

# Pangolin v3.2.4

## User Guide

---

Document Release Date: Jan 2011

Software Release Date: Jan 2011



## **Legal Notices**

### **Warranty**

The only warranties for NOSEC products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. NOSEC shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### **Copyright Notice**

© Copyright 2006-2011 NOSEC

### **Trademark Acknowledgements**

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

### **Other Acknowledgements**

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer:

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the organization nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

## **Support**

For information or assistance regarding Pangolin, contact customer support:

E-mail: [support@nosec.org](mailto:support@nosec.org)

Telephone: +86 133-168-80733

# I. Content

I.	Getting Started.....	5
	Software Installation.....	5
	Licensing .....	5
	Prepare Your System for Pen-testing .....	6
II.	Using the Pangolin .....	8
III.	Settings .....	13
	HTTP.....	13
	Proxy.....	13
	Scan.....	13
	Advance.....	14
	Oracle.....	15
	URL Operation .....	15
	Network.....	15
IV.	HTTP Status Codes .....	17

## II. Getting Started

### Software Installation

Before installing Pangolin, make sure that your system meets the following minimum requirements:

- 1 GB of memory
- 100 MB of free disk space
- 1.0 GHz Processor or better
- Microsoft Internet Explorer 6.0 or 7.0
- Windows 2000/Windows XP/Windows Vista 32bit/ Windows Vista 64bit /Windows 7 32bit/Windows 7 64bit

Pangolin is a green tool. Use the following procedure to install it.

1. Start the extract zip file.
2. Run pangolin.exe;
3. When the process is complete, click **Finish**.

### Licensing

The first time you start Pangolin, the program displays the Pangolin Product

Registration Wizard, which prompts you to select one of the following options:

- Register for a 15-day trial
- Use an existing activation token

### Trial Registration

Use the following procedure to begin a free 15-day trial of Pangolin.

1. On the *Pangolin Product Registration Wizard* window, select **Register for a free 15-day trial** and click **Next**.
2. Enter the requested information.

3. If connecting to the Internet through a proxy, click **Connection Settings**, modify the settings (if necessary) and click **OK**.
4. Click **Next**.
5. The program attempts to contact NOSEC servers, which will send an e-mail message to you containing a 32-character activation token.
6. Click **Finish**.
7. When the e-mail arrives, click the Pangolin **Edit** menu and select **Application Settings**.
8. On the *Application Settings* window, select **License** from the left pane.
9. Enter the 32-digit license token, omitting any hyphens that may appear in the string (or simply copy the token, position your cursor in the first block of the **Activation Token** field, and press **Ctrl + V**).
10. (Optional) Enter a description.
11. Click **OK**.

## **Prepare Your System for Pen-testing**

### **Create a Backup**

Before auditing their production system, create a backup copy of their database and then restore it after the Pen-testing is complete.

## **Pen-testing a web Site**

Pangolin is ideal for penetration testers, With Pangolin Injection Digger, Admin Page Discover, Data dumper you can see what a serious impact an SQL injection can have on the website. You will also be able to enumerate databases, tables, dump data and also read specific files on the file system of the web server, Depending on the settings of website. Using this tool, you can also run command, read registry(Windows System), write file, create users, browse file, custom SQL select queries even control the operating system, Pangolin supports most types of database than any other injection tools: Oracle, PostgreSQL, MySQL, Sybase, SQLite, Access, MSSQL all edition, and DB2. Supported language systems including Korean.

Pangolin submitting complicated HTTP requests to test SQL injection vulnerabilities. Then try to take advantage of SQL injection vulnerabilities on web applications.

