụ thực hiện rà soát hỗ trợ cung cấp tối thiểu hơn 30.000 signature Yara, hơn 3.000 Sigma rules, 30 detection modules, … Hỗ trợ các nền tảng cơ bản như Windows, Linux, MacOS, AIX, …				

Phần D. YÊU CẦU VỀ TIÊU CHÍ KỸ THUẬT

Nhà cung cấp phải cung cấp được các văn bản, chứng chỉ... để chứng minh đạt tiêu chuẩn, tiêu chí lựa chọn:

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
I.	**Kiểm thử bảo mật, kiểm thử xâm nhập hệ thống thông tin**					
1.1	**Yêu cầu về số lượng** Tiêu chí: Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ	Kiểm thử xâm nhập 14 hệ thống thông tin cấp độ 3 public internet/nội bộ, có source code tồn tại nhiều rủi ro có thể bị khai thác hoặc tấn công leo thang.				
1.2	**Yêu cầu về kỹ thuật** Tiêu chí: Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ hoặc đáp ứng 1 phần.					
1.2.1	Kiểm thử thâm nhập với các hệ thống thông tin và bao gồm toàn bộ các API trên ứng dụng từ bên ngoài môi trường internet (thử nghiệm thực tế với các cuộc tấn công như những tin tặc thực hiện nhưng không làm gián đoạn hệ thống) mà đối tác không cần cung cấp bất kỳ thông tin nội bộ.	Phải triển khai phương pháp kiểm thử thâm nhập Black Box, không yêu cầu thông tin nội bộ, nhằm đảm bảo tính khách quan và toàn diện của quá trình kiểm thử.				
		Phải triển khai kiểm thử an ninh mức ứng dụng Web Application/Service, thực hiện các bài kiểm thử bao gồm nhưng				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		không giới hạn những hạng mục sau (theo OWASP top 10) từ bên ngoài				
		Phải sử dụng và triển khai các công cụ kiểm thử thâm nhập hiện đại và đáng tin cậy để phát hiện các lỗ hổng bảo mật một cách chính xác và hiệu quả.				
		Phải triển khai kiểm thử an ninh API, thực hiện các bài kiểm thử bao gồm nhưng không giới hạn những hạng mục sau (theo OWASP API Security Top 10) từ bên ngoài				
		Phải phát hiện và khai thác ít nhất các lỗ hổng bảo mật từ bên ngoài, bao gồm nhưng không giới hạn ở SQL Injection, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), RCE (Remote Code Execution), SSRF (Server-Side Request Forgery), nhằm đảm bảo rằng hệ thống và các API được kiểm tra toàn diện từ bên ngoài				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		Phải tuân thủ các tiêu chuẩn và phương pháp kiểm thử bảo mật như OWASP, PTES…để đảm bảo quy trình kiểm thử theo chuẩn quốc tế và đáng tin cậy.				
		Phải kiểm tra và đánh giá xác thực và ủy quyền trên các API từ bên ngoài, đảm bảo rằng các quy trình bảo mật liên quan đến xác thực và quyền truy cập được kiểm tra kỹ lưỡng để tránh các lỗ hổng có thể bị khai thác.				
		Phải phát hiện các vấn đề bảo mật từ bên ngoài như lộ thông tin nhạy cảm, kiểm soát truy cập không đúng cách, và cấu hình không an toàn trên các hệ thống thông tin và các API trên ứng dụng, để đảm bảo rằng tất cả các thành phần của hệ thống được bảo mật đúng cách.				
		Có kỹ năng xây dựng các phương thức hoặc mẫu tấn công chứng minh lỗ hổng tồn tại				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		Phải đảm bảo quá trình kiểm thử không làm gián đoạn dịch vụ hoặc ảnh hưởng đến hoạt động của hệ thống, bằng cách sử dụng các phương pháp kiểm thử không xâm lấn và đảm bảo rằng các hoạt động kiểm thử diễn ra một cách an toàn và có kiểm soát.				
		Phải cam kết không thu thập hoặc lưu trữ bất kỳ thông tin nội bộ nào từ hệ thống và ứng dụng, để bảo vệ quyền riêng tư và bảo mật của thông tin nội bộ.				
