GiangTester Blog
A passionate tester

API Testing với Postman (Phần 4) – Các chuẩn bảo mật Authentication

Posted on **June 6, 2017**

Sau 3 bài viết, chúng ta đã hiểu thế nào là client và server, cách chúng sử dụng HTTP để nói chuyện với nhau và việc xác định định dạng dữ liệu để hiểu nhau. Có lẽ trong đầu chúng ta sẽ có câu hỏi: Làm thế nào để server biết client mà mình đang nói chuyện là anh nào, chị nào, xinh hay xấu.)))

Xác thực danh tính trong thế giới ảo

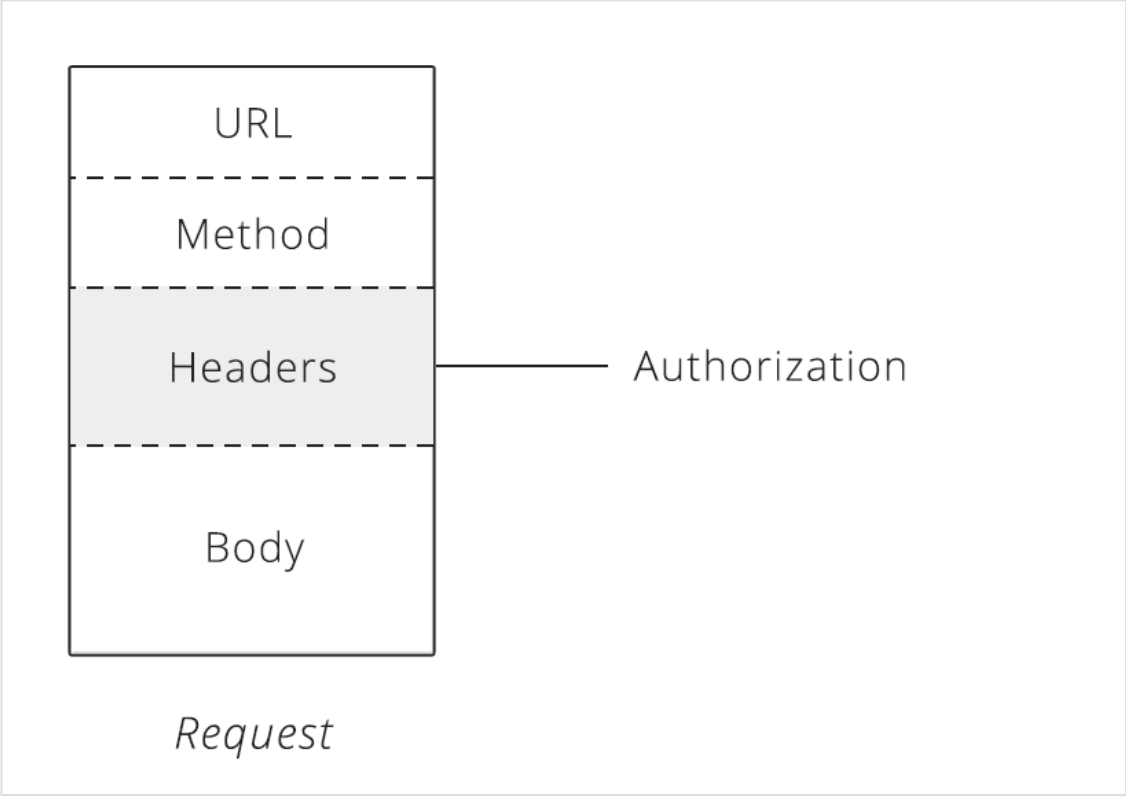
Giả sử bạn đã đăng ký 1 account ở 1 website, 2 thông tin không thể thiếu là username và password. Những thông tin này còn được gọi là "Giấy thông hành" – Credentials. Và những lần sau, để vào website bạn cần đưa ra cái "Giấy thông hành" đó.

Việc đăng nhập với username và password là 1 ví dụ của quá trình xác định danh tính – Authentication. Khi bạn chứng minh Danh tính với 1 server, bạn cung cấp thông tin mà chỉ có bạn và server biết. (không tính tới trường hợp ngy share account fb của nhau nhé :v). Một khi server biết bạn là ai, nó sẽ tin tưởng và cho phép bạn tiếp cận những thông tin bên trong.

