TÓM TẮT LUẬN VĂN THẠC SĨ

Đề tài: Nghiên cứu giải pháp tối ưu hóa tấn công Blind SQL injection

Tác giả luận văn: Hà Bách Nam Khóa: CHAT1

Người hướng dẫn:TS Đỗ Quang Trung – Học viện Kỹ thuật Mật mã.

Từ khóa (Keyword): SQL injection, Blind SQL injection, tối ưu hóa tấn công.

I. Lý do chọn đề tài

Thế giới đang sống trong một thời đại mới, thời đại phát triển của công nghệ thông tin, khi mà CNTT đã ở một bước phát triển cao, số hóa tất cả các dữ liệu thông tin, luân chuyển mạnh mẽ và kết nối mọi người lại với nhau. Mọi loại thông tin, số liệu âm thanh, hình ảnh có thể được đưa về dạng kỹ thuật số để bất kỳ máy tính nào cũng có thể lưu trữ, xử lý và chuyển tiếp cho người khác. Những công cụ và sự kết nối của thời đại kỹ thuật số cho phép chúng ta dễ dàng thu thập, chia sẻ thông tin và hành động trên cơ sở những thông tin này theo phương thức hoàn toàn mới, kéo theo hàng loạt sự thay đổi về các quan niệm, các tập tục, các thói quen truyền thống, và thậm chí cả cách nhìn các giá trị trong cuộc sống. Ứng dụng công nghệ thông tin đã đi tới từng hoạt động, công việc dù là nhỏ nhất. Trong đó, môi trường ứng dụng web được sử dụng nhiều nhất, vì tính tiện dụng, dễ dàng, không yêu cầu cài đặt, triển khai khó khăn phía người dùng cuối.

Tuy nhiên, ứng dụng web luôn phải đối mặt với những nguy cơ mất an toàn thông tin. Nguyên nhân có thể xuất phát từ lỗi lập trình, lỗi khi triển khai, cài đặt ứng dụng, lỗi khi vận hành, khai thác ứng dụng. Những lỗi này có thể tạo điều kiện cho kẻ tấn công khai thác, chiếm quyền điều khiển ứng dụng và máy chủ, gây ảnh hưởng lớn tới công ty, doanh nghiệp, hoạt động sản xuất kinh doanh. Việc sử dụng những phần mềm, ứng dụng không an toàn đã làm hao tổn nhiều chi phí cho các ngành tài chính, y tế, năng lượng.. và nhiều cơ sở hạ tầng quan trọng khác. Khi mà các hệ thống số của chúng ta ngày càng sở nên phức tạp và liên thông, việc bảo vệ nó cũng trở nên khó khăn hơn gấp nhiều lần.

OWASP Top 10 là danh sách được OWASP tổng hợp và công bố theo từng năm, nhằm đưa ra các cảnh báo rủi ro an ninh của ứng dụng web một cách ngắn gọn và xúc tích, giúp các doanh nghiệp, cá nhân xây dựng, phát triển, hay đánh giá an toàn thông tin các ứng dụng web có thể tự đưa ra được các giải pháp phù hợp, nâng cao bảo mật thông tin. Danh sách này luôn được thay đổi và cập nhật liên tục, do sự thay đổi về các tác động ảnh hưởng của các lỗ hổng.

Đứng đầu trong danh sách 10 rủi ro an toàn thông tin của ứng dụng web này chính là lỗi nhũng mã: Injection. Xảy ra trong các ứng dụng như SQL, LDAP khi những dữ liệu không xác thực được gửi đến hệ thống, biên dịch như một phần của mã lệnh. Những dữ liệu này của kẻ tấn công có thể lừa hệ thống biên dịch thực hiện những mã lệnh độc hại hoặc giúp kẻ tấn công xâm nhập đến những dữ liệu quan trọng một cách trái phép.

Tấn công nhúng mã SQL, hay còn được gọi là SQL injection, là dạng tấn công phổ biến nhất của tấn công nhúng mã. Tấn công này tập trung vào đối tượng là các cơ sở dữ liệu SQL. Được coi là trái tim của toàn bộ hệ thống, cơ sở dữ liệu chính là mục tiêu của hầu hết các cuộc tấn công mạng. Khai thác lỗi SQL injection, kẻ tấn công có thể khiến hệ thống mất mát dữ liệu, hư hỏng hoặc không thể kiểm tra hay truy cập đến dữ liệu. Năng hơn có thể dẫn đến toàn bộ hệ thống bị chiếm quyền.