		Phải cung cấp báo cáo chi tiết về các lỗ hổng phát hiện từ bên ngoài, mức độ nguy hiểm của chúng, và đề xuất biện pháp khắc phục				
1.2.2	Thực hiện mô phỏng tấn công bên ngoài/ trong mạng bao gồm các kỹ thuật tấn công leo thang đặc quyền, tấn công khai thác, mô phỏng tấn công hệ thống bị Compromise và tấn công lây lan trên các ứng dụng nội bộ sử dụng.	Phải đánh giá và khai thác các lỗi còn tồn tại trên App Mobile (các thành phần mà tin tặc hacker có thể khai thác như chuyển tiền, đọc thông tin người dùng, thông tin biến động số dư, thông tin thẻ ,...) Mô phỏng lại tình huống tấn công và phương án khắc phục.				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		Phải tiến hành dò quét các phân đoạn mạng, các cổng dịch vụ đang mở của các lớp mạng liên quan để kiểm tra lỗ hổng đăng nhập có thể sử dụng các thông tin này để đi lan ra mạng nội bộ.				
		Các hoạt động trinh sát và các bước chuẩn bị, cần phải tìm cách triển khai các mã tấn công đến mục tiêu là cơ sở hạ tầng và ứng dụng thông qua spearphishing, USB, watering-hole hoặc đơn giản là khai thác các dịch vụ công cộng với rủi ro cao như dịch vụ web hoặc ứng dụng				
		Thực thi mã từ xa - RCE các máy chủ quan trọng trong đó ưu tiên hệ thống quan trọng (Mobile Banking,Internet Banking,AD, Exchange….) Phải khai thác và duy trì quyền điều khiển trên các máy chủ chiến lược hoặc các thiết bị mạng có thể được sử dụng để kết nối ra bên ngoài, lưu trữ và truyền dữ liệu, hoặc đánh cắp dữ liệu mạng được truyền ra và vào mô phỏng tấn công và đưa ra phương án khắc phục. Nếu không khai thác được phải cung cấp				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		quá trình tấn công khai thác chi tiết (quy trình tấn công, Log tấn công)				
		Phải cung cấp báo cáo thử nghiệm xâm nhập chi tiết cùng các phương pháp và kỹ thuật được sử dụng trong quá trình thực hiện dịch vụ. Báo cáo kiểm tra xâm nhập phải mô tả chi tiết về các lỗ hổng, chiến thuật và kỹ thuật MITRE ATT&CK đã được sử dụng, bằng chứng về việc khai thác thành công cũng như hướng dẫn khắc phục triệt để (hoặc biện pháp xử lý lỗ hổng tạm thời nếu lỗ hổng không có cách thức khắc phục triệt để)				
1.2.3	Giám sát và phát hiện các thông tin liên quan đến domain PGBank lộ lọt trên môi trường internet, diễn đàn như: - Đưa ra các thông tin và cảnh báo về các rủi ro lộ lọt gây mất an toàn thông tin liên quan đến khách hàng hoặc bên thứ ba ví dụ như: Thông tin liên quan đến cấu trúc, tài liệu thiết kế CNTT, tài liệu nhạy cảm tại các website mua bán, trao đổi thông tin của	Phải đưa ra các thông tin về các rủi ro lộ lọt thông tin liên quan đến domain PGBank trên môi trường internet, diễn đàn và dark web, bao gồm nhưng không giới hạn các thông tin nhạy cảm như tên người dùng, mật khẩu và khóa truy cập thông tin bí mật.				
		Phải cung cấp các thông tin liên quan tới các CVE liên quan tới lỗ hổng				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
	tin tặc (Darkweb), diễn đàn, forum chia sẻ tài liệu trái phép trên môi trường không gian mạng - Rò rỉ thông tin nhạy cảm, chẳng hạn như Tên người dùng, Mật khẩu và Khóa truy cập thông tin bí mật (Secret token access keys)	Phải tìm kiếm phát hiện và báo cáo về việc thông tin liên quan đến cấu trúc, tài liệu thiết kế CNTT của ngân hàng xuất hiện trên các website mua bán, trao đổi thông tin của tin tặc trên dark web, diễn đàn và forum chia sẻ tài liệu trái phép trên môi trường mạng.				
		Phải đánh giá và phân tích các nguồn dẫn tới lộ lọt thông tin bảo mật phát hiện được từ bên ngoài, đưa ra các báo cáo chi tiết về mức độ nguy hiểm, và đề xuất biện pháp khắc phục.				
