UBND TỈNH BÌNH DƯƠNG **SỞ CÔNG THƯƠNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1822 /TB-SCT	*Bình Dương, ngày 09 tháng 8 năm 2021*

THÔNG BÁO
V/v mời nhà thầu bảo trì cổng thông tin điện tử Sở Công Thương

Căn cứ Quyết định số 08/QĐ-SCT ngày 29/01/2021 của Sở Công Thương tỉnh Bình Dương về việc giao dự toán thu, chi ngân sách nhà nước năm 2021;

Hiện nay, Sở Công Thương tỉnh Bình Dương đang lựa chọn nhà thầu bảo trì cổng thông tin điện tử Sở Công Thương, cụ thể như sau:

1. Gói thầu: "Bảo trì cổng thông tin điện tử Sở Công Thương"

2. Nội dung bảo trì: Theo phụ lục đính kèm

3. Thời gian thực hiện: 03 tháng

4. Nguồn vốn: kinh phí không thực hiện chế độ tự chủ trong dự toán được giao năm 2021 của Sở Công Thương

Đề nghị các đơn vị có chức năng và đáp ứng thực hiện gói thầu như trên (trong và ngoài tỉnh), có nhu cầu tham gia vui lòng gửi báo giá về Sở Công Thương tỉnh Bình Dương chậm nhất vào **lúc 17 giờ 00 phút ngày 15/8/2021** để được tham gia xét chọn.

Nhà thầu muốn biết thông chi tiết thông tin về gói thầu, vui lòng liên hệ Văn phòng Sở Công Thương tỉnh Bình Dương (Số 3 Huỳnh Văn Nghệ, phường Phú Lợi, thành phố Thủ Dầu Một, tỉnh Bình Dương), điện thoại 0933.446.255 (ông Nguyễn Ngọc Dương) để được hướng dẫn, cung cấp thông tin./.

Nơi nhận:
- Nhà thầu;
- BGĐ Sở;
- Website Sở;
- Lưu: VT, VP, Đ, "pdf".

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH BÌNH DƯƠNG

Nguyễn Trường Thi

PHỤ LỤC
KHỐI LƯỢNG CÔNG VIỆC BẢO TRÌ CỔNG THÔNG TIN ĐIỆN TỬ
(Ban hành kèm Thông báo số: 1822 /TB-SCT ngày / 8 /2021)

I. Kiểm thử từ phía người dùng

Đối với ứng dụng web, sau khi sử dụng những công cụ tự động để phát hiện các lỗi bảo mật cơ bản, chúng tôi tiến hành kiểm thử lại bằng cách thủ công đối với các trường giá trị mà người dùng có thể tương tác được với máy chủ. Quy trình đánh giá an toàn thông tin cho một website sẽ được tiến hành từ phía người dùng, sau đó sẽ đánh giá từ phía máy chủ.

Quá trình kiểm thử bảo mật từ phía người dùng bao gồm:

1. Quét sơ bộ
2. Thu thập thông tin đối tượng kiểm thử
3. Khai thác và đánh giá các lỗi được tìm thấy
4. Báo cáo chi tiết.

1. Thu thập thông tin (Information Gathering): để thu thập thông tin về mục tiêu ngay trước khi tiến hành khai thác. Việc thu thập thông tin sẽ bao gồm việc tìm kiếm thông tin công khai có liên quan đến hệ thống và cách tốt nhất để khai thác thông tin đó. Mục đích của việc thu thập là càng nhiều thông tin càng tốt, nó sẽ giúp những kỹ sư bảo mật hiểu cách ứng dụng hoặc hệ thống hoạt động nhằm phát hiện ra những thiếu sót về bảo mật có thể tại.

Để thu nhập thông tin, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Conduct Search Engine Discovery Reconnaissance for Information Leakage
- Fingerprint Web Server
- Review Webserver Metafiles for Information Leakage
- Enumerate Applications on Webserver
- Review Webpage Content for Information Leakage
- Identify Application Entry Points
- Map Execution Paths Through Application
- Fingerprint Web Application Framework
- Fingerprint Web Application
- Map Application Architecture

2. Kiểm tra cấu hình và quy trình triển khai (Configuration and Deployment Management Testing): để hiểu cấu hình đã triển khai của máy chủ lưu trữ ứng dụng web cũng quan trọng như chính việc kiểm tra bảo mật

ứng dụng. Nền tảng ứng dụng rất rộng và đa dạng, nhưng một số lỗi cấu hình nền tảng chính có thể làm ảnh hưởng đến ứng dụng giống như cách một ứng dụng không an toàn có thể giúp “hacker" xâm phạm máy chủ.