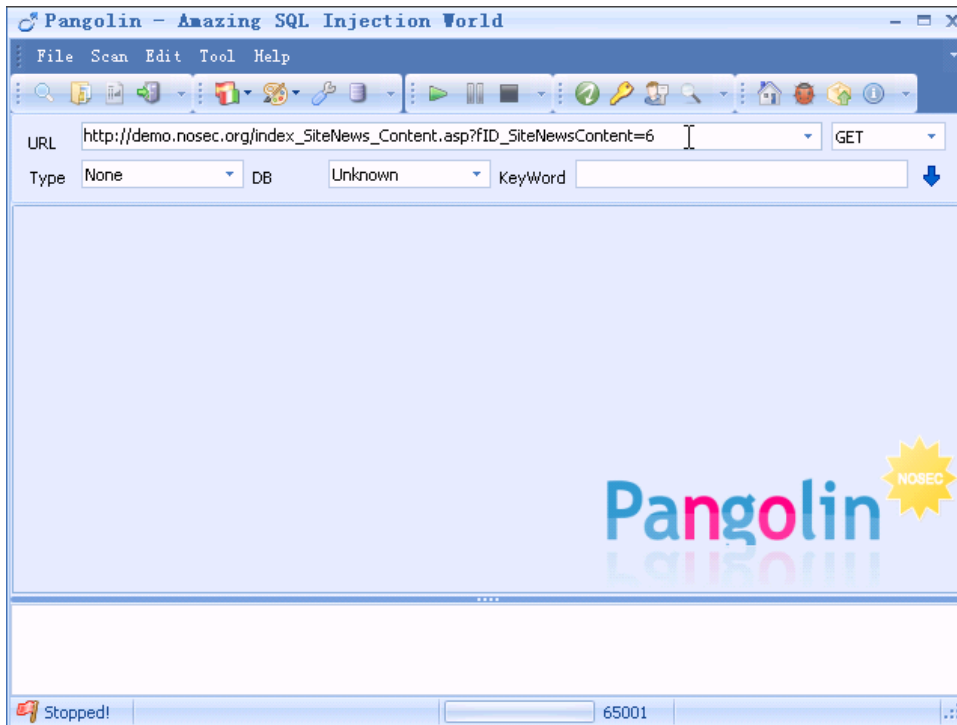
### III. Using the Pangolin

Follow the steps below to test for susceptibility to SQL injection:

If using a proxy server or if the target site requires authentication, click the **Settings** tab and enter the appropriate information. See **Settings** on page 12 for additional information.

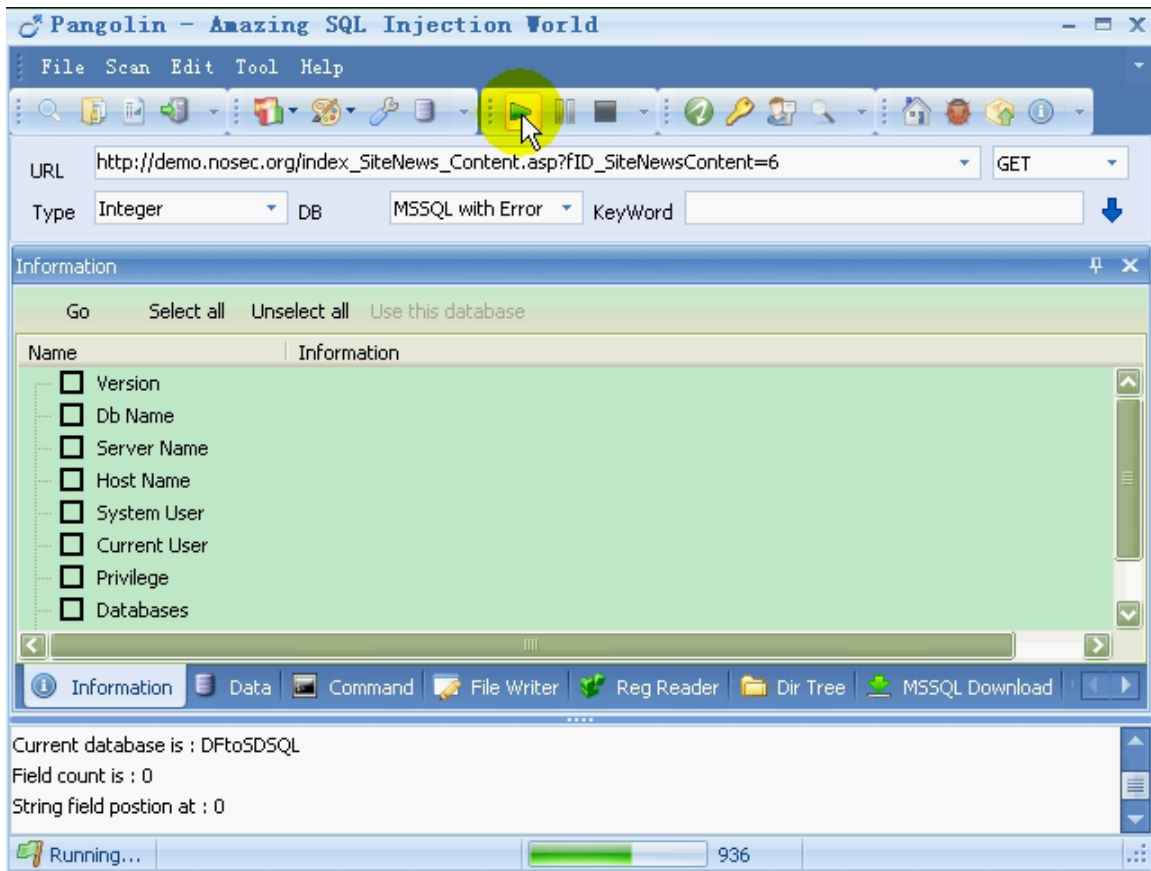
If the url need login to access, Please read **Read Cookie** on Page 12.

