

# HTForm™

## Web-Form Processing Script

- communicates inputs as HTML email
- uploads files as email attachments
- logs input data to server as CSV files
- archives file uploads for easy retrieval
- extensive security features
- easily customized
- designed for UNIX (Apache) servers

### DESCRIPTION

HTForm™ is a full-featured HTML-form-processing CGI script written in Perl and designed to run on UNIX (Apache) servers. HTForm accepts form content via the POST method, and content-type (set using the enctype attribute) may be either "multipart/form-data" or the default "x-www.-form-urlencoded". Form inputs are transmitted as HTML email paragraphs with the input field names as headers. With enctype = "multipart/form-data", file-upload fields may be included in forms, and uploaded files are transmitted as email attachments. HTForm also optionally saves form data as log files in CSV (comma separated values) format for easy import by Excel® or other database applications. HTForm can automatically archive uploaded files on the server with filename prefixed with a unique numeric string for easy reference to corresponding database and email content. The script is extensively annotated with comments as a guide to its use and functionality and can be easily customized by programmers familiar with Perl.

HTForm was written in response to a client project that required graphic files to be uploaded as form input. An online search for scripts purporting to support this feature produced several candidates. However, in testing, these were disappointing and some failed to perform properly. Consequently, an entirely new script was produced. It also appeared that such a script might be of general value to other web programmers. Therefore it was decided to offer HTForm for download as qualified shareware.

### LICENSING

HTForm is a copyrighted program of Paul Chadwick dba Seaview Scientific. You can download HTForm and all of its documentation and use it free for up to 30 days. After that, if you find the script satisfactory and wish to continue to use it, you may purchase an unlimited license for \$100. Commercial web hosting companies that wish to provide HTForm as a utility for their clients are requested to contact Seaview Scientific and obtain a special mass license. For tax reasons, New Mexico residents and programmers or companies that place the HTForm script on web servers located in the state of New Mexico are exempt from licensing fees. In programming HTForm, I have attempted to create a script that provides a useful combination of features previously unavailable for many web programmers. Significant time and effort was expended in this effort. Should you choose to use HTForm in your project, please respect my creative effort and comply with these modest licensing requirements.

### SECURITY

Because form processing scripts are often identified by web spiders and subject to misuse for sending large numbers of anonymous unauthorized emails (spam), HTForm includes numerous security features to thwart such activities. Unauthorized access can be easily monitored, and unauthorized transmittals are short-circuited and prevented from sending emails to the normal or their intended recipients. Unauthorized transmittals may be trapped as email to a special debugging email address with additional information that can help to identify the hacker or inactivate the email transmission entirely.

Security features have been extensively tested, and additional security features have been added to HTForm as a result of experience in use. The security features included in HTForm are believed sufficient to defeat any attempt to hijack the script for sending large quantities of unauthorized email.

## OPTIONS IN THE HTForm CODE

View and edit the code by opening HTForm.cgi with any text-editing program. The code was created on a Macintosh using BBEdit from Bare Bones Software, Inc. ([www.barebones.com](http://www.barebones.com)), highly recommended for Macintosh users.

### General Settings

In this section you can specify a redirect page, to which the browser moves when form processing is completed successfully. The redirect page, if specified, should be referenced by absolute URL (<http://www...> etc.). Alternatively, you can specify the name of a hidden field on the form that will contain the redirect URL specification (also as absolute URL). If no redirect URL is specified, a generic message will be displayed upon successful processing of the form.

The next general setting allows you to specify a hidden field on the form that will contain the list of input fields for which entries are required. If any one or more of these fields has not been completed before the form is processed, an error message with a “back” button will be displayed, indicating that clarification is required.

### Email Settings

The \$sendmail value determines if the form results are to be sent as email. Editing this value to 0 will result in no email record of the form input, in which case a CSV file record will be essential.