		Phải đưa ra báo cáo chi tiết về các thông tin đã phát hiện và đánh giá, bao gồm mô tả về nguồn gốc và mức độ nghiêm trọng của rủi ro				
		Đề xuất các biện pháp khắc phục và cải thiện bảo mật dựa trên những phân tích và đánh giá đã thực hiện.				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
1.2.4	Rà soát phân tích mã nguồn của các ứng dụng theo các phương pháp + Phân tích tĩnh + Phân tích động + Thư viện mã nguồn Để đánh giá các rủi ro an ninh thông tin có thể bị khai thác phân tích các lỗi bao gồm nhưng không giới hạn ở Top 10 OWASP/Top 25 SANS	Phải đọc hiểu mã nguồn và phân tích mã nguồn với các ngôn ngữ lập trình				
		Phải phát hiện và xác định các lỗ hổng bảo mật tiềm ẩn, bao gồm các lỗi liên quan đến xử lý dữ liệu không an toàn, quản lý bộ nhớ không đúng, và sử dụng hàm không an toàn.				
		Phải áp dụng các kỹ thuật phân tích động để kiểm tra luồng điều khiển của chương trình và phát hiện các lỗ hổng bảo mật có thể bị khai thác trong quá trình thực thi.				
		Phải rà soát các thư viện mã nguồn được sử dụng trong ứng dụng để xác định và đánh giá các rủi ro an ninh thông tin có thể phát sinh từ các thư viện này.				
		Phải phân tích xâu chuỗi luồng chạy ứng dụng, phát hiện các điểm yếu dễ bị khai thác trong mã nguồn				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		Đưa ra được các phân tích các lỗ hổng bảo mật được phát hiện để xác định mức độ rủi ro của ứng dụng.				
		Đưa ra được khuyến nghị khắc phục lỗ hổng ở mức tối ưu nhất để giảm thiểu rủi ro và hạn chế khắc phục nhiều điểm làm ảnh hưởng ứng dụng				
II. Dịch vụ rà quét, đánh giá bảo mật 34 hệ thống thông tin						
2.1	**Yêu cầu về số lượng** Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ	Dịch vụ rà quét, đánh giá lỗ hổng bảo mật 34 ứng dụng, dịch vụ xử lý và lưu trữ thông tin quan trọng lớp bên trong.				
2.2	**Yêu cầu kỹ thuật** Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ hoặc đáp ứng 1 phần.					
2.2.1	Rà quét lỗ hổng bảo mật của các hệ thống thông tin cấp độ 2,3 đang hoạt động trên các hệ điều hành như window, opensource, hệ thống ảo hoá máy chủ, hệ thống có mức độ	Phải rà quét và đánh giá lỗ hổng bảo mật trên các hệ điều hành Windows, Linux, và các hệ thống OpenSource.				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
	ảnh hưởng lớn nếu bị tấn công, hệ thống như AD, Radius, lưu trữ source code hoặc một số hệ thống đang chạy các phiên version cũ tồn tại nhiều lỗ hổng bảo mật chưa vá được.	Phải kiểm tra và đánh giá bảo mật các hệ thống ảo hóa máy chủ như VMware, Hyper-V, KVM, và các giải pháp ảo hóa khác, đảm bảo phát hiện và hỗ trợ khắc phục lỗ hổng bảo mật liên quan đến các môi trường ảo hóa.				
		Phải đánh giá và phân tích các hệ thống có mức độ ảnh hưởng lớn nếu bị tấn công, bao gồm các hệ thống quan trọng như Active Directory (AD), Radius, và các hệ thống quản lý định danh (Identity Management Systems). Đánh giá này phải bao gồm phân tích tác động và đề xuất biện pháp khắc phục hoặc giảm thiểu rủi ro.				
		Phải sử dụng các công cụ phân tích mã nguồn tĩnh (SAST) và động (DAST) như SonarQube, Fortify, Checkmarx, để rà soát và phát hiện lỗ hổng bảo mật trong hệ thống lưu trữ source code. Công việc này phải bao gồm kiểm tra các lỗ hổng liên quan đến mã nguồn như SQL Injection, XSS, CSRF, và các lỗi logic khác và đưa				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		ra các khuyến nghị cụ thể về việc nâng cấp hoặc thay thế.				