Để kiểm tra quản lý cấu hình và triển khai, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Test Network Infrastructure Configuration
- Test Application Platform Configuration
- Test File Extensions Handling for Sensitive Information
- Review Old Backup and Unreferenced Files for Sensitive Information
- Enumerate Infrastructure and Application Admin Interfaces
- Test HTTP Methods
- Test HTTP Strict Transport Security
- Test RIA Cross Domain Policy
- Test File Permission
- Test for Subdomain Takeover
- Test Cloud Storage

3. Kiểm tra quản lý danh tính (Identity Management Testing): kiểm tra về cách thức hoạt động của việc đăng ký thông tin người dùng, quá trình người dùng xác thực danh tính cũng như đăng nhập vào hệ thống. Trong quá trình kiểm tra, kỹ sư của chúng tôi sẽ khai thác và đánh giá hệ thống đăng ký và đăng nhập, và vai trò mặc định của từng người dùng.

Để kiểm kiểm tra quản lý danh tính, nnhững hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Test Role Definitions
- Test User Registration Process
- Test Account Provisioning Process
- Testing for Account Enumeration and Guessable User Account
- Testing for Weak or Unenforced Username Policy

4. Kiểm tra xác thực (**Authentication Testing)**: để hiểu cách thức hoạt động của quá trình xác thực và sử dụng thông tin đó để phá vỡ cơ chế xác thực. Điều này giúp chúng tôi kiểm tra xem liệu thông tin đăng nhập mặc định đang được sử dụng, mật khẩu của người dùng có thể bị kẻ tấn công bẻ khóa hay chúng tôi có thể vượt qua cơ chế xác thực bằng cách sử dụng các lỗ hổng đã xác định khác.

Để kiểm kiểm tra xác thực, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Testing for Credentials Transported over an Encrypted Channel
- Testing for Default Credentials
- Testing for Weak Lock Out Mechanism
- Testing for Bypassing Authentication Schema
- Testing for Vulnerable Remember Password
- Testing for Browser Cache Weaknesses
- Testing for Weak Password Policy
- Testing for Weak Security Question Answer
- Testing for Weak Password Change or Reset Functionalities
- Testing for Weaker Authentication in Alternative Channel

5. **Kiểm tra ủy quyền (Authorization Testing)**: tìm hiểu cách thức hoạt động của quy trình ủy quyền và tìm cách phá vỡ cơ chế ủy quyền. Ủy quyền là một quá trình xảy ra sau khi xác thực thành công, vì vậy kỹ sư chúng tôi sẽ xác minh điểm này sau khi họ có bằng chứng xác thực hợp lệ, được liên kết với một tập hợp các vai trò và đặc quyền được xác định rõ ràng. Trong quá trình đánh giá, kỹ sư sẽ tìm cách phá vỡ các cơ chế uỷ quyền được mặc định, tìm lỗ hổng qua đường dẫn hoặc tìm cách nâng cao đặc quyền được chỉ định cho người dùng hay không.

Để kiểm kiểm tra uỷ quyền, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Testing Directory Traversal File Include
- Testing for Bypassing Authorization Schema
- Testing for Privilege Escalation
- Testing for Insecure Direct Object References

6. **Kiểm tra quản lý phiên làm việc (Session Management Testing)**: Trong thử nghiệm này, kỹ sư chúng tôi sẽ kiểm tra xem liệu các cookie được cấp cho máy khách có thể chống lại một loạt các cuộc tấn công nhằm can thiệp vào các phiên của người dùng hợp pháp và với chính ứng dụng hay không. Mục tiêu chung là kiểm tra xem chúng tôi có thể giả mạo một cookie sẽ được ứng dụng coi là hợp lệ và sẽ cung cấp một số loại truy cập trái phép (chiếm quyền điều khiển phiên, leo thang đặc quyền, ...).

Để kiểm kiểm tra quản lý phiên, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Testing for Session Management Schema
- Testing for Cookies Attributes
- Testing for Session Fixation
- Testing for Exposed Session Variables

- Testing for Cross Site Request Forgery
- Testing for Logout Functionality
- Testing Session Timeout
- Testing for Session Puzzling

- Testing for Session Hijacking

7. Kiểm tra xác thực dữ liệu (Data Validation Testing): điểm yếu bảo mật ứng dụng web phổ biến nhất là không xác thực đúng đầu vào từ máy khách hoặc từ môi trường trước khi sử dụng. Điểm yếu này dẫn đến hầu như tất cả các lỗ hổng chính trong các ứng dụng web, chẳng hạn như tập lệnh trang web chéo, chèn SQL, chèn trình thông dịch, tấn công locale / Unicode, tấn công hệ thống tệp và tràn bộ đệm.