The \$mailprog value must be set to contain the path to the Sendmail program on your web server. The most common value is entered as default. Check with your hosting provider to obtain the correct value for this setting. HTForm is designed to operate on Apache servers, which are UNIX based. Linux servers will be similar. Windows servers may or may not offer Sendmail capability.

The \$emailfield value should be set to contain the name of the input field on the form that contains the respondent's email address. The email address entered in this field will be referenced as sender of the form input and will also be sent a CC of the form transmittal email. This email address will be checked for proper syntax during form processing.

**Mandatory:** Edit the value of the \$to variable to contain the email address(es) to which form results are to be sent. Edit the value of the \$bccs variable to contain the email address(es), if any, to which a blind carbon copy of each email is to be sent. If no BCCs are to be sent, leave this value blank. Both the \$to and \$bccs fields may contain multiple email addresses separated by commas.

**Hidden Email Recipients:** HTForm hard-codes recipient addresses in the CGI script itself, so no recipient information is coded in the HTML of the form. This provides the benefit of hiding email recipient addresses from spiders that may comb through the HTML code of the website, thus decreasing unsolicited emails (spam) as a result of advertising your email addresses on the web. If the inputs from several forms are to be sent to different recipient addresses, a separate copy of the script can be renamed and saved in the cgi-bin directory for each form.

The \$subject field contains the default subject of the form-transmittal email. This can be edited. The \$subjectfield value can be set to override the default email subject using the value of the specified form input field, which may be hidden or otherwise.

The values of the \$bgcolor, \$textcolor, and \$hdrcolor fields can be edited to change the default colors of background, text, and headers in the form transmittal email. Color values are entered as standard HTML code values or RGB hex notation values. The values of the \$bgcolorfield, \$textcolorfield, and \$hdrcolorfield variables can be set to specify the form input fields (normally hidden) that will override the default values for colors.

The value of the variable \$emailexclude can be edited to add any form input fields that you do not wish to be included in email transmittal. The most common exclusions are provided as default. Input names are entered as comma-separated values. **(The alternative \$emailinclude variable is provided for cases in which the excludes would be a very long list and the includes are easier to specify. Some knowledge of Perl and commenting/uncommenting code lines will be necessary to take advantage of the \$emailinclude option, which also requires adjustments to commented code lines in the functional processing routines of the parse-multipart and parse\_plain subroutines of the script. Don't mess with this unless you have a good understanding of Perl programming.)**

The \$debugemail value should be set to the address to which you would like to have diagnostic emails sent in case of an irregularity that identifies the form input as being of security concern. In case of such irregularities, the form input is diverted from the normal channel, and additional diagnostic fields are included in the email. This will help identify and analyze when the script is being run by unauthorized processes. If you don't want to deal with debug emails, make the value of this variable a null string.

### Archive Settings

The value of the variable \$archive should be set to 1 (the default) if you want HTForm to create an archive file on your webserver containing the information submitted on the form as comma separated values (CSV). Such CSV files are compatible with Microsoft Excel spreadsheets and may be imported directly by simply opening the file. They are also compatible with many database applications.

The \$archivefile value should be set to a string that specifies the location of the CSV archive file to be created and/or updated relative to the location of the script. Be careful not to duplicate any existing files or directories.

You may wish to password protect the archive directory in order to protect your data. This can usually be done via file-management utilities offered by your hosting provider.

The `$filedirectory` variable should be set to a string that defines the directory in which any files uploaded in response to inputs of type = file on the form are to be saved. Uploaded files will be automatically named with unique reference-number prefixes allowing them to be matched to the form input with which they were submitted.

Finally, the `$archiveexclude` variable should include the names of any fields you do not want to be included in the CSV data file. A list of the most commonly excluded files is default.

## Security Settings

The array `@permitted_urls` defines the list of sites that are authorized to submit form input. Typically this will be the base URL of the website on which the form is located, together with any proxy URLs assigned to the same site. It is recommended to list each URL without the “www” prefix for maximum compatibility. If form transmittal from an unlisted site is attempted, an error condition will be generated.