Run Pangolin then type or paste the URL that you suspect is susceptible to SQL injection. See examples below.

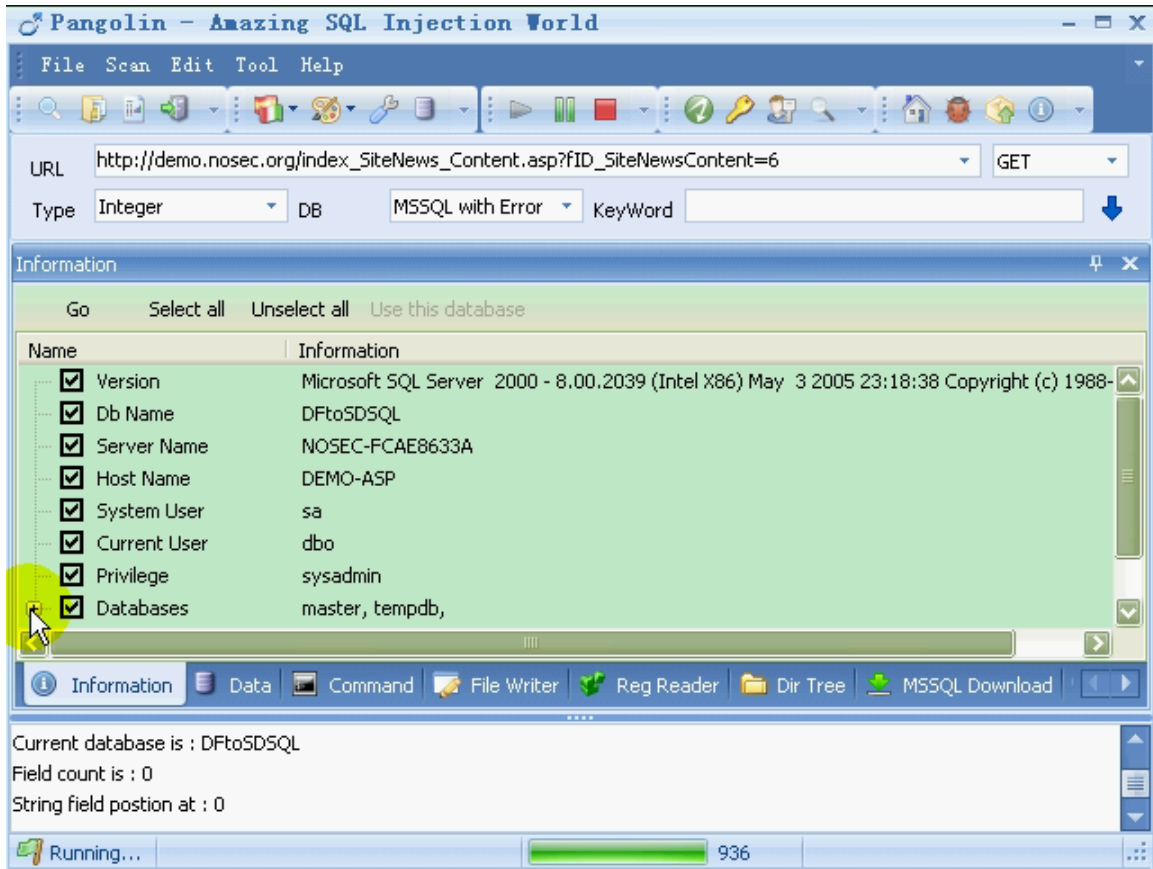


Click **Start**. Pangolin will start try to inject the website. “Running...” appears on the **Status bar** and **Progress bar** convey the progress of inject.

If SQL injection is successful, **Information tab** appear on **Operation Panel**.