Trong API, có rất nhiều kỹ thuật để xử lý phần Authentication này. Chúng được gọi là Authentication schemes.

Basic Authentication

Cái ví dụ vừa nói ở trên là cái form cơ bản nhất của Authentication, tên gọi chuẩn là Basic Authentication, hay được viết tắt là "Basic Auth". Basic Auth thì chỉ yêu cầu username và password thôi. Client nhập 2 thông tin trên rồi gửi chúng qua HTTP header cho server, đây gọi là quá trình xin phép – Authorization.



Khi server nhận được 1 request, nó sẽ soi vào Authorization header và so sánh thông tin đó với thông tin Credential mà chúng cất giữ ở DB. Nếu đúng, server sẽ chấp thuận request của client và trả thêm các thông mà client yêu cầu ở phần Body. Nếu không đúng, server sẽ trả lại mã code 401, báo hiệu rằng quá trình xác thực fail và yêu cầu bị từ chối.

Mặc dù Basic Auth là 1 kỹ thuật thường xuyên được sử dụng nhưng trên thực tế việc nó dùng cùng 1 username và password để truy cập đến API và quản lý tài khoản là không lý tưởng. Nó giống như việc 1 khách sạn đưa cho khách cả chùm chìa khóa của cả khách sạn chứ không phải là chìa khóa của 1 phòng.

API Key Authentication

API Key Authentication là 1 kỹ thuật giúp xử lý điểm yếu của mô hình Basic Auth ở phía trên. Thay vì đưa cả chùm chìa khóa cho khách hàng, chủ khách sạn chỉ đưa cho khách hàng đúng 1 (Key) chìa khóa phòng của họ. Key thông thường là 1 dãy dài số và chữ, là duy nhất và khác biệt với password.

Khi Client xác thực với API Key, server sẽ biết để đồng ý cho client truy cập tới data. Vậy thì API Key sẽ nằm ở vị trí nào trên request. Có thể chúng ta sẽ nghĩ là Key này chắc cũng nằm ở header giống như Basic Auth phía trên. Ơ không, nó nằm ở vị trí mà người lập trình mong muốn vì không có chuẩn nào cả. :v Có thể đặt nó trên header, trên URL (*http://example.com?api_key=my_secret_key*), hoặc là ở Body. Và cho dù có đặt chúng ở đâu đi chăng nữa, chúng cũng sẽ có cùng 1 tác dụng.

(Còn tiếp)

Nguồn: chương 4 của cuốn sách: "An Introduction to APIs" by Brian Cooksey

API Testing với Postman (Phần 5) – Giới thiệu chung về Postman

Sau bao nhiêu bài chém gió linh tinh, bài này mới bắt đầu vào công cụ Postman. Nguyên nhân chính của việc ít bài là do mình bận và mình lười. 😀 Bài này gồm có 3 mục chính: I. … Continue reading

G GiangTester Blog 1

This entry was posted in **API Testing**, **Testing Knowledge** and tagged **API testing**, **Authentication**, **Authorization** by **Giang**. Bookmark the **permalink [http://giangtester.com/api-testing-voi-postman-phan-4-cac-chuan-bao-mat-authentication/]** .

3 THOUGHTS ON "API TESTING VỚI POSTMAN (PHẦN 4) – CÁC CHUẨN BẢO MẬT AUTHENTICATION"

Pingback: API Testing với Postman (Phần 3) – Định dạng dữ liệu JSON và XML | GiangTester Blog

minh
on **July 25, 2017 at 2:36 pm** said:

Mặc dù Basic Auth là 1 kỹ thuật thường xuyên được sử dụng nhưng trên thực tế việc nó dùng cùng 1 username và password để truy cập đến API và quản lý tài khoản là không lý tưởng. Nó giống như việc 1 khách sạn đưa cho khách cả chùm chìa khóa của cả khách sạn chứ không phải là chìa khóa của 1 phòng.

Đoạn này khó hiểu nhỉ 😐

Giang
on **July 27, 2017 at 5:42 pm** said:

Vì với Basic Auth, tất cả các request đều có chứa password và nó tăng nguy cơ bị đánh cắp. Và vì nó là cái chìa khoá duy nhất cho tất cả các request nên một khi bị mất –> tất cả các phần khác đều toi.
Những thằng khác nó dùng cơ chế dạng như token, session nên nếu có bị đánh cắp thì nguy cơ chỉ đến với API đó thôi