CƠ BẢN VỀ BẢO MẬT TRONG AJAX

Công nghệ Ajax đã xuất hiện trên các trang web từ nhiều năm trước nhờ có thuộc tính tương tác của nó. Google Suggest và Google Maps là hai ứng dụng của công nghệ này từ sớm. Ngày nay, các công ty đang nghĩ xem làm thế nào để có

Công nghệ Ajax đã xuất hiện trên các trang web từ nhiều năm trước nhờ có thuộc tính tương tác của nó. Google Suggest và Google Maps là hai ứng dụng của công nghệ này từ sớm. Ngày nay, các công ty đang nghĩ xem làm thế nào để có thể tận dụng được nó, các chuyên gia thiết kế web thì cố gắng học hỏi nó, các chuyên gia bảo mật cố gắng để bảo đảm nó, còn các thanh tra viên về chống thâm nhập đang nghĩ làm thế nào để có thể hack nó. Nói gì đi chăng nữa thì bất cứ một kỹ thuật mới nào mà có thể cải thiện thông lượng của các server, cung cấp việc chuyển trạng thái linh hoạt hơn và tạo ra các ứng dụng web phong phú hơn đến người sử dụng thì cũng rốt cuộc là tìm ra một vị trí đứng chân trong lĩnh vực công nghiệp. Ajax được xem như là bước tiếp theo của thế hệ "web 2.0". Mục đích của bài này là nhằm mục đích giới thiệu một vài vấn đề cơ bản về bảo mật trong công nghệ web Ajax hiện đại. Với Ajax, các ứng dụng có thể khó cho việc kiểm tra do đó các chuyên gia bảo mật đã chuẩn bị các phương pháp phù hợp và các công cụ cần thiết khác. Chúng ta sẽ thảo luận xem có cần nói lời chia tay với các ứng dụng web cũ thay vào đó là việc sử dụng Ajax để rồi cũng có nghĩa là chúng ta đón chào một vài lỗ hổng bảo mật mới. Bây giờ chúng ta sẽ thảo luận vắn tắt về các kỹ thuật bên trong của Ajax và xét ảnh hưởng các ứng dụng Ajax với bảo mật như thế nào. Cốt lõi của Ajax Các ứng dụng web thông thường làm việc trên mô hình đồng bộ, có nghĩa là khi có yêu cầu web của ai đó thì đi cùng với nó là một đáp ứng thực hiện một vài hành động trong lớp trình diễn (presentation). Ví dụ: việc click một link hay nhấn chuột vào nút submit sẽ tạo ra một yêu cầu đến web server với các tham số có liên quan. Thói quen "click và wait" này đã giới hạn sự tương tác của các ứng dụng. Vấn đề này được làm giảm bớt bằng việc sử dụng công nghệ Ajax (Asychronous Javascript and XML). Với mục đích của bài viết này tôi chỉ xem Ajax như một phương thức gọi không đồng bộ của nó tác động đến web server mà không phải refresh toàn bộ trang web. Loại tương tác này có thể thực hiện được bởi ba thành phần: ngôn ngữ scripting trình khách, đối tượng XmlHttpRequest(XHR) và XML. Sau đây chúng ta hãy thảo luận vắn tắt các thành phần này: Ngôn ngữ scripting trình khách được sử dụng để khởi tạo các lệnh call đến server sau đó được sử dụng để truy cập chương trình và update DOM bên trong trình duyệt của trình khách. Sự lựa chọn phổ biến nhất trên trình khách là Javascript bởi vì sự hiển thị của nó với các trình duyệt là khá tốt. Thành phần thứ hai là đối tượng XHR, đây mới thực sự là trái tim của kỹ thuật này. Các ngôn ngữ như Javascript sử dụng đối tượng XHR để gửi các yêu cầu đến web server ẩn dưới kịch bản và sử dụng HTTP như một trung gian truyền tải. XML sẽ định dạng dữ liệu cho các messages mà có thể thay đổi. Nhiều trang sử dụng JSON (Javascript Object Notation) trong phần XML bởi vì cú pháp của nó dễ hơn. Khi sử dụng Javascript để phân tích cú pháp JSON thì nó đơn giản nhiều. Mặt khác ai đó cũng có thể sử dụng Xpath để phân tích quay trở lại cú pháp XML. Cũng có nhiều trang Ajax không sử dụng XML hay JSON, thay vào đó chỉ gửi những mẩu HTML đã được chèn động tính vào trong trang web. Như đã chỉ ra ở trên, Ajax không phải là một công nghệ mới toanh mà thay vào đó là một sự kết hợp các công nghệ tồn tại trước đó cùng nhau để phát triển các ứng dụng web có tính tương tác cao. Trong thực tế, tất cả các thành phần trên đã xuất hiện trước và đã được sử dụng nhiều với IE 5.0. Các chuyên gia thiết kế đã đưa ra các trường hợp sử dụng Ajax như là "Suggestive" textboxes, và các bảng danh sách dữ liệu tự động refresh. Tất cả các yêu cầu XHR vẫn được xử lý bởi server side frameworks điển

hình như các chuẩn giống J2EE, .Net và PHP. Tính không đồng bộ của các ứng dụng Ajax được thể hiện trong hình dưới đây.