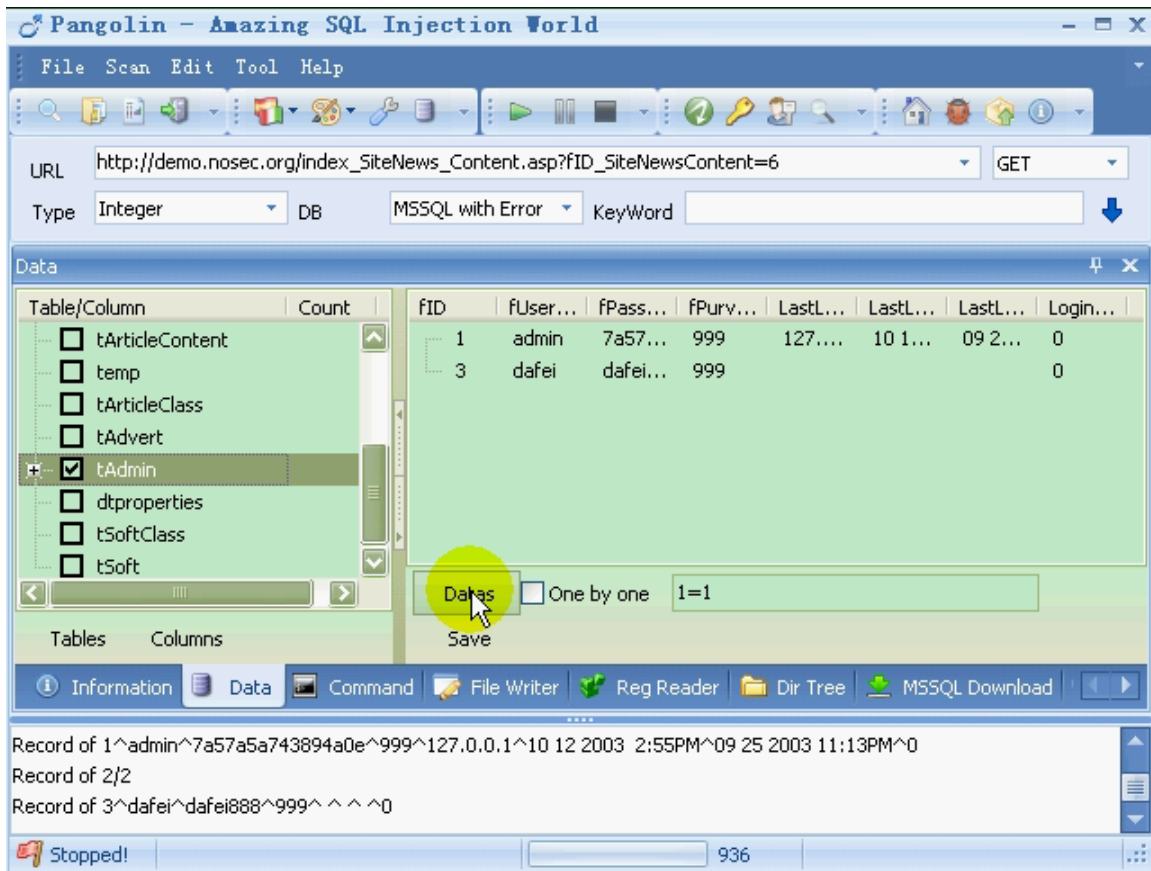
Click “**Select all**” and “**Go**”. Web server information including operating system and database, appears. You can read database version, database name, server name, system user, etc.



To extract all the data from all tables, click **Data** tab.

To investigate tables click **Table** wait until **Status** bar appear “stopped”. Pangolin returns the names of all tables in the targeted database. To fetch column info double click the table and wait until **Status** bar appear “stopped”.

Choose tables by selecting their associated check box. Click **Datas** to fetch data for the selected table.



## Operation Panel Tabs

The operation panel contains following tabs:

**Information** - Displays web server and database information.

**Data** - Displays table, columns and data extracted from the selected tables

**Command** - Execute system command in CMD (MSSQL only).

**File Writer** - Write any file to web server directory you specify (MSSQL only).

**Reg Reader** - Read web server register (MSSQL only).

**Dir Tree** - Enumerate driver and file. Read file content (MSSQL only).

**MSSQL Download** - Upload file to web server (MSSQL only).

**Remote** - Transfer MSSQL data to another MSSQL. This is another way to fast dump data (MSSQL only).

**mssqlqueryFrm** - Execute SQL query. Parts function of MSSQL Query Analyzer.

**File Reader** - Read operating system file (MySQL Only).

**MySQL File Writer** - Write any file to web server directory you specify (MySQL only).

**Oracle Remote Data** - Transfer Oracle data to remote data server. Another way to fast dumps data (Oracle only).

**Oracle Query** - Execute PL/*SQL* query. Parts function of SQL\*Plus

## IV. Settings

To access this feature, click the **Edit** menu and select **Settings**. Then select one of the following categories:

### **HTTP**

#### **Proxy**

#### **Scan**

#### **Advance**

#### **Oracle**

#### **URL Operation**

#### **Network**

### **HTTP**

#### **Read Cookie**

If URL has potential SQL injection vulnerability required login to access. Use this feature to login the page then start inject.