Đối với ứng dụng web, ai cũng có thể gửi các dữ liệu không tin cập đến hệ thống: bao gồm người dùng bên ngoài, nội bộ, hay quản trị viên. Kẻ tấn công có thể gửi những mã tấn công dạng văn bản, khai thac sơ hở trong cú pháp truy vấn SQL. Bằng cách nhúng các mã SQL query/command vào đầu vào từ người dùng, trước khi chuyển cho ứng dụng web xử lý, kẻ tấn công có thể buộc ứng dụng thực thi đoạn mã SQL đó, từ đó có thể chiếm quyền điều khiển ứng dụng và máy chủ.

Trong các dạng tấn công SQL injection, Blind SQL injection là dạng rất phổ biến. Tấn công này sẽ phân tích nội dung trả về để xác định kết quả câu truy vấn được gửi đến ứng dụng web thực thi, để từ đó biết được kết quả câu truy vấn là đúng hay là sai. Có 02 kiểu phân tích phổ biến là: Boolean base (dựa vào nội dung trả về là đúng hay sai) và Time base (dựa trên thời gian trả về).

Phương pháp khai thác lỗ hổng Blind SQL injection truyền thống sẽ tấn công vét cạn, lần lượt gửi các yêu cầu truy vấn để hỏi ký tự cần lấy có phải là ký tự trong bảng mã ASCII hay không. Bảng mã ASCII có 256 ký tự, trong đó có khoảng 128 ký dạng dạng có thể in được (printable character) do đó yêu cầu phải sử dụng đến 128 lần gửi yêu cầu để có thể lấy về một ký tự. Điều này làm tiêu tốn nhiều thời gian, băng thông cho một cuộc tấn công, do đó, dễ dàng cho phép các hệ thống phát hiện xâm nhập phát hiện.

Ngày nay, trên thế giới liên tục có các nghiên cứu nhằm mục tiêu tối ưu hóa tấn công Blind SQL injection, mục tiêu giảm số lượng yêu cầu cần gửi xuống tối đa có thể. Hầu hết các kỹ thuật tối ưu hiện có trên thế giới cho phép với 7 lần yêu cầu có thể lấy về một ký tự, có nghĩa là giảm hơn 18 lần so với phương pháp truyền thống.

Với mục đích tối ưu hóa tấn công Blind SQL injection về số lượng yêu cầu cần gửi đi, em lựa chọn đề tài "Nghiên cứu giải pháp tối ưu hóa tấn công Blind SQL injection" làm đề tài luận văn tốt nghiệp thạc sĩ chuyên ngành An toàn thông tin. Đề tài luận văn sẽ đi sâu vào nghiên cứu, tìm hiểu một kỹ thuật tối ưu hóa mới, dựa vào phân tích thứ tự của dữ liệu trả về để từ đó có thể trích xuất ra dữ liệu mong muốn, giúp tối ưu nữa so với các phương pháp tối ưu hóa hiện có.

Luận văn đề cập đến một phương pháp mới trong việc tấn công Blind SQL injection. Hiện nay các phương pháp tấn công Blind SQL injection thường tận dụng việc phân tích các dạng dữ liệu trả về đơn giản (nội dung cơ bản, thời gian trả về). Các phương pháp này chỉ cho phép trong một lần yêu cầu trả về được hai kết quả (Đúng hoặc sai). Phương pháp được nghiên cứu trong đề tài dựa trên việc phân tích nội dung thứ tự của dữ liệu trả về, từ đó lấy được ra nhiều hơn hai kết quả trả về. Dựa vào đó, giảm số lần yêu cầu xuống, giúp tiết kiệm thời gian, băng thông so với các phương pháp trước đây.

Ý nghĩa khoa học và thực tiễn của luận văn:

- Ý nghĩa khoa học: Xây dựng phương pháp mới trong tấn công Blind SQL injection, giúp giảm số lượng yêu cầu cần gửi đi.

- Ý nghĩa thực tiễn: Hiểu và ứng dụng các kỹ thuật tối ưu hóa tấn công Blind SQL injeciton. Từ đó đưa ra các biện pháp phòng chống tấn công hiệu quả.

II. Mục tiêu nghiên cứu, đối tượng, phạm vi của luận văn

1. Mục tiêu nghiên cứu của luận văn

Tối ưu hóa tấn công Blind SQL injection bằng cách giảm số lượng yêu cầu cần gửi xuống mức tối đa có thể.

2. Đối tượng nghiên cứu của luận văn

Đối tượng nghiên cứu của đề tài là các kỹ thuật liên quan đến tối ưu hóa, giảm số lượng yêu cầu cần gửi đi để lấy dữ liệu trong tấn công Blind SQL injection.