Only forms submitted by the POST method are allowed by HTForm. Any form data submitted by the GET method will create an error condition.

A form submitted by the POST method with no input fields or values will generate an error.

The `$keyfield` and `$keyvalue` variables allow you to specify the name and value, respectively, of an input field that must be present in order for form transmittal to be regarded as valid. Typically these will relate to a hidden field embedded in the form, or to a password field. If no values are entered, the requirement is waived. If values entered are not matched by inputs received from the form, an error will be generated.

The `$inputsequence` variable can be set to a comma separated list of input fields in the order that they must be received from the form in order for the form to be regarded as valid. Do not include any fields in the `$archiveexclude` variable. Assigning values to the `$inputsequence` variable prevents hackers from processing bogus forms that do not contain the desired input sequence.

The `$maxccs` variable (default value 2) determines the maximum number of email addresses that can be entered to receive CC copies of the form submission email. This prevents the CC feature of HTForm from being used to transmit large numbers of unsolicited emails.

Customizing the name of the script when it is placed in the CGI directory will help to prevent unauthorized access.

The `$maxfilesize` variable should be set to the smallest value (in bytes) necessary to allow requested files to be uploaded from any inputs of type=“file” on the form. This maximum limit prevents the uploading of large files that consume undesirable amount of space on the server.

Set the value of the `$scriptuser` variable to any string value that will allow you to easily identify the script or the form being processed in case any error messages are generated.

The `@flaggedheaders`, `@bogusvalues`, and `@emaiyesorno` arrays are provided for the purpose of shortcircuiting repeat-offending hackers if they have found and persist in attempting to use the HTForm script. Normally this will generate a debug email, and no unauthorized email messages will be transmitted. However, you can prevent the debug email from being transmitted for repeat offenders by placing corresponding identifying field names and values in the first two arrays. Setting the corresponding value in the third array to 0 will prevent the debug email from being transmitted. In addition, rejection by this method will result in a reject message being returned to the hacker that may or may not freeze his email client.

The `@noupload` array allows you to enter a list of file extensions or partial names of files not permitted to be uploaded via any inputs of type “file” on the form. Most commonly this would be used to prevent uploading executable files (.exe) for Microsoft Windows-based computers.

## INSTALLING HTForm ON YOUR WEBSITE

(1) In the HTML code for your form, set the attributes as follows.

```
<form method="POST" enctype="multipart/form-data" action="cgi-bin/yourscriptname.cgi">
```

If you omit the “enctype” attribute, the form will be transmitted by the default (x-www.-form-urlencoded) protocol. Most features of HTForm will operate properly, but file uploads will not.

(2) Open the file HTForm.cgi, and save a copy under the new name you choose to use for your script (`yourscriptname.cgi`).

(3) Edit the options in the new file as described in the previous section to suit your application.

(4) Save the file and FTP a copy into the `/cgi-bin/` directory of your website. Make sure your webserver is enabled for Perl scripts.

(5) Set the permissions on the script to UNIX `chmod 711`. If you’re using Fetch, select the file and menu item `Remote>Permissions`. The correct setting should look like this:



(6) Test the form and debug the settings as needed.

## DOWNLOADS

The current version of HTForm can be downloaded from:

**[www.htform.com](http://www.htform.com)**

## PAYMENT

You can download HTForm and all of its documentation and use it free for up to 30 days. After that, if you find the script satisfactory and wish to continue to use it, please send your check for \$100 for unlimited license. Make check payable to:

**Seaview Scientific**

Mail to:

**Attn: Paul Chadwick  
Seaview Scientific  
20 Aventura Road  
Santa Fe, NM 87508**

Be sure to include your name, organization, address, and email address with your check, and note on the check "License HTForm".

New Mexico residents and programmers or companies that place the HTForm script on web servers located in the state of New Mexico are exempt from licensing fees.

Web hosting companies that wish to provide HTForm as a utility to multiple users, please call to discuss obtaining a special mass license:

**(505) 466-4981**