#### **User Agent**

Define http header parameter User Agent.

#### **Proxy**

Define proxy settings.

#### **Scan**

##### **Scan with search type**

Try SQL injection with type search too. So Pangolin will use integer, string, and search.

##### **Scan SQLSERVER first**

Define SQL injection order start from MSSQL. Normally injection with MSSQL will not put into the first.

### **Scan all parameter not the last one**

Try SQL injection with all URL parameter in target URL. Not only the last one.

### **Check blind count method**

Define fetch SQL Query column count method.

### **Check valid page method**

Define how to Normal page and error page.

## **Advance**

### **Replace space as**

Define character to bypass when space is blocked

### **Bypass firewall when 'select' is not allow**

Define bypass firewall when 'select' is blocked

### **Auto analyze keyword**

SQL Injection will generate keywords to inject automatically. One of Pangolin features which is selected by default.

### **Uri encode mode**

Encode HTTP request

### **Enable BT mode (bypass firewall)**

Enable BT mode to bypass firewall

### **Stop after error happens (access data)**

SQL Injection will stop when error happens.

### **Auto check record count of table**

Get each table records count when investigate.

### **Default Charset**

Define Character set of target URL.

## **Oracle**

### **Remote Data URL**

Pangolin investigate database and detect target url backend database is Oracle. When try to inject with Error or Union are failed dump data will be very slow. To fast dump data Pangolin send a request to web server cause backend Oracle send HTTP request to **Remote Data URL**. This result Remote Data URL receives data send from Oracle then saves to Remote Info URL. These configurations are used in **Oracle Remote Data tab** in **Operation** Panel.

### **Remote Info URL**

Remote Info URL is used to save data received from Oracle.

## **URL Operation**

### **URL is case sensitive**

Selected when web server process URL case sensitive.

### **Replacement Table**

Add or delete URL replacement when web application firewall blocks SQL keywords. Such as: select, from, comma, Space.

## **Network**

### **Connect Timeout**

Specify the number of seconds that the SQL Injector will wait for a start connection before terminating the session.

### **Receive Timeout**

Specify the number of seconds that the SQL Injector will wait for a response before terminating the session.

### **HTTP Interval**

Define send HTTP request interval



## V. HTTP Status Codes

### Introduction

The following list of status codes was extracted from the Hypertext Transfer Protocol version

1.1 standard (rfc 2616). You can view the complete standard at <http://www.w3.org/Protocols/rfc2616/rfc2616.html>.

Status Code	Reason Phrase	Description
100	Continue	Client should continue sending its request. This is a special status code; see below for details.
101	Switching Protocols	The client has used the <i>Upgrade</i> header to request the use of an alternative protocol and the server has agreed.
200	OK	Generic successful request message response. This is the code sent most often when a request is filled normally.
201	Created	The request was successful and resulted in a resource being created. This would be a typical response to a <i>PUT</i> method.
202	Accepted	The request was accepted by the server but has not yet been processed. This is an intentionally “non-committal” response that does not tell the client whether or not the request will be carried out; the client determines the eventual disposition of the request in some unspecified way. It is used only in special



		circumstances.
203	Non-Authoritative Information	The request was successful, but some of the information returned by the server came not from the original server associated with the resource but from a third party.
204	No Content	The request was successful, but the server has determined that it does not need to return to the client an entity body.
205	Reset Content	The request was successful; the server is telling the client that it should reset the document from which the request was generated so that a duplicate request is not sent. This code is intended for use with forms.
206	Partial Content	The server has successfully fulfilled a partial GET request. See the topic on methods for more details on this, as well as the description of the Range header.
300	Multiple Choices	The resource is represented in more than one way on the server. The server is returning information describing these representations, so the client can pick the most appropriate one, a process called agent-driven negotiation.
301	Moved Permanently	<p>The resource requested has been moved to a new URL permanently. Any future requests for this resource should use the new URL.</p> <p>This is the proper method of handling situations where a file on a server is renamed or moved to a new directory. Most people don't bother setting this up, which is why URLs “break” so often, resulting in 404 errors as discussed below.</p>
302	Found	The resource requested is temporarily using a different URL. The client should continue to use the original URL. See code