Để kiểm kiểm tra xác thực dữ liệu, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Testing for Reflected Cross Site Scripting
- Testing for Stored Cross Site Scripting
- Testing for HTTP Verb Tampering
- Testing for HTTP Parameter pollution
- Testing for SQL Injection
- Testing for NoSQL injection
- IMAP/SMTP Injection
- Testing for Code Injection
- Testing for Local File Inclusion
- Testing for Remote File Inclusion
- Testing for Command Injection
- Testing for Format string
- Testing for HTTP Splitting/Smuggling

8. Xử lý lỗi (Error Handling): Thông thường, trong quá trình thử nghiệm thâm nhập trên các ứng dụng web, chúng tôi sẽ

chống lại nhiều mã lỗi được tạo ra từ các ứng dụng hoặc máy chủ web. Có thể khiến các lỗi này hiển thị bằng cách sử dụng một yêu cầu cụ thể, được tạo đặc biệt bằng các công cụ hoặc được tạo thủ công. Các mã này rất hữu ích cho người kiểm tra thâm nhập trong các hoạt động của họ, vì chúng tiết lộ nhiều thông tin về cơ sở dữ liệu, lỗi và các thành phần công nghệ khác được liên kết trực tiếp với các ứng dụng web.

Để kiểm kiểm tra các chức năng xử lý lỗi, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Testing for Improper Error Handling
- Testing for Stack Traces

9. Mật mã (Cryptography): Dữ liệu nhạy cảm phải được bảo vệ khi nó được truyền qua mạng. Dữ liệu đó có thể bao gồm thông tin đăng

nhập của người dùng và thẻ tín dụng. Theo nguyên tắc chung, nếu dữ liệu phải được bảo vệ khi nó được lưu trữ, nó cũng phải được bảo vệ trong quá trình truyền.

Để kiểm kiểm tra cơ chế bảo vệ dữ liệu trong quá trình truyền, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Testing for Weak Transport Layer Security
- Testing for Padding Oracle
- Testing for Sensitive Information Sent via Unencrypted Channels
- Testing for Weak Encryption

10. Kiểm tra lỗi logic (Business Logic Testing): Nếu cơ chế xác thực của ứng dụng được phát triển với mục đích thực hiện các bước 1, 2, 3 theo thứ tự cụ thể đó để xác thực người dùng. Điều gì xảy ra nếu người dùng chuyển thẳng từ bước 1 sang bước 3? Trong ví dụ đơn giản này, ứng dụng có cung cấp quyền truy cập không; từ chối quyền truy cập hoặc với thông báo mã lỗi 500.

Loại lỗ hổng này không thể được phát hiện bởi máy quét lỗ hổng và dựa vào kỹ năng và sự sáng tạo của người kiểm tra thâm nhập. Ngoài ra, loại lỗ hổng này thường là một trong những lỗ hổng khó phát hiện nhất và thường dành riêng cho ứng dụng nhưng đồng thời, thường là một trong những lỗ hổng gây bất lợi nhất cho ứng dụng nếu bị khai thác.

Để kiểm kiểm tra logic của ứng dụng, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Test Business Logic Data Validation
- Test Ability to Forge Requests
- Test Integrity Checks
- Test for Process Timing
- Test Number of Times a Function Can Be Used Limits
- Testing for the Circumvention of Work Flows
- Test Defenses Against Application Misuse
- Test Upload of Unexpected File Types
- Test Upload of Malicious Files

11. Kiểm tra phía người dùng (Client-Side Testing): Kiểm tra từ phía người dùng liên quan đến việc thực thi mã độc trên máy khách, thường xảy ra ở trình duyệt web hoặc plugin trình duyệt. Việc thực thi mã độc ở phía máy khách khác với việc thực thi trên máy chủ và trả về nội dung tiếp theo. Lỗ hổng phía máy khách thường ở dạng phần mềm chưa được vá trên máy tính để bàn hoặc máy tính xách tay. Tùy thuộc vào bản

chất của ứng dụng dễ bị tấn công, kẻ tấn công có thể khai thác nó thông qua tệp đính kèm email được thiết kế đặc biệt hoặc bằng cách thuyết phục người dùng truy cập một trang web độc hại. Các trình duyệt web là mục tiêu phổ biến. Các mục tiêu hấp dẫn khác bao gồm Adobe Acrobat, Macromedia Flash, QuickTime và Java Runtime Environment.