		Phải rà soát và đánh giá các hệ thống đang chạy các phiên bản phần mềm cũ tồn tại nhiều lỗ hổng bảo mật chưa được vá. Điều này bao gồm kiểm tra các hệ thống không còn được nhà cung cấp hỗ trợ và đưa ra các khuyến nghị cụ thể về việc nâng cấp hoặc thay thế.				
		Phải sử dụng các công cụ quét bảo mật tự động nổi tiếng nhưng không giới hạn như Nessus, hoặc Burp Suite để phát hiện lỗ hổng bảo mật. Công việc này bao gồm cấu hình công cụ quét để phù hợp với môi trường của khách hàng và thực hiện quét định kỳ để phát hiện lỗ hổng mới xuất hiện.				
		Phải cung cấp báo cáo chi tiết về các lỗ hổng bảo mật được phát hiện, bao gồm mô tả, mức độ nghiêm trọng (theo tiêu chuẩn CVSS hoặc tương đương), hệ thống bị ảnh hưởng, phương thức tấn công có thể, và khuyến nghị khắc phục cụ thể. Báo cáo				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		phải dễ hiểu và có thể sử dụng để thuyết phục các bên liên quan không chuyên về kỹ thuật.				
		Phải cung cấp các biện pháp khắc phục lỗ hổng bảo mật, bao gồm kiểm tra lại sau khi áp dụng biện pháp khắc phục để đảm bảo rằng lỗ hổng đã được vá hoàn toàn và không tồn tại rủi ro.				
		Phải tuân thủ các tiêu chuẩn bảo mật thông tin quốc tế như ISO/IEC 27001, NIST SP 800-115, và OWASP Top Ten trong quá trình rà soát và đánh giá lỗ hổng. Điều này bao gồm việc áp dụng các phương pháp và quy trình tiêu chuẩn để đảm bảo tính toàn vẹn và chính xác của quá trình đánh giá.				
2.2.3	Rà soát mã độc trên các máy chủ để xác định, phát hiện các dấu hiệu bất thường trên máy chủ như Backdoor, Shell,tiến trình…..(tương đương 500 server)	Phải rà soát mã độc trên các hệ điều hành Windows, Linux, và các hệ thống OpenSource, đảm bảo phát hiện mã độc trên các nền tảng khác nhau.				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		Phải sử dụng các công cụ và phương pháp tiên tiến để phát hiện các backdoor, shell script, và các mã độc khác đã được cài đặt trên máy chủ.				
		Phải giám sát và phân tích các tiến trình đang chạy trên máy chủ để phát hiện các hoạt động bất thường hoặc đáng ngờ.				
		Phải giám sát và phân tích lưu lượng mạng để phát hiện các kết nối bất thường hoặc không hợp lệ, bao gồm các kết nối đến các địa chỉ IP đáng ngờ hoặc lưu lượng mạng tăng đột biến.				
		Phải kiểm tra các tệp tin hệ thống quan trọng để phát hiện sự thay đổi không hợp lệ hoặc bất thường.				
		Phải phân tích hành vi của mã độc đã phát hiện được để hiểu rõ hơn về cách thức hoạt động của nó và tác động tiềm tàng đến hệ thống.				
		Phải phát hiện và phân tích các tấn công zero-day và các lỗ hổng bảo mật mới xuất hiện, đảm bảo hệ thống luôn được bảo vệ trước các mối đe dọa mới nhất.				

STT	Mô tả	YÊU CẦU CHI TIẾT	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
		Phải cung cấp báo cáo chi tiết về các mã độc và dấu hiệu bất thường được phát hiện, bao gồm mô tả, mức độ nghiêm trọng, và khuyến nghị khắc phục cụ thể. Báo cáo phải dễ hiểu và có thể sử dụng để thuyết phục các bên liên quan không chuyên về kỹ thuật.				
2.2.4	Thực hiện tư vấn đảm bảo an toàn thông tin	Thực hiện tư vấn, khuyến nghị khắc phục các điểm yếu, lỗ hổng, rủi ro an toàn thông tin phát hiện được trong qúa trình cung cấp dịch vụ				
		Thực hiện kiểm tra an ninh để đảm bảo rằng các biện pháp giảm thiểu đã được triển khai đúng cách và hiệu quả.				
		Khuyến nghị khách hàng thực hiện tấn công định kỳ để đảm bảo rằng hệ thống vẫn an toàn trước các mối đe dọa mới				