Bảo mật Ajax.Chúng ta đã ôn lại về Ajax, bây giờ hãy thảo luận về việc bảo mật nó. Ajax không có lỗ hổng bảo mật mới trong lĩnh vực ứng dụng web. Thay vào đó các ứng dụng đối mặt với các vấn đề bảo mật như các ứng dụng web cổ điển. Không may, các hành động chung nhất của Ajax lại không được phát triển, việc này đã để lại rất nhiều vùng có các vấn đề sai. Việc này bao gồm sự nhận thức đúng đắn, sự cấp phép, điều khiển truy cập và phê chuẩn đầu vào. Một vài lĩnh vực tiềm năng có liên quan đến sử dụng Ajax như sau: * Các điều khiển bảo mật trình khách Một vài người có thể tranh luận rằng sự phụ thuộc vào việc lập trình trên trình khách gây ra khả năng mang đến một vài vấn đề định hướng. Khả năng như vậy liên quan đến việc bảo mật của các chuyên gia thiết kế kém hiệu quả thông qua các điều khiển trình khách. Như chúng ta đã thảo luận trong phần trước trường hợp sử dụng của Ajax là khá ít cho mã scripting trình khách. Tuy nhiên các nhà thiết kế hiện nay đang phải viết cả hai loại mã trên trình chủ và trình khách. Vì vậy có thể thu hút các chuyên gia thiết kế hướng về điều khiển bảo mật trên trình khách. Rõ ràng trên trình khách là không an toàn vì các kẻ tấn công có thể thay đổi bất kỳ code nào đang chạy trên máy tính trình khách của họ. Chính vì vậy các điều khiển bảo mật cần phải bổ sung trên cả server hay luôn luôn phải được thi hành trên máy chủ. * Tăng bề mặt tấn công Một thách thức thứ hai liên quan đến sự khó khăn là việc bảo vệ sự tăng bề mặt tấn công. Ajax chắc chắn làm tăng độ phức tạp của tất cả các hệ thống. Trong quá trình mà Ajax kế tục, các chuyên gia thiết kế có thể viết mã với một số lượng lớn các trang trình chủ, mỗi trang thực hiện một vài chức năng nhỏ (trong cả ứng dụng lớn). Các trang nhỏ này sẽ là một target thêm vào cho các kẻ phá hoại và như vậy một điểm thêm nữa cần phải được bảo đảm để bảo vệ lỗ hổng mới không được giới thiệu. Điều này tương tự như các khái niệm bảo mật đã biết trong các lối đi vào của một ngôi nhà: khó khăn ở đây là chỗ việc bảo đảm cho một ngôi nhà một cửa so với cho một cái có 10 cửa. * Kẽ hở cầu nối giữa người dùng và các dịch vụ. Ajax là một phương pháp mang đến cho người dùng các giao diện thân thiện hơn bởi cấu trúc dịch vụ trực tiếp của nó. Cú hích để làm cho một cặp cấu trúc server-based rời ra là một ý tưởng đầy hứa hẹn với nhiều lợi ích nhất là trong môi trường kinh doanh. Khi có nhiều hơn các "endpoint" này được phát triển và khi Ajax giới thiệu khả năng đẩy việc xử lý tinh vi hơn đến người dùng thì triển vọng chuyển rời mô hình ba lớp sẽ xảy ra. Nhìn chung, nhiều dịch vụ web bên trong hệ thống kinh doanh (cái mà tương phản với toàn bộ mạng Internet) được thiết kế cho B2B (Business to Business), cũng chính vì thế các nhà thiết kế và phát triển thường không mong muốn sự tương tác với người dùng thực sự. Sự không lo xa này dẫn đến một loạt các giả định bảo mật tồi trong suốt quá trình thiết kế. Ví dụ, các nhà thiết kế lúc ban đầu đã thừa nhận sự nhận thức, quyền năng đó và hiệu lực ở đầu vào sẽ được thực hiện ở các hệ thống thuộc tầng giữa. Ai đó cho phép "outsiders" gọi trực tiếp các dịch vụ này thông qua Ajax, một tác nhân không mong muốn đã được giới thiệu trong ảnh. Một ví dụ thực của cuộc sống như vậy là một mắt xích phù hợp từ Microsoft đến sử dụng Atlas hand-in-hand với các dịch vụ web. Giờ đây các chuyên gia thiết kế có thể viết Javascript để tạo đầu vào XML và gọi đúng dịch vụ web từ bên trong trình duyệt của trình khách. Trong quá khứ, điều này đã được thực hiện thông qua các sự ủy nhiệm dịch vụ tại server.

(Còn nữa)

Phạm Văn LinhEmail: vanlinh@quantrimang.com