Để kiểm kiểm tra logic của ứng dụng, những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- Testing for DOM based Cross Site Scripting
- Testing for JavaScript Execution
- Testing for HTML Injection
- Testing for Client Side URL Redirect
- Testing for CSS Injection
- Testing for Client Side Resource Manipulation
- Test Cross Origin Resource Sharing
- Testing for Cross Site Flashing
- Testing for Clickjacking
- Testing WebSockets
- Test Web Messaging
- Test Local Storage

Công cụ: công cụ sử dụng trong quá trình kiểm thử bao gồm: Google, httprint, Netcraft, Browser, curl, wget, dnslookup, dig, nmap, nessus, nikto, acunextic.

II. Kiểm thử từ phía máy chủ

Quy trình kiểm thử

Đối với thử nghiệm xâm nhập mạng lưới bên trong, hệ thống máy chủ là xương sống và đầu cuối của việc truy cập ứng dụng của người dùng. Đó là lý do tại sao điều quan trọng là phải có một lớp bảo mật vững chắc với bất kỳ nền tảng.

Vấn đề bảo mật từ phía máy chủ thường liên quan tới các vấn đề sau: phần mềm, tường lửa và hệ điều hành bị định cấu hình sai; phần mềm và hệ điều hành lạc hậu; Các giao thức không an toàn; cấu hình dịch vụ không cần thiết.

Có ba bước chính để thực hiện kiểm tra thâm nhập mạng bao gồm:

a. Thu thập thông tin,

b. Thăm dò và khám phá,

c. Thực hiện kiểm tra thâm nhập

1. Thu nhập thông tin (Information gathering): để thu thập các thông tin ba đầu về mục tiêu, bao gồm xác định các mục tiêu và mục tiêu của việc kiểm thử bảo mật. Việc thu thập thông tin bao gồm việc tìm kiếm thông tin công khai có liên quan đến hệ thống và tìm cách tiếp cận tốt nhất để khai thác thông tin đó. Mục đích của việc thu thập càng nhiều thông tin càng tốt, là để hiểu cách ứng dụng hoặc hệ thống hoạt động nhằm phát hiện ra những thiếu sót về bảo mật có thể khắc phục được.

2. Thăm dò và khám phá (Reconnaissance and discovery): Trong quá trình thu thập thông tin hệ thống, chúng tôi sẽ sử dụng các công cụ bảo mật để phác thảo mô hình mạng, các máy chủ và các lỗ hổng bảo mật đang tồn tại. Mục tiêu của chúng tôi sẽ là xem các lỗ hổng bảo mật nằm ở đâu để từ đó đưa ra hướng khai thác các lỗ hổng đó.

Dựa trên những thông tin thu thập được từ các bước trên chúng tôi sẽ lên kế hoạch để khai thác các lỗ hổng bảo mật đang tiềm ẩn trong hệ thống.

Những hạng mục được liệt kê dưới đây để sẽ được thực hiện:

- **Whois (DNS, domain names, name servers, IP):** bước này sẽ cung cấp cho chúng tôi thông tin của chủ sở hữu địa chỉ IP. Bao gồm thông tin của công ty đăng ký Internet, người chỉ định IP, chủ sở hữu được giao, vị trí địa lý của IP, thông tin liên hệ và các báo cáo vi phạm của IP(nếu có). Ngoài ra, chúng tôi có thể tìm ra được số lượng và dải IP đang được sở hữu.

- **Liệt kê bản ghi DNS (DNS enumeration):** Để phát hiện và liệt kê tất cả các bản ghi DNS có thể có từ một tên miền. Bao gồm tên máy chủ, tên bản ghi DNS, loại bản ghi DNS, TTL, địa chỉ IP.

