**The HTTP Protocol**

Hypertext transfer protocol (HTTP) is the core communications protocol used to access the World Wide Web and is used by all of today’s web applications. It is a simple protocol that was originally developed for retrieving static text-based resources. It has since been extended and leveraged in various ways to enable it to support the complex distributed applications that are now commonplace.

**Giao thức HTTP (Hypertext Transfer Protocol) là giao thức truyền thông cốt lõi được sử dụng để truy cập World Wide Web và được sử dụng bởi tất cả các ứng dụng web hiện nay. Đây là một giao thức đơn giản ban đầu được phát triển để truy xuất tài nguyên văn bản tĩnh. Sau đó, nó đã được mở rộng và tận dụng theo nhiều cách khác nhau để hỗ trợ ứng dụng phân tán phức tạp mà hiện nay đã trở nên phổ biến.**

HTTP uses a message-based model in which a client sends a request message and the server returns a response message. The protocol is essentially connectionless: although HTTP uses the stateful TCP protocol as its transport mechanism, each exchange of request and response is an autonomous transaction and may use a different TCP connection.

**HTTP sử dụng một mô hình dựa trên tin nhắn, trong đó một máy khách gửi một thông điệp yêu cầu và máy chủ trả về một thông điệp phản hồi. Giao thức này thực chất là không duyệt kết nối: mặc dù HTTP sử dụng giao thức TCP bảo toàn trạng thái làm cơ chế truyền tải của nó, mỗi lần trao đổi yêu cầu và phản hồi là một giao dịch tự động và có thể sử dụng một kết nối TCP khác nhau.**

**HTTP Requests**

All HTTP messages (requests and responses) consist of one or more headers, each on a separate line, followed by a mandatory blank line, followed by an optional message body. A typical HTTP request is as follows:

GET /auth/488/YourDetails.ashx?uid=129 HTTP/1.1

Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/x-shockwaveflash, \*/\*

Referer: <https://mdsec.net/auth/488/Home.ashx>

Accept-Language: en-GB

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; FDM; .NET CLR 1.1.4322)

Accept-Encoding: gzip, deflate Host: mdsec.net

Connection: Keep-Alive

Cookie: SessionId=5B70C71F3FD4968935CDB6682E545476

**Tất cả các thông điệp HTTP (HTTP requests và HTTP responses) đều bao gồm một hoặc nhiều tiêu đề, mỗi tiêu đề trên một dòng riêng biệt, theo sau là một dòng trống bắt buộc, và theo sau là một phần thân thông điệp tùy chọn. Một HTTP request điển hình có dạng như sau:**

**Dòng đầu tiên của mỗi yêu cầu HTTP bao gồm ba phần, được ngăn cách bởi khoảng trắng:**

-A verb indicating the HTTP method. The most commonly used method is GET, whose function is to retrieve a resource from the web server. GET requests do not have a message body, so no further data follows the blank line after the message headers.

**Một động từ (verb) chỉ định phương thức HTTP. Phương thức HTTP được sử dụng phổ biến nhất là GET, có chức năng lấy một tài nguyên từ máy chủ web. Yêu cầu GET không có một phần thân (message body), do đó không có dữ liệu bổ sung sau dòng trống sau các tiêu đề thông điệp (message headers).**

-The requested URL. The URL typically functions as a name for the resource being requested, together with an optional query string containing parameters that the client is passing to that resource. The query string is indicated by the ? character in the URL. The example contains a single parameter with the name uid and the value 129.

**URL được yêu cầu. Thông thường, URL hoạt động như một tên gọi cho tài nguyên mà bạn muốn truy cập trên web, cùng với một chuỗi truy vấn tùy chọn chứa các tham số mà bạn gửi đến tài nguyên đó. Chuỗi truy vấn được chỉ định bằng ký tự "?" trong URL. Ví dụ này bao gồm một tham số duy nhất với tên là "uid" và giá trị là 129.**

-The HTTP version being used. The only HTTP versions in common use on the Internet are 1.0 and 1.1, and most browsers use version 1.1 by default. There are a few differences between the specifi cations of these two versions; however, the only difference you are likely to encounter when attacking web applications is that in version 1.1 the Host request header is mandatory.

**Phiên bản HTTP đang được sử dụng. Trên Internet, phiên bản HTTP phổ biến nhất là 1.0 và 1.1, và hầu hết các trình duyệt sử dụng phiên bản 1.1 mặc định. Có một số sự khác biệt giữa các thông số kỹ thuật của hai phiên bản này; tuy nhiên, sự khác biệt duy nhất bạn có thể gặp khi tấn công các ứng dụng web là trong phiên bản 1.1, tiêu đề yêu cầu "Host" là bắt buộc.**

**Dưới đây là một số điểm đáng chú ý khác trong yêu cầu mẫu:**

**-**The Referer header is used to indicate the URL from which the request originated (for example, because the user clicked a link on that page). Note that this header was misspelled in the original HTTP specifi cation, and the misspelled version has been retained ever since.