		307.
303	See Other	The response for the request can be found at a different URL, which the server specifies. The client must do a fresh <i>GET</i> on that URL to see the results of the prior request.
304	Not Modified	The client sent a conditional <i>GET</i> request, but the resource has not been modified since the specified date/time, so the server has not sent it.
305	Use Proxy	To access the requested resource, the client must use a proxy, whose URL is given by the server in its response.
306	(unused)	Defined in an earlier (draft?) version of HTTP and no longer used.
307	Temporary Redirect	<p>The resource is temporarily located at a different URL than the one the client specified.</p> <p>Note that 302 and 307 are basically the same status code. 307 was created to clear up some confusion related to 302 that occurred in earlier versions of HTTP (which I'd rather not get into!)</p>
400	Bad Request	Server says, "huh?" ☺ Generic response when the request cannot be understood or carried out due to a problem on the client's end.
401	Unauthorized	The client is not authorized to access the resource. Often returned if an attempt is made to access a resource protected by a password or some other means without the appropriate credentials.



402	Payment Required	This is reserved for future use. Its mere presence in the HTTP standard has caused a lot of people to scratch their chins and go “hmm...” ☺
403	Forbidden	The request has been disallowed by the server. This is a generic “no way” response that is not related to authorization. For example, if the maintainer of Web site blocks access to it from a particular client, any requests from that client will result in a 403 reply.
404	Not Found	The most common HTTP error message, returned when the server cannot locate the requested resource. Usually occurs due to either the server having moved/removed the resource, or the client giving an invalid URL (misspellings being the most common cause.)
405	Method Not Allowed	The requested method is not allowed for the specified resource. The response includes an <i>Allow</i> header that indicates what methods the server will permit.
406	Not Acceptable	The client sent a request that specifies limitations that the server cannot meet for the specified resource. This error may occur if an overly-restrictive list of conditions is placed into a request such that the server cannot return any part of the resource.
407	Proxy Authentication Required	Similar to 401, but the client must first authenticate itself with the proxy.
408	Request Timeout	The server was expecting the client to send a request within a particular time frame and the client didn't send it.
409	Conflict	The request could not be filled because of a conflict of some



		sort related to the resource. This most often occurs in response to a <i>PUT</i> method, such as if one user tries to <i>PUT</i> a resource that another user has open for editing, for example.
410	Gone	The resource is no longer available at the server, which does not know its new URL. This is a more specific version of the 404 code that is used only if the server knows that the resource was intentionally removed. It is seen rarely (if ever) compared to 404.
411	Length Required	The request requires a Content-Length header field and one was not included.
412	Precondition Failed	Indicates that the client specified a precondition in its request, such as the use of an <i>If-Match</i> header, which evaluated to a false value. This indicates that the condition was not satisfied so the request is not being filled. This is used by clients in special cases to ensure that they do not accidentally receive the wrong resource.
413	Request Entity Too Large	The server has refused to fulfill the request because the entity that the client is requesting is too large.
414	Request-URI Too Long	The server has refused to fulfill the request because the URL specified is longer than the server can process. This rarely occurs with properly-formed URLs but may be seen if clients try to send gibberish to the server.
415	Unsupported Media Type	The request cannot be processed because it contains an entity using a media type the server does not support.
416	Requested Range Not Satisfiable	The client included a <i>Range</i> header specifying a range of values that is not valid for the resource. An example might be



		requesting bytes 3,000 through 4,000 of a 2,400-byte file.
417	Expectation Failed	The request included an <i>Expect</i> header that could not be satisfied by the server.
500	Internal Server Error	Generic error message indicating that the request could not be fulfilled due to a server problem.
501	Not Implemented	The server does not know how to carry out the request, so it cannot satisfy it.
502	Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from another server it tried to access on the client's behalf.
503	Service Unavailable	The server is temporarily unable to fulfill the request for internal reasons. This is often returned when a server is overloaded or down for maintenance.
504	Gateway Timeout	The server, while acting as a gateway or proxy, timed out while waiting for a response from another server it tried to access on the client's behalf.
505	HTTP Version Not Supported	The request used a version of HTTP that the server does not understand.