- **Thu thập thông tin từ bộ máy tìm kiếm (Information gathering from Search Engine):** Đây là một quá trình thu thập thông tin thụ động, chúng tôi sẽ thu thập thông tin về mục tiêu từ các phương tiện truyền thông xã hội, công cụ tìm kiếm, các trang web, v.v.v. Thông tin thu thập bao gồm tên, chi tiết cá nhân, vị trí địa lý, trang đăng nhập, cổng mạng nội bộ, v.v. Ngoài ra có thể có một số thông tin như hệ điều hành, IP, thông tin Netblock, các công nghệ đang được sử dụng, v.v.v. Việc này có thể được làm bằng cách tìm kiếm thông qua các công cụ tìm kiếm(Ví dụ: Google, Bing, Shodan, DuckduckGo, v.v.v)

- **Tra cứu danh sách đen IP (IP Address Blacklist Check):** tra cứu lịch sử sử dụng của IP có thể chỉ ra các vấn đề về SPAM, các mối đe dọa hoặc điểm gian lận IP cao có thể khiến địa chỉ IP của bạn bị chặn và đưa vào danh sách đen với một trong gần 120 danh sách đen dựa trên DNS.

- **Quét công mạng (Port scanning):** để xác định cổng mạng nào hệ thống đang được sử dụng. Việc này giúp chúng tôi biết được những dịch vụ có thể đang chạy trên hệ thống. Có nhiều phương pháp khác nhau được sử dụng để quét cổng, bao gồm quét SYN, quét ACK và quét FIN.

- **Kiểm tra tường lửa (Firewall scanning):** để kiểm tra cấu hình của tường lửa có đảm bảo an toàn cho hệ thống mạng/ máy chủ.

- **Thu thập thông tin hệ điều hành/Ứng dụng(OS/Application fingerprinting):** để thu thập thông tin ứng dụng, máy chủ web hoặc hệ điều hành mà máy đang chạy. Đây là quá trình xác định hệ điều hành hoặc ứng dụng / máy chủ web của máy chủ từ xa bằng cách thăm dò máy chủ đó và phân tích phản hồi từ máy chủ đó.

- **Kiểm tra chứng thực(Authentication Testing):** Chúng tôi sẽ thực hiện các cuộc tấn công dò mật khẩu trên dịch vụ từ xa(SSH, MySQL). Đây là một kỹ thuật thử mọi sự kết hợp có thể có của các chữ cái, số và ký hiệu cho đến khi chúng tôi tìm ra được mất khẩu đúng để đăng nhập vào dịch vụ đó.

- **Quét lỗi bảo mật(Vulnerability scanning):** để phát hiện và phân loại các điểm yếu bảo mật trong máy chủ / mạng và dự đoán hiệu quả của các biện pháp đối phó. Quét lỗ hổng bảo mật có thể được thực hiện từ bên ngoài hoặc bên trong hệ thống máy chủ / mạng. Thực hiện quét lỗ hổng bảo mật từ bên ngoài để xác định khả năng bị tấn công của các máy chủ và ứng dụng có thể truy cập trực tiếp từ internet. Trong khi đó, việc quét lỗ hổng nội bộ nhằm xác định các lỗ hổng mà những kẻ tấn công có thể khai thác trong hệ thống mạng và máy chủ nếu kẻ tấn công có quyền truy cập vào mạng cục bộ.

- **Kiểm tra bảo mật tên miền phụ(Test for Subdomain Takeover):** lỗi bảo mật tên miền phụ xảy ra khi một tên miền phụ trỏ đến một dịch vụ (ví dụ: các trang GitHub, Heroku, v.v.) đã bị xóa. Điều này cho phép kẻ tấn công thiết lập một trang trên dịch vụ đang được sử dụng và trỏ trang của họ đến miền phụ đó. Ví dụ: nếu subdomain.example.com đã trỏ đến trang GitHub và người dùng quyết định xóa trang GitHub của họ, thì kẻ tấn công hiện có thể tạo trang GitHub, thêm bản ghi CNAME chứa subdomain.example.com và xác nhận quyền sở hữu subdomain.example .com.

3. **Thực hiện kiểm tra thâm nhập (Performing the penetration test):** chuyên viên kiểm thử bảo mật sẽ thực hiện kiểm tra khả năng thâm nhập hệ thống mạng/máy chủ bằng cách khai thác các lỗ hổng mà đã được xác định trong phần **Thăm dò và khám phá (Reconnaissance and discovery)**.

Công cụ: Nessus, Openvas, Nmap, Metasploit, Nexpose, Google, Shodan, DNSenum, DNSrecon, Netcat, HTTPSlowTest, Hydra, Medusa,

Hashcat, AWS Security Tools(Pacu, WeirdASAL, AWS Pwn, s3-fuzzer, S3Scanner, AWSBucketDump)