**Tiêu đề "Referer" được sử dụng để chỉ định URL mà yêu cầu bắt nguồn (ví dụ, do người dùng nhấp vào một liên kết trên trang đó). Lưu ý rằng tiêu đề này đã được viết sai chính tả trong thông số kỹ thuật ban đầu của HTTP, và phiên bản viết sai này đã được duy trì từ đó.**

-The User-Agent header is used to provide information about the browser or other client software that generated the request. Note that most browsers include the Mozilla prefi x for historical reasons. This was the UserAgent string used by the originally dominant Netscape browser, and other browsers wanted to assert to websites that they were compatible with this standard. As with many quirks from computing history, it has become so established that it is still retained, even on the current version of Internet Explorer, which made the request shown in the example.

**Tiêu đề "User-Agent" được sử dụng để cung cấp thông tin về trình duyệt hoặc phần mềm khách khác đã tạo ra yêu cầu. Lưu ý rằng hầu hết các trình duyệt bao gồm tiền tố "Mozilla" vì lý do lịch sử. Đây là chuỗi User-Agent được sử dụng bởi trình duyệt Netscape ban đầu chiếm ưu thế, và các trình duyệt khác muốn khẳng định với các trang web rằng họ tương thích với tiêu chuẩn này. Giống như nhiều điểm kỳ cục trong lịch sử máy tính, nó đã trở nên quen thuộc đến mức nó vẫn được giữ lại, ngay cả trên phiên bản hiện tại của Internet Explorer, mà đã tạo yêu cầu được hiển thị trong ví dụ.**

**-** The Host header specifi es the hostname that appeared in the full URL being accessed. This is necessary when multiple websites are hosted on the same server, because the URL sent in the fi rst line of the request usually does not contain a hostname.

**Tiêu đề "Host" chỉ định tên máy chủ (hostname) xuất hiện trong URL đầy đủ mà đang được truy cập. Điều này cần thiết khi nhiều trang web được lưu trữ trên cùng một máy chủ, bởi vì URL gửi trong dòng đầu tiên của yêu cầu thường không chứa tên máy chủ.**

**-** The Cookie header is used to submit additional parameters that the server has issued to the client

**Tiêu đề "Cookie" được sử dụng để gửi các tham số bổ sung mà máy chủ đã cấp cho máy khách**

**HTTP Responses**

A typical HTTP response is as follows:

HTTP/1.1 200 OK

Date: Tue, 19 Apr 2011 09:23:32 GMT

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

Set-Cookie: tracking=tI8rk7joMx44S2Uu85nSWc

X-AspNet-Version: 2.0.50727

Cache-Control: no-cache

Pragma: no-cache

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Content-Type: text/html; charset=utf-8

Content-Length: 1067

The first line of every HTTP response consists of three items, separated by spaces: The HTTP version being used. A numeric status code indicating the result of the request. 200 is the most common status code; it means that the request was successful and that the requested resource is being returned. n A textual “reason phrase” further describing the status of the response. This can have any value and is not used for any purpose by current browsers.

**Dòng đầu tiên của mỗi phản hồi HTTP bao gồm ba mục, được ngăn cách bởi khoảng trắng:**

**- Phiên bản HTTP đang được sử dụng.**

**- Mã trạng thái số chỉ định kết quả của yêu cầu. Mã trạng thái 200 là mã trạng thái phổ biến nhất; nó có nghĩa rằng yêu cầu đã thành công và tài nguyên được yêu cầu đang được trả về.**

**- Một "reason phrase" văn bản mô tả thêm về trạng thái của phản hồi. Điều này có thể có bất kỳ giá trị nào và không được sử dụng cho bất kỳ mục đích nào bởi các trình duyệt hiện tại.**

Here are some other points of interest in the response: n The Server header contains a banner indicating the web server software being used, and sometimes other details such as installed modules and the server operating system. The information contained may or may not be accurate. n The Set-Cookie header issues the browser a further cookie; this is submitted back in the Cookie header of subsequent requests to this server. n The Pragma header instructs the browser not to store the response in its cache. The Expires header indicates that the response content expired in the past and therefore should not be cached. These instructions are frequently issued when dynamic content is being returned to ensure that browsers obtain a fresh version of this content on subsequent occasions. n Almost all HTTP responses contain a message body following the blank line after the headers. The Content-Type header indicates that the body of this message contains an HTML document. n The Content-Length header indicates the length of the message body in bytes.