Bảo mật trong HTTP

HTTP được sử dụng cho giao tiếp thông tin qua Internet, vì thế các nhà lập trình ứng dụng, các nhà cung cấp thông tin, và những người sử dụng nên nhận biết các giới hạn bảo vệ trong HTTP/1.1. Chương thảo luận này sẽ không bao gồm các giải pháp rõ ràng tới những vấn đề được đề cập tại đây, nhưng nó đưa ra một số gợi ý để giảm các rủi ro.

Sự rò rỉ thông tin cá nhân

Các Client thường giữ bí mật một số lượng lớn thông tin cá nhân như tên người sử dụng, vị trí, địa chỉ mail, các khóa mật mã hóa, …. Vì thế bạn nên rất cẩn thận để ngăn cản sự rò rỉ thông tin này qua các giao thức HTTP tới các nguồn khác.

- Tất cả thông tin bí mật nên được lưu tại Server trong mẫu mật mã hóa.
- Khám phá phiên bản phần mềm riêng của Server có thể cho phép thiết bị Server để trở lên dễ tổn thương hơn khi bị tấn công phần mềm mà được biết tới là các lỗ hổng bảo mật.
- Các trạm ủy quyền mà phục vụ như là một cửa thông qua một bức tường lửa mạng nên thực hiện các biện pháp phòng ngừa đặc biệt tới việc truyền tải của thông tin Header mà nhận diện các host đằng sau tường lửa.
- Thông tin được gửi trong trường “From” có thể xung đột với các quyền lợi cá nhân của người sử dụng hoặc chính sách bảo mật của site, và vì thế, nó không nên được truyền tải mà không có sự giám sát của người sử dụng để không cho phép, cho phép hoặc chỉnh sửa các nội dung của trường.
- Các Client không nên bao gồm một trường Referer trong một yêu cầu HTTP (không an toàn), nếu trang đang hướng tới được truyền trải với một giao thức bảo mật.
- Các tác giả của dịch vụ mà sử dụng giao thức HTTP không nên sử dụng các mẫu dựa trên GET để chấp nhận dữ liệu nhạy cảm, bởi vì nó sẽ làm cho dữ liệu được mã hóa trong Request-URI.

Sự tấn công dựa trên các tên Path và File

Tài liệu nên được giới hạn tới các tài liệu mà được trả về bởi các yêu cầu HTTP tới chỉ những tài liệu mà đã được có dự định bởi người quản lý Server.

Ví dụ, UNIX, Microsoft và các hệ điều hành khác sử dụng `..` như là một thành phần đường truyền để chỉ một mức độ thư mục ở trên thư mục hiện tại. Trên một hệ thống như vậy, một Server PHẢI không cho phép bất cứ sự xây dựng nào trong Request-URI, nếu không thì nó cho phép truy cập tới một nguồn bên ngoài những thư mục này để được có thể truy cập thông qua Server.

Việc đánh lừa DNS (DNS Spoofing)

Các Client đang sử dụng HTTP chủ yếu dựa trên Dịch vụ tên miền (DNS), và là vì vậy thường dễ bị tấn công bảo mật dựa trên sự quên liên kết có chủ tâm của các địa chỉ IP và các tên DNS. Vì thế các Client cần chú ý trong khi đang giả sử rằng tính hiệu lực đang tiếp tục của một sự liên kết giữa IP/tên miền DNS.

Nếu các Client ghi vào bộ nhớ ẩn các kết quả của các sự tra cứu tên host để đạt được sự cải thiện hiệu suất, chúng phải theo dõi thông tin TTl được báo cáo bởi DNS. Nếu các Client không theo dõi quy luật này, chúng có thể bị đánh lừa khi một địa chỉ IP của Server đã truy cập trước đó thay đổi.

Vị trí các Header và việc đánh lừa

Nếu một Server đơn hỗ trợ nhiều tổ chức mà không tin tưởng lẫn nhau, thì khi đó nó PHẢI kiểm tra các giá trị của các trường Location và Content Location trong các phản hồi mà được tạo dưới sự điều khiển của các tổ chức được nhắc đến để đảm bảo rằng chúng không cố gắng chiếm lấy các nguồn tài nguyên không có hiệu lực mà qua đó chúng không có ủy quyền.

Ủy nhiệm xác minh

Các Client đang tồn tại và user agent có đặc trưng là ghi lại thông tin xác minh một cách mập mờ. HTTP/1.1 không cung cấp một phương thức cho Server để chỉ dẫn trực tiếp các Client loại bỏ những ủy nhiệm ghi vào bộ nhớ ẩn mà là một nguy cơ rủi ro bảo mật lớn.

Có một số công việc xung quanh tới các phần của vấn đề này, và vì thế nó được khuyến khích là sử dụng các mật khẩu bảo vệ trong việc bảo vệ màn hình, các thời gian rỗi, và một số phương thức khác mà làm giảm đi các vấn đề an toàn cố hữu trong vấn đề này.

Các sự ủy quyền và việc ghi vào bộ nhớ ẩn

Các sự ủy quyền HTTP là một Server trung gian, và tương ứng là các cơ hội về các nguy cơ tấn công ở trung gian. Các ủy nhiệm có truy cập tới thông tin bảo mật liên quan, thông tin cá nhân về từng người sử dụng và các tổ chức, và thông tin sở hữu riêng của người sử dụng và người cung cấp nội dung đó.

Các nhà điều hành ủy nhiệm nên bảo về các hệ thống mà các ủy nhiệm chạy trên đó, vì họ sẽ bảo vệ bất kỳ hệ thống nào mà chứa hoặc truyền tải thông tin nhạy cảm.

Việc ghi vào bộ nhớ ẩn các ủy nhiệm tạo ra thêm các lỗ hổng tiềm tàng, từ khi các nội dung của bộ nhớ ẩn biểu diễn một mực tiêu hấp dẫn cho sự khái thác ác ý. Vì thế, các nội dung bộ nhớ ẩn phải được bảo vệ như là thông tin nhạy cảm.