3. Phạm vi nghiên cứu của luận văn

Phạm vi nghiên cứu của đề tài tập trung vào:

- Nghiên cứu về các kỹ thuật tối ưu hóa tấn công Blind SQL injection hiện nay: Tìm kiếm nhị phân, kỹ thuật dịch bit, kỹ thuật thu hẹp phạm vi tìm kiếm...
- Thực hiện sử dụng kỹ thuật tối ưu tấn công dựa trên mệnh đề ORDER BY trong ngôn ngữ SQL, từ đó đưa ra phương pháp tối ưu hóa dựa trên phân tích thứ tự nội dung trả về để trích xuất dữ liệu mong muốn.
- Các phương pháp và kỹ thuật phòng chống tấn công SQL injection.

III. Các nội dung chính của luận văn

Luận văn gồm 03 chương với nội dung như sau:

Chương 1: Trình bày về tấn công SQL injection nói chung, Blind SQL injection nói riêng:

- Tổng quan về lỗ hổng SQL injection: Dựa trên nguyên tắc hoạt động của ứng dụng web sử dụng cơ sở dữ liệu, từ đó làm rõ về lỗ hổng SQL injection, nguyên nhân, ảnh hưởng của lỗ hổng.
- Các phương pháp khai thác lỗ hổng SQL injection phổ biến như: Khai thác sử dụng mệnh đề UNION, khai thác sử dụng thông báo lỗi, kỹ thuật khai thác kênh ngoại tuyến (Out-of-band).
- Tấn công Blind SQL injection: Nguyên nhân, sự khác biệt so với các dạng SQL injection khác. Phương pháp cơ bản để khai thác lỗ hổng Blind SQL injection dựa trên phân tích nội dung trả về (Content-Base) và phương pháp phân tích thời gian trả về (Time-base).

Chương 2: Trình bày các phương pháp tối ưu hóa trong tấn công Blind SQL injection trên thế giới và đề xuất phương pháp tối ưu hóa dựa trên phân tích thứ tự nội dung trả về:

- Giới hạn của phương pháp khai thác Blind SQL injection truyền thống sử dụng kỹ thuật tấn công vét cạn đề dò quét ký tự tìm kiếm, từ đó đặt ra yêu cầu cần phải tối ưu hóa tấn công Blind SQL injection.
- Các phương pháp tối ưu hóa tấn công Blind SQL injection trên thế giới như: Tối ưu hóa sử dụng thuật toán tìm kiếm nhị phân, tối ưu hóa sử dụng phương

pháp dịch bit, tối ưu bằng cách dùng Bin2Pos. Thực hiện so sánh giữa các phương pháp

- Phân tích hướng tiếp cận của các phương pháp tối ưu trên dựa vào hình thái trả về của dữ liệu. Từ đó đề xuất hướng tiếp cận mới, có thể trích xuất nhiều hình thái trả về trong một lần yêu cầu, từ đó trích giúp giảm số yêu cầu cần gửi đi.

Chương 3: Đề xuất phương pháp tối ưu hóa dựa trên phân tích thứ tự nội dung trả về và xây dựng thực nghiệm, kiểm chứng thực tế các phương pháp tối ưu đã trình bày trong luận văn. Trong chương cũng trình bày các giải phòng chống lỗ hổng.

- Phương pháp khai thác lỗ hổng Blind SQL injection trong mệnh đề ORDER BY truyền thống. Từ đó đề xuất phương pháp tối ưu dựa trên phân tích thứ tự dữ liệu trả về, giới hạn của phương pháp và mở rộng sang tấn công Blind SQL injection.
- Giải pháp phòng chống lỗ hổng SQL injection nói chung, Blind SQL injection nói riêng: Các kỹ thuật mức lập trình như sử dụng Prepare Statement, kiểm tra đầu vào, mức nền tảng hệ thống.
- Xây dựng thực nghiệm và đánh giá kết quả tối ưu của các phương pháp. Từ đó chứng minh sự tối ưu hơn của phương pháp phân tích thứ tự nội dung trả về so với các phương pháp khác.

IV. Phương pháp nghiên cứu

Phương pháp nghiên cứu của đề tài bắt đầu từ tìm hiểu về tấn công Blind SQL injection: nguyên nhân, kỹ thuật tấn công. Từ đó, tiếp tục tìm hiểu các phương pháp tối tấn công,các kỹ thuật thực hiện tấn công và các hạn chế của các kỹ thuật hiện có.

Bằng việc đi sâu vào khai thác lỗ hổng Blind SQL injection trong trường hợp ứng dụng sử dụng mệnh đề ORDER BY, đề tài đưa ra một hướng tiếp cận mới trong khai thác tấn công: dựa vào phân tích nội dung dữ liệu trả về, cụ thể là thứ tự của dữ liệu. Dựa trên nền tảng đó, hình thành và phát triển kỹ thuật tối ưu hóa tấn công Blind SQL injection.

