Apache mod_userdir Tweak

For cPanel & WHM version 60

(*Home >> Security Center >> Apache mod_userdir Tweak*)

Background

The Apache mod_userdir module allows for visitors to access a user's website via a URL that contains that user's username. For example:

```
http://host.example.com/~username
http://example.net/~username
http://192.168.0.20/~username
```

Most servers use the `mod_userdir` Apache module as a temporary URL system that allows users to view their websites. This temporary URL system functions even if the system has not configured DNS or the domain does not yet point to the server.

> **Note:**
> When you enable the `mod_userdir` module, any virtual host can access any website that uses the same IP address. It does **not** functi on only with the hostname.

Overview

The *Apache mod_userdir Tweak* interface allows you to disable the `mod_userdir` functionality for your users.

> **Warning:**
> We **strongly** recommend that you restrict this access for most of your users. Before you use this interface, make certain that you read the Security Implications and Warnings sections below.

Prevent `mod_userdir` access

To prevent `mod_userdir` access, perform the following steps:

1. Select the *Enable mod_userdir Protection* checkbox.
2. To enable mod_userdir functionality for specific hosts, select the appropriate *Exclude Protection* checkboxes.

   > This will allow for all users to access content on the host via mod_userdir. It is recommend that you only enable mod_userdir functionality on the DefaultHost.

3. If you only wish to allow mod_userdir functionality for specific additional users to access these hosts, enter their usernames in the *Additio nal Users* text box.
   - Resellers can use this feature to allow their customers to access their own websites before DNS information propagates.
   - To enter multiple users, separate each account name with a space.

4. Click *Save*.

> **Notes:**
> To allow all of your users to access their **own** accounts through the `mod_userdir` module, but not steal any bandwidth, select the *Exclude Protection* checkbox for *DefaultHost (nobody)*.

> **Warning:**
> Do **not** select the *Exclude Protection* checkbox on a user's domain if you only wish to allow an individual user to access their site with a `mod_userdir` URL on the default server hostname.

Example

You own the following three cPanel accounts:

- Arthur's cPanel account (`arthur`) owns `arthurexample.com`
- Betty's cPanel account (`betty`) owns `bettyexample.com`
- Charles' cPanel account (`charles`) owns `charlesexample.com`

Arthur's domain resolves, but Betty's and Charles' domains do not yet resolve.

To enable `mod_userdir` protection for the server to deny one user the ability to use another user's bandwidth, select the *Enable mod_userdir Protection* checkbox.

However, if you still want to allow Betty and Charles to use Arthur's domain to see their sites, perform the following steps:

1. Do **not** select the checkbox next to `arthurexample.com` (Arthur)
2. Enter `betty charles` in the *Additional Users* text box.
3. Click *Save*.

Betty and Charles can browse their sites with the following URLs:

- `arthurexample.com/~betty`
- `arthurexample.com/~charles`

Shared SSL Certificates

If a shared SSL certificate is installed for a virtual host on a shared IP address, you can share that SSL certificate with users on the same IP address. This allows them to access their sites securely without a browser warning.

For example, if an SSL certificate is installed on `host.example.com` and you select the *Exclude Protection* checkbox for *DefaultHost (nobody)*, the `username` cPanel user can access `host.example.com/~username`

Security Implications

We **strongly** recommend that you restrict `mod_userdir` functionality for most of your users. There are potential security issues that `mod_userdir` can expose.

- A user's content can be accessed using a domain name and SSL certificate that belongs to another user. This can potentially be used for phishing attacks or other malicious content, that appears to be hosted under the target domain.
- Bandwidth is accounted for per-host rather than per-user. If a user's content is accessed via `mod_userdir`, then their bandwidth usage will not be recorded correctly. This can also potentially allow for one user to use the bandwidth of another.

When you disable `mod_userdir` protection for a host, it is recommended that you do not exclude the entire host, but rather exclude only specific users via the "Additional Users" field.

Warnings

Enabled mod_userdir protection

Before you enable the `mod_userdir` module, be aware of the following information:

- Java servlets do **not** work with `mod_userdir`-based URLs. This is because Tomcat requires that you add additional directives to the virtual host.
- `open_basedir` protection restricts PHP's access to the home directory of the user who owns the base domain, **not** the home directory of the user account that a visitor accesses. If you enable `open_basedir`protection in WHM's *Apache mod_userdir Tweak* interface (*Home >> Security Center >> PHP open_basedir Tweak*), visitors **cannot** access some sites via the `mod_userdir` module.
- Under certain conditions, a user can attack another user's account if they access a malicious script through a `mod_userdir` URL.
- Websites that use the `mod_rewrite` or other directives in their `.htaccess` files will **not** function correctly when visitors view them through `mod_userdir` URLs.
- If you enable Apache's `mod_ruid2` module, then the `mod_userdir` module will **not** function correctly. For more information, read our Apache Module: ModRuid2 documentation.

The Symlink Race Condition Protection option

The following table describes when the *Symlink Race Condition Protection* option blocks `mod_userdir` access:

Condition	`mod_userdir`access	Example URL
The requested URL includes a file and does not belong to the owner of the file.	Blocked.	`example.com/~username/file`
The requested URL includes a file and an IP address that belongs to another account.	Blocked.	`192.168.0.20/~username/file`
The requested URL contains a directory.	Not blocked.	`example.com/~username/dir`
You wish to access the server's hostname.	Not blocked.	`host.example.com/~username`

Disabled mod_userdir protection

Before you disable `mod_userdir` protection, be aware of the following information:

- While this WHM feature allows you to restrict `mod_userdir` functionality, it does **not** remove the module itself. Some PCI compliance sc ans may still detect it.
- This feature does **not** list IP addresses because the `mod_userdir` module uses virtual hosts.
  - You **cannot** use IP addresses to configure this feature.
  - If you do not protect the default host, you can access the server's main IP address through the `mod_userdir` module in **most** c ases.

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

Content by label

There is no content with the specified labels

- cPanel API 1 Functions - OptimizeWS::loadoptimizesettings
- cPanel API 2 Functions - Mime::listhandlers
- cPanel API 2 Functions - Mime::listmime
- UAPI Functions - Mime::add_handler
- UAPI Modules - Mime