Trong quá trình làm đề tài sẽ cần sử dụng nhiều công cụ, cũng như cơ sở lý thuyết liên quan. Về cơ sở lý thuyết, đề tài sẽ sử dụng nhiều đến các lý thuyết liên quan đến:

- Lập trình ứng dụng web, tương tác với cơ sở dữ liệu SQL.
- Phương pháp tấn công SQL injection.
- Kỹ thuật, phân loại tấn công Blind SQL injection.
- Các phương pháp tối ưu tấn công Blind SQL injection hiện nay.
- Các phương pháp phòng chống tấn công SQL injection.

Về công cụ, là một đề tài liên quan đến tấn công vào cơ sở dữ liệu nên đề tài sẽ phải tập trung vào một loại hình cơ sở dữ liệu nào đó. đề tài lựa chọn hệ quản trị cơ sở dữ liệu MySQL, vì đây là hệ quản trị cơ sở dữ liệu rất phổ biến, được sử dụng nhiều trên thế giới. Trong quá trình làm việc cũng có thể đề cập đến nhiều loại cơ sở dữ liệu khác như: Microsoft SQL Server, Oracle Database.

Trong quá trình nghiên cứu các kỹ thuật tấn công, đề tài còn phải sử dụng nhiều kỹ thuật lập trình, phát triển các công cụ, mã tấn công, script tự động hóa. Ngôn ngữ lập trình để phát triển các mã tấn công (exploit) mà đề tài lựa chọn là ngôn ngữ Python. Đây là ngôn ngữ phổ biến, có nhiều thư viện, hàm hỗ trợ cho việc xây dựng mã tấn công, phù hợp với mục đích của đề tài.

V. Kết luận

Từ việc nghiên cứu các về lỗ hổng Blind SQL injection, các phương pháp tấn công phổ biến, luận văn đã đưa ra các kỹ thuật tối ưu hóa tấn công Blind SQL injection, từ đó đưa ra phương pháp phòng chống tấn công SQL injection nói chung, và Blind SQL injection nói riêng trong xây dựng, triển khai hệ thống công nghệ thông tin. Qua những kết quả thực nghiệm cho thấy các phương pháp tối ưu hóa là hoàn toàn khả thi, có thể áp dụng được trong thực tế, tuy nhiên, mỗi phương pháp đều có những yêu cầu cụ thể, cần nắm rõ các yêu cầu này trong triển khai thực tế.

Về mặt nội dung, luận văn đã đạt được những nội dung sau:

- Trình bày về nguyên nhân lỗ hổng SQL injection, Blind SQL injection, phương pháp khai thác cơ bản và cách phòng chống.
- Nghiên cứu các phương pháp tối ưu hóa tấn công Blind SQL injection đã có trên thế giới, phân tích sâu về phương pháp, cách thực hiện và triển khai các phương pháp này.

- Đề xuất một hướng tiếp cận mới trong tối ưu hóa tấn công Blind SQL injection dựa trên phân tích thứ tự nội dung trả về của dữ liệu. Từ đó xây dựng phương pháp, mã tấn công triển khai thực tế.
- Giải pháp phòng chống lỗ hổng SQL injection nói chung và Blind SQL injection nói riêng.
- Xây dựng thực nghiệm kiểm chứng các phương pháp tối ưu hóa đã được trình bày trong luận văn.

Về định hướng nghiên cứu tiếp theo, luận văn có thể phát triển theo các hướng sau:

- Một là nghiên cứu một hướng tiếp cận mới trong phân tích dữ liệu trả về, ngoài dựa trên thứ tự.
- Hai là giảm số lượng bản ghi tối thiểu cần có để phân tích được, để có thể áp dụng phương pháp phân tích thứ tự trên trong nhiều trường hợp khác.

VI. Danh mục các công trình khoa học đã công bố

Dưới sự hướng dẫn của thầy giáo TS Đỗ Quang Trung, em đã có 01 bài báo: "Tối ưu hóa tấn công BLIND SQL INJECTION" trên tạp chí An toàn thông tin – Ban Cơ yếu Chính phủ. Nội dung bài báo trình bày các kỹ thuật tối ưu tấn công Blind SQL injection và hướng tiếp cận dựa trên phân tích thứ tự trả về.

Đường dẫn bài báo: http://antoanthongtin.vn/Detail.aspx?NewsID=8770130c-2615-4621-a534-e877bb81d4ad&CatID=838ca04c-c317-484d-a461-00b464748b71